Strategy Research Project

The Cyberspace Evolution's Impact on the United States' Strategic Culture

by

Colonel Jacqueline D. Brown
United States Army

United States Army War College
Class of 2014

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

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
15-04-2014	STRATEGY RESEARCH PROJECT	

4. TITLE AND SUBTITLE
The Cyberspace Evolution's Impact on the United States' Strategic Culture

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Colonel Jacqueline D. Brown
United States Army

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Captain James E. Boswell
Department of National Security and Strategy

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
Word Count: 5,468

14. ABSTRACT

The accelerated pace of the cyberspace evolution over the last 20 years has introduced a national as well as a global reliance on a manmade infrastructure for economic prosperity, military power, and societal communications all of which affect the United States' Strategic Culture. Cyberspace crosses state boundaries, globally connecting societies, critical infrastructures and commerce, thus enabling unprecedented freedom of communication and access to information and trade. There is now an insatiable appetite for convenience of communication with the ease of use and desire for global reach. This increasing demand creates an environment vulnerable to exploitation and attacks. While both the government and the private sector recognize the threats posed through cyberspace and the risk of doing nothing, the current U.S. strategic culture does not align well to affect required change to secure U.S. interests in cyberspace. To effectively develop and implement a holistic cyberspace strategy, one must understand the cyberspace evolution's impact on the strategic culture. This paper will analyze the current U.S. strategic culture, the impact of the cyberspace evolution on the strategic culture and provide cyberspace security policy and strategy recommendations.

15. SUBJECT TERMS
Cyber, Stuxnet

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

USAWC STRATEGY RESEARCH PROJECT

The Cyberspace Evolution's Impact on the United States' Strategic Culture

by

Colonel Jacqueline D. Brown
United States Army

Captain James E. Boswell
Department of National Security and Strategy
Project Adviser

This manuscript 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

Title:	The Cyberspace Evolution’s Impact on the United States’ Strategic Culture
Report Date:	15 April 2014
Page Count:	32
Word Count:	5,468
Key Terms:	Cyber, Stuxnet
Classification:	Unclassified

The accelerated pace of the cyberspace evolution over the last 20 years has introduced a national as well as a global reliance on a manmade infrastructure for economic prosperity, military power, and societal communications all of which affect the United States' Strategic Culture. Cyberspace crosses state boundaries, globally connecting societies, critical infrastructures and commerce, thus enabling unprecedented freedom of communication and access to information and trade. There is now an insatiable appetite for convenience of communication with the ease of use and desire for global reach. This increasing demand creates an environment vulnerable to exploitation and attacks. While both the government and the private sector recognize the threats posed through cyberspace and the risk of doing nothing, the current U.S. strategic culture does not align well to affect required change to secure U.S. interests in cyberspace. To effectively develop and implement a holistic cyberspace strategy, one must understand the cyberspace evolution’s impact on the strategic culture. This paper will analyze the current U.S. strategic culture, the impact of the cyberspace evolution on the strategic culture and provide cyberspace security policy and strategy recommendations.

The Cyberspace Evolution's Impact on the United States' Strategic Culture

The accelerated pace of the cyberspace evolution over the last 20 years has introduced a national as well as a global reliance on a manmade infrastructure for economic prosperity, military power, and societal communications all of which affect the United States' Strategic Culture. Strategic culture is a nation's view of how the governing authority should approach its security issues.[1] As cyberspace evolves, it introduces new and complex security issues on both a national and global level. The introduction of these new and complex security issues demands a comprehensive strategy towards both operations within cyberspace and security.

The evolution of cyberspace has presented many technological innovations and advancements to societies, economies, government, and national defense; these same innovations and advancements have also introduced vulnerabilities that specifically threaten the U.S. national interest. The four enduring national interests identified in the 2010 National Security Strategy (NSS) are: "the security of the United States, its citizens, and U.S. allies and partners; a strong, innovative, and growing U.S. economy in an open international economic system that promotes opportunity and prosperity; respect for universal values at home and around the world; and an international order advanced by U.S. leadership that promotes peace, security, and opportunity through stronger cooperation to meet global challenges."[2]

The NSS addresses the immediate U.S. "need to prepare for asymmetric threats, specifically those that target the nation's reliance on space and cyberspace."[3] Concurrently, in the Comprehensive National Security Initiative, President Obama identifies "cyber security as one of the most serious economic and national security challenges we face as a nation, but one that we as a government or as a country are

not adequately prepared to counter."[4] This accelerated pace of the cyberspace evolution led the Department of Defense to name cyberspace as a new domain of warfare, equal with the land, sea, space, and air.

While both the government and the private sector recognize the threats posed through cyberspace and the risk of doing nothing, the current U.S. strategic culture is not well aligned to affect required change to secure U.S. interests in cyberspace. To effectively develop and implement a holistic cyberspace strategy, one must understand the cyberspace evolution's impact on the strategic culture. This paper will analyze the current U.S. strategic culture, the impact of the cyberspace evolution on the strategic culture and provide cyberspace security policy and strategy recommendations.

Strategic Culture

Jack Snyder is credited for coining the concept of strategic culture in his 1977 research report about Soviet and U.S. nuclear strategies. Snyder defines strategic culture as "the sum total of ideals, conditional emotional responses, and patterns of habitual behavior that members of the national strategic community have acquired through instruction or imitation and share with each other with regard to [nuclear] strategy."[5] Since then there are varying definitions of strategic culture, beginning with Colin Gray who defines strategic culture as "the persisting socially transmitted ideas, attitudes, traditions, habits of mind, and preferred methods of operation that are more or less specific to a particular geographically based security community that has had a unique historical experience."[6] The Comparative Strategic Cultures Curriculum Project report prepared for the Defense Threat Reduction Agency (DTRA) defines strategic culture as "that set of shared beliefs, assumptions, and modes of behavior, derived from common experiences and accepted narratives (both oral and written), that shape

collective identity and relationships to other groups, and which determine appropriate ends and means for achieving security objectives."[7] This paper applies this definition.

To understand a nation's strategic culture one must understand the genesis of it. The genesis of a nation's strategic culture can be viewed through the lens of a nation's geography, history, experience, society and political culture."[8] For example, the Atlantic and Pacific oceans adjoining the United States' east and west geographical boundaries provide a natural defense barrier. This barrier coupled with the historically limited strife between bordering nations supports the notion that American society experiences an exceptional amount of freedom of security.

The United States' history and the experiences that shape its strategic culture began with the July 4, 1776 declared departure from the rule of the British monarchy. This departure, otherwise known as the Declaration of Independence, fostered a political culture[9] of a government empowered by the society it represents, a society with inalienable rights such as life, liberty and the pursuit of happiness.[10] This marked the beginning of American democratic roots, breaking away from the tyrannical and hierarchical rule of King George's monarchy, thus making America exceptional. Furthermore, the United States' history, while marked by long periods of peace, is also riddled by generational conflicts beginning with the War of 1812 and spanning to the current Middle East conflicts. For the most part, history portrays these conflicts as a crusade of good versus evil.[11] With the exception of the War of 1812 and the Civil War, these conflicts have not occurred in the continental United States, thus providing the United States the advantage of time and space during the conduct of war.

This time and space insulates the American sovereign territory and society from the most devastating effects of war such as the loss of innocent lives, destruction of critical infrastructure, private and personal property, and economic disruption. Therefore, the effects of war experienced by the American society are exceptional and manifest mainly as the loss of American lives and military equipment on foreign soil. While not minimizing the sacrifices of those who defended American freedom in foreign lands, the emotional impact of a war fought on sovereign territory has significantly more impact on the populace. Consequently, the United States pursues the use of overwhelming firepower and technology to swiftly destroy the enemy and expeditiously end the loss of American lives. In summary, the United States Strategic Culture is shaped by free security and imbued with exceptionalism; emphasizing liberal idealism and viewing war as a discontinuation of policy. While the U.S. military culture, or way of war, emphasizes direct strategies leveraging firepower and technology-intensive approaches to combat.[12]

Cyberspace Evolution

Cyberspace History

The inception of cyberspace traces back to World War II (WWII) when the Allies were pursuing electronic technology to boost radar signals and developing computing machines to process complex radar messages.[13] Since WWII, technological disruptions have served as accelerants in cyberspace. For example, on October 4, 1957 the Soviet Union launched the first satellite, Sputnik; thus sparking the mobilization of American college campuses and the Department of Defense (DoD) to bridge the gap of the Russian technological advantage.[14] This created new governmental agencies such as the National Aeronautics and Space Administration (NASA) and Defense Advance

Research Projects Agency. While NASA led the effort to conquer the new space frontier, DARPA soon began the development of the ARPAnet as an effort to improve information sharing and reduce duplication of efforts by networking researchers' computers. Concurrently, the threat of nuclear attacks sparked the development of a distributed node network to assure communications reliability during a nuclear attack.

By the mid 1970s, college campuses and the Government were interconnecting computers via networks for the purpose of sharing information and messaging. This interconnectivity of networks created a gold rush in the 1980s, building fortunes and toppling old empires; zealous engineers and venture capitalists began building a new economy, laying the asphalt of the Information Super Highway.[15]

In 1990, shortly after the decommissioning of ARPAnet, Tim Berners-Lee, a computer programmer at the Conseil Européen pour la Recherche Nucléaire (CERN) in Switzerland began developing a system to provide access to research materials to everyone over the network. This system would enable document sharing between different computer platforms while eliminating the need to reformat documents. In 1991, Lee created the first browser, titling it the World Wide Web.[16]

In 1993, Marc Andreessen, a student at the University of Illinois, began further developing Lee's World Wide Web creating the Mosaic browser. Once Mosaic hit the Internet, the browser had over 1 million users. Shortly thereafter, the creators joined the private sector, began refining the Mosaic browser, and renamed it Netscape. Netscape sparked the explosion of the Internet boom; within a year and half of its debut Netscape reached 65 million users.[17] Some refer to the Internet boom of the 1990s as the

inception of cyberspace; for the purpose of this paper the Internet boom of the 1990s spring-boarded the evolution of cyberspace.

Cyberspace – Today

Over the past 20 years, we have witnessed a tremendous evolution of cyberspace from an easy to use research tool in an open environment, to a place to visit at one's choosing like a tourist resort or library, to an organism that has penetrated and rewoven the fabric of our lives.[18] What used to be Hollywood theatrical creations are now becoming a cyberspace reality such as robots, unmanned aerial vehicles, biometrics, digital signatures, personal navigation systems, etc. Today, cyberspace globally connects societies, critical infrastructures and commerce, enabling unprecedented freedom of communication, access to information, and trade.

Cyberspace encompasses everything from individual devices such as personal computers, mobile devices, unmanned aerial vehicles, medical devices to weapon systems. The cyberspace evolution has brought about an Ecommerce,[19] enabling bargain shopping on a global scale. Online banking is no longer the exception but the norm, facilitating nearly instantaneous banking transactions for such items as homes, vehicles, luxury items, etc.

Cyberspace provides a new medium for societal communications such as instant messaging, YouTube, Facebook, Twitter, Pinterest, Instagram, Snapchat, Tumblr etc. Usage of this medium is growing every day. A recent study shows Facebook is the leading social networking site with 71% of the United States adult Internet users leveraging the site, followed by 22% using Linkedin; 21% Pinterest; 18% Twitter; and Instagram 17%.[20] These new mediums, branded as Social media, provide society a global public stage to share personal experiences, interests, beliefs and random

thoughts. Increasingly occupying this stage are the politicians promoting their platforms and soliciting support. The American free market extends the reach of the consumer base through social media marketing. Cyberspace is also a recreation ground for gamers, specifically online gamers, globally connecting members from different societies sharing a common interest.

The public shares occupancy of cyberspace with the United States Government, Department of Defense (DoD) and the private sector. Therefore, on any given day while someone at home is online shopping or playing online games, the Government may be concurrently viewing satellite images for future military UAV operations both occurring alongside the private sector providing power across the nation during a winter vortex. Cyberspace crosses state boundaries globally connecting societies, critical infrastructures and commerce, thus enabling unprecedented freedom of communications and access to information and trade. There is now an insatiable appetite for convenience with the ease of use and desire for global reach driving continuous innovations in cyberspace. This increasing demand creates an environment vulnerable to exploitation and attacks.

Cyberspace Threats

Recognizing these vulnerabilities and the volatility of security in cyberspace, President Obama identifies cyber security as one of the most serious economic and national security challenges facing the nation, but one that neither the Government nor the country are adequately prepared to counter.[21] In 2011, the DoD named cyberspace as a new domain of warfare, equal with the land, sea, air and space domains.[22] The DoD defines the cyberspace domain “as a collection of computer networks that use a variety of wired and wireless connections, a multitude of protocols, and devices ranging

from supercomputers to laptops to embedded computer systems designed for specific control functions in larger systems."[23]

Protecting U.S. interests in cyberspace is a dynamic and complex challenge. Power infrastructure grids, banking systems, communications systems, transportation systems, and the Defense industrial base all rely on cyberspace. These activities and more are targets of potential U.S. adversaries, consequently leveraging U.S. cyberspace vulnerabilities and disrupting the U.S. national livelihood on a massive scale. Most dangerous is that these adversaries, be they nation-state, non-state actors or criminals have unfettered access to cyberspace.

The four categories of cyberspace threats facing nations today are cyber war, economic espionage, cyber crime, and cyber terrorism. Cyber war is actions taken by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks.[24] Economic espionage, as defined by United States Code 1831 is whoever knowingly performs targeting or acquisition of trade secrets to knowingly benefit any foreign government, foreign instrumentality, or foreign agent. Cyber crime is criminal activity or a crime that involves the Internet, a computer system, or computer technology, examples are identity theft, phishing, money laundering, and child pornography for instance. Cyber terrorism is "the use of computer network tools to shut down critical national infrastructures (e.g., energy, transportation, government operations) or to coerce or intimidate a government or civilian population."[25]

Both state and non-state actors are posing these threats. Generally, state actors will account for the cyber war and economic espionage thefts while non-state actors will

account for cyber crime and cyber terrorism threats. Cyber war, economic espionage and cyber terrorism are of the utmost concern for the DoD.

Impacts to Strategic Culture

While the geography of the United States has provided the American society with a freedom of security, the geographic barriers providing this sense of security are not applicable to cyberspace. The lack of borders combined with the global interdependency of cyberspace is gradually reducing the American sense of security. The far-reaching effects of malicious activity in cyberspace introduce an unprecedented risk to the nation's critical infrastructure such as power, telecommunications, banking etc. The United States has not experienced such a threat since the Soviet Union's development and exploitation of Intercontinental Ballistic Missiles (ICBM).

The United States Government, private sector, and society are experiencing an increasing number of malicious cyber activities. Most recently, cyber criminals stole the Target retail store's point of sales data; resulting in approximately 40 million compromised credit and debit card numbers, expiration dates, card verification value (CCV), also known as security codes, as well as ATM pins. In July, the Rex Mundi hacker group published stolen customer data from 6,000 customers and prospects of Numericable after the cable TV company refused to pay a ransom of 22,000 Euros. This same group threatened Websolutions.it.[26] In July, the Syrian Electronic Army (SEA) hijacked Thompson Reuters' Twitter feed posting seven violent and graphic cartoons. This same group announced it had compromised three personal email accounts belonging to White House staff members.[27] Beginning in August the SEA compromised several websites such as ShareThis.com, the New York Times and the Huffington Post and redirected them to the SEA official site. [28] As one can see from these examples,

cyber attacks are not isolated to just individuals, corporations or the government. All are vulnerable to such attacks.

Cyberspace has presented itself as a rich environment for the breeding of subcultures as well as the expansion of existing subcultures. Random House dictionary defines a subculture as a group having social, economic, ethnic, or other traits distinctive enough to distinguish it from others within the same culture or society. Cyberspace provides a national and global venue, connecting individuals with unique interests and little in common otherwise. Cyberspace provides these subcultures expedient means to energize a group behind a cause. For example, Facebook provides these interest groups a means to connect by becoming a member of a “group.” These “groups” span from military unit alumni; to running enthusiasts, gun and anti-gun organizations to homeschooling. Homeschooling is an excellent subculture example, providing parents a venue to share lessons learned and lessons plans. Homeschooling forums, websites or Facebook pages brings parents together who have all chosen not to educate their children in the public school system. These parents all have different reasons for choosing the homeschooling path, for example religious beliefs, social environment or the dissatisfaction with the public school curriculum. Regardless of their differing views, cyberspace connects these parents through the common interest of homeschooling. Cyberspace through information sharing has helped to proliferate the homeschooling movement.

Cyberspace enables near real time reporting of developing world events not only by the mainstream media but also by society itself. For example, videos and pictures of the chemical weapons attacks in Syria and the demonstrations in Libya surfaced on the

social media stage long before they surfaced in journalists' reports. Mainstream media is increasingly utilizing social media as a reporting source.

The unfettered access to cyberspace is the modern day inalienable right. For example, countries such as Estonia have declared Internet access as a human right. The United States Government will undoubtedly face challenges in its inability to take away what society perceives as freedom of access, navigation and perceived privacy within cyberspace. The recent intelligence leaks by Eric Snowden, a National Security Agency contracted employee, have altered the U.S. government's trustworthiness with its citizens. As the U.S. government develops policies addressing cyberspace security, it must navigate this quagmire in political culture.

Security Objectives

Determining the appropriate ends and means for security objectives impacted by the evolution of cyberspace is a significant challenge for the United States Government. To understand the national security challenge of protecting U.S. interests in cyberspace, one must first understand the cyberspace domain as well as the nature and character of the cyber security challenge. As a domain whose resources do not fall within the jurisdiction of any one particular country, and to which all nations have access;[29] considering cyberspace a global commons just as the sea and space domains is prudent. However, cyberspace is not a geographic global commons; it is a dynamic manmade domain, presently the only one of its kind. As a man-made domain, cyberspace continuously evolves, as does its definition.

Cyberspace provides an unprecedented amount of ambiguity to attackers, concealing the attacker's identity and the attack's point of origin, whether attack initiation occurred outside or within the defender's state or territory. Cyberspace attacks

frequently transmit through third parties without their complicity or knowledge; skilled attackers can potentially repeat these attacks almost indefinitely.[30]

The cyberspace domain provides an alluring environment for the conduct of warfare, especially as a critical enabler to warfare in the other domains. Cyberspace is an appealing domain to conduct attacks with its low entry cost, affordable to both state and non-state actors. No nation is immune from such warfare; the U.S. first learned this lesson in 2008 as illustrated by former Deputy Secretary of Defense, William J. Lynn III.

> In 2008, the U.S. Department of Defense suffered a significant compromise of its classified military computer networks. It began when an infected flash drive was inserted into a U.S. military laptop at a base in the Middle East. The flash drive's malicious computer code, placed there by a foreign intelligence agency, uploaded itself onto a network run by the U.S. Central Command. That code spread undetected on both classified and unclassified systems, establishing what amounted to a digital beachhead, from which data could be transferred to servers under foreign control. It was a network administrator's worst fear: a rogue program operating silently, poised to deliver operational plans into the hands of an unknown adversary.[31]

This attack initiated a counter-operation known as Operation Buckshot Yankee, marking a turning point in U.S. cyber defense strategy. The attack of 2008 is only one of many adversarial attacks compromising files from U.S. networks as well as U.S. allies' and industry partners' networks. Files compromised over the years include weapons blueprints, operational plans, and surveillance data.[32]

The conduct of cyberspace warfare is not limited to military targets only. This is evident by Russia's use of cyberspace warfare against Georgia. Russia's distributed-denial-of-service (DDOS) attacks against Georgia's Internet infrastructure effectively disrupted information dissemination while defacing public and private Web sites.[33] The results of these attacks equated to a cyberspace blockade against Georgia, reducing

Georgia's effectiveness to lead internally and stifled its ability to gain international sympathy.[34]

Russia employed cyberspace attacks, setting the conditions for follow on attacks within the other domains such as land and air. Russia launched the most significant cyberspace attacks just as the tanks began to roll. The official sites in Gori, along with local news sites, were shut down by denial-of-service attacks prior to the arrival of Russian planes."[35] Not only did these cyberspace attacks set the conditions militarily, these attacks were very effective in the economic and information realms of power. For example, these actions forced Georgia's national bank to shut down their Internet connections for 10 days, ceasing all electronic financial actions.[36] As Corbett's maritime theory suggests, if a nation's "commerce and finance stand to lose by war, their influence for a peaceful solution will be great;"[37]

Two years after Russia's effective application of cross-domain synergy in Georgia, Stuxnet, remains the most sophisticated worm virus to date. In 2010, the Stuxnet virus attacked the Iranian nuclear program allegedly delaying progress of the program by two years. Stuxnet is best described as "a self-directed drone: the first known virus that, released into the wild, can seek out a specific target, sabotage it, and hide both its existence and its effects until after the damage is done."[38] The Stuxnet virus is a sophisticated self-replicating worm virus that exploits four zero day vulnerabilities, targeting small gray plastic boxes known as programmable logic controllers (PLC). These PLCs perform functions such as opening and closing valves in water pipes or speeding or slowing the spinning of uranium centrifuges.[39]

The proliferation of Stuxnet went beyond Iran. A study conducted by the U.S. technology company Symnatec showed that the primary affected countries as of August 6, 2010 were Iran, with 62,867 infected computers; Indonesia with 13,336; India 6,552; United States 2,913; Australia 2,436; Britain 1,038; Malaysia 1,013; and Pakistan with 993.[40] Most concerning is the proliferation aspect of this attack. Stuxnet is essentially the proliferation of a blueprint of how to remotely attack industrial control systems which includes critical infrastructures. Similar to the affect that use of the atomic bomb at Hiroshima had on ensuing international relations and warfare; Stuxnet has demonstrated that cyberspace warfare is capable of sophisticated precision strikes with devastating effects.[41] This demonstration may have impacts on international relations, law, and norms far beyond the localized effects of the virus.

Unlike Hiroshima being attributed to the United States, Stuxnet attribution is only speculation. Supposition is that the Stuxnet attack against the Iranian nuclear program was a coordinated effort between the U.S. and Israel, however there remains no definitive proof. Therefore, if Stuxnet achieved the conjectured damage to the Iranian nuclear program, it could be considered the first non-attributable act of war.[42]

The lack of attribution is likely the most concerning element of cyberspace warfare. “Third parties could conceivably use cyber strikes to provoke catalytic wars between two rivals – say, for example, Serbians or Baltics firing cyber bullets into a Russo-Georgian clash or Japanese or Chinese hackers cyber surfing during a war between North and South Korea,”[43] just as the Corinthians provoked war between the Spartans and Athenians. These third party disruptions are not limited to state actors; non-state actors such as terrorist or criminals can initiate these disruptions. The United

States has not faced such a threat to its national security since the proliferation of nuclear weapons and technology.

The Best Ways?

The United States Government's most daunting challenge is understanding the strategic culture metamorphosis being induced by the cyberspace evolution. Critical to the effective development of a comprehensive cyberspace security strategy is determining the acceptable ways while balancing the appropriate ends and means the United States takes to achieve security objectives that protect U.S. interests. Cyber security includes "measures taken to protect a computer network, system, or electronic information storage against unauthorized access or attempted access."[44]

It is worth revisiting the fact that cyberspace is no longer an area apart from its users or a place to visit at one's choosing like a tourist resort or library; it has penetrated and rewoven the fabric of our lives[45]. It is becoming the primary means of societal communications and a global marketplace. The free flow of information and continuous cyberspace access is an essential element to U.S. economic prosperity enabling the United States and its allies to globally trade goods and services instantaneously.[46] Cyberspace is a conduit of major weapons systems for achieving desired effects.

Just as Julian Corbett's maritime theory posits that a war will not be won through command of the sea alone, nor will war be won through the command of cyberspace alone.[47] Neither the Unites States nor any other nation will win a war solely through the command of cyberspace. Commanding cyberspace sets the conditions for dominance in the other domains, such as air, space, land and sea. Conversely, vulnerabilities in the U.S. cyberspace domain present significant risks to the U.S. national interests. These threats are not limited to states with major world powers, "Small-scale technologies can

have an impact disproportionate to their size; potential adversaries do not have to build expensive weapons systems to pose a significant threat to U.S. national security."[48]

Cyberspace warfare is asymmetric. "The low cost of computing devices means that U.S. adversaries do not have to build expensive weapons, such as stealth fighters or aircraft carriers, to pose a significant threat to U.S. military capabilities."[49] The open nature of cyberspace provides rapid expansion capabilities and low barriers to technological innovations, inherently giving the offense the advantage in cyberspace. Therefore the ability to defend the U.S. area of operations in cyberspace will always lag behind an adversaries' ability to exploit weaknesses.[50] Lynn compares cyberspace warfare to maneuver warfare, "in that speed and agility matter most. To stay ahead of its pursuers, the United States must constantly adjust and improve its defenses."[51]

There are those who believe that the Cold War deterrence model is the appropriate cyberspace security strategy. The Cold War strategy of nuclear deterrence focuses on the second-strike capability, surviving a strike long enough to retaliate with an equally effective strike. As the nuclear technology evolved, this strategy moved away from second-strike capability towards "acceptance by all players that engaging in the nuclear game would inevitably bring devastation to all, becoming known as mutual assured destruction (MAD)."[52]

A second strike strategy in cyberspace is complicated by the ambiguous nature of cyber attacks that conceals the identity of cyberspace attackers. "Whereas a missile comes with a return address, a computer virus generally does not. The forensic work necessary to identify an attacker may take months, if identification is possible at all."[53] Coupled with the lack of attribution, the lack of internationally recognized cyberspace

norms of behavior muddles what comprises a cyberspace attack. Therefore pursuing a strategy of second strike is problematic.

On the other hand a cyberspace security strategy modeled after a MAD policy proposes that the United States shift “to an open, transparent policy that seeks to infer deterrence from the efficacy of its offensive cyber capabilities.”[54] This strategy focuses the U.S. cyberspace efforts away from the perfect defensive system of cyber deterrence, but rather to achieve deterrence based on a mutually shared fear of an offensive threat.[55] Therefore, each major player in the global system would come to fear debilitation equally and therefore would not risk being the first-strike initiator.”[56]

This might be an effective strategy if the goal was only to preserve peace and freedom of access among nation states; however the non-state actors do not play by the same rules as nation states. The ambiguity provided by cyberspace is to the advantage of non-state actors. Providing non-state actors cover as they launch attacks that solicit cyberspace soldiers in their efforts to conduct DDOS attacks. Often times these cyberspace soldiers are unwitting participants as the non-state actors elicit assistance via Botnet viruses.

Former Deputy Secretary of Defense Lynn proposed that due to the ambiguous nature of cyberspace attacks, the United States would be better served by denying adversaries the benefits of attacks through a strong defense.[57] However the effectiveness of a strong defense is questionable since as previously mentioned, defensive measures in cyberspace lag behind adversaries’ offensive measures.

While Lynn speaks against modeling a cyberspace security strategy after the Cold War strategy, he does recommend applying the Cold War shared warning doctrine

to cyberspace security. He states that based on the global nature of cyberspace U.S. allies play a critical role in cyberspace security.[58] He submits that “the more signatures of an attack one can see, and the more intrusions one can trace, the better one's defenses will be.”[59] This is a similar approach of linking the United States' air and space defenses with its allies. A cyberspace approach to shared warning is a multi-national effort by the United States and its allies, cooperatively monitoring computer networks for intrusions.[60]

Conclusion and Recommendation

The strategic culture metamorphosis induced by the cyberspace evolution demands the United States takes a whole of nation comprehensive approach towards cyberspace security. This approach is necessary to accommodate the reduced freedom of security, a significant change being experienced by the American society, due to the lack of defensive barriers in cyberspace placing the American way of life and security at risk. The U.S. has a strategic culture of government that is empowered by society and protects society’s inalienable rights; this also prevents the government from imposing a unilateral cyberspace security strategy.

The need for a whole of nation cyber-security approach is driven by the fact that the U.S. Government and American citizens have an increasingly indispensable and integral reliance on the over arching U.S. information technology (IT) infrastructure. This infrastructure is largely provided by the private sector. Not only does the U.S. government, to include the military, depend on the IT infrastructure provided by the private sector, critical infrastructure that supports the daily lives of the U.S. citizens relies on the same IT infrastructure.

While the MAD doctrine of the Cold War is not suitable to achieve cyberspace security, this approach should not be dismissed entirely. The United States' success in the cyberspace domain depends on the effectiveness of a trifecta of mutual reliance, active defense, and assured response. Mutual reliance refers to both a global and national reliance on cyberspace for communications, economic prosperity and defense. A national mutual reliance perspective refers to the U.S. citizens relying on a secure cyberspace as much as the government, DoD and the private sector. Consequently this mutual reliance demands a shared responsibility and interest for securing cyberspace enabling a whole of nation effort towards cyber security.

Active defense refers to "hunting" in the networks for threats that have breached the peripheral security measures. As described by the CYBERCOM J3 "Active defense is used solely on essential networks, data and systems and only works if cued by intelligence information that allows the hunt teams to focus on specific adversaries that have the capability and intent go after the vulnerabilities most important to you. Hunting uses heuristics and big data analytics to identify anomalous behavior that may indicate an adversary is in the network."[61]The security vulnerabilities brought by the cyberspace evolution is transforming the strategic culture environment towards acceptance of an active defense. However, the success of active defense hinges on the private sector and society's consensus, therefore accepting active defense as an acceptable means for the government to approach its cyberspace security issues. .

Finally, assured response is drawing the "red line".[62] We must be willing to retaliate against positively identified attackers. Retaliation must not be limited to the confines of the cyberspace domain; retaliation may be achieved via conventional

weapons. Since cyberspace is a domain equivalent with air, sea, land and space, an attack against the U.S. inside its cyberspace domain must also be considered equivalent to an attack in any of the other domains. Therefore assured response to a cyberspace attack should align with the current U.S. strategic culture, which pursues the use of overwhelming firepower and technology to swiftly destroy an enemy. However, assured response should not be limited to the military instrument of power, assured response extends to the other instruments of power such as diplomatic, economic and information. However, as stated previously, cyberspace is a global commons, therefore one cannot attack the enemy's territory without defending their own. As the United States pursues response against its adversaries, the government must work with the U.S.'s commercial agencies, such as the banking, power, and Internet service providers as well as their allies and multi-national partners' to ensure their continued protection from cyberspace attacks.

This trifecta not only depends on a whole of nation approach it also depends on strong international relationships and cooperation with U.S. allies and multi-national partners. The U.S. requires stronger agreements with a greater number of allies to facilitate the sharing of information, technology, and intelligence.[63] This cooperation requires collaboration amongst nations, sharing monitored network intrusion information as well as sharing intelligence on the affects of incurred cyber attacks. Additionally, the U.S. must be a key player in establishing a framework of international norms and behavior in cyberspace. Cyberspace security is a global and national interest requiring societal support as the strategic culture morphs.

Endnotes

[1] Stephen B. Smith, "The Geographic Origins of Strategic Culture," *Khazar Journal of Humanities and Social Sciences* 14, no. 4 (2011): 41, http://dspace.khazar.org/jspui/bitstream/123456789/1515/1/04The-Geographic-Origins-of-Strategic-Culture2011new.pdf (accessed February 10, 2014).

[2] Barack Obama, *National Security Strategy* (Washington, DC: U.S. Department of Defense, May 2010), 6, http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf (accessed January 10, 2014).

[3] Ibid.

[4] The White House, *Comprehensive National Cybersecurity Initiative* (Washington, DC: The White House, May 2011), 1, http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative (accessed October 22, 2013).

[5] Jack Snyder, *The Soviet Strategic Culture: Implications for Limited Nuclear Operations, R-2154-AF* (Santa Monica, CA: RAND, September 1977), 8, http://www.rand.org/content/dam/rand/pubs/reports/2005/R2154.pdf (accessed March 10, 2014).

[6] Colin S. Gray, *Modern Strategy* (Oxford: Oxford University Press, 1999), 131.

[7] Thomas G. Mahnken, *United States Strategic Culture*, Comparative Strategic Culture Curriculum (Defense Threat Reduction Agency Advanced Systems and Concepts Office, November 13, 2006), 4, http://www.au.af.mil/au/awc/awcgate/dtra/mahnken_strat_culture.pdf (accessed January 15, 2014).

[8] Gray, *Modern Strategy*, Ch. 5.

[9] Smith, "The Geographic Origins of Strategic Culture," 41. Defines political culture as the group's view of the proper role of the governing authority.

[10] Declaration of Independence.

[11] Mahnken, *United States Strategic Culture*, 6.

[12] Ibid., 4.

[13] Robert X. Cringely, "Nerds 2.01- Networking the Nerds," http://www.pbs.org/opb/nerds2.0.1/networking_nerds/ (accessed February 28, 2014).

[14] Ibid.

[15] Ibid.

[16] Ibid.

[17] Robert X. Cringely, "Nerds 2.01- Serving the Suits," http://www.pbs.org/opb/nerds2.0.1/serving_suits/ (accessed February 28, 2014).

[18] Roger Hurwitz, "Depleted Trust in the Cyber Commons," *Strategic Studies Quarterly*, Fall 2012, 4, http://www.au.af.mil/au/ssq/2012/fall/fall12.pdf (accessed January 12, 2014).

[19] Merriam-Webster Dictionary defines E-Commerce as activities that relate to the buying and selling of goods and services over the Internet, http://www.merriam-webster.com/dictionary/e-commercecomme(acccrce (accessed March 23, 2014).

[20] Maeve Duggan and Aaron Smith, "Frequency of Social Media Use," *Pew Research Internet Project,* December 30, 2013, 2, http://www.pewinternet.org/2013/12/30/demographics-of-key-social-networking-platforms/ (accessed March 24, 2014).

[21] The White House, *Comprehensive National Cybersecurity Initiative*, 1.

[22] *U.S. Department of Defense Home Page,* http://www.defense.gov/home/features/2013/0713_cyberdomain (accessed October 19, 2013).

[23] Cheryl Pellerin, "Cyber Command Adapts to Understand Cyber Battlespace," March 7, 2013, http://www.defense.gov/news/newsarticle.aspx?id=119470 (accessed October 19, 2013).

[24] *RAND Organization Home Page*, http://www.RAND.org (accessed March 11, 2014).

[25] James Lewis, *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats* (Washington, DC: Center for Strategic and International Studies), http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf (accessed October 28, 2010).

[26] McAfee, *McAfee Labs Threat Report: Third Quarter 2013* (Santa Clara, CA: McAfeee, 2013), 9, http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q3-2013.pdf (access December 14, 2014).

[27] Ibid.

[28] Ibid., 12.

[29] United Nations, *Global Governance and Governance of the Global Commons in the Global Partnership for Development beyond 2015* (New York: United Nations), 3, http://www.un.org/en/development/desa/policy/untaskteam_undf/thinkpieces/24_thinkpiece_global_governance.pdf (accessed October 21 2013).

[30] Stephen J. Cimbala, "Nuclear Crisis Management and "Cyberwar" Phishing for Trouble?" *Strategic Studies Quarterly*, Spring 2011, 118, http://www.au.af.mil/au/ssq/2011/spring/spring11.pdf (accessed February 11, 2014).

[31] William F. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* 89, no. 5 (September/October 2010): 97, http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain (accessed February 20, 2014).

[32] Ibid., 98.

[33] Rosemary M. Carter, Brent Feick, and Roy C. Undersander, "Offensive Cyber for the Joint Force Commander: It's Not That Different," *Joint Force Quarterly*, no. 66 (3rd Quarter 2012): 22, http://www.ndu.edu/press/offensive-cyber.html (accessed March 1, 2014).

[34] Ibid.

[35] David Hollis, "Cyberwar Case Study: Georgia 2008," *Small Wars Journal Online,* January 2011, 5, http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008 (accessed March 5, 2014).

[36] Carter, Feick, and Undersander, "Offensive Cyber for the Joint Force Commander: It's Not That Different," 22.

[37] Julian S. Corbett, *Some Principles of Maritime Strategy* (New York: Longmans, Green and Co., 1911), 170, http://www.gutenberg.org/files/15076/15076- h/15076-h.htm (accessed June 10, 2013).

[38] Michael Joseph Gross "A Declaration of Cyber-War," *Vanity Fair Online*, April, 2011, 2, http://www.vanityfair.com/culture/features/2011/04/stuxnet-201104 (accessed January 15, 2014).

[39] Ibid.

[40] "Factbox: What is Stuxnet," *Reuters Online,* September 24, 2010, http://www.reuters.com/article/2010/09/24/us-security-cyber-iran-fb-idUSTRE68N3PT20100924 (accessed March 5, 2014).

[41] Michael Joseph Gross, "A Declaration of Cyber-War," *Vanity Fair Online*, April, 2011, http://www.vanityfair.com/culture/features/2011/04/stuxnet-201104 (accessed January 15, 2014).

[42] Ibid.

[43] Cimbala, "Nuclear Crisis Management and "Cyberwar" Phishing for Trouble?" 120.

[44] Pellerin, "Cyber Command Adapts to Understand Cyber Battlespace."

[45] Hurwitz, "Depleted Trust in the Cyber Commons,"4.

[46] U.S. Department of Defense, *Department of Defense Strategy for Operating in Cyberspace* (Washington, DC: U.S. Department of Defense, July 2011), 1, http://www.defense.gov/news/d20110714cyber.pdf (accessed October 19, 2013).

[47] Ibid., 168.

[48] U.S. Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*, 3.

[49] Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," 98.

[50] Ibid., 99.

[51] Ibid.

[52] Matthew D. Crosston, "World Gone Cyber MAD: How 'Mutually Assured Debilitation' Is the Best Hope for Cyber Deterrence," *Strategic Studies Quarterly*, Spring 2011, 101, http://www.au.af.mil/au/ssq/2011/spring/spring11.pdf (accessed February 11, 2014).

[53] Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," 99.

[54] Crosston, "World Gone Cyber MAD: How 'Mutually Assured Debilitation' Is the Best Hope for Cyber Deterrence," 101.

[55] Ibid.

[56] Ibid.

[57] Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," 100.

[58] Ibid., 104.

[59] Ibid.

[60] Ibid., 103.

[61] Brett Williams, "Cyberspace: What is it, Where is it and Who Cares?" *Armed Forces Journal Online*, March 13, 2014, http://www.armedforcesjournal.com/cyberspace-what-is-it-where-is-it-and-who-cares/ (accessed March 13, 2014)

[62] Ibid.

[63] Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," 105,