Strategy Research Project

DEFINING OUR NATIONAL CYBERSPACE BOUNDARIES

BY

COLONEL JEFFERY R. SCHILLING
United States Army

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

USAWC CLASS OF 2010

This SRP 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.

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

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

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
17-02-2010	Strategy Research Project	

4. TITLE AND SUBTITLE

Defining our National Cyberspace Boundaries

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

COL Jeffery Schilling

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

LTC John Mowchan, Strategic Intelligence Officer, Center for Strategic Leadership

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: Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

In February 2009, the Obama Administration commissioned a 60-day review of the United States' cyber security. A near-term action recommended by the 60-day review was to prepare an updated national strategy to secure information and communications infrastructure. In order to accomplish this recommended near-term action, the United States must first develop a policy that defines our international cyberspace boundaries. This precursor action must happen before we can assign responsibilities and jurisdictions to government agencies, international bodies, and global corporations for the collective defense of cyberspace. Currently, the United States has no policy that articulates a cyberspace boundary framework. Indentifying our national cyberspace boundaries is a fundamental step required before the United States can define hostile acts and intent by cyberspace adversaries and assign jurisdictions for a collective defense. In order for the United States to execute a unilateral cyberspace response action (RA) against hostile actors, we must be able to declare that the hostile act or intent took place within our national cyberspace boundaries.

15. SUBJECT TERMS

Cyber Borders, Cyberspace National Policy, Convention On The Law Of Cyberspace, Cyberspace Law, Cyberspace Theory

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** *(include area code)*
UNCLASSIFED	UNCLASSIFED	UNCLASSIFED	UNLIMITED	30	

USAWC STRATEGY RESEARCH PROJECT

DEFINING OUR NATIONAL CYBERSPACE BOUNDARIES

by

Colonel Jeffery R. Schilling
United States Army

Lieutenant Colonel John Mowchan
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 Jeffery R. Schilling

TITLE: Defining our National Cyberspace Boundaries

FORMAT: Strategy Research Project

DATE: 17 February 2010 WORD COUNT: 6,434 PAGES: 30

KEY TERMS: Cyber Borders, Cyberspace National Policy, Convention On The Law Of Cyberspace, Cyberspace Law, Cyberspace Theory

CLASSIFICATION: Unclassified

In February 2009, the Obama Administration commissioned a 60-day review of the United States' cyber security. A near-term action recommended by the 60-day review was to prepare an updated national strategy to secure information and communications infrastructure. In order to accomplish this recommended near-term action, the United States must first develop a policy that defines our international cyberspace boundaries. This precursor action must happen before we can assign responsibilities and jurisdictions to government agencies, international bodies, and global corporations for the collective defense of cyberspace. Currently, the United States has no policy that articulates a cyberspace boundary framework. Indentifying our national cyberspace boundaries is a fundamental step required before the United States can define hostile acts and intent by cyberspace adversaries and assign jurisdictions for a collective defense. In order for the United States to execute a unilateral cyberspace response action (RA) against hostile actors, we must be able to declare that the hostile act or intent took place within our national cyberspace boundaries.

DEFINING OUR NATIONAL CYBERSPACE BOUNDARIES

In February 2009, the Obama Administration commissioned a 60-day review of the United States' cyber security which was completed in May 2009. The study was led by Melissa Hathaway who was the Cybersecurity Chief on the National Security Council. A near-term action recommended by the 60-day review was to prepare an updated national strategy to secure information and communications infrastructure.[1] In order to accomplish this recommendation, the United States must first develop a policy that defines our national cyberspace boundaries. This precursor action must happen before we can assign responsibilities and jurisdictions to U.S. government agencies that will facilitate effective collaboration and partnership with international bodies and global corporations for the collective defense of cyberspace. Government agencies in the Intelligence Community (IC), the National Security Council (NSC), Department of Homeland Security, and the Department of Defense (DoD) have all commissioned studies on cyberspace security. While each of these studies mentions the difficulty in defining cyberspace boundaries, the United States Government has no policy that articulates a cyberspace border framework. Indentifying our national cyberspace boundaries is a fundamental step required before the United States can define hostile acts and intent by cyberspace adversaries and assign jurisdictions for cyberspace Response Actions. In order for the United States to execute a unilateral cyberspace response action against hostile actors, we must be able to declare that the hostile act or intent took place within our national cyberspace boundaries. There must be a line drawn around cyberspace that the United States can claim as its territory before it can exercise governance.[2]

This research paper will assess two approaches to defining international cyberspace boundaries. The first approach will orient on the physical location of the equipment and software that creates the cyberspace environment. The second approach will orient on the "logical" location of the equipment and software that creates the virtual cyberspace environment. Each alternative will be compared against the evaluation criteria of feasibility/complexity, acceptability and suitability.

Cyberspace Theory and Definitions

Cyberspace is a relatively new concept. Global communications, sharing of information and ideas, has been happening for most of our recorded history. During this time, the speed at which this global communication and collaboration occurred was measured in years, weeks and days until Tim Berners-Lee invented the World Wide Web in 1989.[3] With a user-friendly web browsing capability, the Internet became a tool that anyone could use to discover, process, communicate, and store information. The speed of communication and collaboration that was measured in weeks and days now moves at the speed of light.

Defining cyberspace is a difficult task. Definitions range from the very complex to the overly simplified. The Merriam-Webster dictionary simply defines cyberspace as "the online world of computer networks and especially the Internet."[4] The United Kingdom recently defined cyberspace as "encompassing all forms of networked, digital activities; this includes the content of and actions conducted through digital networks."[5] It is interesting to assess how cyberspace defines itself. Wikipedia is an online resource that bills itself as the online encyclopedia that "anyone can edit." The global Internet community, which edits Wikipedia, defines cyberspace as

"the global domain of electromagnetics as accessed and exploited through electronic technology and the modulation of electromagnetic energy to achieve a wide range of communication and control system capabilities."[6] The Chairman of the Joint Chiefs of Staff, in Joint Publication (JP) 1-02, defines cyberspace as "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."[7] A common element to both the Wikipedia and the JP 1-02 definition is the assertion that cyberspace is a global domain.

In 2004, Admiral Arthur Cebrowski, former Director of the Office of Force Transformation in DoD, furthered the discussion of cyberspace as a global domain in his article, "Transformation and the Changing Character of War." Admiral Cebrowski, described cyberspace as the 21st Century's new strategic global common analogous to the sea and air.[8] The primary purpose of this global common is to conduct trade and international communications. Admiral Cebrowski uses the naval theories of Alfred Mahan to develop the theory of cyberspace; however, the framework from which Mahan discusses the sea domain has limited utility for the discussion of cyberspace.[9] Mahan's theory mostly centers on naval theory. The foundation of Mahan's theory is based on dominating the sea commons to achieve "command of the seas" in a "Jomini fashion." This is achieved by searching for your enemy and seeking the destruction or culmination of your threat in a decisive battle.[10] Cyberspace, as a global common, is impossible to dominate as Mahan envisions as the "command of the sea." In cyberspace, there are bad actors that have both state and non-state origins. The "buy

in" to become a bad actor in cyberspace is relatively low compared with the significant investment of a blue water navy or strategic air force. The other domains have similar challenges such as piracy on the high seas and illegal drug trafficking through the air. Nevertheless, cyberspace is dominated by non-state, bad actors and sophisticated state actors that use the advantage of anonymity to mask their actions, making them unattributed.[11] This makes the "command of cyberspace" unachievable with a very dynamic threat.

If you instead consider Julian Corbett's theory on maritime operations, you get a more comprehensive theory that translates well to cyberspace operations. Corbett's maritime operations theory incorporates the interaction between the land and sea, not just naval theory. The objective in Corbett's theory of maritime operations was not to command the sea nor look for that decisive battle to defeat your enemies. Corbett's objective in maritime theory was to ensure no one else controls the global common and access to the sea lines of communication is unfettered.[12] Commander John J. Klein used this approach effectively to fill the void in Strategic Space Theory in his article, "Corbett in Orbit: A Maritime Model for Space Operations," published in the Naval College Review. Space, like cyberspace, has no leading theorist or theories that help define an operational framework.[13] It is important to define the strategic framework of a global common before you attempt to define how you will draw your borders.

If we use Corbett's maritime operations theory, as applied to cyberspace, we must establish key terms and analogies to be consistently used throughout this analysis. In order to provide analysis at a non-technical level, these definitions and

analogies will remain high level and based on activities and functions that occur in cyberspace and not the technical aspects and capabilities that help define this domain.

The term cyberspace itself can be defined as the virtual common created by the global interconnection of information technology (IT) systems. "IT systems" are the IT equipment and software that create the virtual environment defined as cyberspace. There are several components of an IT system that we must understand to help visualize how we delineate our cyberspace borders.

The first component is "IT capabilities." For the purpose of this analysis, IT capabilities are any computing devices that can process, store, communicate or discover information for a user upon request. Examples of IT capabilities are email, web service, cloud computing, and data storage. An analogy that can be drawn to maritime operations is that IT capabilities are like the ports and harbors in the sea commons that receive goods and then either transfer or temporarily store them prior to movement to a final destination inland.

In order to globally interconnect IT capabilities, you must establish secure lines of communications between the IT capabilities in the same manner of establishing secure sea lines of communications between ports. This interconnectivity ensures the free flow of information between the user and the IT capabilities he or she is accessing. The term used to describe this concept in a cyberspace framework is "physical transport." Physical transport can take many forms. For example, fiber optic cable, satellite communications, and line of sight microwave communications are three forms of physical transport. The physical transport systems interconnect globally dispersed IT

capabilities, creating IT systems, thus allowing the creation of a virtual environment such as the Internet.

While the physical transport provides the interconnectivity, the component of an IT system that packages the information and ensures it gets delivered to the user is called the “network.” The network uses a globally recognized addressing scheme called Internet Protocol (IP). IP addressing ensures the information is delivered through the physical transport to the required destination.

A collection of networks, which adhere to centrally established rules and is governed by a centralized authority, is referred to as a “Domain.” Two examples of Domains are Dot MIL (.mil) and Dot IC (.ic) which are governed by the Department of Defense and the Intelligence Community respectively.

The last component of an IT system is the Input/Output (I/O) Device, which gives a user access to IT capabilities and provides that “on ramp” into cyberspace. Examples of I/O devices would include personal computers (both desktops and laptops), mobile computing devices, such as cellular smart phones, and bar code readers that track merchandise.

When you interconnect these IT system components, you create the cyberspace virtual environment that can process, discover, store or communicate information globally at the speed of light. Cyberspace, like all other global commons, is an avenue of approach for nation states and non-nation state actors to attack and conduct espionage on those who conduct operations in cyberspace. Computer network attack is defined in Joint Publication 1-02 as “actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and

computer networks, or the computers and networks themselves."[14] Computer network exploitation is defined in the same publication as "enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks."[15] Each of the IT system components discussed above is an avenue of approach or a target for a hostile actor to conduct cyber attack or espionage. Now that we have these common points of reference and terms, the next step is to figure out how to draw a border around these IT systems such that a policy can be written that would protect United States national interests in cyberspace.

Cyberspace's Geography Problem

There is one area where cyberspace operations do not compare very well to maritime operations. In maritime operations, you have a sea line of communication that delivers goods and services across the commons. These sea lines of communications are considered exterior lines of communication because they are moving goods and services from one nation-state's port to another, crossing international boundaries; however, in cyberspace, the physical transport that interconnects a user to IT capabilities through a network can simultaneously act as exterior lines of communications (data traffic between domains) and interior lines of communications (data traffic between an I/O device and an IT capability). This data traffic traversing the physical transport is electronically addressed using Transport Control Protocol (TCP). This protocol does not allow an observer to distinguish between which data traffic is an exterior line of communications and which data traffic is an interior line of communications. The data traffic is combined into one stream of bytes and transmitted

down the physical transport path. Essentially, the IT system component and physical transport can function as interior and exterior lines of communications at the same time.

Another limitation on the analogy with maritime operations is that unlike the sea lines of communication, multinational telecommunications corporations and consortiums privately own the majority of the cyberspace lines of communications (physical transport). Nation-state ownership of the physical transport infrastructure used for international communications is mostly held in satellite communications by those nation's militaries. Ensuring guaranteed access to the lines of communication is in the best interest of these global telecommunications corporations and consortiums since this access is a "fee for service" business. When defining our cyberspace boundaries, U.S. policy does not need to address unfettered access to lines of communication. The assumption is that global telecommunications corporations and consortiums will remain neutral and profit driven to provide unfettered access to the cyberspace domain.

Unlike the other global commons, cyberspace has another geographic challenge. Air, sea and even space have ways to draw lines on a map to articulate boundaries that have definite geographical references. Cyberspace has both physical geography, which is the actual location of the IT systems that create cyberspace, and logical geography. Logical geography is a concept that the location of the I/O device and the IT capability the user is accessing in cyberspace may be distributed across multiple physical locations that extend over multiple national boundaries; however, to the user the IT capability supporting their I/O device is as accessible as if it were in a server room within the same building. This in effect establishes a virtual environment, which has no physical geography. This logical geography defines a boundary that encircles the

physical location of IT capabilities, the user's I/O device, and the network and physical transport that provides connectivity. For example, while a soldier deployed to Iraq relies on web or email services that reside at his home base in the continental United States, the IT system that supports this IT capability are as accessible as if it were in a server room within the forward operating environment. This logical geography defines a boundary that encircles the physical location of equipment and the user of the IT capability spanning multiple jurisdictions. To better understand the complexity of this concept, the United States Military operates a global, logical domain (Dot MIL) that spans over 88 countries in over 3,500 locations. This logical domain interconnects with more than 20,000 leased circuits and supports over 2.8 million users.[16]

The Physical Border Approach

The first approach to defining our cyberspace boundaries is to simply state our cyberspace borders mirror the physical national boundaries of the United States and its protectorates. The policy would articulate that all information technology systems (I/O devices, network, IT capabilities, and physical transport) located on U.S. soil would be subject to United States governance, regulation, and protection. In a July 2008 speech at the Information Security Group Alumni Conference, Robert Carolina, an international law expert on cyber crime, proclaimed that cyberspace no longer has a border problem. Mr. Carolina asserted that borders that pertain to cyberspace are the same borders already found in the real world. To make his point, he cited case law and prosecutions of cyber criminals and legal actions in which jurisdictions were determined in the same way other crimes where prosecuted. In his speech, he stated "for better or for worse, we as a species have chosen to organize our international existence around the theory

of geographical sovereign states. These sovereigns continue to apply their laws as appropriate to online activity."[17]

The Logical Border Approach

A second approach to defining our national cyberspace boundaries is to state any logical domains or networks controlled by organizations located within the jurisdiction of the United States are subject to U.S. policy and protection, regardless of the global position of the IT systems that make up those virtual environments. In a 1996 Stanford Law review article, "Law and Borders: The Rise of Law in Cyberspace," David Johnson and David Post assert that physical boundaries are not "arbitrary creations." In order for borders to make sense, a government must be able to "exert control over the space; have physical proximity to the claimed area to effect behavior; have their claim generally accepted as legitimate; and post appropriate notices defining the actual border locations."[18] In their article, Johnson and Post state "cyberspace has no territory based on boundaries, because the cost and speed of message transmission on the Net is almost entirely independent of physical location."[19]

Comparison of Approaches

To determine the best approach for developing a cyberspace border policy, this analysis will apply the Feasibility, Acceptability and Suitability (FAS) Test to each of these concepts.[20] In order to ensure uniformity in this assessment of these policy approaches, the criteria for feasibility, acceptability and suitability will remain constant. The criteria for feasibility are: can the United States Government (USG) implement with resources available; an assessment of the level of complexity; and an assessment of likelihood of successful implementation. The criteria for acceptability are: an assessment of the level of risk; consistency with current laws; and assessment of

legitimacy with international partners. The criteria for the assessment of suitability are: likelihood of successful policy implementation and the likelihood of policy effectiveness.[21] This analysis will first apply these criteria to each individual approach and then compare the results for each criterion to assess the best option.

The physical geographical approach to defining our cyberspace borders is a very straight forward approach. When you assess the feasibility of this approach, it does well because this is the traditional method we discern boundaries in other domains. The advantage to this approach is our cyberspace international boundary demarcation points would be straightforward and easy to identify. It would be relatively easy to define which IT systems would be protected by the United States since our physical international boundaries are all currently recognized. To implement the strategy behind this policy would simply require the U.S. Government to determine the IT systems that reside within our physical borders and declare them as U.S. cyberspace territory. Any cyber non-kinetic attacks or espionage perpetrated on the equipment within these physical borders would constitute a hostile act against the United States.

The acceptability of the physical borders approach for cyberspace boundaries is also a positive aspect when it comes to assessing legal and international legitimacy. The theories, policies, and international agreements currently used to govern other global commons should easily translate to cyberspace operations since this approach most closely mirrors the way we assess our sea, air, and space boundaries. Maritime law is complex and has taken many centuries to develop. Written maritime agreements date back as early as the 6th Century with the “Digest of Justinian” to the more recent United Nations “Convention on the Law of the Sea” approved in 1982 by 150

countries.[22] The process of developing international cyberspace law, commensurate with the UN Conventions of the sea, would take time. Maritime law has well-established, professional associations and credentialing paths for attorney's who chose to serve in this branch of law. Cyberspace law may not take centuries to develop, but it will take a significant amount of time to develop the professional associations and credentialing paths of cyber law professionals to help conceptualize the international agreements.

Risk is an area that is not as positive for this approach. Discussed in the next paragraph under suitability, there is significant risk that U.S. national interests may not always be protected if we use this approach to developing our cyberspace borders.

Suitability is really where the physical border approach falls short of expectations. The globalization of IT capabilities makes this approach to defining our cyberspace boundaries inadequate to protect all of our IT systems. Many U.S. corporations, DoD, government agencies and non-governmental agencies outsource their IT capabilities to multinational corporations.[23] These IT capabilities may be hosted outside the physical boundaries of the United States. A hostile act against one of these off shore-hosted IT capabilities would not fall under United States' jurisdiction for a unilateral cyberspace Response Action. This would leave a great deal of our critical IT systems unprotected. Additionally, U.S. personnel traveling outside the physical boundaries of the United States, yet accessing IT capabilities with a mobile I/O device would also be outside of the cyberspace boundary.

The logical geographical approach to defining our cyberspace borders is very complex. As we assess the feasibility of this policy, complexity weighs high as a

negative when judging the evaluation criteria. There is no clear-cut way to establish a permanent or even semi-permanent cyberspace boundary using the logical boundary approach. The demarcation point would be in a constant state of fluctuation. Every time a user creates a session, this logical boundary could change depending on the physical location of the IT capabilities he or she is accessing. This would make a consistent defensive plan to secure our cyberspace borders problematic. The United States would have to maintain a dynamic and possibly reactive collective defensive plan. It is also not always clear, from the user's point of view in cyberspace, the location of the IT capabilities supporting his or her cyberspace experience. For example, many multinational corporations are caching their web capabilities in foreign countries to improve the performance of the customer's cyberspace experience.[24] Web caching is forward staging of web services (e.g., HTML pages, images, applications) to reduce bandwidth usage, server load, and perceived lag.[25] For example, an American living in a European country may conduct web-enabled banking at a U.S. Bank; however, when they access the U.S. banking website, the U.S. bank might be redirecting the user to a cached web server in Europe so the user has better performance. The user may not realize the U.S. bank is redirecting him or her to another website. This is just one of the complexities that highlight how hard it would be to draw a logical cyberspace boundary.

Acceptability is also a disadvantage to the logical boundary approach. Other nations and national organizations may dispute the United States' authority to conduct unilateral cyberspace response actions if the hostile act or intent is perpetrated on IT capabilities within their physical borders. Cyberspace RA is generally offensive or defensive in nature. Offensive RA involves some of the same tactics, techniques, and

procedures used in cyber attacks. The difference is that offensive RA is focused on disrupting the hostile cyber actor's ability to achieve their desired effects. An example of Offensive RA would be to use cyber attack to disable or destroy an IT capability that is being used to command and control a botnet army conducting a denial of service attack. Defensive RA involves improving the defensive posture of the IT systems to make it more difficult for cyber hostile actors to achieve their desired effects. Examples of Defensive RA include updating antivirus and sensor grid signatures or just simply disconnecting an infected IT capability. However, the severity of this problem is limited.[26] If the cyberspace RA is offensive in nature, the response action will be focused on the perpetrator of the hostile act and should have no impact on the third party IT capability provider. If the RA is defensive in nature, it will be in the best interest of the IT capability provider to comply with the defensive response action since lack of compliance would negatively affect their business revenue. A third cyberspace RA technique used to disrupt cyberspace hostile acts is to take legal actions against IT capability providers such as a court order that directs these providers to cease and desist certain activities. For example, a court order could require an IT capability provider to stop hosting a hostile server being used to launch a cyber attack, such as a denial of service attack on DoD. If cyberspace RA uses legal actions to achieve defensives effects, the complexity of legal authority to prosecute and convict perpetrators would be difficult to accomplish because it would span multiple legal jurisdictions.

As we assess the suitability of this logical boundary approach, there is a gap for state or non-state bad actors to commit hostile acts on IT capabilities located within the

physical boundaries of the United States, but provide capabilities to other countries or multinational corporations outside the United States. For example, in August 2008, the country of Georgia was hit by unattributed cyber attacks on its government websites as a precursor to an invasion by Russian forces into that country. Georgia moved its government websites to a service provider within the United States' physical boundaries in an attempt to stop the cyber attacks. This action did not stop the cyber attacks against Georgian government websites.[27] Under this proposed policy for defining our cyberspace boundaries, the United States would not have the authority to respond against the perpetrators of the Georgian cyber attacks because the IT capabilities were not considered to be within the logical boundaries of the United States.

Analysis of Comparison

A FAS Test assessment of these two approaches reveals that neither the physical approach nor the logical approach to defining our cyberspace borders is adequate. The physical approach is the more feasible of the two options and would be widely acceptable by the international system since it closely mirrors how the international community defines the boundaries of other global commons such as the sea. Nevertheless, the physical approach is not suitable to draw borders around all of our critical IT systems that may be important to U.S. national interests due to the globalization of IT capabilities. An example of this is DoD hosts IT capabilities in foreign countries in computing centers, which sometimes lie outside of what is considered to be sovereign U.S. territory.

The logical approach to defining our cyberspace borders also does not fare well when assessing the FAS Test. While this solution is suitable to protecting all of our IT capabilities from hostile acts, the feasibility of being able to consistently manage our

cyberspace borders in this very dynamic logical environment becomes impossible. The acceptability of declaring United States jurisdiction on IT systems located in foreign countries also becomes problematic if those countries are defining their cyberspace borders by the physical location of the IT capabilities that define cyberspace

This analysis of the comparison drives the consideration of another approach. This third approach takes the best aspects of the physical and logical approach and blends them into a hybrid approach.

In the previous legal opinions cited by Carolina, and Post/Johnson, they appeared to support the physical and logical approaches respectively; however, that assumes these legal opinions are anchored on the position, location, or status (U.S. property or not) of the IT systems that create the virtual environment. If you change the reference point from the IT systems to the status or position of the user of the IT systems, you may interpret the legal opinions from Mr. Carolina and Post/Johnson as in agreement with a third approach to defining our cyberspace borders.

This third approach is to anchor the cyberspace boundaries in relation to the geographic location or status of the user instead of the IT systems that create cyberspace. This approach is a blended course of action, using some of the best attributes of the physical and logical geography approaches. The policy would state that any user of an IT system, located within the jurisdiction of the United States, would be subject to United States policy and protection in cyberspace. Any hostile act or intent perpetrated on the IT systems being accessed by a user, whose status is determined to be within the jurisdiction of the United States, (even if the IT capabilities

itself or the user is located outside the United States), could be subject to a unilateral cyber RA.

Cyberspace is truly a virtual domain. Unlike other global commons (maritime, air, sea), a firm, physical geographical boundary or demarcation point between international and national domains is impossible to establish. Trying to establish these boundary parameters in reference to the IT systems that create the virtual cyberspace domain would not fully encircle all United States IT capabilities. By its nature, cyberspace is not geographical.[28] This brings us back to the analogy of cyberspace as a global domain. There is a theory in International Law with respect to assigning jurisdiction in sovereignless, international spaces such as the sea, Antarctica, and outer space. In international spaces, the nationality, not the territoriality of the entity, drives legal jurisdiction. When discussing intellectual property rights in cyberspace, Darrel Menthe argues that cyberspace is the 4th sovereignless space.[29] Robert Carolina states in his speech at the Information Security Group: "The way in which we experience the Internet is increasingly driven by our physical location."[30]

As with the physical approach to defining our cyberspace borders, this hybrid approach is a very straight forward application. When you assess the feasibility of this approach, it does well because, like the physical approach, this is the traditional method for which we discern our boundaries and territoriality in other domains. The advantage to this approach is our cyberspace international boundary demarcation points would be straightforward and easy to identify. It would be relatively easy to define who or what entity would be protected by the United States since our physical boundaries and jurisdictions are all currently recognized. Any cyber non-kinetic attacks or espionage

perpetrated on users or entities within these physical borders would constitute a hostile act against the United States.

The acceptability of the hybrid approach for cyberspace boundaries is also a positive aspect when it comes to assessing legal and international legitimacy. The theories, policies and international agreements used to govern other sovereignless or international spaces such as Antarctica, outer space and the sea commons should translate well to cyberspace operations. This may require the development of a "flagging" process, similar to what is used for international shipping, for which IT system users and capability providers declare their nationality.[31] One down-fall to this approach could be the similar pitfall of international flagging of ocean-going vessels where ship owners will pick a country with the cyber law framework and tax codes that are most advantageous to their business instead of which country best defines the status of their organization.

There is another consideration for this approach that may cause concern from those organizations that advocate for privacy in cyberspace. This hybrid approach requires that anonymity in cyberspace is no longer the "default" setting.[32] Governments have limited ability to influence behavior in cyberspace.[33] But, behavior in cyberspace is promulgated by people and organizations. Governments can influence the behavior of people and organizations if they are identifiable as the victim or perpetrator of a hostile act in cyberspace.

The major factor driving anonymity in cyberspace is the shortage of IP addresses used in IP version 4 (IPv4)[34] to support all IT devices connected to the Internet. With the proliferation of IT systems registered after the invention of the World Wide Web in

1989, the Internet Corporation for Assigned Names and Numbers (ICANN) (the international organization that assigns and manages IP addresses)[35] quickly exceeded the capacity of the IP addresses available. Without enough IP addresses to register every user I/O device and IT capability with a permanent address, this drove organizations to use Network Address Translation (NAT) and Dynamic Host Configuration Protocol (DHCP) to reuse IP addresses behind their firewall routers. The application of these techniques to reuse IP addresses created the situation now where anonymity is very easy to achieve in cyberspace. Lawrence Lessig, in an address at Taiwan Net '98, stated that "the default in cyberspace is anonymity." Mr. Lessig went on to say that "because it is so easy to hide who one is, it is practically impossible for the laws and norms, to apply in cyberspace."[36] Mr. Lessig is correct. In order for this construct of "cyberspace borders" anchored on the user, we must overcome the "default" setting of anonymity in cyberspace. IP version 6 (IPv6)[37] offers hope in that area. IPv6 will provide over a trillion IP addresses as compared to IPv4's approximate 4 billion. As we develop the network infrastructure to support IPv6, this will eliminate the need for NAT and DHCP to reuse IP addresses. IPv6 could provide a method of permanently assigning an IP address to an I/O device or IT capability. As a part of assigning these permanent IP addresses, the nationality of these addresses could be declared at the same time. Drawing our cyberspace borders anchored on the user would be as simple as ensuring the IP addresses issued to IT capabilities and I/O devices are organized by national jurisdictions. This will make anonymity in cyberspace more difficult vice the "default setting."[38]

If anonymity in cyberspace is abolished, there will be transparency on the status of the user or entity in order to determine within whose cyberspace borders they reside. This will allow us to truly define cyberspace as a global common domain analogous to the sea. International agreements and law can be constructed from existing laws that regulate sovereignless spaces, to include a method for "flagging" or declaring the nationality of a cyberspace user or entity. That nationality would follow the user or entity no matter where they are located in physical space and protect them by U.S. policy and defense. Jurisdictions and area of responsibilities for cyberspace RA within the U.S. cyberspace borders could be coordinated between government, law enforcement, and commercial industry. As observed by Mr. Carolina, this is the direction the legal community is driving in the absence of a policy that defines cyberspace borders.[39]

Cyberspace privacy advocates who are concerned that stripping anonymity from users will violate privacy in cyberspace may be making the mistake that anonymity and privacy are synonymous terms. Arguably they are very different. An analogy that illustrates this difference is that a person driving on an interstate highway has an expectation of privacy to the extent that a person driving in the next lane would not be able to identify them. That same person does not have a reasonable expectation that authorities charged with enforcing law, order and discipline on the highway would not be able to identify them by their license plate if they are breaking the law. Privacy deals with the ability of a user to be unidentifiable to other users of cyberspace. The concept of anonymity, used in the context of cyberspace, deals with the inability of enforcement bodies to identify bad actors in cyberspace.

Conclusion and Recommendations

The fundamental step of defining our cyberspace borders is a precursor action that must happen before national policy makers address other complicated questions such as defining what constitutes cyber warfare, how we respond to cyber attack, and how we define our internal national jurisdictions within cyberspace. The studies commissioned to recommend national cyberspace policy all remark that defining borders is a hard problem. Nevertheless, none of the studies make definitive recommendations on how to approach this problem.

The evolution of cyberspace, since the invention of the World Wide Web in 1989, is a major contributing factor to the rapid globalization of the world by improving the speed of global communication from weeks and months to minutes and seconds. The cyberspace global common has evolved over the last 21 years with little to no international agreements or consensus on how to govern this space. Unlike cyberspace, international policy and consensus, which has evolved over centuries, has shaped the governance over other global commons, such as the sea. Given the rate of technological change, U.S. policymakers do not have the luxury of time to develop international consensus on the cyberspace governance. The first step towards gaining global consensus on governing cyberspace should be to establish a boundary framework for cyberspace.

Based on an analysis of the findings in this paper, it is clear the virtual world created by IT systems and software do not have geographical dimensions that can be used to demarcate cyberspace borders. The legal community, by default, is determining jurisdictions based on the nationality of the actors in cyberspace instead of the geographic orientation of the equipment or cyberspace itself. By assessing previous

legal precedence in copyright law and from the analysis presented in this paper, drawing cyberspace boundaries in relation to the physical world is not feasible.

The legal community understands that cyberspace is a sovereingnless space where a plethora of actors operate in anonymity with little to no legal framework to govern their actions. These actors and entities (e.g. multinational corporations) should be required to declare their nationality or "flag" as they operate in and through cyberspace. Eliminating anonymity as the "default setting" in cyberspace is the key step to establishing this process for "flagging" actors and entities in cyberspace. Eliminating anonymity in cyberspace could be accomplished through the issuing of IP addresses as the Internet transitions from IPv4 to IPv6. ICANN should issue blocks of IP addresses in a such way that they can be traced back to a country of origin for responsibility. Nation-states would then be responsible for governing their IP spaces and enforcing international agreements within their cyberspace areas of responsibilities.

Eliminating anonymity and emphasizing nation-state accountability will facilitate the development of U.S. policies in cyberspace. As Howard Schmidt, the Obama Administration appointed Cyber Czar, follows up on Ms. Hathaway's cyberspace Policy Review, the first step should be to coordinate a new memorandum of agreement (MOA) between the U.S. Department of Commerce and ICANN. This new MOA should define which blocks of IP addresses will be used for entities declaring their nationality as U.S. territory. The next step should be to develop USG legislation that defines the process of how individuals and entities declare their U.S. nationality or "flagging." Once the U.S. defines its internal process for "flagging" then the USG should coordinate with the United Nations to develop a "Convention on the Law of Cyberspace" which closely

mirrors the way the Convention on the Law of the Sea was developed. As a part of this Convention on the Law of Cyberspace, the techniques to reuse IP addresses behind firewalls should be prohibited to ensure anonymity is globally abolished. This would then allow the National Security Council to form U.S. policy that declares the United States reserves the right to conduct unilateral cyberspace response actions against any hostile actors who may perpetrate cyber attack, crime or espionage on any persons or entity declared or flagged as under the jurisdiction of the United States. This jurisdiction would be declared through assigned IP addresses used by the IT users and capabilities, regardless of their physical location on the globe. Nations would be able to identify all of the IT systems and users that fall under their jurisdiction and develop an integrated defensive plan to ensure the lawful, peaceful use of cyberspace.

IT professionals who make it their business to protect operations in cyberspace often refer to the Internet as "The Wild."[40] By implementing these recommendations, U.S. policy makers would build a solid foundation for the development of a legal framework to govern cyberspace. This foundation could help frame other national and international cyberspace policy to protect U.S. National interests such as determining the difference between what constitutes criminal activity and war in this new sovereignless, global common. With the growing dependence on cyberspace to support the globalization of the world's economies, now is the time to tame "The Wild" and bring law and order to this sovereignless common.

Endnotes

[1] Cyberspace Policy Review, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf, (accessed December 2, 2009).

[2] Brian Kahin and Charles Nesson, *Borders in Cyberspace*, Third Printing 1999, (President and Fellows of Harvard College), 1997, 6.

[3] Time, http://www.time.com/time/time100/scientist/profile/bernerslee.html, (accessed December 2, 2009).

[4] Merriam-Webster Dictionary Online, http://www.merriam-webster.com/dictionary/Cyberspace, (accessed November 29, 2009).

[5] Government of the United Kingdom, *The Cyber Security Strategy of the United Kingdom*, http://www.cabinetoffice.gov.uk/media/216620/css0906.pdf, (access December 10, 2009).

[6] Wikipedia, http://en.wikipedia.org/wiki/Cyberspace, (access November 20, 2009).

[7] Joint Chiefs of Staff, *Joint Publication 1-02*, http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf, pg 141, (access November 30, 2009).

[8] Arthur Cebrowski, "Transformation and the Changing Character of War," Department of Defense, Office of Force Transformation, *Transformation Trends* (June 17, 2004), 7.

[9] Barry R. Posen, "Command of the Commons: The Military Foundation of U.S. Hegemony," International Security*,* Vol. 28, No. 1, Summer 2003*,* 5-46.

[10] John Gooch, *Maritime Command: Mahan and Corbett*, Reprinted by the Army War College, Theory of War and Strategy, Carlisle PA, Aug 09, 123-130.

[11] Martin C. Libicki, *Cyberdeterrence and Cyberwar*, RAND Corporation, Santa Monica, 2009, 2-5.

[12] Julian Corbett, *Principles of Maritime Strategy*, (Dover Publications, Mineola NY), 2004, 13-15.

[13] Commander John J. Klien, "Corbett in Orbit: A Maritime Model for Strategic Space Theory," *Naval War College Review*, Winter 2004, Vol. LVII, No. 1, 1.

[14] Joint Chiefs of Staff, *Joint Publication 1-02*, http://www.dtic.mil/doctrine/dod_dictionary/data/c/01182.html, (accessed December 11, 2009).

[15] Ibid.

[16] Joint Task Force Global Network Operations, *Command Brief for Capstone Visit*, July 2, 2009, Slide 4.

[17] University of London, Information Security Group, http://www.isg.rhul.ac.uk/node/285, (accessed December 3, 2009).

[18] Ibid.

[19] David R. Johnson, David Post, "Law and Borders: The Rise of Law in Cyberspace," *Stanford Law Review*, Vol. 48, No. 5 (May, 1996), 1367-1402.

[20] J. Boone Bartholomees, Jr, *A Survey of Strategic Thought*, chapter 7, 81.

[21] Planning Skills.Com, http://planningskills.com/askdan/9.php, (accessed on December 4, 2009).

[22] Britannica Online, http://www.britannica.com/EBchecked/topic/365510/maritime-law, (accessed on December 4, 2009).

[23] Catherine L. Mann, *Globalization of IT Services and White Collar Jobs: The Next Wave of productivity Growth*, http://www.ciaonet.org/pbei/iie/mac01/mac01.pdf, 1-2, (accessed December 4, 2009).

[24] University of London, Information Security Group.

[25] Telstra Geoff Huston, *Web Caching, Internet Protocol Journal*, Volume 3, Number 2, http://www.cisco.com/web/about/ac123/ac147/ac174/ac199/about_cisco_ipj_archive_article09186a00800c8903.html, accessed on December 4, 2009).

[26] Chairman of the Joint Chiefs of Staff, *Instruction 6510.01*, http://www.dtic.mil/cjcs_directives/cdata/unlimit/6510_01.pdf, (access on January 7, 2010).

[27] Stephen Korns and Joshua E. Kastenberg, "Georgia's Cyber Left Hook," *Parameters*, Winter 2008-2009, Vol. 38, No. 4, 60-61.

[28] David R. Johnson, David Post, *Stanford Law Review*, 1367-1402.

[29] Darrel Menthe, *Jurisdiction In Cyberspace: A Theory of International Spaces*, 4 MICH.TELECOMM.TECH.L.REV.96 (1998), http://cyber.law.harvard.edu/ilaw/Jurisdiction/menthe_Full.html, (access on December 4, 2009).

[30] University of London, Information Security Group.

[31] Darrel Menthe, *Jurisdiction In Cyberspace: A Theory of International Spaces*.

[32] Lawrence Lessig, The Laws of Cyberspace, Essay presented at Taiwan Net '98, March 1998, 6.

[33] Ibid.

[34] TCP/IP Guide.com, http://www.tcpipguide.com/free/t_ IPHistoryStandards Versions andCloselyRelatedProtoco.htm, (accessed on January 3, 2010).

[35]Memorandum of Understanding between the US Department of Commerce and the Internet Corporation for Assigned Names and Numbers, http://www.icann.org/en/general/icann-mou-25nov98.htm, (access January 13, 2010).

[36] Lawrence Lessig, 6.

[37] TCP/IP Guide.com.

[38] Lawrence Lessig, 6.

[39] University of London, Information Security Group.

[40] CA Security Blog, http://community.ca.com/blogs/securityadvisor/archive/2009/12/15/adobe-pdf-0-day-in-the-wild.aspx, (accessed February 13, 2010).