Strategy Research Project

Responding to Cyber Attacks and the Applicability of Existing International Law

by

Lieutenant Colonel Joseph L. Hilfiker
United States Army

United States Army War College
Class of 2013

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
xx-03-2013	STRATEGY RESEARCH PROJECT	

4. TITLE AND SUBTITLE
Responding to Cyber Attacks and the Applicability of Existing International Law

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Lieutenant Colonel Joseph L. Hilfiker
United States Army

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Professor Brian A. Gouker
Department of Military Strategy, Planning, and Operations

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: 5,945

14. ABSTRACT

The ever increasing technology of the information age has led to unprecedented access to information, increases in capabilities and the evolution of cyberspace. However, the great advances come with a danger. Information stored on both government and private networks, the networks themselves and the operating systems of infrastructures essential to the security and well being of the United States are exposed to cyber access, disruption and attack operations. The purpose of this paper is to identify how the United States should respond to the threat of cyber operations against essential government and private networks. The paper first examines the applicability of established international law to cyber operations. It next proposes a method for categorizing cyber operations across a spectrum synchronized with established international law. The paper finally discusses actions already taken by the United States to protect critical government and private networks and concludes with additional steps the United States should take to respond to the threat of cyber operations.

15. SUBJECT TERMS
Cybersecurity, Law of War, Cyber Operations

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)*
UU	UU	UU	UU	34	

USAWC STRATEGY RESEARCH PROJECT

Responding to Cyber Attacks and the Applicability of Existing International Law

by

Lieutenant Colonel Joseph L. Hilfiker
United States Army

Professor Brian A. Gouker
Department of Military Strategy, Planning, and Operations
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: Responding to Cyber Attacks and the Applicability of Existing International Law

Report Date: March 2013

Page Count: 34

Word Count: 5,945

Key Terms: Cybersecurity, Law of War, Cyber Operations

Classification: Unclassified

The ever increasing technology of the information age has led to unprecedented access to information, increases in capabilities and the evolution of cyberspace. However, the great advances come with a danger. Information stored on both government and private networks, the networks themselves and the operating systems of infrastructures essential to the security and well being of the United States are exposed to cyber access, disruption and attack operations. The purpose of this paper is to identify how the United States should respond to the threat of cyber operations against essential government and private networks. The paper first examines the applicability of established international law to cyber operations. It next proposes a method for categorizing cyber operations across a spectrum synchronized with established international law. The paper finally discusses actions already taken by the United States to protect critical government and private networks and concludes with additional steps the United States should take to respond to the threat of cyber operations.

Responding to Cyber Attacks and the Applicability of Existing International Law

The ever increasing technology of the information age has led to many advances in information technology, allowing unprecedented access to information and the automation of many previously manual functions. Formerly stand alone systems are now connected by government and private networks into systems of systems accessible from the Internet. The technology has led to increases in capabilities and efficiencies and the evolution of cyberspace. Cyberspace is defined as the physical infrastructure, user devices and network equipment, the information contained in it, and the software required to operate it. However, these great advances come with a danger to the security and well being of the United States. Information stored on both government and private networks, the networks themselves and the operating systems of government and private infrastructures essential to the security and well being of the United States are exposed to cyber operations. Cyber operations are those malicious actions taken in cyberspace intended access, disrupt or attack the information, the enabling physical infrastructures or to cause effects in the physical world. Examples of key infrastructure include: local, state and federal government management systems; financial and banking systems; petroleum production and distribution systems; electrical production and distribution systems; telecommunications systems; and the production and distribution of other essential goods and services to include food. Cyber operations against key infrastructures have the potential to cause physical effects outside the virtual world. Examples include: interfering with a government's ability to communicate with its population; disrupting the flow of goods and services essential to the economy and the physical destruction of infrastructures such as nuclear power plants; power

grids; or petroleum pipelines. Cyber operations directed against key infrastructures have the potential to impose catastrophic impact on the United States. The purpose of this paper is to identify how the United States should respond to the threat of cyber operations against government and private networks essential to the security and well being of the nation. The paper will examine the applicability of established international law to the cyber domain in order to identify what can be done within the framework of existing law. The discussion of existing internal law will focus on *jus en bellum*, the law governing the use of force, and *jus in bello*, the law governing the conduct of armed conflict. The paper continues with a proposed method for categorizing cyber operations across a spectrum tied to their legality under existing international law. Next the paper discusses the United States' response to date across the elements of national power**,** Diplomatic, Information, Military, Economic, Financial, Intelligence and Law Enforcement (DIMEFIL), to protect critical government and private networks. The paper concludes with recommendations spanning the national elements of power for additional steps the United States should take to respond to the threat of cyber operations against essential government and private networks.

United States policy concerning the applicability of existing international law to cyberspace as stated in the 2011 International Strategy for Cyberspace is: "The development of norms for State conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete. Long-standing international norms guiding State behavior in times of peace and conflict also apply in cyberspace."[1] However the document goes on to state the "unique attributes of networked technology require additional work to clarify how these norms

apply and what additional understandings might be necessary to supplement them."[2] Most accepted existing international law based on treaties, agreements and customary international law was developed prior to the invention of the Internet and evolution of cyberspace. Additionally, most cyber operations are carried out clandestinely and have therefore had limited effect on the development of international law.[3] Greater clarification of how these standards apply to actions taken in cyberspace is required. In order to remedy the lack of clarity, a comprehensive analysis of the applicability of existing international law to conduct in cyberspace was completed by the North Atlantic Treaty Organization Cooperative Cyber Defense Center of Excellence, or NATO CCD COE. Beginning work in 2009, the NATO CCD COE brought together a group of independent international legal and technical experts, as well as researchers, in order to produce a legal manual based on existing law to govern cyber warfare. In 2013 the group published the *Manual on the International Law Applicable to Cyber Warfare* also more commonly known as the *Tallinn Manual*. The *Tallinn Manual* focused particular attention to international law concerning *jus en bellum*, law governing the use of force, and *jus in bello*, law governing the conduct of armed conflict. The legal experts unanimously agreed existing international law pertaining to *jus ed bellum* and *jus in bello* do apply to operations in the cyber domain. The manual includes ninety five rules, based on existing international law, applicable to cyber operations.[4]

The Tallinn Manual details a number of key concepts relevant to responding to cyber operations. The first concept is "sovereignty." No state has "sovereignty" over cyberspace, but it has sovereign control over cyber infrastructure physically located within its geographic territory. Significantly, the state may regulate cyber infrastructure

within its borders. Additionally, the territorial "sovereignty" of the state protects cyber infrastructure residing within it.[5] States are also responsible for knowingly allowing cyber infrastructure within its territory to be used to negatively or illegally affect another state. Victims of cyber operations originating from the territory of another state may be legally entitled to respond proportionately, to include the use of force, in self defense. However, absent aggression rising to the level of "armed attack," "proportionality" limits a state's response to only that of compelling the aggressor to return to compliance with international law [6] An additional concept of international law is state "responsibility." States are responsible for acts and omissions attributed to entities of the state not just in the traditional physical domains, but also in the cyber domain. States are also responsible for acts and omissions committed by proxies if the proxies are acting at the direction of the state.[7] Of important note, definitive "attribution" of cyber operations is challenging. However, if cyber operations can be attributed to states or proxies then the principle of "responsibility" applies.

One of the most important concepts discussed in the *Tallinn Manual* is the "use of force" pertaining to actions committed virtually. Cyber operations equating to the "use of force" or the threat of the "use of force" are clear violations of international law unless undertaken in self defense or under the aegis of the United Nations. Existing international law does not define the exact threshold for a cyber operation to be a "use of force." To assist in determining if a cyber operation is a "use of force," the *Tallinn Manual* provides eight evaluation criteria. The first criteria is severity. Cyber operations causing physical harm to individuals or property are a "use of force." Those cyber operations causing only inconvenience are not. Also, the greater the effects of a cyber

operation on the essential interests of a nation, the more likely they are to be categorized as a “use of force.” A second criteria is immediacy. Cyber operations producing an immediate effect are more likely to be considered a “use of force.” Directness is the third evaluation criteria. Cyber operations with direct links between cause and effect are more likely to be considered a “use of force.” The next criteria is invasiveness. Cyber operations against protected systems and networks that are more invasive are likelier to be considered a “use of force.” Attacks against undefended targets are less likely to be a “use of force.” Measurability of the effects of a cyber operation is the fifth evaluation criteria in determining the “use of force.” The more observable, or measurable, the affect of a cyber operation; the greater the likelihood it is a “use of force.” The sixth criteria is military character. Cyber operations tied to, or complimenting, military operations are likelier to be a “use of force.” For example a cyber operation disrupting the integrated air defense of a nation prior to air strikes is likely a “use of force.” State involvement is a seventh evaluation criteria. The greater the appearance of state involvement in a cyber operation; the more likely it is to be considered a “use of force.” The final evaluation criteria to assist in determining if a cyber operation is a “use of force” is presumptive legality. International law is usually prescriptive. Therefore cyber operations whose effects are not prescribed are less likely to be a “use of force.” Cyber operations are legally considered the threat of the “use of force” if the operation’s execution would equal an act of force.[8]

Being the victim of a cyber operation equaling a “use of force” alone does not entitle a state to respond with force in accordance with international law. The “use of force” must rise to the level of an “armed attack” for a state to legally respond in self

defense with its own “use of force.” As with the “use of force,” the threshold for an “armed attack” is not specifically defined. Determination as to whether a “use of force” rises to the level of “armed attack” is largely determined by its scale and effects. Cyber operations injuring or killing people or damaging and destroying property certainly have sufficient scale and effect to constitute an “armed attack.” A cyber operation targeting a nation’s critical infrastructures with effects resulting in injury, death, damage or destruction is an “armed attack.” The larger the scale and the impact of the effects the greater the likelihood it is for a “use of force” to rise to the level of an “armed attack.”[9]

How a state responds to a “use of force” equating to an “armed attack,” including attacks committed in cyberspace, is constrained by *the jus ad bellum* concepts of “necessity” and “proportionality.” First, a state may respond with the “use of force” only out of “necessity” to defeat the attack or imminent threat of attack. If measures not rising to the level of the “use of force” are sufficient to defeat the attack, then the “use of force” in self defense is not permissible. Secondly, for the response to an attack to be acceptable it must show “proportionality.” In the context of *jus ad bellum* this means only the amount of force necessary to repel an attack is permissible. Additionally, international law governing the “use of force” does not require the act of defense to be in the same domain as the attack. A kinetic attack in self defense, that is both necessary and proportionate, may be made in response to a cyber attack.[10]

Cyber operations are commonly divided into two broad categories, exploitation and attack. Cyber exploitation generally is considered the less severe cyber threat and consists of activities such as the theft of information and denial of service attacks. Cyber attacks are considered more severe and are generally characterized by the destruction

of information or by actions in the virtual world causing destruction in the real world. The two category definitions are also based on the perceived intent of the individual, organization or nation state conducting the cyber activity. Intent is not always simple to identify when the identity of the malicious actor may be unknown. These two broad categories also do not take into account the most important aspect of a malicious cyber event, the effects the attack achieves.

According to Colonel Gary Brown and Lieutenant Colonel Owen Tullos, United States Cyber Command, a different and more effective way to define cyber operations is to consider them along a horizontal spectrum, based on the effects they achieve. (See figure 1 below) On the left end of the spectrum are access operations. Access operations are conducted to gain and sometimes maintain access to computer networks. Typically access operations do not adversely affect the system being exploited but may prepare the way for future malicious cyber activities. Access operations are unlikely to violate international law or equate to the "use of force." In the center of the spectrum are disruption operations. Disruption operations cause no physical damage or injury but impede the normal intended function of the information system. The majority of what are typically called cyber attacks fall into this category. Cyber disruption operations may or may not equal a "use of force" and do not rise to the level of "armed attack." On the right end of the spectrum are cyber attack operations. Attack operations are actions in cyber space equaling a "use of force" and an "armed attack."[11] Defining cyber attacks along a spectrum also conforms to the *Tallinn Manual's* evaluation criteria of severity, measurability and legality for defining the "use of force." Cyber operations to the left of the spectrum are less severe, less measurable, less likely

to be illegal or equal a “use of force.” Cyber operations to the right of the spectrum are more severe, more measurable, more likely to be illegal or equal a “use of force.”

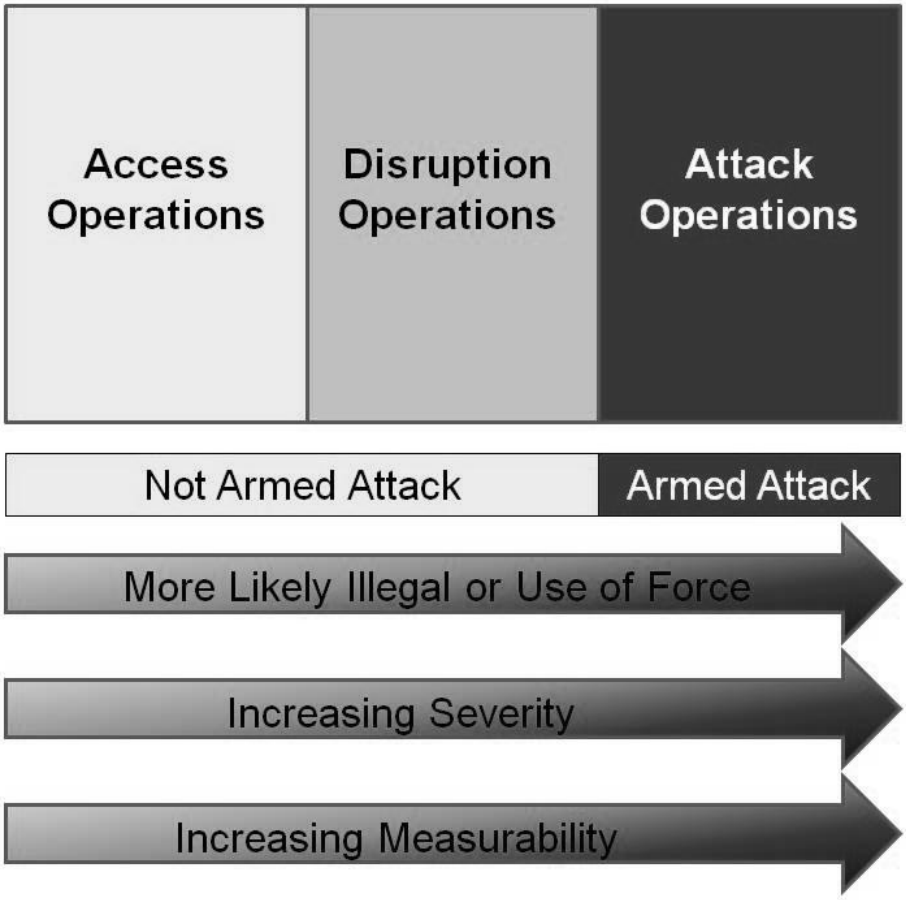

Figure 1: Cyber Operations Spectrum

Examples of cyber access operations are the 2008 Agent.btz, the 2009 GhostNet and the 2012 Project Blitzkrieg events. The Agent.btz access operation targeted United States Department of Defense, or DoD, secure and non-secure networks by using removable flash drives. “When inserted into a universal serial bus port on a desktop computer connected to the Internet, the malware loaded itself onto the host hard drive and beaconed back to its originator. When unsuspecting users inserted the infected flash drives to transfer data between secure and non-secure systems, the access

gained enabled follow-on activities on both systems."[12] The 2009 GhostNet access operation affected government networks in more than one hundred countries. GhostNet malware allowed an entity to remotely turn on the microphones and webcams of computers and to capture the data.[13] The Project Blitzkrieg access operation targeted thirty banks in the United States, attempting to steal funds from individual accounts.[14]

The following are examples of cyber disruption operations, the 2007 Estonian cyber disruption operation, the 2012 Shamoon virus and the 2012 denial of service attacks against United States banks. During a 2007 dispute with Russia concerning the removal of a Soviet era statue, a cyber disruption operation shut down Estonian government and commercial networks for approximately one month.[15] The 2012 Shamoon virus targeted the Saudi Arabian oil company ARAMCO, deleting data from approximately 30,000 computers and uploading the image of a burning American flag.[16] Another example of disruption operations are the 2012 denial of service attacks against United States banks, believed to have originated from Iran in retaliation for economic and political sanctions levied against them for their nuclear weapons program.[17]

The best know example of a cyber attack operation is the 2010 Stuxnet attack. The Stuxnet attack operation meticulously targeted the Supervisory Control and Data Acquisition, or SCADA systems of one thousand centrifuges being used by Iran to enrich uranium. The attack operation caused the centrifuges to be destroyed.[18] The Stuxnet cyber attack operation resulted in physical destruction and could therefore be considered a "use of force" and likely an "armed attack" under recognized international law.

Recently the United States has begun to take concrete, yet incomplete, steps to address the menacing threat of cyber operations against essential government and private networks. Recognition of the threat of cyber operations has led to actions taken across the elements of national power. The actions include overarching national policy guidance such as the President's Comprehensive National Cybersecurity Initiative, the National Security Strategy, the Quadrennial Defense Review, the National Military Strategy and the DoD Strategy for Operation in Cyberspace. These policy documents seek to integrate the efforts of the government across the elements of national power as well directing specific actions within them. Also the United States has begun to establish doctrine for operations in cyberspace by declaring it a military domain along with the physical domains of air, maritime, land and space. In order to inform and influence cyber adversaries, the State Department and the Secretary of Defense have made policy statements asserting that cyber attacks against the United States can constitute a "use of force" and the equivalent of an "armed attack" under existing international law.

President Barak Obama's Comprehensive National Cybersecurity Initiative, or CNCI, seeks to secure the United States in cyberspace utilizing the Military, Intelligence and Law Enforcement elements of national power. The CNCI is composed of twelve initiatives whose purpose is to integrate government efforts and was developed based on the finding of the 2009 Cyberspace Policy review. The twelve initiatives of the CNCI are:

- Manage the Federal Enterprise Network as a single network enterprise with Trusted Internet Connections.

- Deploy an intrusion detection system of sensors across the Federal enterprise.
- Pursue deployment of intrusion prevention systems across the Federal enterprise.
- Coordinate and redirect research and development (R&D) efforts.
- Connect current cyber ops centers to enhance situational awareness.
- Develop and implement a government-wide cyber counterintelligence (CI) plan.
- Increase the security of our classified networks.
- Expand cyber education.
- Define and develop enduring “leap-ahead” technology, strategies, and programs.
- Define and develop enduring deterrence strategies and programs.
- Develop a multi-pronged approach for global supply chain risk management.
- Define the Federal role for extending cybersecurity into critical infrastructure domains.[19]

To focus and integrate efforts in the Military and Intelligence elements of national power, the United States included guidance emphasizing cyber security in the National Security Strategy, the Quadrennial Defense Review and the National Military Strategy. Additionally, in 2011, the DoD published the DoD Strategy for Operating in Cyberspace to provide more detailed guidance in applying the Military and Intelligence elements of

national power. The DoD Strategy for Operating in Cyberspace focuses on five strategic initiatives:

- Treat cyberspace as an operational domain to organize, train, and equip so that DoD can take full advantage of cyberspace's potential.
- Employ new defense operating concepts to protect DoD networks and systems.
- Partner with other U.S. government departments and agencies and the private sector to enable a whole-of-government cyber security strategy.
- Build robust relationships with U.S. allies and international partners to strengthen collective cyber security.
- Leverage the nation's ingenuity through an exceptional cyber workforce and rapid technological innovation.[20]

Strategic Initiative One designating cyberspace as an "operational domain" is of particular significance. Designating cyberspace as a domain establishes it as an equal to the traditional military physical domains of air, land, maritime and space. It allows the DoD to organize, train and equip formations to conduct operations in cyberspace. Combined with guidance from the National Security Strategy, it requires the DoD to have the resources necessary to operate effectively in cyberspace.[21] However, the DoD designating cyberspace a domain does not establish an accepted shared international framework for conduct in cyberspace. For example the maritime and air domains have an accepted shared international framework for conduct, the United Nations Convention on the Law of the Sea or UNCLOS. Although not yet ratified by the United States Senate, UNCLOS establishes accepted standards such as twelve nautical mile

territorial limits and 200 nautical mile Economic Exclusion Zones, or EEZs. This accepted shared framework further details conduct with these limits. Cyberspace as an emerging domain lacks an accepted shared international framework.

An important step to begin establishing an accepted shared international framework for conduct in cyberspace occurred in September 2012. Utilizing the Diplomatic and Information elements of national power the State Department specified United States policy is that established international laws, including those concerning hostilities, apply to cyberspace. Speaking to an inter-agency legal conference on behalf of the State Department was Harold Koh, the department's Chief Legal Adviser. Mr Koh identified ten fundamental aspects of established international law applying to United States policy for cyberspace. The first policy is that established international law applies to cyberspace. The second policy is hostile activities in cyberspace cannot be conducted without rules or restraint. Specifically *jus in bello*, also known as the law of armed conflict, applies to cyberspace. United States policy with regard to the law of armed conflict is that cyberspace is a technological evolution, and the existing rules apply to the new innovation. The third policy is cyber operations resulting in death, injury or significant destruction would likely be considered a "use of force" rising to the level of an "armed attack." Three examples of cyber operations likely to be considered a "use of force" include attacks resulting in the meltdown of a nuclear reactor, opening a dam and causing physical destruction and disrupting an air traffic control system causing aircraft to crash. Cyber operations producing the same physical destruction as caused by a kinetic weapon would be considered a "use of force." The fourth policy statement is Article 51 of the United Nations Charter allowing states' the right to self defense applies

to cyberspace if a cyber operation equates to the “use of force” or the imminent threat of the “use of force.” The fifth, sixth and seventh policies are the *jus in bello* principles of “necessity,” “distinction” and “proportionality” all apply to cyber operations. Cyber operations must be necessary to accomplish the mission, must target valid military targets and not cause greater collateral damage compared to the military gain. The eighth policy is that states should analyze cyber weapons to determine if they are inherently indiscriminate and violate the principles of “distinction” and “proportionality.” The ninth policy is national “sovereignty” must be considered for cyber operations to be lawful. The physical infrastructure enabling cyberspace to exist in the real world resides in nearly all countries. Consideration must be given to the second order effects on other nations caused by a cyber operation. The tenth and final policy is states are culpable for cyber operations conducted by agents acting on their behalf.[22]

In 2012 the United States Secretary of Defense Leon Panetta delivered a policy speech to the Business Executives for National Security in New York City. His speech complemented and reinforced the State Departments Diplomatic and Information policy statements concerning cyber operations given the previous month, and added the Military element of national power. Secretary Panetta’s speech was intended to inform and influence both international and domestic audiences. He emphasized the importance of cyberspace to the nation’s and world’s economy and reinforced the concept of treating it as its own domain. The Secretary of Defense discussed the growing threat posed by cyber operations to the well being of the United States. In particular he highlighted the threat posed to the United States’ critical infrastructures including power grids, transportation networks and industrial plants. He also discussed

the worst case scenario where multiple cyber operations against our critical infrastructures were coordinated with physical attacks against the United States. In a warning to adversaries wishing to harm the United States in cyberspace, he stressed the significant advancements made by the DoD to identify the origin of a cyber attack (attribution) and the ability to respond across the full spectrum of operations to imminent threats or attacks, at the direction of the President. Secretary Panetta stressed the importance of three main axes to defend America in cyberspace: First is to develop new capabilities by improving our cyber warriors and developing new capabilities to detect and attribute operations. Second he stressed developing the policies and organizations required to defend the nation such as the creation of United States Cyber Command, or USCYBERCOM, and delineating roles and responsibilities between and among different government organizations. Thirdly he stressed the need for legislation to improve cooperation between the government and industry partners. For companies handling sensitive information, or providing essential services and infrastructure, he highlighted the need for the United States Congress to pass legislation requiring those companies to share the details of cyber operations against their networks with the government. He also stated the legislation must establish cyber security standards to protect the United States' critical infrastructure.[23]

In 2010 the United States took a significant step toward protecting Department of Defense network's, and the country as a whole, by establishing USCYBERCOM. USCYBERCOM's mission is:

> USCYBERCOM plans, coordinates, integrates, synchronizes and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations in order to

> enable actions in all domains, ensure US / Allied freedom of action in cyberspace and deny the same to our adversaries.[24]

USCYBERCOM's creation consolidates Department of Defense cyber activities, both offensive and defensive, into a single sub-unified combatant command. Additionally, by dual-hatting the Director of the National Security Agency as also the Commander of USCYBERCOM it enables synchronization between Title 10 and Title 50 functions. Title 10 functions are those associated with United States legal statutes regulating the armed forces. Title 50 are those legal statutes associated with national defense pertaining both to national security and intelligence functions.[25] USCYBERCOM has five priorities: The first priority is trained and ready cyber forces. The priority focuses on growing today's cyber warrior team to operate, maintain, protect and defend our networks and to conduct offensive cyber operations. Establishing a defensible architecture is the second priority. The focus is to employ cloud based network architectures to build agile, secure, defensible and reliable networks. The third priority is to operationalize the cyber concept to ensure unity of effort, between domestically focused organizations such as Department of Homeland Security, or DHS, and those foreign focused such as DoD. The fourth priority is creating a cyber common operation picture fusing relevant information from government, DoD, law enforcement, industry, critical infrastructure providers, and friends and allies to enable decision making in the cyber domain. The final priority is the authority to act in defense of the nation. The priority's emphasis is on integrating DoD, DHS and Department of Justice, or DOJ, functions to defend the nation in cyberspace.[26]

In the realm of Diplomatic, Informational and Law Enforcement elements of power the United States DOJ announced plans in 2012 to indict state sponsored cyber

attackers. The plan calls for special training for more than one hundred prosecutors to assist DHS and DoD agencies to identify cases that can be brought to trial. Cases could be brought against both private citizens and officials in a government. Potentially, the most advantageous entity for the United States to indict would be a foreign corporation who used and profited from the theft of intellectual property.[27] The companies convicted could be fined, enforcing a monetary penalty. In addition, or if imposing a fine is unpractical, sanctions could be imposed targeting the company, its executives and its products.

A concrete action taken by the United States to confront the threat of cyber attacks is the Defense Industrial Base Cyber Security / Information Assurance Program, or DIB CS/IA. Defense Industrial Base networks, or DIB networks, are those containing sensitive defense related information and processes. Created in 2011, the DIB CS/IA is a limited pilot program operated jointly by the DoD and DHS. Industry participation in the program is voluntary. The purpose of the DIB CS/IA program is to improve the defense of DIB networks and to mitigate the consequences of the compromise of information. Under the program, participating companies report intrusions and other relevant cyber security issues to the government and may participate in government damage assessments. Additionally the DoD provides DIB companies with unclassified cyber threat indicators and additional classified information to provide more information on the threat. Companies may then use the information provided to improve the defense of their networks. An additional element of DIB CS/IA is the DIB Enhanced Cybersecurity Services program, or DECS. The DECS program provides additional classified cyber threat information to both the DIB company as well as their Internet

Service Provider in order to further protect sensitive defense related information and DIB networks.[28]

The United States Congress repeatedly failed to pass comprehensive cyber legislation throughout the summer and fall of 2012. Citing privacy concerns and costs to industry of the additional proposed regulation, Congressmen and Senators were unable to come to agreement on a comprehensive cyber bill. However, the National Defense Authorization Act for Fiscal Year 2013, passed by the Congress and signed into law by the President, now requires designated companies to share information on the compromise of corporate networks. Designated companies are those who conduct business with DoD and whose networks contain military information. The Act also requires the Secretary of Defense to implement a strategy to consolidate and bring modern, efficient methods to DoD networks and to develop a human resources plan to support the DoD's networks and USCYBERCOM's requirement to conduct offensive cyber operations.[29]

In February 2013, absent comprehensive cyber legislation, the President issued Presidential Policy Directive 21--*Critical Infrastructure Security and Resilience* and Executive Order--*Improving Critical Infrastructure Cybersecurity*. Directive 21 formally establishes policy to strengthen the security and resilience of critical infrastructures and establishes three strategic imperatives. The first imperative is to "refine and clarify functional relationships across the Federal Government to advance the national unity of effort to strengthen critical infrastructure security and resilience."[30] The second is to "enable effective information exchange by identifying baseline data and systems requirements for the Federal Government."[31] The third is to "implement an integration

and analysis function to inform planning and operations decisions regarding critical infrastructure."[32] Paralleling the policy directive, the President's executive order directs the designation of critical infrastructures where a cyber operation could cause a catastrophe of regional or national effect. It also directs increased information sharing between the government and industry through the publication of unclassified cyber threat reports and expansion of the voluntary DIB CS/IA program already discussed. Additionally, the executive order directs the development of a baseline Cyber Security Framework to establish voluntary best practices to better protect critical infrastructures.[33]

Although the United States has taken significant actions, more can, and needs to be done to respond to the threat of cyber operations against government and private networks essential to the nation. The United States should extend the concept of free access for all nations to the global commons including cyberspace. The expansion should include the development of an internationally shared framework for conduct in cyberspace. The United States should treat our international cyber adversaries, both state and non-state, as we do terrorists. The United States should update federal cyber security policy and guidance utilizing existing authorities. Finally, legislation is required to address deficiencies that cannot be remediated with existing authorities. Specifically, legislation is required to: Clarify reporting requirements for cyber events; codify the authorities and responsibilities of organizations charged with defending against cyber attacks; establish a mechanism for private companies to share information on cyber attacks; and to establish minimum cyber standards to protect critical infrastructure.

The United States has long maintained a policy to provide the nation guaranteed access to the global commons in order to ensure our economic prosperity and national security. Just as UNCLOS is providing a framework for nations to interact in the global commons of air and maritime, a similar international framework should be also be established for interactions in the global commons of cyberspace. For example, UNCLOS establishes acceptable conduct inside a 200 nautical mile Economic Exclusion Zone. Such a framework for the cyber domain would provide more clarity for all parties to predictably interact with each other. The framework should be established in accordance with existing international laws of *jus ad bellum* and *jus in bello*, reinforcing that their principles apply to the new domain. Additionally the concept of cross domain effect, actions taken in the cyber domain having effects in the physical domains and vice versa, should be addressed in the framework. The framework should categorize cyber operations based on the effects they cause, either access operations, disruption operations or attack operations as previously discussed. The effects based categories must be synchronized with established international law to provide clarification to the legality of actions taken in cyberspace. The UNCLOS example should be used as the model to develop and implement a shared framework for cyberspace. Using the United Nations to internationalize the creation of the cyberspace framework will increase legitimacy and transparency while decreasing the perception of American hegemony over cyberspace. However care must be taken to ensure the framework does not become a mechanism for the United Nations to control, regulate or tax cyberspace. As more and more nations adopt the framework it will increasingly become

the internationally accepted law of cyberspace just as UNCLOS has become the accepted standard in the maritime domain.

In addition, where attributable and prosecutable, the United States should indict private individuals and members of foreign governments who commit aggressions against the United States in cyberspace. Individuals indicted may be out of the physical reach of extradition by the United States. In those circumstances the individuals should be added to the list of Specially-Designated Nationals and Blocked Persons and sanctions and penalties should be imposes on businesses and financial institutions having interactions with them. State or non-state organizations committing cyber aggression against the United States should be treated the same as terrorist organizations such as the Iranian Revolutionary Guard's Quds Force. The organizations themselves should be cut off from all international systems of business and finance and their members added to the Specially-Designated Nationals and Blocked Persons list.

Also, following the advice of the Center for Strategic and International Studies, the United States Office of Manage and Budget should update Circular A-130. The circular is applicable to all elements of the executive branch of government and has not been updated since 2000. Circular A-130 sets policy for the management of federally controlled information systems. Key changes should include the continuous monitoring of networks versus compliance based inspections. Compliance based inspections measure only whether an information system is in compliance with published regulations and standards at the time the inspection is conducted. Continuous monitoring provides a real-time assessment of the security of an information system, protecting it in more proactively. Also the new circular should direct the migration of

networks to more secure architectures. The updated circular should establish standards for the protection of information based on the nature of the information itself, not the agency or the information system it is on. Additionally the circular should reassign and define roles, responsibilities and definitions for cyber security within the United States government. The updating of roles responsibilities and definitions should be done in conjunction with cyber legislation.[34]

Finally the United States should implement comprehensive cyber legislation, as stated in the President's Cybersecurity Legislative Proposal, with the purpose of protecting the citizens, critical infrastructures and government networks of the United States in cyberspace. The legislation should include the following key features: harmonize existing state cyber intrusion reporting requirements; clarify penalties for cyber crimes; establish authorities for the DHS and the DoD to provide assistance to industry, states and local governments when requested; require the DHS to establish a system for industry, states and local governments to share information concerning cyber threats while protecting civil liberties; address industries' legal liability concerns; also require the DHS to establish baseline security standards for critical infrastructure as well as identify what is critical infrastructure; and update the Federal Information Security Management Act, or FISMA, to formalize DHS's roles and responsibilities to protect United States networks.[35]

The newest of the domains, cyberspace, is essential to the continued prosperity, security and well being of the United States. Although the existing international concepts of *jus ad bellum* and *jus in bello* can and should apply to cyberspace, a shared international framework similar in concept to UNCLOS is needed to provide specificity

and predictability for interactions in cyberspace. Cyber aggressors should also be held to the full weight of justice available. Domestically, the United States should update regulations and legislation to improve the efficiency and effectiveness of the protection of essential government and private networks.

Endnotes

[1]Office of the President of the United States, *International Strategy for Cyberspace* (Washington, DC: The White House, May, 2012), 9.

[2]Ibid.

[3]Gary D. Brown and Owen W. Tullos, "On the Spectrum of Cyberspace Operations," December 11, 2012, http://smallwarsjournal.com/print/13595 (accessed December 17, 2012).

[4]Michael N. Schmitt, ed, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (New York, NY: Cambridge University Press, 2013), 6-19.

[5]Ibid, 25.

[6]Ibid, 33-35.

[7]Ibid, 35-37.

[8]Ibid, 47-52.

[9]Ibid, 53-56.

[10]Ibid, 59-60.

[11]Brown and Tullos, "On the Spectrum of Cyberspace Operations."

[12]Ibid.

[13]Ibid.

[14]David Goldman. "Massive Bank Cyberattack Planned," December13, 2012, http://money.cnn.com/2012/12/13/technology/security/bank-cyberattack-blitzkrieg/index.html (accessed December 12, 2012).

[15]Brown and Tullos, "On the Spectrum of Cyberspace Operations."

[16]Thom Shanker and David Sanger, "U.S. Suspects Iran Was Behind a Wave of Cyberattacks," *New York times*, October 14, 2012.

[17]David Goldman, "The Real Iranian Threat: Cyberattacks," November 5, 2012, http://money.cnn.com/2012/11/05/technology/security/iran-cyberattack/index.html (accessed November 5, 2012).

[18]Robert L. Mitchell, "After Stuxnet: The New Rules of Cyberwar," November 5, 2012, http://www.computerworld.com.au/article/441030/after_stuxnet_new_rules_cyberwar/ (accessed November 5, 2012).

[19]Executive Office of the President of the United States, *The Comprehensive National Cybersecurity Initiative* (Washington, DC: The White House, accessed December 27, 2012), 1-5.

[20]United States Department of Defense, *Department of Defense Strategy for Operating in Cyberspace* (Washington, DC: The Department of Defense, July 2011), 5-11.

[21]Ibid.

[22]Harold Koh, "International Law in Cyberspace," scripted commentary, Ft. Meade, MD USCYBERCOM, September 18, 2012.

[23]Leon Panetta, "Remarks by Secretary Panetta on Cybersecurity to the Executives for Nation Security," scripted commentary, New York, NY, October 11, 2012.

[24]George Franz, "The Cyber Domain Operations in Cyber Battlespace," briefing slides, Carlisle Barracks, PA, U.S. Army War College, December 14, 2012.

[25]Ibid.

[26]Ibid.

[27]Aram Roston, "DOJ Plans to Indict State-Sponsored Cyber Attackers," December 18, 2012, http://www.defensenews.com/article/20121218/C4ISR01/312180009/DOJ-Plans-Indict-State-Sponsored-Cyber-Attackers?odyssey=tab|topnews|text|FRONTPAGE (accessed December 19, 2012).

[28]Department of Defense, *Fact Sheet: Defense Industrial Base (DIB) Cybersecurity Activities* (Washington, DC: The Department of Defense, May, 2012).

[29]U.S. Senate Committee on Armed Services, *Senate Armed Services Committee Completes Conference of National Defense Authorization Act for Fiscal year 2013* (Washington, DC: U.S. Senate Committee on Armed Services, December 2012), 25.

[30]Executive Office of the President of the United States, *Presidential Policy Directive – Critical Infrastructure Security and Resilience* (Washington, DC: The White House, accessed February, 2013), 1-2.

[31]Ibid.

[32]Ibid.

[33]Executive Office of the President of the United States, *Executive Order – Improving Critical Infrastructure Cybersecurity* (Washington, DC: The White House, accessed February, 2013), 1-4.

[34]Franklin S. Redder, Daniel Chenok, Karen S. Evans, James Andrew Lewis & Alan Paller, "Updating U.S. Federal Cybersecurity Policy and Guidance: Spending Scarce Taxpayer Dollars on Security Programs that Work," Center for Strategic and International Studies, October 23, 2012.

[35]Executive Office of the President of the United States, *Fact Sheet: Cybersecurity Legislative Proposal* (Washington, DC: The White House, accessed December 27, 2012).