Strategy Research Project

STRATEGIC IMPACT OF CYBER WARFARE RULES FOR THE UNITED STATES

BY

MR. PAUL A. MATUS
National Security Agency Civilian

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

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

1. REPORT DATE *(DD-MM-YYYY)* 23-03-2010	**2. REPORT TYPE** Strategy Research Project	**3. DATES COVERED** *(From - To)*

4. TITLE AND SUBTITLE Strategic Impact of Cyber Warfare Rules for the United States	**5a. CONTRACT NUMBER**
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) Mr. Paul A. Matus	**5d. PROJECT NUMBER**
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Mr. William O. Waddell 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

Despite the growing complexities of cyberspace and the significant strategic challenge cyber warfare poses on the United States' vital interests few specific rules for cyber warfare exist. The United States should seek to develop and maintain cyber warfare rules in order to establish internationally accepted norms, mitigate damage to critical governmental, commercial and private resources, and help hold belligerent actors accountable. The cyber attacks against Georgia in the summer of 2008 provide a contemporary example of the complexities associated with cyber attack attribution, application of the Law of Armed Conflict's principles of war, and the international community's ineptitude in responding. These along with other justifications exemplify the need for multilaterally prepared cyber warfare rules that will reduce the negative influence cyber warfare presently has on the United States' national interests.

15. SUBJECT TERMS
Cyberspace, Computer Network Operations, Georgia, Russia

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT UNCLASSIFED	**b. ABSTRACT** UNCLASSIFED	**c. THIS PAGE** UNCLASSIFED	UNLIMITED	46	**19b. TELEPHONE NUMBER** *(include area code)*

USAWC STRATEGY RESEARCH PROJECT

STRATEGIC IMPACT OF CYBER WARFARE RULES FOR THE UNITED STATES

by

Mr. Paul A. Matus
National Security Agency Civilian

Mr. William O. Waddell
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:	Mr. Paul A. Matus
TITLE:	Strategic Impact of Cyber Warfare Rules for the United States
FORMAT:	Strategy Research Project
DATE:	25 March 2010 WORD COUNT: 9,362 PAGES: 46
KEY TERMS:	Cyberspace, Computer Network Operations, Georgia, Russia
CLASSIFICATION:	Unclassified

Despite the growing complexities of cyberspace and the significant strategic challenge cyber warfare poses on the United States' vital interests few specific rules for cyber warfare exist. The United States should seek to develop and maintain cyber warfare rules in order to establish internationally accepted norms, mitigate damage to critical governmental, commercial and private resources, and help hold belligerent actors accountable. The cyber attacks against Georgia in the summer of 2008 provide a contemporary example of the complexities associated with cyber attack attribution, application of the Law of Armed Conflict's principles of war, and the international community's ineptitude in responding. These along with other justifications exemplify the need for multilaterally prepared cyber warfare rules that will reduce the negative influence cyber warfare presently has on the United States' national interests.

STRATEGIC IMPACT OF CYBER WARFARE RULES FOR THE UNITED STATES

> So cyberspace is real. It's the great irony of our Information Age--the very technologies that empower us to create and to build also empower those who would disrupt and destroy.
>
> —Barack Obama[1]

The cyberspace domain is becoming increasingly complex interconnecting commercial, governmental and private equipment, networks and systems. Actors in cyberspace are a diverse set of law-abiding citizens, groups, corporations, and governments, belligerent state and non-state actors, and military elements acting by direction of their host states. Activities vary along a continuum in severity from legal commerce to what may be considered acts of war. And yet, few laws, treaties or other rules specifically for this domain have been implemented. Why is this so?

This paper attempts to examine the existing framework of cyber warfare rules, use the summer of 2008 cyber attacks against Georgia as an example, and determine the strategic impact of existent and non-existent cyber warfare rules for the United States.

The United States along with a host of other information age countries are becoming increasingly more vulnerable to belligerent activities in cyberspace. In 2007, Sami Saydjari, President and Founder of the nonprofit Cyber Defense Agency, testified before the House Subcommittee on Emerging Threats, Cybersecurity and Science and Technology and described a digital “Hurricane Katrina” for the entire country following a cyber attack.[2] He stated the cyber attackers are a well-funded cadre biding their time against would-be victims increasingly dependent on integrated information systems.[3] Others have warned of a “digital Pearl Harbor” where U.S. electrical grids, air traffic control systems or nuclear power plants are infiltrated and disrupted or destroyed.[4] During World-Wide Threat Hearings in early 2009, Admiral Blair, Director of National Intelligence stated "our information infrastructure is… becoming vulnerable to catastrophic disruption in a way that the old analog decentralized systems were not. Cyber systems are being target(ed) for exploitation and potential(ly) for disruption or destruction by a growing array of both state and non-state actors."[5]

Others argue the United States is not as vulnerable as these experts suggest. According to Jim Lewis, Director and Senior Fellow at the Technology and Public Policy Program at the Center for Strategic and International Studies (CSIS) it is difficult to cause mass casualties in this manner against a country, like the United States, which is reliant on many different infrastructures.[6] The cyber attacks against Estonia in 2007 and Georgia in 2008, while conducted on a large scale caused little tangible damage[7] according to an anonymous writer in the Economist.

Admiral Blair further testified on the need to build U.S. defenses against nations like Russia and China which "can disrupt elements of the U.S. information infrastructure. We must take proactive measure(s) to detect and prevent intrusions before they do significant damage. We must recognize that cyber defense is not a one-time fix. It requires continual involvement in hardware, in software, in cyber defenses, and in personnel."[8] More specifically, Admiral Blair cited the ability of an adversary to "doctor" computer chips associated with communications and military equipment. Adjustments to the chips, which are embedded with virtually all equipment operating system software, would permit the adversary to disrupt or destroy the targeted system.[9]

These vulnerabilities incur a cost to the United States. “The compromise of our nation through this invisible battleground has cost billions of dollars from our economy in terms of theft of both intellectual property and the destruction of information systems”[10] according to Michael Assante, Chief Security Officer, North American Electric Reliability Corporation before the House Subcommittee on Emerging Threats, Cybersecurity and Science and Technology. General Chilton, Commander United States Strategic Command (USSTRATCOM)—the combatant command assigned the cyber defense mission—also cited the vulnerabilities our nation faces “…we’re seeing a lot of… intrusions into our military networks” for the purposes of “exploitation or espionage.”[11]

In addition to presenting vulnerabilities to the United States, cyberspace and actions in that domain continue to become more complex. According to Assante, “cyber weapons are often not flagged and their true origins are unknown and therefore un-attributable, and most importantly, they have been largely successful in evading the instruments available to prevent and deter it.”[12] General Chilton described the actions against Estonia and Georgia as “coordinated cyber attacks that were aimed at the computer infrastructure of those countries or those operations and tried to take away their ability to use their computer networks to conduct operations.”[13] In contrast to other domains of warfare, “in cyberspace, enemy combatants can pry, spy, implant, extract and dismantle more quickly and more secretly”[14] according to Amber Corrin, SIGNAL’s Assistant Editor.

Many experts believe the volume of belligerent acts will continue to grow exponentially. According to a Defensetech.org online posting by Kevin Coleman in January 2010, “cyber attack volume(s will) escalate dramatically.” In support of this forecast, he further stated “malware (malicious software) grew (in 2009) at the highest rate in 20 years. Multiple security reports showed that more than 25 million new strains of malware were identified” with predictions of this continued trend.[15]

Trends also suggest an increasing variety of cyberspace belligerents, possibly an increase in the numbers as well. The types of actors can be characterized in several ways. According to General Chilton “our threats actually span the spectrum from the… bored teenage hacker… to the criminal element… to the organized nation-state.”[16] Admiral Blair in testimony before the Senate Select Committee on Intelligence affirmed for Senator Mikulski that high-tech states, organized crime groups and individual hackers for hire “could pose threats to our critical infrastructure.”[17] Admiral Blair further testified that the main threats to the United States come from these groups of actors (i.e. hackers, organized crime and state-sponsored) in Russia and China and that the bulk of cyber intrusions against the United States come from Internet Protocol (IP) addresses in China and Russia.[18]

In her presiding remarks before the Subcommittee on Emerging Threats, Cybersecurity and Science and Technology, Representative Yvette Clarke cited a Wall Street Journal article from April 2009 stating cyber intruders from Russia and China have already penetrated the electric power grid and were “positioned to activate malicious code that could destroy portions of the grid.”[19] Further testimony elaborated that China’s cyber warfare doctrine seeks “global electronic dominance by 2050, to include the capability to disrupt financial markets, military and civilian communications capabilities, and the electric grid prior to the initiation of a traditional military operation.”[20]

North Korea and Iran were also cited as countries having offensive cyber attack capabilities in addition to Russia and China.[21]

Given the vulnerability to the United States—not to mention her allies—the complexity of cyberspace, increasing volume of belligerent acts and wide variety of legitimate and belligerent actors, the cyberspace domain calls for rules to establish accepted norms and govern activity. The primary conclusion from Major Arie Schaap's 2009 article "Cyber Warfare Operations: Development and Use Under International Law" in the Air Force Law Review eloquently concluded "as states begin to focus their energies on developing doctrine and weapons for conducting cyber warfare operations, it is essential that we move beyond just the realization that cyberspace is an important new battleground for conducting warfare operations and recognize the need to come to an understanding of what rules regulate this new battlefield."[22] Two year earlier, Duncan Hollis discussed the notion of "e-war rules of engagement" where "nations could agree to waive sovereignty and permit a direct response to cyber attacks (e.g. Rules of Cyberwar)."[23] Both of these studies justified the need for cyber warfare rules.

What are U.S. strategic objectives in cyberspace? According to Colonel Jeffrey Caton, a professor at the U.S. Army War College, they are "to prevent cyber attacks, reduce national vulnerability to cyber attacks, and minimize damage and recovery time should attacks occur."[24] Two of the five national priorities for the 2003 cyberspace strategy were to secure governments' (not just the United States) cyberspace and international cooperation[25] with the realization that the U.S. domain is only as secure as the weakest domain with which it is connected.

As can be seen, there are many variables to analyzing the U.S. approach toward international collaboration in cyberspace. In addition to the topics already presented, providing definitions will help provide a common understanding of the terms. For example, how is a cyber attack different from exploitation, and counter-attack? The existing international rules to include treaties and laws will be reviewed. The cyber attacks against Georgia will be examined for relevance to the topic of international rules. These will be used as examples for determining the strategic impact to the United States. Finally, analytic conclusions will be drawn from the work along with recommendations for the future.

Definitions

The cyber domain (e.g. cyberspace) is a complex system of systems that literally spans the globe and extends into space. In a virtual sense it makes every state and non-state actor a next-door neighbor and yet does not recognize the rules of sovereignty (e.g. national borders) or private property in many ways. Transactions in cyberspace occur at a velocity of the speed of light, an almost infinite volume, and with a variety that changes almost daily. The three V's (i.e. volume, velocity, and variety) of cyberspace further complicate efforts to codify international rules and U.S. government policy. The October 2008 update to Joint Publication 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."[26]

Actions in cyberspace can be categorized three ways; legitimate (i.e. lawful and not considered illegitimate), criminal (e.g. unlawful—a law cites the action as criminal), and illegitimate (i.e. considered malicious by a state or non-state actor, but no law exists to cite as criminal). Both legitimate and criminal actions in cyberspace are reasonably understood. The international community (IC) has little disagreement once actions can be categorized as such. The contention among parties comes with illegitimate actions in cyberspace.

A further delineation of actions in cyberspace is helpful when considering U.S. and other state or non-state actor offensive actions. While all things cyber are not computer and vice versa, computer network operations (CNO), specifically computer network attack (CNA) and computer network exploitation (CNE) [27] are cyberspace activities likely considered illegitimate and possibly criminal to the IC. At this point it is helpful to step back and review the United Nations' (UN) point of view and look for analogies in cyberspace.

Article 1 of the UN Charter cites its purpose "to maintain international peace and security, and to that end: to take effective collective measures for the prevention and removal of threats to the peace, and for the suppression of *acts of aggression* or other breaches of the peace…"[28] The article further defines aggression as "the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the (UN)."[29] Arguably, illegitimate actions in cyberspace (i.e. CNA and CNE) could fit the definition of an act of aggression according to Article 1 of the UN. The debatable point is likely the reference to "armed force."

Article 2 of the UN Charter cites "all members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any manner inconsistent with the Purposes of the United Nations."[30] Illegitimate activities in cyberspace arguably fit this definition, however, the debate again rests along the reference to the ""use of force." War as defined by the UN Article 2(4) of the UN Charter and UN General Assembly Resolution 3314 is "the use of armed force by a state against the sovereignty, territorial integrity, or political independence of another state."[31] The reference excludes non-state actors, however.

> According to Article 3 of the UN Charter
>
> "any of the following acts, regardless of a declaration of war, shall, subject to and in accordance with the provision of article 2, qualify as an act of aggression:
>
> (a) The invasion or attack by the armed forces of a State or of the territory of another State, or any military occupation, however temporary, resulting from such invasion or attack, or any annexation by the use of force of the territory of another State or part thereof;
>
> (b) bombardment by the armed forces of a State against the territory of another State or the use of any weapons by a State against the territory of another State; or
>
> (c) the blockade of the ports or coast of a State by the armed forces of another State."[32]

Again, these definitions limit belligerents to state actors. While there may have been some doubt whether an illegitimate cyberspace action was an "act of aggression," Article 3 provides examples of situations, whether in the cyber domain or not, where illegitimate actions in cyberspace (i.e. CNA and CNE) are "acts of aggression." Cyber warfare like denial of service attacks that "block" a host nation's servers may be regarded as a "blockade." Similarly, installation of malware on a host nation's telecommunications infrastructure may be regarded as an "invasion."

How are acts of war and acts of aggression defined? The United Nations has defined “acts of aggression” which could be interpreted an act of war. There is potentially a slight difference between the two in that an act of war suggests a measure of response from the victim, while an act of aggression merely states an event rather than a scale of an event reaching the level of war. Martin Libicki of RAND Corporation defined acts of war along three axes: universally, multilaterally, and unilaterally.[33] Basically, a universally declared act of war is one where all states believe an event to be an act of war. Those along the multilateral axis suggests more than one nation declares the event as an act or war, and the unilateral axis provides that one state declares an event an act of war. While counter-actions can be debated, ultimately, it will be in the interest of the victimized state to declare an event an act of war. Having agreement from other nations (i.e. multilateral or universal) will provide improved justification (i.e. the moral high ground) for counter actions and potentially increased levels of support from other nations, however.

Rules for Cyber Warfare

In 2007, Duncan Hollis asked the question about rules for cyberwar suggesting there were limited regulations that prescribed how state and non-state actors should fight in cyberspace.[34] In 2009, Libicki characterized deterrence and war in the cyberspace environment (e.g. cyber warfare) as “its own medium with its own rules.”[35] He further elaborated on the complexities for establishing rules.

> Cyber attacks, for instance, are enabled not through the generation of force but by the exploitation of the enemy’s vulnerabilities. Permanent effects are hard to produce. The medium is fraught with ambiguities about who attacked and why, about what they achieved and whether they can do so again.[36]

Webster's New World College Dictionary defines rule as "authoritative regulation for action or established practice that serves as a guide."[37] Using this as a contemporary framework for discussion, there are potentially several categories of rules for fighting in cyberspace. For example, existing treaties, conventions (e.g. Geneva Convention) and laws (e.g. Law of Armed Conflict) could articulate accepted and non-accepted rules for performing cyber warfare. Additionally, prescribed rules of engagement (ROE) and collaborative operations can help define levels of acceptance for cyber warfare. According to Hollis, "war has entered the Information Age, and it's time for the international law to get a needed update,"[38] but laws may be one of several ways to provide the requisite governance. Examining existing rules (i.e. laws, treaties, conventions, ROEs and collaborative operations) may help identify and potentially codify acceptable boundaries for cyber warfare.

In 1960, the UN Security Council concluded that the United States U-2 over-flight of the Soviet Union's sovereign airspace did not constitute an unlawful use of force in accordance with Article 2(4) of the UN Charter.[39] Applying this scenario to the cyber domain suggests that computer network exploitation, a form of cyberspace intelligence, surveillance and reconnaissance (ISR), might also not meet the threshold of an unlawful use of force in accordance with Article 2(4) of the UN Charter.

The Geneva Conventions and Council of Europe Convention on Cybercrime (CoECC) may have applicability to cyber warfare. The United States joined the CoECC which went into effect in January 2007. [40] The convention, which is the only legally binding multilateral instrument for computer-related crime, was designed to protect citizens from hacking, organized crime and terrorism.[41] The CoECC has several purposes including “a common criminal policy aimed at the protection of society against cybercrime, inter alia, by adopting appropriate legislation and fostering international co-operation.”[42] This objective recognizes “the risk that computer networks and electronic information may also be used for committing criminal offenses and that evidence relating to such offenses may be stored and transferred by these networks.”[43] The protection of society and use of computer networks to commit crimes have applicability to cyber warfare. Chapter II, Substantive Criminal Law, Title 1, Offenses against the confidentiality, integrity and availability of computer data and systems, of the CoECC identifies three articles which have direct applicability to cyber warfare.

> Article 2 – Illegal access; Each party shall adopt such legislative and other measures as may be necessary to establish as criminal offenses under its domestic law, when committed intentionally, the *access to the whole or any part of a computer system without right.*
>
> Article 4 – Data interference; Each party shall adopt such legislative and other measures as may be necessary to establish as criminal offenses under its domestic law, when committed intentionally, the *damaging, deletion, deterioration, alteration or suppression of computer data without right.*
>
> Article 5 – System interference; Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offenses under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by *inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.*”[44]

Each of these articles specifies criteria including illegal access, data interference, and system interference which are reasonably considered first order consequences of cyber warfare. Even acts of CNE can be determined to fit this criterion. Of course, attribution of the CNE will also need to be determined before pursuing criminal charges—the belligerent actor will need to be identified.

While not providing specific language relating to cyber warfare, Protocol 1 to the Geneva Conventions also provides rules through analogy. Article 51 “protects civilian populations and defines unlawfully indiscriminate attacks as: 1) not directed at a specific military objective; 2) which cannot be directed to a specific military objective; or 3) which cannot be limited as required by this protocol.”[45] The language suggests CNA performed against specific military objectives would be considered as lawful action, while events against non-military objectives as unlawful or criminal. The subjectivity arises when non-military resources are attacked which are determined by the belligerent as military associated. In 2008, Stephen Korns and Joshua Kastenberg judged that CNA rose to the level of an armed attack in accordance with Article 51.[46] Air Force Major Arie Schaap further assessed Korns and Kastenberg’s interpretations in the Air Force Law Review that CNA which causes physical damage to a sovereign nation’s assets could meet the threshold of an armed attack[47] in accordance with Article 51.

While the United States is involved in no international treaties directly tied with cyber warfare, it is worth highlighting recent dialogue on the subject. As recent as June 2009, an anonymous Department of State (DoS) official noted that the United States and Russia disagreed on the implementation of a cyberspace treaty.[48] According to the DoS official, Russia favored a treaty along the lines of those implemented for the production of chemical weapons, while the US argued a treaty was unnecessary. The focus should be toward international law enforcement cooperation which would increase security against cyber crime and thus extend into military campaigns, according to the U.S. official. Russia, on the other hand, suggested without a treaty, a cyber arms race would begin. Earlier that same year, Vladislav P. Sherstyuk, a Deputy Secretary of the

Russian Security Council described their bottom line position which banned a state actor from secretly embedding malicious codes or circuitry in computer systems that could be later activated in the event of war.[49] Other proposals include applying humanitarian laws against the application against noncombatants and banning deception operations; however, U.S. officials argued these proposals would be ineffective given the difficulty in ascertaining attribution of an attack from a state, a proxy, or an independently acting non-state actor.[50]

During the DNI's testimony before the Senate Select Committee on Intelligence in early 2009, Senator Feinstein pressed the issue of developing cyber treaties in order to help hold belligerents accountable for their actions.

> …and yet it seems to me that there is—other than the intelligence world, there is a very real policy gap out there where the diplomatic world needs to step in. And when things happen, countries need to get demarched, as opposed to keeping all of this under raps so that all one does is build one's own technology to get closer and closer to cyber warfare… I am interested in holding countries responsible for the behavior of their entities. And I think it's a much more responsible course in the long-run if you have American policymakers heavily engaged with their counterparts in other countries, driving toward international treaties and agreements which prevent cyber intrusions which could result one day, if left unaddressed, a cyber war?[51]

Although Admiral Blair acknowledged the Senator's remarks, he diverted the language from "international treaties or agreements" to a "code of conduct," language—presumably—less binding. Admiral Blair's exact response was "I agree that if we could develop some sort of a *code of conduct* an approach that the major nations agreed on to cyber space… And it (code of conduct) would apply some regulation to these (cyber) activities more at the source than having to deal with it the way we do now."[52]

Presently, no international laws specifically address the issue of cyber warfare; however, the Law of Armed Conflict (LOAC) can be applied to determine whether cyber warfare (i.e. attack) is criminal as recognized by the international community. In 2009, Major Schaap concluded that cyber attack is generally viewed as acceptable (e.g. non-criminal) in accordance with the LOAC principles of military necessity, distinction, proportionality, unnecessary suffering, perfidy, and neutrality.[53] Of course each principle would be assessed individually given the relative circumstances of the belligerent cyber event.

For example, the "international law community appears to be coalescing around the general concept that use of the Internet to conduct cross-border cyber attacks violates the principle of neutrality."[54] According to Jeffrey Kelsey, for a state actor to remain neutral in a cyber conflict, that nation must refrain from assisting either side of the conflict, not originate the attack, and must take action to prevent a cyber attack from transiting its cyber domain[55]—a difficult task to say the least. And, a state that takes no action against actors using its territory for cyber attack risks losing its neutral status.[56] Lawrence Greenberg went further to suggest "a belligerent (actor) violates neutrality law when it launches a cyber attack that crosses the Internet nodes of a neutral state."[57] The International Telecommunications Union (ITU) took a tougher position and cited that "cyber attacks could be treated as acts of war and be brought within the scope of arms control or the Law of Armed Conflict."[58]

As recent as 2007, Duncan Hollis argued for a new legal framework for cyberspace; an international law for information operations (ILIO). "Existing rules have little to say about the non-state actors that will be at the center of future conflicts…the technology is mostly inexpensive, easy-to-use, and capable of deployment from virtually anywhere."[59] Hollis identified four substantial flaws toward the existing "law by analogy" approach for cyberspace. First, there are translation problems extending existing rules to cyberspace with regard to armed conflict. Second, the majority of language extending existing rules to cyberspace focus on state versus state conflict, when recent history suggests irregular warfare to be more popular in cyberspace. Third, absent *lex specialis,*[60] conflict in cyberspace applies to multiple and overlapping legal regimes. Fourth, existing rules focus on restrictions for cyber warfare rather than include the potential benefits like limited physical and collateral damage, for example.[61] At present, no international law exists nor pressure toward its establishment despite Hollis' assessment that "devising a new legal framework—may offer the most effective response to the challenges of regulating cyberspace conflicts."[62]

With respect to the 2008 cyber attacks against Georgia, Hollis' assertions received support from the NATO-accredited Cooperative Cyber Defense Center of Excellence in Tallinn, Estonia. The center concluded "it is highly problematic to apply the Law of Armed Conflict to the Georgian cyber attacks—the objective facts of the case are too vague to meet the necessary criteria of both state involvement and gravity of effect."[63] Meanwhile, the debate continues.

Rules of engagement, while not internationally formed or accepted treaties, laws or conventions, provide self-policing, unilateral guidelines for operation in cyberspace—or within other domains—and if made public, share those guidelines with other state and non-state actors. Whether a state restricts its actions to the ROEs is another matter, of course. In 2002, the U.S. President signed the National Security Presidential Directive (NSPD) 16, "which called for a national policy on the rules of engagement for using cyber warfare as a weapon."[64] The NSPD also notes the U.S. government reserves the right to respond as necessary if the U.S. comes under cyber attack and in that response could employ cyber weapons.[65]

In January 2008, the President published two classified directives, the NSPD-54, and Homeland Security Policy Directive (HSPD)-23 for Cyber Security and Monitoring.[66] These classified directives are outside the scope of this paper, but it is likely ROEs for cyber warfare are articulated in one or both of these documents. The drawback is; however, that the classified nature of the texts restricts the ability to share these ROEs with the international community beyond those states with which the U.S. has security cooperation agreements.

Like ROEs, cooperative operations provide activities acceptable in a multilateral fashion, so arguably may provide a step of clarity beyond the mere publishing of ROEs. Over time, operations in cyberspace provide accepted examples from which rules can be formed, whether formally (i.e. laws, conventions, treaties) or informally.

According to John Lynch, Deputy Chief for Computer Crime at the Department of Justice (DOJ), the DOJ has been working with Romanian law enforcement officials to combat the threat of organized crime groups stealing hundreds of millions of dollars from the U.S. economy.[67] In April 2008, the U.S. Attorney General announced the Law Enforcement Strategy to Combat International Organized Crime, citing “cybercrime operations efforts with foreign law enforcement agencies (which) specifically addresses the threats these groups pose in cyberspace.”[68] The strategy builds on DOJ’s cooperation with the G8, Interpol and the Council of Europe, through which operations with other foreign nations is achieved. Given that suspected state-sponsored cyber crime is pushed to the DOJ as a law enforcement issue, it is fortuitous that existing statutes permit law enforcement officials to request search warrants in order to obtain evidence from service providers, for example. While changes to U.S. Codes for computer crimes are enacted—some as recently as August 2008—these statutes are purposefully kept broad to mitigate the slowness of the process to build laws associated with the velocity and variety of cyberspace.[69]

Cyber crimes are just one element of the triad of cyberspace events (i.e. legitimate, criminal, and illegitimate). In 2008, allies of the North American Treaty Organization (NATO) signed an agreement to fund a center in Tallinn, Estonia, to boost defenses against cyber attacks. Defense chiefs from Estonia, Latvia, Lithuania, Germany, Italy, Spain and Slovakia signed an agreement to staff and fund the center, while the U.S., noticeably joined the project only as an observer.[70] In October 2008, China reportedly started engaging with regional states through the Shanghai Cooperation Organization to help shape the legal framework and rules of engagement for cyber warfare.[71] The Obama administration is now studying how laws of war and international obligations need to be reworked to account for cyber attacks.[72]

Cyber Attacks on Georgia

In the summer of 2008, Georgia came under cyber attack from what was thought to be Russia. While the debate continues whether the Russian government originated, sponsored, or served as a neutral party in the attack, the events as they continue to be analyzed provide a case study for framing the debate on international rules for cyber warfare. Before these series of events are analyzed; however, it is worth providing context for the attacks against Georgia by listing other recent cyber warfare events leading up to and beyond these attacks.

> April to May 2007: Web sites of Estonia’s parliament, banks, ministries, newspapers and broadcasters were shut down by hackers. Estonia accused Russia of conducting a cyber war in retaliation for a decision to move a Soviet-era war memorial.[73]
>
> June-July 2008: Hundreds of government and corporate Web sites in Lithuania were hacked, and some were covered in digital Soviet-era graffiti, implicating Russian nationalist hackers.[74]
>
> *August 2008: Cyber attackers hijacked government and commercial Web sites in Georgia during a military conflict with Russia.*[75]
>
> January 2009: Attacks shut down at least two of Kyrgyzstan’s four Internet service providers during political squabbling among Russia, the ruling Kyrgyzstan party and an opposition party.[76]
>
> April 2009: An attack on Kazakhstan shut down a popular news Web site.[77]
>
> July 2009: Servers in South Korea and the United States sustained a series of attacks reportedly by North Korea.[78]

The summer of 2008 cyber attacks against Georgia, which were performed over several weeks, have still not been pinned to the Russian government; however, the series of events suggest that Russian government involvement was reasonable to affirm. The conventional ground war, which commenced on 8 August, lasted five days, left hundreds of people dead, crushed the Georgian army, and left Abkhazia and South Ossetia—Georgian territory—in Russian occupation. And, the non-conventional cyber attacks disrupted Georgian communications by disabling 20 web sites for more than a week.[79]

Three weeks prior to the ground war, on 19 July, unidentified entities used a U.S.-based, commercial IP address to launch a distributed denial of service attack (DDoS) against the Georgian President’s web site.[80] The malware was identified as a “MachBot” DDoS controller written in Russian and commonly used by Russian hackers.[81]

During the evening of 7 August, one day before the Russian ground invasion, Georgian governmental web sites came under further cyber attack.[82] On 8 August, a larger number of Georgian governmental, bank (National Bank of Georgia)[83] and media web sites were attacked by a larger wave of DDoS attacks[84] and defaced.[85] The owner of TSHost, a U.S.-incorporated company, who happened to be visiting Georgia at the time, offered to help reconstitute Georgian internet capabilities. One day later, the Georgian government transferred key web sites, including those of the President and Ministry of Defense, two of the attacked sites, to servers in the United States.[86] Other servers in Poland and Estonia were also used to host more key Georgian Internet assets.[87] By 10 August, most of Georgian governmental web sites were shut down by the apparent DDoS attacks[88] and the "Georgian government found itself cyber-locked, barely able to communicate on the Internet."[89]

Post event analysis of the cyber attacks revealed several interesting results. The findings of Project Grey Goose—a voluntary compilation of more than 100 Internet security members from organizations as diverse as Microsoft, Oracle, the Defense Intelligence Agency (DIA), SAIC, the Department of Homeland Security (DHS) and Lexis-Nexus—showed no direct link with the Russian government; however the assault was coordinated through a Russian on-line forum prepped with target lists and Georgian web site vulnerabilities before the conventional war started. The on-line forum *Xaker.ru* encouraged pro-Russian hackers to join a private, password-protected forum called *StopGeorgia.ru.* Within this forum, members were provided targets lists of Georgian web sites with associated vulnerabilities, exploitation methods, and the procedures to render them inaccessible. "The level of advance preparation and reconnaissance strongly suggests that Russian hackers were primed for the assault by officials within the Russian government and or military" according to Jeff Carr, a Project Grey Goose principle investigator.[90] The investigation also revealed contradictory evidence to a DDoS attack. According to Billy Rios, a Grey Goose investigator, the "benchmark" feature of MySQL (a software suite used to manage back end databases) was manipulated to send bogus database queries which in effect overwhelmed the web servers, making the web sites they hosted inaccessible. Previously, investigations suggested an army of disparate computers querying the web site caused the servers to crash. Rios further elaborated that the event "indicate(d) that all the information from the attacked systems was most likely already compromised and pilfered before the injection point was posted"[91] showing premeditation and coordination, and possible Russian government collusion.

In contrast to manipulating Microsoft Corporation MySQL software, the U.S. Cyber Consequences Unit (CCU) reported that the hackers coordinated their "botnet" attacks against Georgia on Twitter and Facebook, two U.S.-based social networking sites.[92] The CCU identified the source of the "botnet" (ordinary computers hijacked by viruses to perform such attacks without their owner's knowledge[93]) attacks to 10 web sites registered in Russia and Turkey, which were previously used by Russian cyber crime groups.[94] In typical DDoS fashion, the commandeered computers attempted to access the targeted web sites simultaneously, thus rendering them inaccessible. Once the attacks occurred, would-be-attackers started collaborating on the forums--including Twitter and Facebook—exchanging attack codes, sharing target lists and recruiting others to join.[95]

According to the CCU Chief Technical Officer, John Bumgarner, “taking out communications systems at the onset of an attack is standard military practice.”[96] The denial-of-service attacks were accomplished with precision and discipline, according to Scott Borg, co-writer of the CCU report. While Russian military direction is still uncertain, the military and the attackers exchanged a significant amount of information on message boards.[97]

While the target and intent of the cyber attacks against Georgia were clear, attribution still remains elusive. Shortly after the attack, the Los Angeles Times reported no clear Russian military involvement, only that the originating Russian servers were associated with organized crime groups and the perpetrators may have been nationalists.[98] A week after this report, another news agency pondered official Russian involvement or that of “rogue hackers supportive of the South Ossetian cause.”[99] Two seasons later, other labels of “cyber criminal, cyber citizen-mobs, and self-styled cyber militia”[100] were used to characterize the attackers. No matter what labels were used, there remains a “growing trend of cyber conflict between nations and ad-hoc assemblages.”[101]

Despite the lack of evidence against Russian government direction of the cyber attacks against Georgia, the timing of the main thrust—just hours after the conventional war began—suggests the Russian government may have coordinated with the cyber attackers.[102] Despite the accusations, Yevgeniy Khorishko, a Russian Embassy spokesman in Washington stated “Russian officials and the Russian military had nothing to do with the cyber attacks on the Georgian Web sites.”[103]

While the attacks were occurring and afterward, the Georgian government protested, but to no avail. There was no formal avenue to appeal—the existing treaties and defense pacts obligate no parties to perform a cyber or reciprocal counter-attack.

Strategic Impact to the United States

First and foremost, the cyber attacks against Georgia represent a strategic challenge to U.S. national security. In May 2009, President Obama characterized the cyber threat as "one of the most serious economic and national-security challenges we face as a nation."[104] According to William Lynn, Deputy Secretary of Defense (DepSecDef) the "cyber threat to the Department of Defense represents an unprecedented challenge to our national security by virtue of its source, its speed and its scope."[105] The DepSecDef further elaborated in the June 2009 speech that criminal groups and individual hackers were building global capabilities and then selling their services to the highest bidder, becoming in effect "cyber mercenaries."[106] In May 2009, several thousand U.S. military computers became infected with malware, intentionally placed by an adversary. The event, characterized as an "attack," forced military personnel to discontinue their use of external memory devices and thumb drives—a drastic change from existing protocols.

The anonymity and efficiency of cyber warfare help promote its use. According to Brigadier General Mark Schissler, USAF Director for Cyber Operations, "the ability to attack an organization or even a nation surreptitiously is precisely what makes cyber warfare so dangerous and attractive."[107] General Schissler continued to suggest the exponential increase in cyber warfare activity will increasingly make it more difficult to secure U.S. networks. "Cyberspace is one of the most asymmetric approaches to warfare" according to Schissler, who added, military officers include this type of warfare in defensive and offensive plans.[108]

According to some, the United States critical infrastructure is increasingly becoming vulnerable to attack despite defense expenditures. The DepSecDef noted that DoD is spending billions of dollars annually to proactively protect and defend its networks, but the U.S. infrastructure remains vulnerable to attack. Representative Yvette Clarke stated that "because of expanding digital and computerized connections, our electric grid is now, more than ever, vulnerable to cyber and physical attacks."[109] Nation state and rogue nation adversaries of the United States can attack the critical infrastructure from remote locations with less cost than a conventional campaign and anonymously, cited Representative Dan Lundgren during the same Subcommittee on Emerging Threats, Cyber Security and Science and Technology hearings in July 2009.[110] But the risk of cyber attack is not limited to the government alone.

Cyber defenses need to be bolstered in the commercial and private sectors as well. McAfee Incorporated published a cyber security report in November 2009 which noted that a cyber conflict between nation-states would very likely cause collateral damage to private sector resources.[111] General Schissler earlier insisted that government, academia and businesses all share the same risks, especially if they are "unwilling to cooperate and collaborate" on cyber issues. He further stated the need to be creative in this cooperation.[112] In July 2009, General Robert Kehler, Commander Air Force Space Command, characterized cyber warfare as that which occurs in an urban environment citing the variety and density of legitimate and illegitimate actors. Critical to an effective U.S. approach is to organize with the “appropriate authorities to behave in cyberspace the right way” according to General Kehler. [113]

To mitigate the risk of “a growing array of cyber threats and vulnerabilities” [114], in June 2009, the Secretary of Defense created U.S. Cyber Command (USCYBERCOM) as a subordinate unified command under USSTRATCOM. Mr. Gates stated “to address this risk effectively and to secure freedom of action in cyberspace, the DoD requires a command that possesses the required technical capability and remains focused on the integration of cyberspace operations.” He further elaborated on the need to collaborate across departments and nations. “(T)his command must be capable of synchronizing warfighting effects across the global security environment as well as providing support to civil authorities and international partners”[115] according to Gates.

While the United States spends vast amounts of money on defensive measures, other countries including Russia and China continue to develop their offensive cyber capabilities. Russia’s armed forces in collaboration with academia and the information technology sector have developed a cyber warfare doctrine[116] with much of the attention focused on offensive cyber warfare capabilities. [117] According to the doctrine, Russia’s cyber arm is to be employed as a force multiplier, in effect serving to compliment other forms of military power, including conventional and irregular warfare. The primary target of the cyber offensive is the opponent’s critical infrastructure including the financial market, telecommunications networks, both military and civilian, all of which is to be carried out prior to initiation of conventional force on force warfare.[118] According to the U.S. Cyber Consequences Unit, someone on the Russian side exercised “considerable restraint” by not inflicting physical damage to Georgia’s critical infrastructure through its use of cyber weapons[119] or arguably, the Russian military did not lead the attack. As previously stated China's cyber warfare doctrine seeks "global electronic dominance by 2050, to include the capability to disrupt financial markets, military and civilian communications capabilities, and the electric grid prior to the initiation of a traditional military operation."[120]

Mere words will not create the necessary change in order to deal with this strategic challenge. The U.S. will need to drastically change its culture in order to leverage capabilities and avoid catastrophes in cyber space. According to the DepSecDef, the DoD needs to "respond rapidly, at network speed, before the networks could become compromised and ongoing operations or the lives of our military are threatened."[121] The "Pentagon must ultimately change its culture"[122] in order to collaborate across the military, the rest of government, and commercial sectors—a necessity to ascertain and respond to any given threat.[123] Arguably, given the global interconnectedness of the telecommunications infrastructure—the medium through which most attacks will occur—this collaboration should extend beyond the U.S. borders with other nation states and the world's stakeholder companies.

As with the seas, the Internet and the global telecommunications infrastructure has become part of the global commons. The global commons have long been recognized as a vital U.S. interest and therefore have been improved, maintained and policed by U.S. resources. According to Richard Mereand of the National Security Watch, "the United States, as a major beneficiary of all that cyberspace has to offer, should take the lead—vigorously and without delay" in "maintaining a free and open Internet."[124] But, maintenance of the global commons is not entirely up to the United

States. International cooperative efforts, even those short of official agreements are needed to ensure a holistic approach is achieved. In a summer 2009 interview with the National Public Radio, General Chilton, USSTRATCOM Commander, suggested a need to improve the military dialogue with other nations in order to deal with international threats. “Threats in cyberspace are being taken seriously by all governments around the world… we already [do] have dialogues with… Australia, the United Kingdom, (and) France,”[125] stated General Chilton. The NATO-generated Cooperative Cyber Defense Center of Excellence, headquartered in Tallinn, Estonia, could serve as an example of solidifying roles and responsibilities across national boundaries for securing the global infrastructure.[126]

Preventing other nation or non-nation state actors from disrupting the global cyberspace domain would be accomplished in a variety of ways; however, deterrence is likely not one. During the Cold War, nuclear deterrence based on mutually assured destruction had value, but in a domain where it is difficult at best to determine the source of the attack, eliminating a viable retaliation defeats a necessary element for successful deterrence.[127] William Lynn, DepSecDef, reiterated the difficulty in attribution as it relates to deterrence. He said “deterrence is predicated on the assumption that you know the identity of your adversary, but that is rarely the case in cyberspace.” [128]

Absent deterrence, internationally recognized rules would help prevent wrongly perceived actions during cyber warfare. Lynn stated how the DoD defines the “rules of the road” will help “ensure our cyber security in the decades ahead.”[129] While no international laws exist that prohibit cyber warfare operations, the application of cyber warfare has legal limitations. Under the LOAC cyber warfare operations have the potential of constituting an illegal use of force. For example, the principle of neutrality presents a scenario where ambiguities lie. The U.S. incorporated company TSHost inadvertently broke the United States' position of neutrality in its actions to transfer Georgian governmental web servers to those in the U.S. Further complicating the matter, the U.S. declared no official stance in the Georgia-Russian conflict. If the United States "linked its cyber support to its overall humanitarian aid effort it would have signaled that US Internet support to Georgia was for humanitarian purposes, and therefore not in violation of any Hague Conventions."[130] The position of neutrality is also potentially broken by an aggressor who uses a third party's cyber domain to launch or otherwise enable an attack against an adversary. A third party who inadvertently allows a belligerent to use its cyber domain to launch or otherwise enable an attack potentially breaks its position of neutrality as well. A void of international rules up to and immediately following a cyber "Pearl Harbor" will cause the creation of overly restrictive and reactionary regulations rather than ones that are purposefully and unemotionally developed with more rational minds.[131]

Part of the dilemma with current international laws is that the line between cyber crime and cyber war is blurred. According to the McAfee cyber security report, the recent attacks against Georgia showed that "nation-states have already demonstrated that they are willing to tolerate, encourage or even direct criminal organizations and private citizens to attack enemy targets." Were these acts against Georgia's Internet resources an act of war or a crime?[132]

It may be beneficial for the U.S. government to "clearly demarcate its cyber relationship vis-à-vis cyber belligerents" given that "current international laws are ambiguous and ill-suited to define contemporary cyber rules of engagement." [133] Even though the U.S. government did not officially sanction the actions of TSHost and Google to support Georgia during the second wave of DDoS attacks--internationally recognized as cyber war—Russia and other parties could have viewed the U.S. companies' actions as offensive and launched attacks against those portions of the U.S. commercial infrastructure.[134] Although, shortly after the attacks the Pentagon refused to take a position whether the cyber attacks against Georgia were acts of war.[135] In light of these risks and ambiguities, U.S. policymakers should consider "invigorating multinational efforts to clarify the terms and conditions of cyber neutrality" and "the wisdom of continuing a cyber strategy that appears to rely heavily on the loosely controlled actions of private industry."[136]

An arms control treaty would be another example of internationally recognized rules for cyberspace; however it appears the U.S. was reluctant to move toward that end. Shortly before the cyber attacks on Georgia, the Russian government "called for a ban on cyber attacks as part of arms control deals, but the U.S. government refused" [137] to take part in any discussions. In the fall of 2009, a Russian delegation led by General Vladislav Sherstyuk met with U.S. DoS, DoD, DHS, and National Security Council officials to "limit the development and military use of cyber weapons," [138] but the results of the meetings were not available. Some argue that cyber arms control treaties would only cause the weapons development to move underground causing greater uncertainty among adversaries.[139] Certainly, developing treaties is complicated. The executive branch leads foreign policy development, but the Congress regulates foreign commerce and the Senate must agree to any treaties the U.S. may consider,[140] so the development just within the U.S. would be complicated to say the least.

Short of developing treaties for cyberspace, countries could form alliances or agreements to help guide warfare. The DepSecDef stated that cooperation internationally is logically needed in order to defend against cyber attacks, the majority of which originate overseas. Additionally confronting the complexities of national sovereignty and international law as it relates to cyber warfare is not something one country could tackle, according to Lynn. [141] In November 2009, a Russian delegation met with U.S. government officials on the topic of cyberspace. One of the two topics General Sherstyuk discussed with DHS, DoD, DoS and NSC officials was international cooperation for investigating cyber attacks. Given the broad publicity of recent cyber attacks, concern is growing that terrorists will begin to use this form of warfare more frequently.[142]

While it appears the U.S. government remains reluctant to enter into any cyber warfare treaties, unilateral cyber assaults to preempt attacks is an issue of current debate. Arguably, belligerent actions in cyberspace are enabled through actions in other domains and vice versa, so it seems reasonable for a potential victim of an attack to counter-attack in whatever domain effectively stops the attack and mitigates the damage. Three recent terrorist attacks or attempted attacks against the U.S. were facilitated through the belligerent actors' use of the Internet. The Nigerian Umar Farouk Abdulmutallab who attempted to down Delta Flight 253 on Christmas 2009 viewed a blog and web site of the radical cleric al-Awlaki for "counseling and companionship." The five young Americans recently arrested by the FBI in New York for planning a terrorist attack contacted militant groups over the Internet, and U.S. Army Major Nidal Malik Hasan, who killed 14 soldiers in November 2009, used the Internet to also communicate with the radical cleric Awlaki. In a recent House Armed Services Committee meeting the question was posed whether the U.S. should launch preemptive cyber attacks against those Internet assets used to facilitate these three terrorist attacks against the United States.[143]

A preemptive attack against a potential belligerent actor would require an offensive capability; however, most countries like the U.S. are reluctant to reveal their true offensive capabilities. In the August 2009 interview when asked about U.S. offensive cyber capabilities, General Chilton, although reluctant to elaborate stated “it’s an area that we’re focused on… because we recognize that a good defense also incorporates elements of an offensive capability.”[144] Some argue developing these new kinds of weapons is a dangerous practice, however. The “ability to disable a nation’s infrastructure and cripple its military defenses without firing a shot sounds appealing, (however) condoning and launching cyber warfare is a slippery slope.” [145] The U.S. should carefully consider second and third order effects before unleashing these new weapons. [146]

Conclusions

The United States remains and is arguably increasingly more vulnerable to cyber attack than ever before. Government reliance on the internet for communications, commerce and governance, and computer-automated systems for infrastructure control, and the interdependence of sector networks (i.e. financial, energy, military, and telecommunications) all complicate state-supported defensive operations and increase network weaknesses. The volume, velocity and variety of Internet activity further complicate defensive strategies. While a single cyber attack launched by a belligerent state or non-state actor may not disrupt all of the U.S. critical infrastructures, significant damage can result. Illegitimate and criminal cyber activities cost the U.S. significant amounts, estimated in the billions of dollars annually in terms of theft, destruction and defensive measures.

Cyberspace continues to become more complex. In addition to the difficulties in attributing cyber attacks, state and non-state actors continue to grow and increase their cyber warfare capabilities. China, Russia, North Korea, and Iran—non-allies of the U.S.—have cyber warfare capabilities, and non-state actor belligerent activities are growing almost exponentially. Recent attacks against Georgia and Estonia show a pattern of premeditation and coordination not previously witnessed.

Few international rules exist that specifically address accepted norms in cyberspace and those that do are contradictory. Short of internationally accepted rules, cyber warfare is judged mostly through analogy with existing norms. Computer network exploitation appears to remain a legitimate form of cyber intelligence, surveillance and reconnaissance according to the articles of the U.N. While possibly an act of aggression, according to the U.N. Charter, computer network attack used in accordance with the LOAC principles of military necessity, distinction, proportionality, unnecessary suffering, perfidy, and neutrality are arguably legal. Determining CNA’s congruence with the LOAC principles is subjective, however. On the contrary, the Council of Europe Convention on Cybercrime’s Articles 2, 4 and 5 cite descriptions of criminal offenses specifically associated with CNE and CNA.

The argument for developing internationally-accepted cyber warfare rules appears to be gaining momentum within U.S. government circles. Although DoS officials opted away from developing a cyberspace arms treaty with Russia, the Chairman of the Senate Select Committee on Intelligence pressed for treaties, although the DNI, Admiral Blair preferred a “code of conduct.” The NSPD-54 and HSPD-23, both classified documents and outside the scope of this project, likely provide U.S. government rules for cyber warfare, but because of their confidentiality cannot be used by the international community, a necessary partner.

The 2008 cyber attacks against Georgia exemplify the complexities of cyber warfare. While Russian government involvement whether through collaboration or incitement was likely, attribution of the cyber attacks remains elusive. The collection of *hactivists* formed via the Internet are less likely to be considered warriors than criminals, but current international laws call for investigation and prosecution via the host nation, Russian government—an unlikely administrator of justice. The TSHost’s actions to mitigate damage to Georgian government communications by hosting their servers in U.S. networks arguably broke the U.S. government’s position of neutrality during this conflict and potentially opened U.S. infrastructure to attack. The fact that U.S.-hosted social networking sites were used to coordinate attacks against Georgia could also jeopardize the U.S. government’s position of neutrality. Finally, no published rules provide clarity regarding a proportional counter-attack if one was waged by Georgia. For example, would it have been appropriate for Georgia to attack hosts in Russia and Turkey from which the DDoS attacks were launched?

Cyber warfare appears to represent a greater strategic challenge than opportunity to U.S. national security. As a form of asymmetric warfare, cyber attack is increasingly popular given its source anonymity, quickness in operation, relative simplicity in accomplishment, and breadth across an array of sectors. As a hegemonic power, the U.S. will naturally attract belligerent actors seeking asymmetric means to achieve their objectives. With DoD network security spending greater than a billion dollars annually, the cost to the U.S. government could be overwhelming by itself, especially in the current economic environment. Despite public awareness of network and infrastructure vulnerabilities, the U.S. government, commercial and private sectors increasingly move toward a greater information systems reliance creating greater interdependencies between systems and networks. A network is only secure as its weakest link. China, Russia, North Korea and Iran, some with published cyber warfare doctrines seek capabilities to degrade and destroy critical national infrastructures. And, like the seas, the U.S. will feel the need to maintain “freedom of navigation” in cyberspace as a primary beneficiary of its existence. Most of these issues represent significant strategic challenges to U.S. national security.

Recommendation

Given the significant strategic challenge that cyber warfare poses on U.S. national security, the U.S. should seek to establish rules to clarify accepted norms. The existence of cyber warfare rules will identify thresholds for legitimate and illegitimate actions in cyberspace, mitigate collateral damage during times of war, and help hold belligerent actors accountable. The safety and security of U.S. citizens and property are of vital interest to the U.S., therefore the government has an obligation to protect and respond to attacks against these resources in all domains including cyberspace. The flow of commerce much of which now occurs in cyberspace (e.g. financial transactions) is arguably also of vital interest to the U.S., and therefore must be protected. Since cyber attacks can harm lives, property and commerce, the U.S. government should develop clear rules for cyber warfare and a synchronized U.S. government response to mitigate further destruction, fratricide, and hold the belligerent actor accountable. Therefore the U.S. and the international community need rules to identify accepted norms and provide governance to help hold belligerent actors accountable and deter would be assailants.

The U.S. should develop these cyber warfare rules multilaterally. This approach will be difficult to accomplish, but consensus achieved through participation will provide the best result—rules by which most nation states abide. Even though non-state belligerent actors would likely not participate in the development of cyber warfare rules, state actor involvement is a necessary component of non-state actor prosecution. Gaining IC consensus on cyber warfare rules will be difficult to achieve, if not impossible, nonetheless, a multilateral approach is best. Even if a formalized international policy is not achieved, the dialogue at an international scale will help clarify thresholds and appropriate responses that will be accepted by the U.S. government and international community.

Manifestation of these rules should be accomplished in a holistic manner. For example, the U.S. should use a variety of means to develop and maintain cyber warfare rules to include treaties, laws, multinational operations and directives/policies. These means through which cyber warfare rules will be documented will extend beyond the contemporary model of interpretation through analogy. Although in some cases interpretation through analogy may be sufficient.

Endnotes

[1] Barack H. Obama, "Remarks by the President on Securing Our Nation's Cyber Infrastructure," The White House, Washington D.C., May 29, 2009.

[2] U.S. Congress, House of Representatives, House Subcommittee on Emerging Threats, Cybersecurity and Science and Technology, *Addressing the Nation's Cybersecurity Challenges: Reducing Vulnerabilities Requires Strategic Investment and Immediate Action,* 110th Cong., 1st sess., April 25, 2007.

[3] Amber Corrin, "Cyber warfare: Sound the alarm or move ahead in stride?" *Federal Computer Week,* October 15, 2009, http://fcw.com/Articles/2009/10/19/FEAT-DOD-cyber-warfare.aspx?Page=5&p-1 (accessed October 23, 2009).

[4] Anonymous, "Leaders: Battle is joined; Cyberwar," *The Economist,* April 25, 2009, 20.

[5] U.S. Congress, Senate, Senate Select Committee on Intelligence's 15th Annual World-Wide Threat Hearing, *Current and Projected National Security Threats to the United States;* 111th Cong., 1st sess., February 12, 2009.

[6] Corrin, "Cyber warfare."

[7] Anonymous, "Leaders," 20.

[8] U.S. Congress, Senate, *Current and Projected National Security Threats.*

[9] Ibid.

[10] U.S. Congress, House of Representatives, House Subcommittee on Emerging Threats, Cybersecurity and Science and Technology, *Securing the Modern Electric Grid from Physical and Cyber Attacks,* 111th Cong. 1st sess., July 21, 2009.

[11] Gen Kevin Chilton, "U.S. Strategic Command – Cyber and Space Defense," Interview by Lynn Neary, National Public Radio, August 11, 2009.

[12] U.S. Congress, House of Representatives, House Subcommittee on Emerging Threats, *Securing the Modern Electric Grid.*

[13] Gen Chilton, "U.S. Strategic Command."

[14] Corrin, "Cyber warfare."

[15] Kevin Coleman, "The 2010 Cyber Threat Environment," January 11, 2010, http://defensetech.org/category/cyber-warfare/ (accessed on January 12, 2010).

[16] Gen Chilton, "U.S. Strategic Command."

[17] U.S. Congress, Senate, Senate Select Committee on Intelligence's 15th Annual World-Wide Threat Hearing, *Current and Projected National Security Threats to the United States*.

[18] Ibid.

[19] U.S. Congress, House of Representatives, House Subcommittee on Emerging Threats, *Securing the Modern Electric Grid.*

[20] Ibid.

[21] Ibid.

[22] Maj Arie J. Schaap, "Cyber Warfare Operations: Development and Use Under International Law," The Air Force Law Review, 2009; 64, Military Module, 123.

[23] Duncan B. Hollis, "Rules of Cyberwar?" *Los Angeles Times,* October 8, 2007.

[24] Col Jeffrey Caton, *What do Senior Leaders Need to Know about Cyberspace?* (Carlisle Barracks, PA: U.S. Army War College, 4.

[25] Ibid.

[26] Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms,* (Washington DC: U.S. Department of Defense, April 12, 2001, 141.

[27] Computer network attack (and counter attack) is action taken to destroy nodes or links or disrupt transactions in cyberspace that may or may not have intended second order effects in other domains (i.e. land, sea, air and space). Computer network exploitation is action taken to gather intelligence in cyberspace.

[28] United Nations, "Charter of the United Nations," http://www.un.org/en/documents/charter/chapter1.shtml (accessed January 6, 2010).

[29] Ibid.

[30] Ibid.

[31] United Nations, General Assembly Resolution 3314, "Definition of Aggression," December 14, 1974, http://www.un-documents.net/a29r3314.htm, (accessed January 6, 2010).

[32] United Nations, "Charter of the United Nations."

[33] Martin C. Libicki, "Cyberdeterrence and Cyberwar," RAND Corporation, 2009, 179.

[34] Hollis, "Rules of Cyberwar?"

[35] Libicki, "Cyberdeterrence and Cyberwar,"iii.

[36] Ibid.

[37] Webster's New World College Dictionary

[38] Hollis, "Rules of Cyberwar?"

[39] Thomas C. Wingfield, "The Law of Information Conflict: National Security Law in Cyberspace" (Aegis Research Corp. 2000), 352-3.

[40] "U.S. Joins Council of Europe Convention on Cybercrime," US Fed News Service, Washington D.C., September 29, 2006.

[41] Kristin Archick, "Cybercrime: The Council of Europe Convention," CRS Report for Congress RS21208, September 28, 2006, 1.

[42] Council of Europe Convention on Cybercrime, Budapest, 23.XI.2001, 2.

[43] Ibid.

[44] Council of Europe, 4-5.

[45] *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), June 8, 1977,* http://www.icrc.org/ihl.nsf/7c4d08d9b287a42141256739003e636b/f6c8b9fee14a77fdc125641e0052b079 (accessed February 12, 2010).

[46] Stephen W. Korns, and Joshua E. Kastenberg, "Georgia's Cyber Left Hook," *Parameters,* (Winter 2008–09): 60.

[47] Schaap, 147.

[48] John Markoff and Andrew E. Kramer, "US, Russia disagree on cyberspace treaty; Nations to address handling growing threat of attacks," *The Boston Globe,* June 28, 2009.

[49] Ibid.

[50] Ibid.

[51] U.S. Congress, Senate, Senate Select Committee on Intelligence's 15th Annual World-Wide Threat Hearing, *Current and Projected National Security Threats to the United States*.

[52] Ibid.

[53] Schaap, 149–53.

[54] Korns and Kastenberg, 61.

[55] Jeffrey T. G. Kelsey, "Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare," *Michigan Law Review,* 106 (May 2008): 1444.

[56] Korns and Kastenberg, 63.

[57] Korns and Kastenberg, 64.

[58] Korns and Kastenberg, 63.

[59] Duncan B. Hollis, "Why States Need an International Law for Information Operations," *Lewis & Clark Law Review,* 11:4, 1023-24.

[60] When two or more laws contradict, the more specific law has precedence over the general law.

[61] Hollis, "Why States Need an International Law." 1023-24.

[62] Ibid, 1028.

[63] Schaap, 146.

[64] Tony Bradley, "Pandora's Box," http://netsecurity.about.com/library/weekly/aa031703b.htm (accessed on 11 February 2010).

[65] Clay Wilson, "Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress 15, October 17, 2003, http://www.fas.org/irp/crs/RL32114.pdf (accessed 11 February 2010).

[66] Homeland Security Policy Directive-23, Federation of American Scientists http://www.fas.org/irp/offdocs/nspd/index.html (accessed on 11 February, 2010).

[67] Rita Roland, "Government Works to Stop Actual Bad Guys in the Virtual Realm," *Signal,* March 2009, 57-60.

[68] Ibid.

[69] Ibid.

[70] Paul Ames, "NATO allies sign agreement to fund center to boost defenses against cyberattacks," *Associated Press Worldstream,* May 14, 2008.

[71] Jason Fritz, "How China Will Use Cyber Warfare to Leapfrog in Military Competitiveness," *Culture Mandala,* Vol. 8, No. 1, October 2008, 43.

[72] Siobhan Gorman, "World News: Cyber Attacks on Georgia Used Facebook, Twitter, Stolen IDs," *Wall Street Journal,* August 17, 2009, A.5.

[73] Hollis, "Why States Need an International Law," 1024.

[74] Amber Corrin, "Some key events in the history of cyber warfare," *Federal Computer Week,* October 15, 2009, http://fcw.com/Articles/2009/10/19/FEAT-DOD-cyber-timeline.aspx?p=1 (accessed October 23, 2009).

[75] Ibid.

[76] Ibid.

[77] Ibid.

[78] Choe Sang-Hun and John Markoff, “Cyberattacks Jam Government and Commercial Web Sites in U.S. and South Korea,” *New York Times,* July 9, 2009, http://www.nytimes.com// 2009/09/10/technology/10cyber.html (accessed January 7, 2010).

[79] Gorman, “World News,” A.5.

[80] Korns and Kastenberg, 65.

[81] Ibid.

[82] Eneken Tikk et al, “Cyber Attacks Against Georgia: Legal Lessons Identified,” http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf (accessed January 11, 2010).

[83] Gorman, “World News,” A.5.

[84] Korns and Kastenberg, 65.

[85] Anonymous, “War, redefined; Even before Russian troops arrived, Georgian government websites were under cyber attack,” *Los Angeles Times,* August 17, 2008, A.25.

[86] Korns and Kastenberg, 67.

[87] Peter Svenson, “Georgian President’s Web Site Moves to Atlanta,” *Associated Press News,* August 11, 2008, http://www.usatoday.com/tech/products/2008-08-11-2416394828_x.htm (access January 11, 2010).

[88] Steven Adair, “Website for the President of Georgia Under Distributed Denial of Service Attack,” *CyberInsecure.com,* July 20, 2008, http://cyberinsecure.com/website-for-the-president-of-georgia-under-distributed-denial-of-service-attack/ (accessed January 17, 2010).

[89] Svenson, “Georgian President’s.”

[90] Brian Krebs, “Report: Russian Hacker Forums Fueled Georgia Cyber Attacks,” *The Washington Post,* October 16, 2008, http://voices.washingtonpost.com/securityfix/2008/10/ report_russian_hacker_forums_f.html (accessed January 12, 2010).

[91] Ibid.

[92] Gorman, “World News,” A.5.

[93] Hollis, “Why States Need an International Law,” 1025.

[94] Gorman, “World News,” A.5.

[95] Ibid.

[96] Ibid.

[97] Amber Corrin, “Cyber Warfare: Sound the alarm or move ahead in stride?” *Federal Computer Week online,* October 15, 2009, http://fcw.com/Articles/2009/10/19/FEAT-DOD-cyber-warfare.aspx?sc_lang=en&Page=1 (accessed January 12, 2010).

[98] Anonymous, “War, redefined; Even before Russian troops arrived, Georgian government websites were under cyber attack,” *Los Angeles Times,* August 17, 2008, A.25.

[99] Katie Paine, “Reputation Redux: Russia Invades Georgia by Land and by Server,” *PR News,* August 25, 2008, Vol. 64, Issue 33.

[100] Korns and Kastenberg, 70.

[101] Ibid.

[102] Gorman, “World News.”

[103] Ibid.

[104] William J. Lynn, Deputy Secretary of Defense, *Cyber Security,* Speech at the Center for Strategic and International Studies, June 15, 2009 (Washington D.C.).

[105] Ibid.

[106] Ibid.

[107] Maryann Lawlor, “Launching stealth warfare; Attacks in cyberspace may be prelude to future conventional conflicts,” *Signal,* March 2009, 63, 7, 47-50.

[108] Ibid.

[109] U.S. Congress, House of Representatives, House Subcommittee on Emerging Threats, *Securing the Modern Electric Grid.*

[110] Ibid.

[111] Kevin Coleman, “McAfee’s Take on the Cyber War,” November 23, 2009, http://defensetech.org/category/cyber-warfare/ (accessed January 12, 2010).

[112] Lawlor, “Launching Stealth Warfare,” 47-50.

[113] Gen Robert Keller, “Military must look at cyberspace as an ‘urban environment,’” *Inside the Air Force,* July 17, 2009, http://www.insideddefense.com/secure/display.asp?docnum= AIRFORCE-20-28-6&f=defense (accessed October 1, 2009).

[114] U.S. Secretary of Defense Robert M. Gates, “Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for military Cyberspace Operations,” memorandum for Secretaries of the Military Departments, Washington D.C., June 23, 2009.

[115] Ibid.

[116] Charles Billo & Welton Change, “Cyber Warfare Analysis of the Means and Motivations of Selected Nation States,” http://ists.dartmough.edu/docs/execsum.pdf (accessed January 12, 2010).

[117] Kevin Coleman, “Russia’s Cyber Forces,” *Defensetech.org,* http://www.defensetech.org/archives/cat_cayberwarfare.html (accessed January 10, 2010).

[118] Schaap, 133.

[119] Corrin, “Cyber warfare.”

[120] U.S. Congress, House of Representatives, House Subcommittee on Emerging Threats, *Securing the Modern Electric Grid.*

[121] Lynn, *Cyber Security,* Speech at the Center for Strategic and International Studies, June 15, 2009 (Washington D.C.).

[122] Corrin, “Cyber warfare.”

[123] Ibid.

[124] Richard Mereand, “Securing Cyberspace: Guarding the New Frontier,” *National Security Watch,* The Institute of Land Warfare, August 25, 2009, 2.

[125] Gen Chilton, “U.S. Strategic Command.”

[126] Renata Goldirova, “NATO picks Estonia for high-tech crime centre,” May 15, 2008, http://euobserver.com/?aid=26138 (accessed February 12, 2010).

[127] Corrin, “Cyber warfare.”

[128] Lynn, *Cyber Security.*

[129] Ibid.

[130] Korns and Kastenberg, 70.

[131] Schaap, 173.

[132] Coleman, “McAfee’s Take.”

[133] Korns and Kastenberg, 71.

[134] Korns and Kastenberg, 72.

[135] John Lister, “Are cyber-attacks an act of war?” August 16, 2008, http://tech.blorge.com/Structure:%20/2008/08/16/are-cyber-attacks-an-act-of-war/ (accessed January 12, 2010.)

[136] Korns and Kastenberg, 72.

[137] Lister, “Are cyber-attacks an act of war?”

[138] Kevin Coleman, “A Thaw in the Cyber Cold War,” December 14, 2009, http://defensetech.org/category/cyber-warfare/ (accessed January 12, 2010).

[139] Coleman, “A Thaw in the Cyber Cold War.”

[140] Korns and Kastenberg, 62.

[141] Lynn, *Cyber Security.*

[142] Coleman, “A Thaw in the Cyber Cold War.”

[143] Kevin Coleman, “The Time for Preemptive Cyber Strikes Has Come,” January 4, 2010, http://defensetech.org/category/cyber-warfare/ (accessed January 12, 2010).

[144] Gen Chilton, “U.S. Strategic Command.”

[145] Bradley, “Pandora’s Box.”

[146] Ibid.