View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by University of New Mexico

SCHOOL OF LAW FACULTY SCHOLARSHIP DIGITAL REPOSITORY

7-1-2009

Non-Intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law

Joshua E. Kastenberg
University of New Mexico - School of Law

Follow this and additional works at: https://digitalrepository.unm.edu/law_facultyscholarship

 Part of the Law Commons

Recommended Citation

Joshua E. Kastenberg, *Non-Intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law*, 64 Air Force Law Review 43 (2009).
Available at: https://digitalrepository.unm.edu/law_facultyscholarship/436

This Article is brought to you for free and open access by the UNM School of Law at UNM Digital Repository. It has been accepted for inclusion in Faculty Scholarship by an authorized administrator of UNM Digital Repository. For more information, please contact amywinter@unm.edu, lsloane@salud.unm.edu, sarahrk@unm.edu.

SCHOOL OF LAW
SMALL SCHOOL. BIG VALUE.

NON-INTERVENTION AND NEUTRALITY IN CYBERSPACE: AN EMERGING PRINCIPLE IN THE NATIONAL PRACTICE OF INTERNATIONAL LAW

LIEUTENANT COLONEL JOSHUA E. KASTENBERG

Lieutenant Colonel Joshua E. Kastenberg (B.A., University of California, Los Angeles (1990); J.D., Marquette University (1996); LL.M., Georgetown University (2003)) is the Staff Judge Advocate, 332d Air Expeditionary Wing, Balad Air Base, Iraq. Prior to his current assignment, he served as Staff Judge Advocate, Joint Task Force-Global Network Operations, a standing joint task force under the command of United States Strategic Command. Under the Unified Command Plan, it is the sole cyber-defense operational command for the Department of Defense. He is a member of the Wisconsin Bar.

I. INTRODUCTION[1]

Of all the recent legal literature examining the role of nations and corporations in cyberspace, very little has been devoted to the relationship between state-sponsored information operations—the roles and uses of cyberspace in interstate conflict—and neutrality. Most of the legal scholarship has been devoted to applying the laws of war to cyberspace operations. Issues such as proportionality, lawful targeting, and when an action constitutes a hostile act, appear to have taken preeminence over other matters. This article departs from that construct and addresses a related and equally important issue: the enforcement of neutrality in cyberspace. The United States will not always be a party to a conflict, and the executive branch's official stated policy may be to adhere to a position of non-intervention or even strict neutrality.

Admittedly, unlike in mid-twentieth century conflicts, it has become increasingly difficult for a state to regulate commerce, particularly electronic commerce, because of the internationalization of global business and the worldwide transit of electronic information across cyberspace. At present, roughly eighty percent of the Internet traffic traverses through the United States, chiefly through servers owned by private enterprise.[2] As a result, transactions which occur between London and Tokyo will still likely travel through the United States. Electronic information which flows through cyberspace is unlike any other type of physical transaction. Physical mails and shipped goods may leave London and reach Tokyo without ever traversing the geographic territory of a third state. Even an undersea telephone wire cable theoretically enables a predictable flow between two points, without transiting a third state.

Historically, national governments tried to remain neutral in third-party conflicts because conflict eroded commerce and the addition of interested states into a conflict tended to lengthen wars, thereby increasing the loss of lives. Neutrality, as discussed below, was recognized as a set of behavioral norms that limited the damage of warfare to warring states, notwithstanding commercial losses attendant with warfare. The United States, since its existence, has both recognized the importance of neutrality principles and demanded that other states act similarly. But, while it is well-understood that the behavioral requirements of neutral states are usually enforceable in the

---

[1] This issue was first addressed by Colonel Steven Korns and (then) Major Joshua Kastenberg in *Georgia's Cyber Left Hook*, PARAMETERS, 2008, at 60. The author thanks Colonel Korns for his insight and assistance in developing the concepts of cyber neutrality further. Sections of this law review article incorporate themes from the article in Parameters. However, the intended audience here is practitioners of operations law.

[2] *See, e.g.*, GABRIEL WEIMANN, TERROR ON THE INTERNET: THE NEW ARENA, THE NEW CHALLENGE 183-87 (2005).

physical realm, the advent of cyberspace makes this more difficult, particularly in the realm of information and electronic warfare.

The executive branch of the United States, with legislative checks, is the arm of government charged with determining and enforcing foreign policy. The executive branch may conclude that it is not in the best interests of the nation to remain fully neutral. Certainly, the enforcement of neutrality in cyberspace has not yet occurred, and there appears to be no policy for enforcement. This article suggests a rubric using existing laws for exerting executive authority.

Section I of this article discusses the emergence of conflict in cyberspace. Importantly, this article does not address either criminal enforcement or a state's duty in that realm but instead focuses on the executive branch's authority to enforce neutrality in cyberspace. Section II provides a basic rubric of neutrality rules as applied to conflict in cyberspace. Section III analyzes the most recent cyber-conflict, the Georgian-Russian War of 2008, and the potential consequences the United States risked because it lacked a cyber neutral position. Finally, the article concludes with an assessment of the need for a greater exertion of authority from the executive branch to police cyberspace. Importantly, this article does not advocate that the United States must take a wholly neutral position in conflicts which do not involve it. However, the executive branch should make clear that it has the authority to enforce cyber neutrality when it is determined by that branch to be necessary to national policy.

II. EMERGENCE OF CYBER WARFARE

Although the concept of cyber warfare is not new, since 2005 there has been an escalation of proxy conflict within cyberspace, particularly in two notable instances. In 2007, the Estonian government suffered cyber attacks on its infrastructure.[3] The attack degraded enough critical media and communications systems that it rendered the government impotent to conduct its essential functions of monitoring the country's economy and command and control over military forces.[4] The Estonia "911" emergency equivalent was off-line for an extended period. The natural inclination of several observers was to suspect the Russian government of orchestrating the attack.[5] No public evidence

[3] Jeffrey T.G. Kelsey, *Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare*, 106 MICH. L. REV 1427, 1428-29 (2008) (citing *Newly Nasty*, ECONOMIST, May 26, 2007, at 63); Korns & Kastenberg, *supra* note 1, at 63.

[4] Kelsey, *supra* note 3, at 1429.

[5] Korns & Kastenberg, *supra* note 1, at 65.

has emerged to sustain this suspicion.[6] In response to the attacks, Estonia appealed to the United States and the North Atlantic Treaty Organization for assistance.[7]

On July 19, 2008, an Internet cyber security firm reported on a distributed denial of service (DDoS) cyber attack against the country of Georgia.[8] Three weeks later, on August 8, security experts observed a second round of DDoS attacks against Georgia, this time more substantial, with multiple command and control (C2) servers concentrated against Georgian governmental and commercial websites. Analysts noted that this second round of DDoS attacks appeared to coincide with the movement of Russian troops into South Ossetia in response to Georgian military operations a day earlier in this region.[9] By August 10, DDoS attacks rendered most Georgian governmental websites inoperable.[10]

As a result of the DDoS attacks, the Georgian government found itself cyber-locked, barely able to communicate on the Internet.[11] In response to the situation, the Georgian government took an unorthodox step and sought "cyber refuge" in the United States.[12] Without first seeking U.S. government approval, Georgia relocated its

---

[6] *Id.*; *see also*, Scott Shackelford, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, 27 BERKELEY J. INT'L L., 192, 193 (2009).

[7] Korns & Kastenberg, *supra* note 1, at 63; Shackelford, *supra* note 5.

[8] Korns & Kastenberg, *supra* note 1, at 64-65; Steven Adair, *The Website for the President of Georgia Under Attack – Politically Motivated?*, SHADOWSERVER FOUNDATION, July 20, 2008, http://www.shadowserver.org/wiki/pmwiki.php/Calendar/20080720 (last visited Sept. 2, 2009). Shadowserver specifically reported:

> For over 24 hours, the website of President Mikhail Saakashvili of Georgia has been rendered unavailable due to a multi-pronged distributed denial of service (DDoS) attack. The site began coming under attack very early Saturday morning. Shadowserver has observed at least one web-based command and control (C2) server taking aim at the website hitting it with a variety of simultaneous attacks. The C2 server has instructed its bots to attack the website with TCP, ICMP, and HTTP floods . . . the C2 server involved in these attacks is on IP address 207.10.234.244, which is subsequently located in the United States.

[9] Adair, *supra* note 8; Korns & Kastenberg, *supra* note 1, at 65.

[10] Steven Adair, *Georgian Websites Under Attack - DDoS and Defacement*, SHADOWSERVER FOUNDATION, Aug. 11, 2008, http://www.shadowserver.org/wiki/pmwiki.php/Calendar/20080811 (last visited Sept. 2, 2009); Shaun Waterman, *Georgia Hackers Strike Apart From Russian Military*, WASH. TIMES, Aug. 19, 2008, http://www.washtimes.com/news/2008/aug/19/georgia-hackers-strike-apart-from-russian-military (last visited Sept. 7, 2009); Karl Zimmerman, Webhosting Report, Steadfast Networks, comment posted July 20, 2008, http://www.webhostingtalk.com/showpost.php?p=5220780&postcount=41 (last visited Sept. 11, 2009).

[11] Korns & Kastenberg, *supra* note 1, at 66.

[12] *Id.*

Presidential website to a U.S. web hosting company and moved its Ministry of Foreign Affairs (MFA) press dispatches to Google's Blogspot.[13] The MFA also mirrored its Internet services at a site in Estonia and on the website of Poland's president, Lech Kaczynski.[14]

Georgian-Russian hostilities in South Ossetia generated a substantial amount of analysis and speculation regarding the underlying cyber conflict.[15] Most of the focus has centered on who conducted the cyber attacks, and why. However, the Georgian-Russian conflict provides an opportunity to examine a more subtle, intriguing, and perhaps overlooked aspect of cyber conflict—the concept of cyber neutrality. The Georgian case raises two fundamental questions: can the United States remain neutral (or cyber neutral) during a cyber conflict, and how did the actions of the Georgian government and private U.S. information technology (IT) companies impact U.S. status as a cyber neutral?

The implications of these two questions should concern U.S. policy makers and military strategists. Even if the United States is not a belligerent in a cyber conflict, incursions on the U.S. Internet infrastructure will likely occur. Private industry owns and operates the Internet. The unregulated action of these third party actors during a cyber conflict could unintentionally impact U.S. cyber neutrality. There is little, if any, modern legal precedence which resolves this question. Nonetheless, the fact that U.S. IT companies provided cyber assistance to the Georgian government, without any apparent U.S. government involvement, exemplifies a significant cyber policy issue. Although nations still bear ultimate responsibility for the acts of their citizens or surrogates, translating this protocol to fit the modern realities of cyber conflict is a complex challenge. By relocating its cyber assets to the

---

[13] Adair, *supra* note 10; *see also* MINISTRY OF FOREIGN AFFAIRS OF GEORGIA, http://georgiamfa.blogspot.com (last visited Sept. 7, 2009); Noah Shachtman, *Estonia, Google Help "Cyberlocked" Georgia*, WIRED: DANGER ROOM, Aug. 11, 2008, http://blog.wired.com/defense/2008/08/civilge-the-geo.html (last visited Sept. 7, 2009); Peter Svensson, *Georgian President's Web Site Moves to Atlanta*, USATODAY.COM, Aug. 11, 2008, http://www.usatoday.com/tech/products/ (last visited Sept. 7, 2009); Tulip Systems Incorporated, http://www.tshost.com (last visited Sept. 11, 2009).

[14] John Markoff, *Georgia Takes a Beating in the Cyberwar With Russia*, N.Y. TIMES: BITS BLOG, Aug. 11, 2008, http://bits.blogs.nytimes.com/2008/08/11/georgia-takes-a-beating-in-the-cyberwar-with-russia (last visited Sept. 7, 2009); *see also Information About The Latest Developments In Georgia*, MINISTRY OF FOREIGN AFFAIRS OF GEORGIA, http://www.president.pl/x.node?id=20043119 (accessed on the web site of the President of Poland) (last visited Sept. 7, 2009); Shachtman, *supra* note 13.

[15] Korns & Kastenberg, *supra* note 1, at 67-68; Markoff, *supra* note 13; *see also* Kim Hart, *Longtime Battle Lines Are Recast In Russia And Georgia's Cyberwar*, WASH. POST, Aug. 14, 2008, at D1, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2008/08/13/AR2008081303623.html; Noah Shachtman, *Georgia Under Online Assault*, WIRED: DANGER ROOM, Aug. 10, 2008, http://blog.wired.com/defense/2008/08/georgia-under-o.html (last visited Sept. 7, 2009).

United States, Georgia's unconventional response to the July and August 2008 DDoS attacks, supported by U.S. industry, adds a new element of complication that strategists need to consider in planning for future cyber operations.

This is not to argue that the United States failed to plan for the eventuality of a cyber conflict, and it is important to note that defense capabilities may be used to enforce cyber neutrality if the need to do so arises. The Executive Branch of the U.S. Government has prepared for the eventuality of a cyberwar. In 1997, President William J. "Bill" Clinton established the President's Commission on Critical Infrastructure Protection. The Commission predicted that by 2002, 19 million people would have the ability to launch cyber attacks. It also noted that since little in the way of specialized equipment is needed to conduct such attacks, governments could expect an exponential growth in increasingly sophisticated malicious cyber activity.[16]

On May 22, 1998, President Clinton issued Presidential Decision Directive/NSC-63.[17] In it, the President noted, "The United States possesses both the world's strongest military and its largest national economy. Those two aspects of our power are mutually reinforcing and dependent. They are also increasingly reliant upon certain critical infrastructures and upon cyber-based information systems."[18] In 2002, President George W. Bush issued National Security Presidential Directive (NSPD) 16, which directed the government to review offensive capabilities against enemy computer networks.[19] In 2004, President Bush issued NSPD-38, *National Strategy to Secure Cyberspace*.[20] The two strategy documents are related in the same manner in which offense and defense are related in a military operational construct. Both documents are not releasable to the general public due to classification considerations.

In 2008, President Bush promulgated NSPD 54/Homeland Security Presidential Directive (HSPD) 23, *Cyber Security and Monitoring*. While NSPD 54/HSPD 23 remains classified, its definition of cyberspace is: "'Cyberspace' means the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded

---

[16] COMMISSION ON CRITICAL INFRASTRUCTURE PROTECTION, WHITE PAPER, THE CLINTON ADMINISTRATION'S POLICY ON CRITICAL INFRASTRUCTURE POLICY: PRESIDENTIAL DECISION DIRECTIVE 63 (May 22, 1998), *available at* http://www.fas.org/irp/offdocs/paper598.htm.

[17] *See generally* Presidential Decision Directive NSC-63, Critical Infrastructure Protection (May 22, 1998), *available at* http://www.fas.org/irp/offdocs/pdd/pdd-63.htm.

[18] *Id.*

[19] *See* Bradley Graham, *Bush Orders Guidelines for Cyber Warfare*, WASH. POST, Feb. 7, 2003, at A1.

[20] National Security Presidential Directive 38, National Strategy to Secure Cyberspace (2004) (quotation is unclassified portion of a classified document).

processors and controllers in critical industries."[21] Later, Deputy Secretary of Defense Gordon England, issued a memorandum that defined 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."[22]

Presently there are two proposed bills pending in the United States Senate that will enable the executive branch to exert greater control over cyberspace during emergencies. Senator Jay Rockefeller (D - West Virginia) introduced Senate Bill 773 titled the Cybersecurity Act of 2009.[23] Section 18 of the proposed act enables the President to declare an emergency and order the limitation or shutdown of a Federal Government or United States critical information infrastructure system or network.[24] While the pending bill is designed to place the Director of National Intelligence and the Secretary of Commerce as the primary agencies for ensuring cyber-security, the Department of Defense will have an advisory role.[25] Senator Thomas Carper (D - Delaware) introduced the second bill, the United States Information and Communications Enhancement Act of 2009.[26] This bill would establish a National Office for Cyberspace in the White House, charged with overseeing the execution of cybersecurity policies and procedures in the federal government.[27] Neither act expressly touches on the subject of cyber neutrality, but both would give to the executive branch a leverage of control over the internet to enforce neutrality during national emergencies.

The U.S. Department of Defense (DOD) has prepared for the eventuality of cyber operations in a wartime context as evidenced in directives, instructions, and doctrine. The Joint Functional Component Command for Network Warfare is the sole agency for network attack. However, with the pending creation of the sub-unified command, the authority to conduct network warfare will fall to the commander of the

---

[21] National Security Presidential Directive 38/ Homeland Security Presidential Directive 23, Security and Monitoring (2008) (quotation is unclassified portion of a classified document).

[22] Both definitions are contained in the Memorandum from the Deputy Secretary of Defense Memo to the Military Departments et al., subject: "The Definition of Cyberspace" (12 May 2008), and its accompanying staff papers (on file with author).

[23] S. 773, 111th Cong. (2009); *see also* R. Michael Senkowski & Mimi W. Dawson, *Cybersecurity: A Briefing - Part II*, METRO. CORP. COUNS., Aug. 2009, at 34.

[24] S. 773, 111th Cong. (2009), § 18.

[25] *Id.* § 3.

[26] S. 921, 111th Cong. (2009).

[27] *Id.* § 3552.

new command. This command is slated to be fully operational in October 2009. [28]

DOD Directive (DODD) O-3600.3, *Technical Assurance Standard for Computer Network Attack (CNA) Capabilities*, was promulgated on May 13, 2005. This directive is classified "Top Secret," except for the name. Presumably, it contains, as the name implies, capabilities requirements for conducting CNA. Because CNA is defined as "[o]perations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves," in DODD 3600.01, *Information Operations*, dated August 14, 2006, it can also be assumed that the classified document approaches network attack in a like manner. Likewise, DODD O-8530.1, *Computer Network Defense*, dated January 8, 2001, is classified.

The DOD's doctrinal view of cyberspace is found in Joint Publication (JP) 6-0, *Joint Communications System*, dated March 20, 2006. It states:

> The GIG [global information grid] operates as a globally interconnected, end-to-end, interoperable network-of-networks, which spans traditional boundaries of authority. Given the inherent global reach of the GIG, many NETOPS [network operations] activities are not under the command authority of a using CCDR [combatant commander]. Therefore, a great deal of coordination and collaboration (unity of effort) is essential to fully enable NETOPS capabilities.[29]

JP 5-0, *Joint Operation Planning*, dated December 26, 2006, notifies commanders of combatant commands and service commanders to plan for asymmetrical threats. In terms of computer operations, the doctrine states, "one example of a persistent, asymmetric threat that is inherently global and poses risk cross-AOR [area of responsibility] boundaries is adversary exploitation and attack of DOD computer networks on the global information grid."[30] But in none of these rules is there a consideration for policing cyber neutrality.

---

[28] Siobahn Gorman, *Gates to Nominate NSA Chief to Head New Cyber Command*, WALL STREET J., Apr. 24, 2009, http://online.wsj.com (last visited Sept. 11, 2009).

[29] JOINT CHIEFS OF STAFF, JOINT PUB. 6-0, JOINT COMMUNICATIONS SYSTEM, at 71 (20 Mar. 2006), *available at* http://www.dtic.mil [hereinafter JP 6-0].

[30] JOINT CHIEFS OF STAFF, JOINT PUB. 5-0, JOINT OPERATION PLANNING, at I-22 (26 Dec. 2006), *available at* http://www.dtic.mil/doctrine/jel/new_pubs/jp5_0.pdf [hereinafter JP 5-0].

III. CYBER NEUTRALITY, A BASIC RUBRIC

Neutrality, in the United States, is primarily the executive branch's province, as a matter of its constitutional authority over foreign policy.[31] In 1908, Woodrow Wilson, then president of Princeton University, articulated, "One of the greatest of the President's powers I have not yet spoken of at all: his control, which is very absolute, of the foreign relations of the nation. The initiative in foreign affairs, which the President possesses without any restriction whatever, is virtually the power to control them absolutely."[32] Yet, at the beginning of World War I, U.S. President Wilson declared the United States a neutral nation, but American banks continued providing loans to Britain and France, and American industry sold armaments almost exclusively to Britain, France and their allies.[33] The German government responded by waging unrestricted submarine warfare, maritime commerce raiding, and espionage activities within the continental United States.[34]

Wilson's neutrality stance was more emotional than actual, in that he did not exercise executive authority to halt U.S. loans and arms shipments to belligerents.[35] Over a half century later, Supreme Court Justice William O. Douglas penned sentiments similar to Wilson's in writing, "my view of foreign affairs is that Congress has the power to declare war, and that all diplomacy short of that is under the guidance of the President."[36] Even as Douglas harshly criticized the Nixon administration's policies in Vietnam and concluded the conflict was "unlawful," Douglas held fast to the principle of executive authority in foreign policy.[37]

It must be noted that although the executive branch is preeminent in foreign policy, as a matter of checks and balances, Congress does retain the authority to regulate foreign commerce and no treaty can obligate the United States without the Senate's advice and consent.[38] In 1920, the Supreme Court determined that individual states, of the United States, do not possess the authority to act contrary

---

[31] U.S. CONST. art. II, § 2; Korns & Kastenberg, *supra* note 1, at 61-62.
[32] WOODROW WILSON, CONSTITUTIONAL GOVERNMENT IN THE UNITED STATES 77 (1908); Korns & Kastenberg, *supra* note 1, at 61-62.
[33] JENNIFER KEENE, WORLD WAR I: DAILY LIFE THROUGH HISTORY 5 (2006); RONALD STEELE, WALTER LIPPMAN AND THE AMERICAN CENTURY 89 (1999).
[34] WILLIAM MCNEILL, THE PURSUIT OF POWER 341-42 (1982); THEODORE ROPP, WAR IN THE MODERN WORLD 257-58 (1959).
[35] ANNE RICE PIERCE, WOODROW WILSON AND HARRY TRUMAN: MISSION AND POLICY IN AMERICAN FOREIGN POLICY 22 (2003).
[36] WILLIAM O. DOUGLAS, THE COURT YEARS: 1939-1957, AN AUTOBIOGRAPHY 270 (1980).
[37] *Id.*
[38] U.S. CONST. art. II, § 2.

to a treaty.[39] More importantly, this finding also extends to individual corporations, which may not conduct trade with a foreign government against the executive branch's prohibition of such trade. Indeed, where a corporation violates this prohibition, it may be subject to criminal sanctions. If the U.S. government establishes a strict position of neutrality, corporations based in the United States may not provide material support to a belligerent state, except where the government permits.[40] Corporations may, however, engage in non-military trade or provide humanitarian support.[41]

For the purpose of this article, cyber neutrality does not depart from the traditional international law of neutrality. This rubric of laws requires combatant states to recognize the rights of neutrals. In addition, neutral states must refrain from assisting either side in a conflict, other than to effectuate peace.[42] Neutrality laws as codified in the 1907 Hague V Conventions give states certain legal rights when not participating in a conflict, especially the right to remain neutral and maintain relations with all belligerents.[43] States that declare themselves to be neutral, and act accordingly, are entitled to immunity from attack.[44] Neutrality does not require neutral states to shut off all commerce with combatant states, although such commerce must not expressly provide military aid to a combatant state during conflict.[45] The Conventions also dictate that the territory of a neutral state is inviolable; belligerents may not move troops, weapons, or other materials of war across the territory of a neutral state.[46] Belligerent states may not conduct hostilities from the territory or waters of a neutral state, and a belligerent's aircraft may not penetrate neutral airspace.[47] The Conventions require that neutral states prevent belligerents from engaging in these violations.[48] A neutral state that

---

[39] *See* U.S. CONST. art. I, § 8, cl. 3; Missouri v. Holland, 252 U.S. 416 (1920); U.S. v. Curtiss-Wright Export Corp., 299 U.S. 304 (1936).

[40] When the United States is in conflict with another nation, the President's power to suppress trade with belligerent nations is almost absolute. *See* Trading with the Enemy Act, 50 U.S.C. app. § 5(b) (2006).

[41] *Id.* The U.S. State Department list of state sponsors of terrorism is at http://www.state.gov/s/ct/c14151.htm (last visited Sept. 12, 2009).

[42] Convention Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, arts. 1–3, Oct. 18, 1907, 36 Stat. 2310, 1 Bevans 654 [hereinafter Hague Convention V]; *see also* Convention Concerning the Rights and Duties of Neutral Powers in Naval War, Oct. 18, 1907, 36 Stat. 2415, 1 Bevans 723 [hereinafter Hague Convention XIII]; STEPHEN C. NEFF, THE RIGHTS AND DUTIES OF NEUTRALS 1 (2000).

[43] Hague Convention XIII, *supra* note 42, art. 1.

[44] *Id.*

[45] Hague Convention V, *supra* note 42, art. 7.

[46] *Id.* art. 5.

[47] *See* Detlev Vagts, *The Role of Switzerland: Neutrality Law in World War II*, 20 CARDOZO L. REV. 459, 465-67 (1998).

[48] Hague Convention V, *supra* note 42, art. 9.

takes no action jeopardizes its neutrality status. In 1917, the Supreme Court cemented this framework into American jurisprudence.[49]

As an emerging form of warfare, cyber war is not explicitly addressed under current international law, thus neither is cyber neutrality. However, overarching principles apply to both.[50] Cyber warfare implicates the principle of neutrality because a belligerent may launch attacks using the international structure of the Internet. The core issue is the routing of these cyber attacks through neutral countries, which is likely given the Internet's architecture. Cyber attacks routed across the Internet nodes of neutral states would appear to violate conventional neutrality law, despite the lack of physical intrusion.[51] The same would apply to cyber attacks launched from a neutral state, even if the neutral state did not control the attack. International law would appear to require a belligerent state (or third party neutral) to stop its citizens from engaging in such acts.

International law is not definitive on whether cyber techniques such as DDoS are legally considered "attacks" or "weapons,"[52] and whether cyber attacks can be considered legitimate acts of "armed conflict."[53] Malicious software, or malware, is not an "arm" of war, yet

---

[49] *See* The Steamship Appam, 243 U.S. 124 (1917). The *Appam* involved a British vessel which had been seized on the high seas by the German Navy, but brought into an American port for fuel. The Court found the seizure lawful under international law, but once the German Navy brought the vessel into neutral American jurisdiction, the British ship owners possessed standing to sue for recovery of the vessel because the Germans had violated neutrality by bringing a war prize through neutral territory. Of importance, the Court held: "The violation of American neutrality is the basis of jurisdiction, and the admiralty courts may order restitution for a violation of such neutrality. In each case the jurisdiction and order rests upon the authority of the courts of the United States to make restitution to private owners for violations of neutrality where offending vessels are within our jurisdiction, thus vindicating our rights and obligations as a neutral people." *Id.* at 128.

[50] Knut Dörmann, *Computer Network Attack and International Humanitarian Law*, INT'L COMM. OF THE RED CROSS, May 19, 2001, *available at* http://www.icrc.org/web/eng/siteeng0.nsf/htmlall/5p2alj; *see also* Robert G. Hanseman, *The Realities and Legalities of Information Warfare*, 42 A.F. L. REV. 187 (1997); Bruce Smith, *An Eye for an Eye, a Byte for a Byte*, FED. L., Oct. 1995, at 12; George K. Walker, *Information Warfare and Neutrality*, 33 VAND. J. TRANSNAT'L L. 1079 (2000).

[51] Lawrence T. Greenberg et al., *Information Warfare and International Law* 10 (1998), *available at* http://permanent.access.gpo.gov/lps1804/iwilindex.htm.

[52] Kelsey, *supra* note 3, at 1443; *see also* Steven M. Barney, *Innocent Packets? Applying Navigational Regimes from the Law of the Sea Convention by Analogy to the Realm of Cyberspace*, *in* THE CHAIRMAN OF THE JOINT CHIEFS OF STAFF STRATEGY ESSAY COMPETITION 1 (Nat'l Def. Univ. Press, 2001), *available at* http://www.ndu.edu/inss/books/Books_2001/essays2001/Essays01.pdf; Davis Brown, *A Proposal for an International Convention To Regulate the Use of Information Systems in Armed Conflict*, 47 HARV. INT'L L.J. 179 (2006); Duncan B. Hollis, *Why States Need an International Law for Information Operations*, 11 LEWIS & CLARK L. REV. 1023 (2007).

[53] Kelsey, *supra* note 3, at 1443; *see also* Greenberg et al., *supra* note 51, at 30–33; Hanseman, *supra* note 50, at 183; Gregory F. Intoccia & Joe W. Moore,

the effects of cyber attacks can equal that of kinetic attacks. Arguably, a cyber attack that causes physical destruction could constitute an "armed attack" under the United Nations (UN) Charter.[54] The Charter appears to define an "armed attack" as a crossing of geographic domains by the use of armed force.[55]

Some advocates articulate that beyond transmitting a mere communication signal, cyber attacks effectively move a weapon across the Internet.[56] For example, in issuing National Security Directive 16, President George W. Bush ordered the development of guidelines to regulate the use of "cyber weapons in war."[57] The Estonian Defense Minister initially characterized the April 2007 Estonian cyber event as an "extensive cyber attack."[58] He contemplated invoking NATO Article V, which considers an "armed attack" against any NATO country to be an attack against all.[59] A 2008 Defense Science Board report stated that terrorists are using the Internet as an "asymmetric weapon."[60] A past assistant to the President for cyber security indicated that "[a]ttacks on the Internet itself . . . could cause widespread problems."[61]

On the other hand, some skeptics stress that no international legal precedents clearly define cyber weapons, and point to the Law of Armed Conflict (LOAC) as being unsettled with respect to cyber attacks.[62] Admittedly, there is a rationale for this view. The Council of Europe Convention on Cybercrime (COE Convention), to which the

---

Communications Technology, Warfare, and the Law: Is the Network A Weapon System?, 28 HOUS. J. INT'L L. 469 (2006).

[54] U.N. Charter art. 51.

[55] *Id.*

[56] *See* Brown, *supra* note 52.

[57] Bradley Graham, *Bush Orders Guidelines for Cyber-Warfare: Rules for Attacking Enemy Computers Prepared as U.S. Weighs Iraq Options*, WASH. POST, Feb. 7, 2003, at A1; Korns & Kastenberg, *supra* note 1, at 63.

[58] Kevin Poulsen, *Cyberwar and Estonia's Panic Attack*, WIRED: THREAT LEVEL, Aug. 22, 2007, http://blog.wired.com/27bstroke6/2007/08/cyber-war-and-e.html (last visited Sept. 7, 2009); *see also* Jeremy Kirk, *Estonia Recovers from Massive DDoS Attack*, COMPUTERWORLD.COM, May 17, 2007, http://www.computerworld.com (last visited Sept. 7, 2009).

[59] North Atlantic Treaty art. 5, Apr. 4 1949, 63 Stat. 2241, 34 U.N.T.S. 243, *available at* http://www.nato.int/docu/basictxt/treaty.htm ("The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defense recognized by Article 51 of the Charter of the United Nations . . . ").

[60] DEFENSE SCIENCE BOARD, FINAL REPORT OF THE DEFENSE SCIENCE BOARD TASK FORCE ON STRATEGIC COMMUNICATION 27 (2008).

[61] John Schwartz, *When Computers Attack*, N.Y. TIMES.COM, June 24, 2007, http://www.nytimes.com (last visited Sept. 7, 2009) (quoting Paul Kurtz' statement that "[a]ttacks on the Internet itself, say, through what are known as root-name servers, which play a role in connecting Internet users with Web sites, could cause widespread problems").

[62] Intoccia & Moore, *supra* note 44, at 484.

United States is a party, does not contain any reference to cyber attacks, and instead considers as criminal acts all offenses against "the confidentiality, integrity or availability of computer systems."[63] The Center for Strategic and International Studies points out that DDoS attacks are more commonly used for illicit activities like fraud than for cyber war.[64] NATO defense ministers declined to define the Estonia cyber event as an attack requiring military action.[65] The Estonian Justice Minister ultimately conceded that independent civilians, rather than the Russian government, conducted cyber attacks against his country. The Estonian government now classifies the incident as an act of terrorism rather than cyber war.[66]

In 2005, the U.S. Air Force Operations and International Law division published a memorandum stating "the network is not a weapon system."[67] An Internet security expert recently observed "there are good reasons to reject the idea that timeout errors (DDoS) are an act of war."[68] Until the obfuscation surrounding cyber attacks is better clarified, many in the legal and technical communities will continue to see DDoS events as acts for the criminal justice system—not the national defense system—to resolve.

Although the debate over cyber conflict remains unsettled, the international law community does appear to be coalescing around the general principle that use of the Internet to conduct cross-border cyber attacks violates the principle of neutrality. As one legal scholar has noted, "[w]hen an information packet containing malicious code travels

---

[63] *United States Joins Council of Europe Convention on Cybercrime*, DEP'T OF STATE, Sept. 29, 2006, http://www.america.gov/st/washfile-english/ (last visited Sept. 7, 2009); *see also* Convention on Cybercrime, Nov. 23, 2001, 2296 U.N.T.S. 167 [hereinafter COE Convention], *available at* http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

[64] Schwartz, *supra* note 52 (quoting James Andrew Lewis' statement that "[t]hese 'botnets' are more commonly used for illicit activities like committing online fraud and sending spam").

[65] Ian Traynor, *Russia Accused of Unleashing Cyberwar to Disable Estonia*, GUARDIAN, May 17, 2007, http://www.s.co.uk/world/2007/may/17/topstories3.russia (last visited Sept. 7, 2009).

[66] *EU Should Class Cyber Attacks as Terrorism: Estonia*, BRISBANE TIMES.COM, June 8, 2007, http://news.brisbanetimes.com.au/technology/eu-should-class-cyber-attacks-as-terrorism-estonia-20070608-h9r.html (last visited Sept. 7, 2009); *see also* Joel Hruska, *Student Behind DoS Attack that Rekindled Bad Soviet Memories*, ARS TECHNICA, Jan. 24, 2008, http://arstechnica.com/news.ars/post/20080124-student-behind-dos-attack-that-rekindled-bad-soviet-memories.html (last visited Sept. 7, 2009); Jeremy Kirk, *Student Fined for Attack Against Estonian Web Site*, INFOWORLD (Internet edition), Jan. 24, 2008, http://www.infoworld.com/article/08/01/24/Student-fined-for-attack-against-Estonian-Web-site_1.html (last visited Sept. 7, 2009).

[67] Memorandum from U.S. Air Force Operations and Int'l L. Div., to Staff Judge Advocate, U.S. Air Force Comm. Agency, subject: Legal Issues Related to "Network as a Weapon System" (13 May 2005) (on file with author).

[68] Poulsen, *supra* note 58.

through computer systems under the jurisdiction of a neutral state, a strict construction of the law of neutrality would result in that state's neutrality being violated."[69] This evolution in thought should concern the United States, because as cyber conflict increases it is likely that the United States will see increased incursions on or across its Internet assets.

A surrender of neutrality or acquiescence to belligerent activity may draw a neutral state into the conflict.[70] Under this rule, if a neutral state cannot or does not take action to halt a cyber attack, a belligerent may choose to counter by physically attacking the neutral state's communications infrastructure. Thus, even without the physical violation of a neutral state's territory, a cyber attack may force a neutral state to become unwillingly involved. This loss of non-belligerent status is precisely what the Hague laws of neutrality seek to avoid. In short, although there is a growing body of legal thought, the concept of cyber neutrality remains ill-defined under current U.S. and international law. U.S. planners will likely see an increase in the number of situations where U.S. cyber neutrality is brought into question. The challenge for U.S. strategists is how to plan for cyber neutrality with little precedence.

Neutrality law also defines a limited telecommunications exception. Under Article VIII of the 1907 Hague Convention V, "[a] neutral Power is not called upon to forbid or restrict the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraphy apparatus," so long as the neutral state impartially permits the use of those structures by all belligerents.[71] The United States interprets this article as applying to modern communications.[72] Article VII implies that as long as a neutral party allows all belligerents equal passage on its communications infrastructure, neutrality is not violated. However, legal experts question whether the Article VIII exception applies to modern IT systems which can generate and transmit malicious data packets from, or across, a neutral party's Internet infrastructure to attack another belligerent's computer systems.[73]

Cyber neutrality may be defined as the right of any state to maintain relations with all parties in a cyber conflict, and the right not to

---

[69] William J. Bayles, *The Ethics of Computer Network Attack*, PARAMETERS, Spring 2001, at 44, 44-45, *available at* http://www.carlisle.army.mil/usawc/Parameters/01spring/bayles.htm.

[70] Hague Convention V, *supra* note 33, art. 8.

[71] *Id.*

[72] DEP'T OF DEF. OFFICE OF GEN. COUNSEL, AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS (1999), *available at* http://www.au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf (last visited Sept. 7, 2009); *see also* Roger D. Scott, *Legal Aspects of Information Warfare: Military Disruption of Telecommunications*, 45 NAVAL L. REV. 57, 62 (1998).

[73] Kelsey, *supra* note 3, at 1442.

support or take sides with any cyber belligerent. Under a traditional international law rubric, to remain neutral in a cyber conflict, a cyber neutral state must not originate a cyber attack, and it must also, within its capabilities, take action to prevent a cyber attack from transiting its Internet nodes.[74] A neutral state also has the obligation to police its peoples from independently taking action. Admittedly, this may be difficult in states which emphasize the almost unlimited right of free speech, but, if a neutral state takes no action, it risks losing its cyber neutral status. The U.S. Constitutional framework is more than adequate to allow for appropriate action.

IV. CASE STUDY: THE CYBER ATTACK ON GEORGIA CONSEQUENCES FOR U.S. CYBER NEUTRALITY

On July 19, 2008, unknown persons used a computer located at a U.S. ".com" Internet protocol address[75] to command and control (C2) a DDoS attack against the website of Georgia's president, Mikheil Saakashvili.[76] The DDoS attack rendered the Georgian website inoperable for over 24 hours. Some security analysts speculate that this DDoS attack may have been a dress rehearsal for larger cyber operations against Georgia that ensued later in August 2008.[77] Analysts were unable to pinpoint the party who controlled the U.S. computer. However, cyber security experts identified the C2 server as a MachBot DDoS controller written in Russian and frequently used by Russian hackers. Therefore, analysts speculated on ties to Russia.[78]

---

[74] *Id.* at 1443.

[75] A computer with a ".com" Internet address implies a commercial entity; a ".gov" Internet address is reserved for U.S. Government use. Use of a ".com" computer in this specific DDoS attack implies the computer was not under direct U.S. government control.

[76] Adair, *supra* note 7; *see also* Dancho Danchev, *Georgia President's Web Site Under DDoS Attack From Russian Hackers*, ZDNET, July 22, 2008, http://blogs.zdnet.com/security/?p=1533 (last visited Sept. 7, 2009); John Markoff, *Before the Gunfire, Cyberattacks*, N.Y. TIMES, Aug. 13, 2008, at A1, *available at* http://www.nytimes.com.

[77] Markoff, *supra* note 13.

[78] Adair, *supra* note 8. Adair writes,

> [Although] DDoS attacks against various other neighbors of Russia to include Estonia have been quite popular in the last few years . . . we do not have any solid proof that the people behind this C&C [C2] server are Russian. However, the HTTP-based botnet C2 server is a MachBot controller, which is a tool that is frequently used by Russian bot-herders. On top of that, the domain involved with this C2 server . . . does tie back to Russia . . . . This server recently came online in the past few weeks and has not issued any other attacks . . . all attacks we have observed have been directed right at www.president.gov.ge.

Id.

The COE Convention characterizes the July 2008 DDoS attack against Georgia as cyber crime, not cyber war.[79] Within the COE Convention construct, the United States should have taken action under Article II (illegal access) and Article IV (system interference) to prevent the DDoS attack, a crime against Georgia.[80] Apparently, the attack stopped only after a private company took action on its own and blocked access to the U.S computer that controlled that DDoS attack.[81] The implication is that the international community prefers viewing DDoS attacks as criminal in nature. The result has been a growing body of cybercrime law, yielding additional clarity and cooperation. In fact, the U.S. Department of Justice successfully prosecuted several cases over the past two years involving DDoS attacks.[82] From the COE Convention's perspective, Interpol, rather than NATO, would have been the proper response to the Estonian (April 2007) and Georgian (July 2008) DDoS attacks. This same level of clarity is lacking when the nature of a cyber event changes from criminal to war between nation states.

On August 8, 2008, cyber security experts observed a second wave of DDoS attacks against Georgian websites.[83] This time, analysts speculate that the attacks coincided with Russia's movement of military forces into South Ossetia. Some have even characterized this incident as the first time a known cyber attack coincided with a "ground war."[84] The DDoS attack spread to computers throughout the Georgian government.[85] The Georgian Foreign Ministry blamed Russia for the

---

[79] *United States Joins Convention on Cybercrime*, *supra* note 63; *see also* COE Convention, *supra* note 63.

[80] Korns & Kastenberg, *supra* note 1, at 63.

[81] Adair, *supra* note 8.

[82] *See, e.g.*, *Botherder Dealt Record Prison Sentence for Selling and Spreading Malicious Computer Code*, U.S. DEP'T OF JUSTICE, May 8, 2006, http://www.cybercrime.gov/anchetaSent.htm (last visited Sept. 7, 2009) ("Concluding the first prosecution of its kind in the United States, [U.S. v. Ancheta], a well known member of the 'botmaster underground' was sentenced this afternoon to nearly five years in prison for profiting from his use of botnets--armies of compromised computers--that he used to launch destructive attacks . . . [the defendant] was sentenced to 57 months in federal prison . . . the longest known sentence for a defendant who spread computer viruses.); *see also Operator of a 'Bot-net' Network of Thousands of Virus-Infected Computers Sentenced to 12 Months in Federal Prison*, U.S. DEP'T OF JUSTICE, Oct. 23, 2007, http://www.cybercrime.gov/downeySent.pdf (last visited Sept. 7, 2009); *Indictment and Arrest for Computer Hacking*, U.S. DEP'T OF JUSTICE, Oct. 1, 2007, http://www.cybercrime.gov/kingIndict.pdf (last visited Sept. 7, 2009).

[83] Korns & Kastenberg, *supra* note 1, at 65.

[84] Markoff, *supra* note 13; *see also* Brandon Griggs, *U.S. at Risk of Cyberattacks, Experts Say*, CNN.COM, Aug. 18, 2008, http://www.cnn.com (last visited Sept. 7, 2009).

[85] Adair, *supra* note 8; *see also Russian Business Network (RBN) Now Nationalized, Invades Georgia Cyber Space*, RUSSIAN BUS. NETWORK, Aug. 9, 2008, http://rbnexploit.blogspot.com/2008/08/rbn-georgia-cyberwarfare.html (last visited Sept. 7, 2009); Waterman, *supra* note 10.

attacks.[86] Others pointed to the Russian Business Network (RBN), a criminal syndicate suspected of being under Russian government influence.[87] Conversely, an Internet journalist visited a website where he downloaded pre-packaged software that enabled him within minutes—had he chosen to do so—to join in the DDoS attacks against Georgia. His assessment:

> In less than an hour, I had become an Internet soldier. I didn't receive any calls from Kremlin operatives; nor did I have to buy a Web server or modify my computer in any significant way . . . [m]y experiment also might shed some light on why the recent cyberwar has been so hard to pin down . . . . Paranoid that the Kremlin's hand is everywhere, we risk underestimating the great patriotic rage of many ordinary Russians, who . . . are convinced they need to crash Georgian Web sites. Many Russians undoubtedly went online to learn how to make mischief, as I did. Within an hour, they, too, could become cyber-warriors.[88]

Some cyber security analysts have concluded that the August 2008 DDoS attack against Georgia was a mix of government incentivized, organized cyber crime syndicates such as RBN, as well as ordinary cyber-citizen protestors.[89] Gadi Evron, former head of cyber security for the Israeli government, stated "this is not warfare, but just some unaffiliated attacks by Russian hackers."[90] Arbor Networks, a security firm, "found no evidence . . . of state-sponsored cyber-warfare"

---

[86] *Cyber Attacks Disable Georgian Websites*, MINISTRY OF FOREIGN AFF. OF GEORGIA, Aug. 11, 2008, http://georgiamfa.blogspot.com/2008_08_01_archive.html (last visited Sept. 7, 2009).

[87] *RBN Now Nationalized*, RUSSIAN BUS. NETWORK, Aug. 9, 2008, http://rbnexploit.blogspot.com/2008/08/rbn-georgia-cyberwarfare.html (last visited Sept. 7, 2009).

[88] Evgeny Morozov, *An Army of Ones and Zeroes - How I Became a Soldier in the Georgia-Russia Cyberwar*, SLATE, Aug. 14, 2008, http://www.slate.com/id/2197514 (last visited Sept. 7, 2009); *see also* Evgeny Morozov, http://evgenymorozov.com/blog/?p=416 (last visited Sept. 7, 2009).

[89] Waterman, *supra* note 10; *see also* Dancho Danchev, *Coordinated Russia vs Georgia Cyber Attack In Progress*, ZDNET, Aug. 11, 2008, http://blogs.zdnet.com/security/?p=1670 (last visited Sept. 7, 2009); Joel Hruska, *Russians May Not be Responsible for Cyberattacks on Georgia*, ARS TECHNICA, Aug. 13, 2008, http://arstechnica.com (last visited Sept. 7, 2009).

[90] Gadi Evron, *Internet Attacks Against Georgian Websites*, CIRCLEID, Aug. 11, 2008, http://www.circleid.com/posts/88116_Internet_attacks_georgia (last visited Sept. 7, 2009).

and characterized the attackers as most likely "non-state actors."[91] Experts at cyber security firm Shadowserver indicated "it would appear that these cyber attacks have certainly moved into the hands of the average computer using citizen."[92]

While receiving less attention than analysis of the DDoS attacks against Georgia, perhaps of greater importance to U.S. policy makers is the Georgian government's novel reaction. If the responsibilities of states during cyber conflict are somewhat unclear, they are even more ambiguous when a belligerent seeks cyber refuge in a neutral state's territory.

Tulip Systems (TSHost) is a private web hosting company in Atlanta, Georgia. On August 8, while in the country of Georgia, the owner of TSHost apparently contacted Georgian government officials directly and offered assistance.[93] That the owner of TSHost is a U.S. resident of Georgian birth cannot be overlooked.[94] On August 9, the Georgian government transferred critical governmental Internet services to TSHost servers in the United States, including the Georgian President's website. In an admission, the TSHost Chief Executive Officer (CEO) stated that the company had volunteered its servers to "protect" the nation of Georgia's Internet sites from malicious traffic.[95] TSHost further revealed that after it relocated Georgian websites to the United States, DDoS attacks, traced to Moscow and St. Petersburg, ensued against TSHost's servers.[96] The TSHost CEO confirmed the company reported the attacks to the FBI, but he did not claim to obtain government sanction for his activities.

This important fact is not widely publicized: a U.S. company with no clear authority and no apparent U.S. government approval

---

[91] Kelly Jackson Higgins, *Botnets Behind Georgian Attacks Offer Clues*, DARK READING, Sept. 9, 2008, http://www.darkreading.com/document.asp?doc_id=163342 (last visited Sept. 7, 2009).

[92] Adair, *supra* note 8 ("Since August 8, 2008, a large number of Georgian websites, both government and non-government alike, have come under attack...one of the Georgian government websites was being attacked by dozens of Russian computers from several different ISPs throughout the country... lots of ICMP traffic and Russian hosts sounds a lot more like users firing off the 'ping' command...much like in the attacks against Estonia, several Russian blogs, forums, and websites are spreading a Microsoft Windows batch script that is designed to attack Georgian websites...it would appear that these cyber attacks have certainly moved into the hands of the average computer using citizen."); Korns & Kastenberg, *supra* note 1, at 66. A redacted version of the actual software script used in the DDoS attacks is also available at the site hosting Adair's article.

[93] Peter Svensson, *Russian Hackers Continue Attacks on Georgian Sites*, AP NEWS, Aug. 12, 2008, http://www.usatoday.com/tech/products/2008-08-12-2416394828_x.htm (last visited Sept. 7, 2009); *see also* Griggs, *supra* note 84; Korns & Kastenberg, *supra* note 1, at 63; Svensson, *supra* note 13.

[94] Korns & Kastenberg, *supra* note 1, at 63.

[95] Griggs, *supra* note 84.

[96] Svensson, *supra* note 13.

directly contacted the Georgian government and arranged to protect its Internet assets by moving them to U.S. territory.[97] Undeterred, cyber attackers followed and turned their DDoS attacks against the U.S. site. As a result of TSHost actions, the U.S. effectively experienced cyber collateral damage.[98]

On August 8, the Georgian government sought additional protection within the United States by transferring its official MFA and government news sites to Google's Blogspot.[99] While Georgia's combat troops were retreating to Tbilisi to defend the capital, Georgia's cyber forces were turning to the United States to defend the country's Internet capabilities. Google effectively became the cyber refugee camp for Georgia's cyber property.[100] The Georgian government used equipment located in U.S. territory—specifically Google's Internet servers in California—to protect its Internet capabilities and ensure continued war-time communications with its citizens and forces. Georgia's creative cyber strategy relied on relocation to the United States because the Georgian government did not believe DDoS attackers could take down Google's servers, given the company's vast infrastructure and ability to defend it.[101] It does not appear that the Georgian government coordinated this strategy with the U.S. prior to execution. There were also accusations, later refuted, that Google removed details of Georgian maps from its on-line mapping service.[102]

In the Georgian-Russian cyber conflict, the actions of the Georgian government and a well-intentioned, patriotic CEO could have imperiled U.S. cyber neutrality. Apparently, neither Google's nor TSHost's actions had U.S. government involvement or approval.[103]

As noted above, Article III of Hague Convention V forbids belligerents from erecting on the territory of a neutral Power a wireless

---

[97] Korns & Kastenberg, *supra* note 1, at 67.

[98] *Id.*

[99] Jon Swaine, *Georgia: Russia Conducting Cyber War*, TELEGRAPH, Aug. 11, 2008, http://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/-Georgia-Russia-conducting-cyber-war.html (last visited Sept. 7, 2008); *see also* Larry Dignan, *Georgia Turns to Google's Blogger to Counter Alleged Cyber Attack*, SEEKING ALPHA, Aug. 11, 2008, http://seekingalpha.com (last visited Sept. 7, 2009); Pete Swabey, *Google Embroiled in Georgian Conflict*, INFO. AGE, Aug. 12, 2008, http://www.information-age.com (last visited Sept. 7, 2009).

[100] Korns & Kastenberg, *supra* note 1, at 67.

[101] *Id.*

[102] *Id.*; *see also* Dave Barth, *Where is Georgia on Google Maps?*, GOOGLE LAT LONG BLOG, Aug. 12, 2008, http://google-latlong.blogspot.com/2008/08/where-is-georgia-on-google-maps.html (last visited Sept. 7, 2009); *see also* Miguel Helft, *Google: We Did Not Erase Maps of Georgia*, N.Y. TIMES BITS BLOG, Aug. 12, 2008, http://bits.blogs.nytimes.com/2008/08/12/google-we-did-not-erase-maps-of-georgia (last visited Sept. 7, 2009); Katie Hunter, *Tuesday Map: Georgia's Google Vanishing Act*, FOREIGN POL'Y: PASSPORT, Aug. 12, 2008, http://blog.foreignpolicy.com/node/9515 (last visited Sept. 7, 2009).

[103] Korns & Kastenberg, *supra* note 1, at 68.

telegraphy station or other apparatus for the purpose of communicating with belligerent forces on land or sea.[104] One could argue that the Georgian government, as a cyber belligerent, violated this law when it established websites on U.S. cyber neutral territory, and then used the websites as "other apparatus" to communicate with its forces back in the territory of Georgia. The United States took no action to halt these operations. Further, it did not direct TSHost or Google to terminate support for Georgia. By allowing U.S. private companies to protect the Georgian government's Internet assets, one could make the case that the U.S. government jeopardized, or even relinquished, its cyber neutrality, and subjected the U.S. cyber infrastructure to potential attack.

Added to this issue, cyber corps or cyber warriors are terms often used in reference to U.S. government civilian and military personnel who conduct cyber operations.[105] This military nomenclature may be problematic. Given that the U.S. private industry operates the majority of the Internet, there is concern as to whether the category of cyber combatant could be extended to include private civilians operating the Internet.[106] When speaking about the success of her company in blocking DDoS attacks against Georgia's website, the TSHost CEO stated, "our people aren't getting any sleep."[107] Article IV of Hague V prohibits neutrals from forming "corps of combatants" to assist belligerents. Although unlikely, TSHost and Google actions could be interpreted as a violation of Hague V in that they formed a quasi-corps of cyber combatants on behalf of the U.S. government to protect Georgia's Internet assets.

Hague V Articles VIII and IX provide that a neutral state is not required to restrict a belligerent's use of the neutral's telecommunications systems, as long as these services are provided impartially to all belligerents.[108] The U.S. government could have required TSHost and Google to terminate Internet services for the Georgian government. By its silence, the U.S. government may have unknowingly established an unwanted precedence. Conceivably, future cyber belligerents, taking note of U.S. inaction in the Georgian case, could under the Hague V impartiality clause (Article IX) demand similar cyber refuge, or use of U.S. Internet infrastructure. The potential implications are disturbing.

---

[104] Hague Convention V, *supra* note 42, art. 3.

[105] *Fact Sheet: Protecting America's Critical Infrastructure – Cyber Security*, DEP'T OF HOMELAND SEC., Feb. 15, 2005, http://www.dhs.gov/xnews/releases/ (last visited Sept. 7, 2009); DEP'T OF DEF. CHIEF INFORMATION OFFICER, ANNUAL INFORMATION ASSURANCE REPORT ES-1 (2000), *available at* http://stinet.dtic.mil/cgi-bin/ ("The new warfighter is the cyber-warrior with technical and non-traditional skills").

[106] Intoccia & Moore, *supra* note 13, at 1.

[107] Svensson, *supra* note 13.

[108] Hague Convention V, *supra* note 42, art. 3.

Clearly, the Georgian and Russian governments were conventional belligerents in the Ossetian theater of conflict. It is unclear, however, if they were cyber belligerents. When bombs and bullets fly, identification is relatively easy; not so for cyber weapons. Both governments claim they did not participate in the DDoS attacks.[109] Expert analysis appears to substantiate, to a degree, that technically the governments themselves did not directly participate in cyber conflict.[110] The July and August DDoS attacks could be characterized as cyber conflict by proxy. Instead of states, it appears that cyber criminals as well as hundreds of loosely self-organized, non-combatant citizens and self-styled cyber-militias inflicted the attacks. This leads to uncertainty as to which attackers were officially cyber belligerents, and which ones were cyber neutrals.

Existing international laws of war focus primarily on conflicts between nation states, and are fundamentally weak in addressing non-state actor participation in cyber conflict. The 2007 Estonian cyber event serves as a superb case study. Although it was originally called cyber war, this changed in the post conflict retrospective analysis. Governments and experts concluded that unknown, non-state actors conducting DDoS attacks against a Baltic nation-state is not cyber war; at best, according to Estonian officials, it is terrorism.[111] The DDoS attacks against Georgia were strikingly similar to the Estonian case, and therefore place in doubt whether an actual state of cyber conflict existed between the governments of Georgia and Russia. This interpretation certainly raises questions regarding the legal status of U.S. cyber neutrality. The Georgian case stands as the latest example of the untidy nature of cyber conflict. Clearly, the Estonian and Georgian cyber events have established new precedents and subtexts for cyber war and neutrality.

The terms "cyberspace" and "global electronic village" imply that the Internet is a stateless and borderless entity used by all and owned by none.[112] Some in the legal community have used these notions to define cyberspace as a "separate place," governed by its own legal framework, where international treaties don't apply and governments have yielded sovereignty to "netizens" and self-regulatory initiatives.[113] These symbolic notions do not stand up to reality. The

---

[109] Korns & Kastenberg, *supra* note 1, at 70.

[110] *Id.*

[111] *See, e.g., EU Should Class Cyber Attacks as Terrorism*, *supra* note 66; Hruska, *supra* note 66; Kirk, *supra* note 66.

[112] *See, e.g.,* David Howes, *e-legislation: Law-Making in the Digital Age*, 47 MCGILL L.J. 39, 41-44 (2001).

[113] *See, e.g.,* John Perry Barlow, *A Declaration of the Independence of Cyberspace*, ELECTRONIC FRONTIER FOUND., Feb. 8, 1996, http://www.eff.org/~barlow/Declaration-Final.html (last visited Sept. 7, 2009); Michael Geist, *Cyberlaw 2.0*, 44 BOSTON

Internet in fact does have borders. Internet equipment is government or corporate owned. Internet assets are located in facilities within the territories of recognized nation states. Internet equipment is connected to national electric grids.[114]

When the government of Georgia relocated its Internet capabilities to TSHost and Google servers, it did not move its cyber assets to "space"; rather, it moved actual government data and information capabilities to equipment located in the states of Georgia and California, within U.S. territory. Under traditional Hague V Conventions, this act could be interpreted as a violation of U.S. neutrality. Nonetheless, there remains a lack of international agreement on how "border-centric" laws relate to the notion of a "borderless" Internet. This impinges on the cyber neutrality concept, which is built upon the traditional notion of absolute, recognizable borders.

V. CONCLUSION

As noted in the introduction, this article does not advocate that the United States must enforce neutrality in cyberspace in conflicts to which it is not a party. It does argue, however, that based on the current and future nature of interstate conflict, the executive branch should consider whether it is in the national interest to assert its authority to enforce neutrality in cyberspace. This is important because belligerent governments may consider U.S. corporations assisting their opponent states as a legitimate target for a cyber counter-strike (or perhaps a kinetic strike). Whether the executive branch determines that cyber neutrality is important to advocate for as an international law principle is outside the scope of this article as well. However, it is clear that the executive branch should be prepared to assert its Constitutional authority to enforce cyber neutrality before two belligerent states enter into conflict. And, commensurate with this authority, the federal government can organize and train to preserve this neutrality should the need arise.

COLLEGE L. REV. 323 (2003); David R. Johnson & David Post, *Law and Borders: The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996).

[114] *See, e.g.*, Dan Jerker B. Svantesson, *Borders on, Border Around – The Future of the Internet*, 16 ALB. L.J. SCI. & TECH. 433, 434-35 (2006).