Georgia's Cyber Left Hook

STEPHEN W. KORNS and JOSHUA E. KASTENBERG

"In the very near future, many conflicts will not take place on the open field of battle, but rather in spaces on the Internet, fought with the aid of information soldiers . . . . This means that a small force of hackers is stronger than the multi-thousand force of the current armed forces."

– Former Duma member Nikolai Kuryanovich[1]

On 19 July 2008 an Internet security firm reported a distributed denial of service (DDoS) cyber attack against Web sites in the country of Georgia.[2] Three weeks later, on 8 August, security experts observed a second, more substantial round of DDoS attacks against Georgian Web sites. Analysts noted that these additional DDoS attacks appeared to coincide with the movement of Russian troops into South Ossetia in response to Georgian military operations launched a day earlier in the region. By 10 August the DDoS attacks had rendered most Georgian governmental Web sites inoperative.[3]

As a result of these attacks, the Georgian government found itself cyber-locked, barely able to communicate on the Internet. In response, the government took the unorthodox step of seeking cyber refuge in the United States. Without first obtaining US government approval, Georgia relocated critical official Internet assets to the United States, Estonia, and Poland.[4]

Georgian-Russian hostilities in South Ossetia have generated a substantial amount of analysis and speculation regarding the accompanying cyber conflict.[5] Most of the focus has centered on identifying the parties who conducted the cyber attacks. The Georgian cyber event provides an intriguing opportunity to examine a more subtle and perhaps overlooked aspect of cyber conflict—the concept of cyber neutrality. The Georgian case

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2008		**00-00-2008 to 00-00-2008**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Georgia's Cyber Left Hook	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **US Army War College,ATTN: Parameters,47 Ashburn Drive,Carlisle,PA,17013**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**17**	

raises two fundamental questions: (1) How did the combined actions of the Georgian government and US information technology (IT) companies impact American status as a cyber neutral? (2) Can the United States remain neutral (or cyber neutral) during a cyber conflict?

The underlying implications of the overall issue should be of great concern to US policymakers and strategists. Even if the United States is not a belligerent in a cyber conflict, incursions against the US Internet infrastructure are likely. Private industry owns and operates the majority of the Internet system. During a cyber conflict, the unregulated actions of third-party actors have the potential of unintentionally impacting US cyber policy, including cyber neutrality. There is little, if any, modern legal precedent. The fact that American IT companies provided assistance to Georgia, a cyber belligerent, apparently without the knowledge or approval of the US government, illustrates what is likely to become a significant policy issue. Although nations still bear ultimate responsibility for the acts of their citizens, applying that dictum to the modern realities of cyber conflict is a complex challenge. Georgia's unconventional response to the August 2008 DDoS attacks, supported by US private industry, adds a new element of complication for cyber strategists.

Cyber Neutrality: A Basic Rubric

In the United States, the executive branch can choose to follow a neutrality policy as a matter of its constitutional authority regarding foreign relations. In 1908, Woodrow Wilson, then president of Princeton University, posited, "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."[6] At the beginning of World War I, President Wilson declared the United States a neutral nation, yet American banks provided loans to Britain

---

Colonel Stephen W. Korns, USAF, is the Vice Director of Strategy, Plans, Policy, and International Relations for the Joint Task Force-Global Network Operations (JTF-GNO/J5). He assists in development of cyber policy and strategy for operations and defense of Department of Defense networks, including the Global Information Grid.

Major Joshua E. Kastenberg, USAF, is the JTF-GNO Staff Judge Advocate. He previously served as the Chief, Law of War Branch, Air Force Office of the Judge Advocate General.

---

and France, and American industry sold armaments to those nations. The German government eventually responded by waging submarine warfare and maritime commerce raiding against the United States. Wilson's neutrality stance was more rhetorical than real, in that he did not exercise executive authority to halt US loans and arms shipments to belligerents. More than half a century later, Supreme Court Justice William O. Douglas would pen sentiments similar to Wilson's: "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."[7]

Although the executive branch is preeminent in foreign policy, Congress retains the authority to regulate foreign commerce, and the Senate must consent before any treaty may obligate the United States. In the early twentieth century, the Supreme Court determined that neither individual states nor private corporations possess the authority to act contrary to a treaty. If the US government establishes a strict position of neutrality, American industry may provide nonmilitary and humanitarian support to a belligerent, but firms are required to halt all commerce that militarily aids a combatant.[8] When a corporation violates this prohibition, it may be subject to criminal sanctions.

For the purposes of this article, cyber neutrality stems from the Hague (V) Conventions of 1907, which require combatant nations to recognize the rights of neutrals.[9] Neutrality law affords nations the right to maintain relations with all belligerents; however, neutral countries are expected to refrain from assisting either side in a conflict, other than to effectuate peace. Nations that declare themselves to be neutral, and act accordingly, are entitled to immunity from attack. The Hague Conventions also dictate that the territory of a neutral nation is inviolable. Belligerents may not move forces, weapons, or war materiel across a neutral country's territory, or conduct hostilities within a neutral's territory, waters, or airspace. A neutral nation jeopardizes its status if it permits belligerents to engage in such violations. In a 1917 decision, the US Supreme Court cemented this framework into American jurisprudence.[10]

Cyber neutrality, therefore, is the right of any nation to maintain relations with all parties engaged in a cyber conflict. Under a traditional international law rubric, to remain neutral in a cyber conflict a nation cannot originate a cyber attack, and it also has to take action to prevent a cyber attack from transiting its Internet nodes.[11] These stipulations may be difficult

to implement in the United States, where the constitutional framework emphasizes the right of free speech. Nonetheless, if a neutral nation takes no action against parties that violate its territory, it risks losing its cyber neutral status.

As an emerging form of conflict, cyber war and cyber neutrality are not explicitly addressed under current international law.[12] The international community remains unsettled on whether cyber techniques such as DDoS are legally considered "weapons,"[13] and whether cyber attacks can be considered legitimate acts of "armed" conflict.[14] Malicious software, or malware, is not considered an "arm" of war, yet the effects of cyber attacks can potentially be equal to kinetic attacks. Arguably, a cyber attack that causes physical damage might constitute an "armed attack" under the United Nations Charter.[15] In fact, the International Telecommunication Union (ITU) posits that cyber attacks "could in theory be treated as acts of war and be brought within the scope of arms control or the laws of armed conflict."[16]

Proponents who view malware as weapons argue that cyber attacks effectively transmit an actual weapon across the Internet.[17] 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."[18] A 2005 ITU report states that "cyber-weapons are easily copied and distributed on the Internet."[19] A 2006 Defense Science Board report identifies the US military network as "a critical weapon system."[20] A 2006 *Harvard International Review* article labels cyber threats as "a new weapon."[21] In January 2007, the United States Patent and Trademark Office issued a patent for "the public network weapons system," effectively recognizing the Internet protocol (IP) as a weapon system component.[22] During the April 2007 Estonian cyber event, the Estonian Defense Minister contemplated invoking Article 5 of the North Atlantic Treaty, which considers an "armed attack" against any North Atlantic Treaty Organization (NATO) member to be an attack against all members.[23] In April 2007 testimony before the US Congress, the president of the Professionals for Cyber Defense stated that "cyber attack weapon(s) . . . may well be deployed already."[24]

Conversely, skeptics stress that few international legal precedents recognize cyber weapons and point to the Law of Armed Conflict as being unclear with respect to cyber attacks.[25] There is a basis for this view. The 2001 Council of Europe Convention on Cybercrime (COE Convention), to which the United States is a party, omits any reference to the terms "cyber

attack" or "cyber weapons."[26] A gun, universally recognized as a weapon, can be used to commit a crime. The COE does not extend this weapon analogy to cyber tools. Instead, the COE Convention considers as criminal acts "damaging, deleting, deteriorating, altering, or suppressing computer data."[27] In 2005, the US Air Force Judge Advocate General published a memorandum stating "the network is not a weapon system."[28] NATO defense ministers declined to declare the 2007 Estonia cyber event as an attack requiring military action.[29] In June 2008, James Lewis of the Center for Strategic and International Studies stated that DDoS attacks are "more commonly used for illicit activities like committing online fraud than for cyber war."[30] Kevin Poulsen, an infamous reformed hacker and cyber security consultant, observed in August 2008 that "there are good reasons to reject the idea that timeout errors (DDoS) are an act of war."[31] In short, until the haze regarding the nature of cyber attacks is dispersed, many observers in the legal and technical communities continue to view DDoS events as matters for the criminal justice system, not the national defense system, to resolve.

Although the debate over cyber conflict remains active, the international law community does appear to be coalescing around the general concept that use of the Internet to conduct cross-border cyber attacks violates the principle of neutrality. Legal scholar Davis Brown notes: "When an information packet containing malicious code travels through computer systems under the jurisdiction of a neutral nation, a strict construction of the law of neutrality would result in that nation's neutrality being violated."[32] Lawrence Greenberg emphasizes: "A belligerent violates neutrality law when it launches a cyber attack that crosses the Internet nodes of a neutral state."[33] Jeffrey Kelsey further argues: "The text of the 1907 Hague Convention (V) . . . support(s) the view that cyber attacks crossing the Internet nodes of neutral states violate international humanitarian law."[34] Even with this growing body of thought, the challenge for US cyber strategists is how to plan, with little prior experience, for increased cyber incursions that will undoubtedly bring American cyber neutrality into question.

Consequences for US Cyber Neutrality

On 19 July 2008 unknown parties used a computer located at a United States ".com" IP address[35] to command and control (C2) a DDoS

attack against the Web site of Georgia's President, Mikheil Saakashvili.[36] The DDoS attack overwhelmed the Georgian Web site. Although unable to pinpoint the party that seized the US computer, experts were able to identify the software as a "MachBot" DDoS controller written in Russian and frequently used by Russian hackers. Therefore, analysts speculated the attack had ties to Russia.[37]

The COE Convention, in Article 4 (data interference) and Article 5 (system interference), characterizes this type of attack as cyber crime, not cyber war. As such, the US Department of Justice (DOJ) might have pursued criminal action. Prior examples exist, as the DOJ has successfully prosecuted several criminal cases during the past two years involving DDoS attacks.[38] From the COE Convention's perspective, an investigation by Interpol, rather than NATO, would have been the proper response to both the Estonian (April 2007) and Georgian (July 2008) DDoS attacks. The Assistant Director of the US Federal Bureau of Investigation's (FBI) Cyber Division recently confirmed this view when he stated that the FBI is "seeing an increase in the use of botnets . . . to commit cybercrime."[39] The result has been a growing body of cybercrime law, yielding additional clarity for law enforcement agencies and prosecutors. This same level of clarity is lacking when the nature of a cyber event changes from cyber crime to apparent cyber war.

On 8 August cyber security experts observed a second, much larger wave of DDoS attacks against Georgian Web sites. The experts speculated that these attacks were associated with Russia's movement of military forces into South Ossetia. Some analysts even declared this incident was the first time a cyber attack had coincided with a conventional shooting war.[40] Others characterized the Georgian cyber incident as "the birth of true, operational cyber warfare" and "the most significant development ever seen in . . . cyber conflict studies."[41] The DDoS attack spread to computers throughout the Georgian government.[42] The Georgian Foreign Ministry blamed Russia for the attacks.[43] Others pointed to the Russian Business Network, a criminal syndicate suspected of being under direct Russian government influence.[44] Conversely, an Internet journalist accessed a Web site and downloaded prepackaged software that would have enabled him, had he chosen to do so, to join in the attacks. His assessment:

> In less than an hour, I had become an Internet soldier. I didn't receive any calls from Kremlin operatives . . . . Paranoid that the Kremlin's hand is everywhere, we risk underestimating the great patriotic rage of many ordinary Russians, who . . . undoubtedly went online to learn how to make mischief, as I did. Within an hour, they, too, could become cyber warriors.[45]

Project Grey Goose, an organization of 100 volunteer US security experts from government and the private sector, conducted a comprehensive investigation into the cyber attacks. Grey Goose investigator Jeff Carr stressed that "the level of advance preparation and reconnaissance strongly suggests that Russian hackers were primed for the assault by officials within the Russian government."[46] While Grey Goose members did not find a direct link between Russian government officials and the hackers, they claim it is unreasonable to assume that no such connection existed.

Most cyber security experts have generally concluded that an amalgam of government-incentivized agents, hackers, and cyber-citizen protestors carried out the 2008 DDoS attacks.[47] Gadi Evron, former head of cyber security for the Israeli government, stated, "This is not warfare, but just some unaffiliated attacks by Russian hackers."[48] Arbor Networks, a well-respected security firm, "found no evidence" of government-sponsored cyber warfare.[49] 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."[50] Bobbie Johnson of *The Guardian* commented that "many of these strikes seem to be cases of so-called 'hacktivism' . . . (a) collective grassroots movement—a sort of 'click for victory' campaign."[51] Although there are other competing classified intelligence views, they are beyond the scope of this article.

While a great deal of effort has been applied to identifying the parties that conducted the cyber attacks against Georgia, perhaps of greater importance to US policymakers is the Georgian government's innovative reaction. This element of the Georgia-Russia cyber conflict has received less attention, yet potentially does have significant implications for US cyber policy. If the responsibilities of nations are somewhat unclear during cyber conflict, they are even more ambiguous when a belligerent takes cyber refuge in a neutral country's territory.

Tulip Systems (TSHost) is a private Web hosting company in Atlanta, Georgia. On 8 August 2008, while in the nation of Georgia, the owner of TSHost apparently contacted Georgian government officials and offered

assistance in reconstituting Georgian Internet capabilities.[52] A day later the Georgian government transferred critical cyber capabilities to TSHost servers in the United States, including the Web sites of Georgia's President and the Ministry of Defense.[53] In a startling 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.[54] TSHost further revealed that after it relocated Georgian Web sites to the United States, DDoS attacks ensued against the company's servers.[55] The TSHost CEO confirmed the company reported the attacks to the FBI, but at no point did he claim to have obtained government sanction for his activities.[56]

An important aspect of the Georgia-Russia conflict is not widely known: An American company, with no clear authority and no apparent US government approval, directly contacted the Georgian government and arranged to protect its Internet assets by moving them to US territory. While Georgia's combat troops retreated to Tbilisi to defend the capital, the nation's cyber forces retreated to the United States to defend their capabilities. Undeterred, cyber attackers followed and turned their DDoS attacks against the US site. As a result of TSHost's actions, the United States effectively experienced cyber collateral damage.

The Georgian government also sought additional protection within the United States by transferring its Ministry of Foreign Affairs media releases and government news sites to Google's Blogspot.[57] Google became an additional cyber refugee camp for Georgia. There were also accusations, later refuted, that Google, out of sympathy to Georgia, removed details of Georgian maps from Google's online mapping service.[58]

Implications

Using the 2008 Georgian cyber event as a case study, the authors seek to illuminate two issues regarding cyber neutrality. The first question is how did the combined actions of the Georgian government and private US companies impact America's cyber neutrality? Analysis of Georgia's reaction to the cyber attacks provides some insight.

The core feature of Georgia's creative cyber strategy was the belief that cyber attackers lacked the capability to defeat TSHost or Google's Internet security measures. During the conflict, an astute analyst noted that "Georgia has turned to using the Google Blogger service as a method of communication . . . and it has proved to be a sustainable resource.

Governments will need to have strategies in place to prepare for this type of attack."[59] When Estonia experienced cyber attack, it essentially defended in place; Georgia, on the other hand, maneuvered. Georgia relocated strategic IP-based cyber capabilities to America, thereby ensuring continued wartime communication with Georgian citizens and military forces. The Georgian government partially defeated the cyber attack by flowing a portion of its strategic C2 through the United States.

Arguably, cyber planners might hail Georgia's "cyber left hook" maneuver as a new precedent in strategic cyber operations. On the other hand, US policymakers have reason to be concerned. While Georgia's cyber tactics may have appeal operationally, the combined actions of the Georgian government and private US companies potentially imperiled US cyber neutrality. There is no evidence to suggest that the Georgian government coordinated its cyber strategy with the US administration. Although the US government was apparently not directly involved, the actions of Georgia, TSHost, and Google nevertheless gave the appearance of US political sanction. For example, one Internet media source reported that Georgia had found "allies" in reference to Georgia's use of international and US IT facilities during the conflict.[60] Before seeking cyber refuge in the United States, the Georgian government would have been well-served to inform the US Embassy in Tbilisi and afford the US government the opportunity to review the matter and consider its implications.

The second question is can the United States maintain cyber neutrality during cyber conflict? Unsettled legal protocol, compounded by the lack of prior precedents, impairs the ability to provide concrete answers. Analysis utilizing the neutrality elements of the Hague (V) Conventions, however, can provide additional insight.

Hague (V) Article 3 forbids belligerents from erecting on the territory of a neutral power a "wireless telegraphy station or other apparatus" for the purpose of communicating with belligerent forces. Georgia did not relocate its Internet capabilities to nebulous cyber "space;" rather, it moved them to equipment physically located in US territory. One possible argument is that the Georgian government, as a cyber belligerent, violated Hague (V) when it used Web sites in the United States as "other apparatus" to communicate with its military forces. By allowing these actions to continue after the media revealed Georgia's cyber transfer, the US government potentially jeopardized its cyber neutrality. Conversely, it is possible to argue that

private US IT firms simply engaged in routine commerce while assisting a foreign government to overcome the effects of a criminal act.

Article 4 of Hague (V) establishes that "corps of combatants" cannot be formed on the territory of a neutral power to assist belligerents. "Cyber corps" and "cyber warriors" are terms often used in reference to US government personnel who conduct cyber operations.[61] Given that private industry operates the majority of the Internet, there is concern as to whether the category of "combatant" could also be extended to civilian IT technicians during cyber conflict.[62] Speaking about the success of his company in defending Georgia's Web site, the TSHost CEO stated, "Literally, our people aren't getting any sleep."[63] The actions of TSHost and Google might be interpreted as a violation of Hague (V) in that they formed a quasi-corps of "cyber combatants" on US territory to assist Georgia, a presumed cyber belligerent.

According to Hague (V) Article 6, a neutral power is not held responsible when a person "crosses the frontier separately" to offer services to a belligerent. It may be argued that TSHost and Google "crossed the cyber frontier" without US government cognizance when they offered services to Georgia. Under this interpretation, the US government would be seen as innocent, and therefore American neutrality remained intact.

Hague (V) Article 7 holds that a neutral power is not required to "prevent the export or transport" of arms or munitions to belligerents. One may advance the case that Article 7 permits the export or provision of cyber services to belligerents. If that instance is true, TSHost and Google legally exported or transported Internet capabilities to Georgia without jeopardizing US cyber neutrality.

Hague (V) articles 8 and 9 establish that a neutral nation is "not required to restrict" a belligerent's use of a neutral's telecommunications systems if these services are provided impartially to all nations. The US government possibly may claim that it impartially allowed use of US cyber systems: in July 2008, to Russian-supported cyber attackers; and in August 2008, to the Georgian government. In doing so, however, the United States may have unknowingly established an undesired precedent. Conceivably, future cyber belligerents, taking note of US action in the Georgian case, might demand similar use of the US Internet infrastructure under the Hague (V) impartiality clause. The potential implications are disturbing.

Based on this analysis, it is clear that the United States can maintain cyber neutrality during cyber conflict, but it needs to be proactive in doing so. Ultimately, the single greatest peril to US cyber neutrality during the

Russian-Georgian conflict was the lack of US government assertiveness in establishing its official stance on cyber usage. During the conventional conflict, the United States proactively signaled its position by airlifting 2,000 Georgian troops from Iraq and delivering humanitarian aid to Georgian ports.[64] In addition, the US government-funded Voice of America (VOA) doubled its Georgian-language broadcasts to ensure that Georgians were "fully informed about what's happening in their country."[65] The US government might have linked the notion of "humanitarian cyber support" to its overall humanitarian aid effort. Doing so would have signaled that US Internet support to Georgia, similar to VOA broadcasts, was for humanitarian purposes, and therefore not in violation of any Hague Conventions.

It is clear that 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 of warring parties is relatively easy; but not so for cyber activities. Both governments claim they did not participate in the DDoS attacks. Expert analysis substantiates, to a degree, these claims. The DDoS attacks possibly were cyber conflict by proxy, not through nations. Instead, the proxy operators were cyber criminals, cyber citizen-mobs, and self-styled cyber militia. This distinction leads to uncertainty as to which parties were cyber belligerents.

Existing international laws of war are generally based on the notion of "borders" in that these laws primarily govern conflicts between nation-states with recognized geographic boundaries. This construct is fundamentally weak in addressing borderless, nonstate actor participation in cyber conflict where individuals organize their own cyber campaigns. In his book *Here Comes Everybody*, Clay Shirky notes that "ridiculously easy group formation" is a defining characteristic of the contemporary Internet.[66] Cyber conflict between nations is a serious concern, but as the Georgian DDoS attacks demonstrate, perhaps of even greater concern is the growing trend of cyber conflict between nations and ad hoc assemblages.

Until the Georgian case, the 2007 Estonian cyber event was the quintessential example of this nation versus group phenomenon. Originally labeled as cyber war, this assessment changed in the post-conflict retrospective analysis. The international community now appears to have concluded that unattributable, nonstate actor DDoS attacks are not cyber war. At best, according to Estonian officials, they are terrorism, which is a crime.[67] The

DDoS attacks against Georgia and Estonia were strikingly similar. Given the ultimate characterization of the Estonian case as cyber crime or cyber terror, this similarity places in serious doubt whether a legally recognizable state of cyber war existed between the governments of Georgia and Russia. A legal task team from the NATO-accredited Cooperative Cyber Defense Center of Excellence in Tallinn, Estonia, drew a similar conclusion in stating that "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."[68]

As Ethan Zuckerman, of Harvard University's Berkman Center for Internet and Society, notes: "It's unclear whether 'cyberwar' is even an appropriate term for what's taken place . . . in Georgia. It's worth remembering that in this 'cyberwar,' the most serious consequence is that a Web site becomes temporarily inaccessible."[69] If a state of cyber war does not exist, then cyber neutrality is clearly established. This interpretation certainly raises questions as to whether the United States was even in a state of cyber neutrality during the Russian-Georgian conflict. The Georgian case now stands as an 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.

Conclusion

The cyber conflict associated with the Georgian-Russian crisis is a likely indicator of future cyber scenarios and will undoubtedly impact the United States, either directly or indirectly. Conventional wisdom suggests that existing law extends by analogy to encompass cyber conflict. As the Georgian case shows, however, current international law is ambiguous and ill-suited to define contemporary cyber rules of engagement. In future cyber conflict, it might serve the US government well to clearly demarcate its "cyber relationship" vis-à-vis cyber belligerents. In addition, the US State Department should consider invigorating multilateral efforts to clarify the terms and conditions of cyber neutrality in future cyber protocols.

The COE Convention and current US law view the July 2008 DDoS attack against Georgia as cyber crime.[70] Under these rules, the United States had the option of partnering with Georgia in apprehending and prosecuting the offenders. Nearly identical DDoS attacks against Georgia occurred three weeks later, in August. By that time Georgia and Russia were recognized

belligerents in a conventional shooting war. As a result, many governments throughout the international community viewed the second DDoS attacks as cyber war, potentially subject to the Hague (V) Conventions. By that definition, the US relationship with Georgia apparently switched from cyber partner to cyber neutral, compelling the United States to avoid direct material assistance to Georgia. This complex scenario is fraught with legal and operational intricacies, and highlights the compelling need for strategists to have a clear grasp of cyber neutrality concepts.

Under the Law of Armed Conflict, civilians and civilian property that make a "direct contribution" to a war effort may be subject to attack.[71] When TSHost and Google provided cyber defense to Georgia, adversaries potentially may have concluded that those companies were proxies acting on behalf of the US government. Even if the US government did not officially sanction TSHost and Google's actions, their activities nonetheless might have been construed as contributing to Georgia's war effort, possibly exposing the US Internet infrastructure and assets of computer-server firms to cyber attack. In light of this risk, US policymakers should consider the wisdom of continuing a cyber strategy that appears to rely heavily on the loosely controlled actions of private industry.

US government actions, or lack thereof, during the Georgian cyber crisis have the potential of creating false impressions regarding official cyber policy. Other countries might see the Georgian event as a green light to seek cyber refuge in the United States during future cyber conflicts. Following the Georgian example, a nation undergoing a cyber attack might conceivably seek to relocate all of its critical cyber capabilities to the United States. Potential adversaries might mistakenly see that step as indicative of a defensive US cyber umbrella over allies and friends, and prepare strategies to prevent the United States from successfully providing cyber sanctuary. Fortunately, rather than seeking cyber refuge on US government-controlled ".gov" or ".mil" domains, Georgia relocated its Internet assets to private ".com" sites. This decision served as an indicator—albeit weak—to the international community that the Georgian government was not seeking direct protection from the US government. Still, these sites were located within US territory; their involvement brings Georgia's intent, and US cyber neutrality, into question. The US government should take steps to determine if it will allow future cyber belligerents to make use of Internet

assets in the United States, and if so, what protocol is appropriate to control the situation.

Neutrality is an essential tenet of international law. When strictly observed, it prevents the spread of conflict. History shows that neutrality is inherently fragile during war, however, and now even more so during cyber war. Events surrounding the Georgian-Russian cyber conflict should remind US policymakers of the serious nature of cyber neutrality and motivate an in-depth assessment and refinement of US policies and procedures regarding this concept.

NOTES

1. Brian Krebs, "Report: Russian Hacker Forums Fueled Georgia Cyber Attacks," *The Washington Post*, 16 October 2008, http://voices.washingtonpost.com/securityfix/2008/10/report_russian_hacker_forums_f.html?nav=rss_blog; see also Brian Krebs, "Lithuania Weathers Cyber Attack, Braces for Round 2," *The Washington Post*, 3 July 2008, http://blog.washingtonpost.com/securityfix/2008/07/lithuania_weathers_cyber_attac_1.html.

2. Steven Adair, "The Website for the President of Georgia under Attack—Politically Motivated?" *Shadowserver*, 20 July 2008, http://www.shadowserver.org/wiki/pmwiki.php?n=Calendar.20080720.

3. Adair, "The Website for the President of Georgia;" see also Karl Zimmerman, "Webhosting Report," Steadfast Networks, 20 July 2008, http://www.webhostingtalk.com/showpost.php?p=5220780&postcount=41; Shaun Waterman, "Georgia Hackers Strike Apart from Russian Military," *The Washington Times.com*, 19 August 2008, http://www.washingtontimes.com/news/2008/aug/19/georgia-hackers-strike-apart-from-russian-military.

4. Peter Svensson, "Georgian President's Web Site Moves to Atlanta," *AP News*, 11 August 2008, http://www.usatoday.com/tech/products/2008-08-11-2416394828_x.htm; Noah Shachtman, "Estonia, Google Help 'Cyberlocked' Georgia," *Wired,* 11 August 2008, http://blog.wired.com/defense/2008/08/civilge-the-geo.html; Ministry of Foreign Affairs of Georgia, "Statement of the Ministry of Foreign Affairs of Georgia," 8 August 2008, http://georgiamfa.blogspot.com/2008/08/statement-of-ministry-of-foreign.html; Tulip Systems, Inc., "Online Media and Newspapers," http://www.tulsys.com/news; John Markoff, "Georgia Takes a Beating in the Cyberwar with Russia," *The New York Times*, 11 August 2008, http://bits.blogs.nytimes.com/2008/08/11/georgia-takes-a-beating-in-the-cyberwar-with-russia; see also Ministry of Foreign Affairs of Georgia, "Information About the Latest Developments in Georgia" (as accessed on the Web site of the President of Poland), http://www.president.pl/x.node?id=20043119; Shachtman, "Estonia, Google Help."

5. Markoff, "Georgia Takes a Beating;" see also Noah Shachtman, "Georgia under Online Assault," *Wired***,** 10 August 2008, http://blog.wired.com/defense/2008/08/georgia-under-o.html; Kim Hart, "Longtime Battle Lines Are Recast in Russia and Georgia's Cyberwar," *The Washington Post*, 14 August 2008, D1.

6. Woodrow Wilson, *Constitutional Government in the United States* (Boston: Harvard University, 1908), 77.

7. William O. Douglas, *The Court Years: 1939-1975, The Autobiography of William O. Douglas* (New York: Random House, 1980), 270.

8. See *Missouri v. Holland*, 252 U.S. 416 (1920); *United States v. Curtiss-Wright Export Corp.*, 299 U.S. 304 (1936); and US Constitution, art. I, sec. 8; see also Trading with the Enemy Act of 1917, 50 U.S.C. App. 5(b).

9. *Convention Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land***,** articles 1 to 3, 18 October 1907, 36 Stat. 2310; *Convention Concerning the Rights and Duties of Neutral Powers in Naval War*, 18 October 1907, 36 Stat. 2415; see also Stephen C. Neff, *The Rights and Duties of Neutrals: A General History* **(**Manchester, U.K: Manchester Univ. Press, 2000), 1.

10. See *The Steamship Appam*, 243 U.S. 124 (1917).

11. 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.

12. Knut Dörmann, "Computer Network Attack and International Humanitarian Law," The Cambridge Review of International Affairs, Internet and State Security Forum (Cambridge, U.K.: 19 May 2001), http://www.icrc.org/web/eng/siteeng0.nsf/htmlall/5p2alj, para. 29; see also Robert G. Hanseman, "The Realities and Legalities of Information Warfare," *Air Force Law Review*, 42 (1997), 187; Bruce Smith, "An Eye for an Eye, a Byte for a Byte," *Federal Lawyer*, 42 (October 1995), 12; George K. Walker, "Information Warfare and Neutrality," *Vanderbilt Journal of Transnational Law,* 33 (November 2000), 1079.

13. Kelsey, 1443; see also Davis Brown, "A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict," *Harvard International Law Journal*, 47 (Winter 2006), 179; Steven M. Barney, "Innocent Packets? Applying Navigational Regimes from the Law of the Sea Convention by Analogy to the Realm of Cyberspace," in *Essays 2001: Chairman of the Joint Chiefs of Staff Strategy Essay Competition* (Washington: National Defense Univ. Press, 2001), http://www.ndu.edu/inss/books/Books_2001/essays2001/Essays01.pdf, 1; Duncan B. Hollis, "Why States Need an International Law for Information Operations," *Lewis and Clark Law Review*, 11 (Winter 2007), 1026.

14. Thomas C. Wingfield, "When Is a Cyber Attack an 'Armed Attack?'" Cyber Conflict Studies Association, 1 February 2006, http://www.cyberconflict.org/pdf/WingfieldCCSAArticle1Feb06.pdf, 8; see also Kelsey, 1443; Gregory F. Intoccia and Joe W. Moore, "Communications Technology, Warfare, and the Law: Is the Network a Weapon System?" *Houston Journal of International Law*, 28 (Winter 2006), 469; Lawrence T. Greenberg, Seymour E. Goodman, and Kevin J. Soo Hoo, *Information Warfare and International Law* (Washington: National Defense Univ. Press, 1998), http://www.dodccrp.org/files/Greenberg_Law.pdf, 30-33; Hanseman, 183.

15. "Charter of the United Nations" (1945) in *The United Nations and Human Rights 1945-1995* (New York: United Nations, 1995).

16. International Telecommunication Union, *A Comparative Analysis of Cybersecurity Initiatives Worldwide* (Geneva: 10 June 2005), http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Comparative_Analysis_Cybersecurity_Initiatives_Worldwide.pdf, 23.

17. Brown, 179.

18. Bradley Graham, "Bush Orders Guidelines for Cyber-Warfare; Rules for Attacking Enemy Computers Prepared as U.S. Weighs Iraq Options," *The Washington Post*, 7 February 2003, A1.

19. International Telecommunication Union.

20. Defense Science Board, *2006 Summer Study on Information Management for Net-Centric Operations*, Vol. I (Washington: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, April 2007), xv.

21. Michael Vatis, "The Next Battlefield: The Reality of Virtual Threats," *Harvard International Review*, 28 (Fall 2006), http://www.harvardir.org/articles/1581/1/, 1.

22. John Goree and Brian Feldman, "Public Network Weapon System and Method," United States Patent no. 7,159,500 (Washington: US Patent and Trademark Office, 9 January 2007), http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PALL&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.htm&r=1&f=G&l=50&s1=7159500.PN.&OS=PN/7159500&RS=PN/7159500.

23. Kevin Poulsen, "'Cyberwar' and Estonia's Panic Attack," *Wired*, 22 August 2007, http://blog.wired.com/27bstroke6/2007/08/cyber-war-and-e.html; see also Jeremy Kirk, "Estonia Recovers from Massive DDoS Attack," *Computerworld*, 17 May 2007, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9019725; North Atlantic Treaty Organization, "The North Atlantic Treaty" (Washington: 4 April 1949), http://www.nato.int/docu/basictxt/treaty.htm.

24. O. Sami Saydjari, "Addressing the Nation's Cyber Security Challenges: Reducing Vulnerabilities Requires Strategic Investment and Immediate Action," testimony before the House Committee on Homeland Security, Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, 25 April 2007, http://homeland.house.gov/SiteDocuments/20070425145307-82503.pdf.

25. Intoccia and Moore, 484.

26. US Department of State, "United States Joins Council of Europe Convention on Cybercrime," press statement, 29 September 2006, http://www.state.gov/r/pa/prs/ps/2006/73353.htm; see also Council of Europe, *Convention on Cybercrime* (Budapest: 23 November 2001), http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

27. Council of Europe, Article 5.

28. US Air Force Office of Judge Advocate, "Legal Issues Related to Network as a Weapon System,"

memorandum, 13 May 2005 (copy on file with the authors).

29. Ian Traynor, "Russia Accused of Unleashing Cyberwar to Disable Estonia," *The Guardian*, 17 May 2007**,** http://www.guardian.co.uk/world/2007/may/17/topstories3.russia, 1.

30. James Andrew Lewis, as quoted in John Schwartz, "When Computers Attack," *The New York Times*, 24 June 2007, http://www.nytimes.com/2007/06/24/weekinreview/24schwartz.html?pagewanted=print, WK1.

31. Poulsen.

32. Brown, 210.

33. Greenberg, Goodman, and Hoo, 10.

34. Kelsey, 1443.

35. E.g., a computer with a ".com" Internet address implies a commercial entity; a ".gov" or ".mil" Internet address is reserved for government use. Use of a ".com" address implies the computer was not under direct US government control.

36. Adair, "Website for the President of Georgia;" see also Dancho Danchev, "Georgia President's Web Site under DDoS Attack from Russian Hackers," *ZDNet*, 22 July 2008, http://blogs.zdnet.com/security/?p=1533; John Markoff, "Before the Gunfire, Cyberattacks," *The New York Times*, 13 August 2008, http://www.nytimes.com/2008/08/13/technology/13cyber.html?hp, A1.

37. Adair, "Website for the President of Georgia."

38. See, for example, US Department of Justice, Central District of California, "'Botherder' Dealt Record Prison Sentence for Selling and Spreading Malicious Computer Code," news release, 8 May 2006, http://www.cybercrime.gov/anchetaSent.htm (a known member of a botmaster underground was sentenced to 57 months in federal prison, the longest sentence at that time for a defendant who spread computer viruses); see also US Department of Justice, Eastern District of Michigan, "Operator of 'Bot-net,' a Network of Thousands of Virus-Infected Computers, Sentenced to 12 Months in Federal Prison," news release, 23 October 2007, http://www.cybercrime.gov/downeySent.pdf; US Department of Justice, Eastern District of California, "Indictment and Arrest for Computer Hacking," news release, 1 October 2007, http://www.cybercrime.gov/kingIndict.pdf.

39. Grant Gross, "FBI: Several Nations Eyeing U.S. Cyber Targets," *PC World.com*, 15 October 2008, http://www.pcworld.com/businesscenter/article/152288/fbi_several_nations_eyeing_us_cyber_targets.html.

40. Markoff, "Before the Gunfire;" see also Brandon Griggs, "U.S. at Risk of Cyberattacks, Experts Say," *CNN*, 18 August 2008, http://www.cnn.com/2008/TECH/08/18/cyber.warfare/index.html?section=cnn_latest.

41. Iain Thomson, "Georgia Gets Allies in Russian Cyberwar," *vnunet.com*, 12 August 2008, http://www.vnunet.com/vnunet/news/2223776/georgia-gets-allies-russian-cyberwar.

42. Adair, "Website for the President of Georgia;" see also "RBN (Russian Business Network) Now Nationalized, Invades Georgia Cyber Space," *RBNExploit*, 9 August 2008, http://rbnexploit.blogspot.com/2008/08/rbn-georgia-cyberwarfare.html; Waterman.

43. Ministry of Foreign Affairs of Georgia, "Cyber Attacks Disable Georgian Websites," 11 August 2008, http://georgiamfa.blogspot.com/2008/08/cyber-attacks-disable-georgian-websites.html.

44. Siobahn Gorman, "Georgia States Computers Hit by Cyberattack," *The Wall Street Journal.com*, 12 August 2008, http://online.wsj.com/article/SB121850756472932159.html?mod=googlenews_wsj; see also Jon Swaine, "Georgia: Russia 'Conducting Cyber War,'" *The Telegraph.co.uk*, 11 August 2008, http://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html; "RBN (Russian Business Network) Now Nationalized."

45. Evgeny Morozov, "An Army of Ones and Zeroes: How I Became a Soldier in the Georgia-Russia Cyberwar," *Slate.com*, 14 August 2008, http://www.slate.com/id/2197514; see also Evgeny Morozov, "My Article in Slate," 14 August 2008, http://evgenymorozov.com/blog/?p=416.

46. Krebs, "Report: Russian Hacker Forums."

47. Waterman; see also Dancho Danchev, "Coordinated Russia vs. Georgia Cyber Attack in Progress," *ZDNet*, 11 August 2008, http://blogs.zdnet.com/security/?p=1670; see also Joel Hruska, "Russians May Not Be Responsible for Cyberattacks on Georgia," *Ars Technica*, 13 August 2008, http://arstechnica.com/news.ars/post/20080813-georgian-attacks-might-not-be-russians-after-all.html.

48. Gadi Evron, "Internet Attacks Against Georgian Websites," *CircleID*, 11 August 2008, http://www.circleid.com/posts/88116_Internet_attacks_georgia; see also Gadi Evron, "Mobilizing Russian Population Attacking Georgia: Similar to the Estonian Incident?" *CircleID*, 13 August 2008, http://www.circleid.com/posts/88131_mobilizing_russian_attacking_georgia.

49. Kelly Jackson Higgins, "Botnets Behind Georgian Attacks Offer Clues," *Dark Reading*, 9 September 2008, http://www.darkreading.com/document.asp?doc_id=163342.

50. Steven Adair, "Georgian Attacks: Remember Estonia?" *Shadowserver*, 13 August 2008, http://www.shadowserver.org/wiki/pmwiki.php?n=Calendar.20080813.

51. Bobbie Johnson, "Cyberwar Isn't a Grand Struggle—It's a Scary Prospect of Pure Chaos," *The Guardian*, 21 August 2008, http://www.guardian.co.uk/technology/2008/aug/21/blogging.internet.

52. Peter Svensson, "Russian Hackers Continue Attacks on Georgian Sites," *AP News*, 12 August 2008, http://www.wjla.com/news/stories/0808/543487.html; see also Svensson, "Georgian President's Web Site;" Griggs; Tulip Systems, Inc.

53. Ben Bain, "Tracking a Cyberattack," *Federal Computer Week*, 15 August 2008, http://www.fcw.com/online/news/153529-1.html.

54. Griggs.

55. Svensson, "Georgian President's Web Site."

56. Svensson, "Russian Hackers."

57. Larry Dignan, "Georgia Turns to Google's Blogger to Counter Alleged Cyber Attack," *Seeking Alpha*, 11 August 2008, http://seekingalpha.com/article/90392-georgia-turns-to-google-s-blogger-to-counter-alleged-cyber-attack; see also Pete Swabey, "Google Embroiled in Georgian Conflict," *Information Age*, 12 August 2008, http://www.information-age.com/home/information-age-today/460666/google-embroiled-in-georgian-conflict.thtml; Adair, "Georgian Websites under Attack;" Swaine.

58. Dave Barth, "Where is Georgia on Google Maps?" *Google Lat Long*, 12 August 2008, http://google-latlong.blogspot.com/2008/08/where-is-georgia-on-google-maps.html; see also Miguel Helft, "Google: We Did Not Erase Maps of Georgia," *The New York Times*, 12 August 2008, http://bits.blogs.nytimes.com/2008/08/12/google-we-did-not-erase-maps-of-georgia; Katie Hunter, "Tuesday Map: Georgia's Google Vanishing Act," *Foreign Policy*, 12 August 2008, http://blog.foreignpolicy.com/node/9515.

59. Thomson.

60. Ibid.

61. Department of Homeland Security, "Fact Sheet: Protecting America's Critical Infrastructure—Cyber Security Education and Training," 15 February 2005, http://www.dhs.gov/xnews/releases/press_release_0620.shtm; Department of Defense, *DoD CIO Annual Information Assurance Report* (Washington: Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, April 2000), http://stinet.dtic.mil/cgi-bin/GetTRDoc?AD=ADA391407&Location=U2&doc=GetTRDoc.pdf, ES-1.

62. Intoccia and Moore.

63. Svensson, "Russian Hackers."

64. Kim Gamel, "US Begins Flying Georgian Troops Home from Iraq," *International Herald Tribune*, 10 August 2008, http://www.iht.com/articles/ap/2008/08/10/news/Iraq-Georgia.php; Deborah Haynes, "Petraeus: US is Flying Georgian Troops into Battle Zone," *TimesOnline*, 10 August 2008, http://www.timesonline.co.uk/tol/news/world/iraq/article4498032.ece; Steven Lee Myers, "Bush, Sending Aid, Demands that Moscow Withdraw," *The New York Times*, 14 August 2008, http://www.nytimes.com/2008/08/14/world/europe/14georgia.html?hp, A1; see also Tom Baldwin, "George Bush Squares up to Vladimir Putin over Georgia," *TimesOnline*, 14 August 2008, http://www.timesonline.co.uk/tol/news/world/europe/article4524831.ece.

65. Voice of America, "VOA Doubles Broadcasting into the Republic of Georgia," press release, 8 August 2008, http://www.voanews.com/english/About/2008-08-08-Doubling-Georgian.cfm.

66. Clay Shirky, *Here Comes Everybody: The Power of Organizing without Organizations* (New York: Penguin Press, 2008), 155.

67. "EU Should Class Cyber Attacks as Terrorism: Estonia," *BrisbaneTimes.com.au*, 8 June 2007, http://news.brisbanetimes.com.au/technology/eu-should-class-cyber-attacks-as-terrorism-estonia-20070608-h9r.html; see also Jeremy Kirk, "Student Fined for Attack Against Estonian Web Site," *Computer World*, 24 January 2008, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9058758&source=rss_topic17; Joel Hruska, "Student Behind DoS Attack that Rekindled Bad Soviet Memories," *Ars Technica*, 24 January 2008, http://arstechnica.com/news.ars/post/20080124-student-behind-dos-attack-that-rekindled-bad-soviet-memories.html.

68. Eneken Tikk, Kadri Kaska, Kristel Rünnimeri, Mari Kert, Anna-Maria Talihärm, and Liis Vihul, *Cyber Attacks Against Georgia: Legal Lessons Identified* (Tallinn, Estonia: Cooperative Cyber Defense Center of Excellence, 2008), http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf, 23.

69. Ethan Zuckerman, "Misunderstanding Cyberwar," 16 August 2008, http://www.ethanzuckerman.com/blog/2008/08/16/misunderstanding-cyberwar.

70. See the Computer Fraud and Abuse Act, as amended, 18 U.S.C. 1030, http://www4.law.cornell.edu/uscode/18/1030.html.

71. *Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field*, 12 August 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31.