THE LAW OF CYBER-ATTACK

Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix,
Aileen Nowlan, William Perdue, Julia Spiegel[1]

(Forthcoming in the *California Law Review*, 2012)

Iran's nuclear program grinds to a halt, the subject of a sophisticated computer attack that sent centrifuges spinning wildly out of control. A "distributed denial of service" attack takes the entire population of Burma offline immediately before the country's first national election in twenty years. China's military mounts an attack on a Falun Gong Web site based in Alabama. What law regulates these "cyber-attacks"? Does the law of war apply? If not, what other bodies of law might help address the problem? This Article examines these questions and, in the process, offers new insights into how existing law may be applied—and adapted and amended—to meet the distinctive challenge posed by cyber-attacks. It does so in two principal ways. First, the Article clarifies what cyber-attacks are and how they relate to existing bodies of law, including the law of war, recent international efforts to directly regulate cyber-attacks, international bodies of law that may be used to indirectly regulate cyber-attacks, and domestic criminal law. Second, the Article shows how existing law is deficient and what needs to be done to improve it. Although existing bodies of law do offer some tools for responding to cyber-attacks, these tools are far from complete or adequate. The law of war, for example, provides a useful legal framework for only the very small slice of cyber-attacks that amount to an armed attack or that take place in the context of an ongoing armed conflict. Other existing legal frameworks—both domestic and international—offer equally fragmentary assistance in addressing cyber-attacks through law. Examining existing law leads to a clear conclusion: A new, comprehensive legal framework is needed to address cyber-attacks. That framework includes a more robust system of domestic enforcement, but a truly effective solution to this global challenge will require global cooperation. This Article thus outlines the key elements of a cyber-treaty that would provide a more comprehensive solution to the emerging threat of cyber-attacks.

---

[1] Gerard C. and Bernice Latrobe Smith Professor of International Law, Yale Law School; law clerk, Judge Mark Kravitz (D. Conn.); J.D. Candidate 2012, Yale Law School; J.D. Candidate 2012, Yale Law School; J.D. Candidate 2012, Yale Law School; Associate, Arnold & Porter; J.D. Candidate, Yale Law School, and MPA Candidate, Woodrow Wilson School, Princeton University, respectively. We thank Sara Solow, Elizabeth Nielsen, Chelsea Purvis, Saurabh Sanghvi, and Teresa Miguel for their assistance in preparing this Article.

CONTENTS

Last year, Iran's nuclear program ground to a halt, the subject of a sophisticated attack that sent centrifuges spinning wildly out of control. The weapon? Stuxnet, a computer "worm" that appears to have many authors from around the world and was likely tested by Americans and Israelis at the Israeli Dimona complex in the Negev desert.[2]

A few months later, a so-called "distributed denial of service" attack took the entire population of Burma offline immediately preceding the country's first national election in twenty years.[3] It is widely believed that the military junta in Burma coordinated the attack to shut down the Internet,[4] but American public officials have resisted blaming the attack on the government, even as they have criticized the election.[5]

In the summer of 2011, evidence emerged of a long-suspected government-sanctioned cyber-attack program in China. In late August, a state television documentary aired on the government-run China Central Television appeared to capture an in-progress distributed denial of service attack by China's military on a Falun Gong Web site based in Alabama.[6] This revelation followed on the heels of a report by the McAffee cyber-security

---

[2] The seeds for this attack were apparently sewn well before 2010. The worm was first detected in 2008, when it infected networks around the world. It did no damage to most systems. At first, it was assumed that the attack, which appeared to target nuclear facilities in Iran, was not successful. Yet in the fall of 2010 reports that Iran's uranium enriching capabilities had been diminished. *A Cyber-Missile Aimed at Iran?*, The Economist Babbage Blog (Sept. 24, 2010, 1:32 PM), http://www.economist.com/blogs/babbage/2010/09/stuxnet_worm. *See also* Jonathan Fildes, *Stuxnet Worm 'Targeted High-Value Iranian Assets,'* BBC News (Sept. 23, 2010, 6:46 AM), http://www.bbc.co.uk/news/technology-11388018.William J. Broad, John Markoff & David E. Sanger, *Israeli Test on Worm Called Crucial in Iran Nuclear Delay*, N.Y. TIMES (Jan. 15, 2011), available at http://www.nytimes.com/2011/01/16/ world/middleeast/16stuxnet.html. Stuxnet is the first computer virus known to be capable of specifically targeting and destroying industrial systems such as nuclear facilities and power grids. Jonathan Fildes, *Stuxnet Worm 'Targeted High-Value Iranian Assets,'* BBC News (Sept. 23, 2010, 6:46 AM), http://www.bbc.co.uk/news/technology-11388018.

[3] *Burma Hit by Massive Net Attack Ahead of Election*, BBC NEWS (Nov. 4, 2010, 11:33 AM), http://www.bbc.co.uk/news/technology-11693214.

[4] *See id.*

[5] *See, e.g.*, Barack Obama, Remarks by the President and the First Lady in Town Hall with Students in Mumbai, India (Nov. 7, 2010), *available at* http://www.whitehouse.gov/the-press-office/2010/11/07/remarks-president-and-first-lady-town-hall-with-students-mumbai-india;
Barack Obama, Statement by President Obama on Burma's November 7 Elections (Nov. 7, 2010), *available at* http://www.whitehouse.gov/the-press-office/2010/11/07/statement-president-obama-burmas-november-7-elections.

[6] Ellen Nakashima and William Wan, China's *Denials About Cyberattacks Undermined By Video Clip*, WASH. POST (Aug. 24, 2011).

company that a "state actor"—widely believed to be China—had engaged in a years-long cyber-attack program aimed at a range of governments, U.S. corporations, and United Nations groups.[7]

What law governs these attacks? Some have referred to these and similar attacks as "cyber-warfare," suggesting that the law of war might apply. Yet the attacks look little like the conventional warfare that the law of war traditionally regulates. And if they are "warfare," does that mean that victims of such attacks might claim the right to use conventional force in self-defense—potentially legally authorizing Iran, for example, to respond to Stuxnet with a physical attack?

This Article examines these questions and, in the process, offers new insights into how existing law may be applied—and adapted and amended—to meet the distinctive challenge posed by cyber-attacks. It does so in two principal ways. First, the Article clarifies what cyber-attacks are and how they relate to existing bodies of law, including the law of war,[8] recent international efforts to directly regulate cyber-attacks, international bodies of law that may be used to indirectly regulate cyber-attacks, and domestic criminal law.

Second, the Article shows how existing law is deficient and what needs to be done to improve it. Although existing bodies of law do offer some tools for responding to cyber-attacks, these tools are far from complete or adequate. The law of war, for example, provides a useful legal framework for only the very small slice of cyber-attacks that amount to an armed attack or that take place in the context of an ongoing armed conflict. Other existing legal frameworks—both domestic and international—offer equally fragmentary assistance in addressing cyber-attacks through law. Examining existing law leads to a clear conclusion: A new, comprehensive legal framework is needed to address cyber-attacks.

The starting challenge in examining cyber-attacks may seem mundane, but is a critical starting point for any reform effort—that is, defining a "cyber-attack." The terms "cyber-attack," "cyber-warfare," and "cyber-crime" are frequently used with little regard for what they are meant to include. This lack of clarity can make it all the more difficult to design a meaningful legal response. We therefore begin this Article in Part I by defining these terms. We

---

[7] David Barboza & Kevin Drew, *Security Firm Sees Global Cybersyping*, N.Y. TIMES (Aug. 3, 2011). This was not the first suggestion of a program of cyberattacks on private and government actors by China. Computer attacks on Google that originated in China were believed to be part of a broader political and corporate espionage effort and prompted Google to withdraw from the Chinese market. Ariana Enjung Cha & Ellen Nakashima, Google *China Cyberattack Part of Vast Espionage Campaign, Experts Say*, WASH. POST (Jan. 14, 2010).

[8] For simplicity's sake, this report refers collectively to *jus in bello* and *jus ad bellum* as the "law of war."

define "cyber-attack" as "any action taken to undermine the functions of a computer network for a political or national security purpose." We also explain the difference between "cyber-attacks," "cyber-warfare," and "cyber-crime," and describe three common forms of cyber-attacks: distributed denial of service attacks, planting inaccurate information, and infiltration of a secure computer network.

In Part II, we turn to examining how the law of war might govern cyber-attacks. We parse the way the law of war, most of which was developed at a time when cyber-attacks were inconceivable, applies to this new zone of conflict. We conclude that only a small slice of cyber-attacks are addressed by the law of war. Most cyber-attacks do not rise to the level of an armed attack and do not take place in the context of an ongoing conflict—and thus are not sufficiently harmful to justify the use of armed force in response. The small subset of cyber-attacks that do rise to this level we call "cyber-warfare." This definition is crucial because it limits the application of the "war" framework to those actions that actually constitute "war" as a matter of international law. We then explore how the *jus in bello* regulations apply to cyber-attacks occurring in the context of an ongoing armed conflict.

Because the law of war regulates only a small subset of cyber-attacks, in Part III we examine other existing legal regimes that could regulate cyber-attacks. These include (1) the law of countermeasures, which governs how states may respond to international law violations that do not justify uses of force in self-defense; (2) international agreements and other cooperative efforts to directly regulate cyber-attacks; (3) international agreements that regulate means or locations of cyber-attacks, including telecommunications, aviation, space, satellites, and the sea; and (4) U.S. criminal law regulating cyber-attacks. We conclude that, as with the law of war, these existing bodies of law effectively address only a small part of the problem—leaving many harmful cyber-attacks unregulated and uncontrolled by either domestic or international law.

Finally, in Part IV we consider how the problem of cyber-attacks might be more effectively addressed, offering recommendations for both domestic and international reforms. At the domestic level, states may expand extraterritorial reach of domestic criminal law and develop plans for the deployment of customary countermeasures in response to cyber-attacks. Yet an effective solution to this global challenge cannot be achieved by individual states acting alone. It will require global cooperation. We therefore outline the key elements of a cyber-treaty that would provide a more comprehensive and long-term solution to the emerging threat of cyber-attacks.

I. WHAT IS A CYBER-ATTACK?

The first challenge in evaluating how domestic and international law might be used to address cyber-attacks is to determine the nature and scope of the problem we face. Activities in cyberspace defy many of the traditional categories and principles that govern armed conflict under the law of war. This Part first offers a precise definition of "cyber-attack." This step is not only necessary to the legal analysis that follows, but it also fills a gap in the existing literature, which often uses the term without clarifying what it is meant to include and exclude. We then offer three categories of activities that fall within this definition, illuminating the extraordinary range of activities that fall under even a carefully constructed and limited definition of "cyber-attacks." This serves as a prelude to an analysis of what portion of cyber-attacks are governed by the law of war and other existing bodies of law.

A. Defining "Cyber-Attack"

For well over a decade, analysts have speculated about the potential consequences of a cyber-attack. The scenarios—ranging from a virus that scrambles financial records or incapacitates the stock market,[9] to a false message that causes a nuclear reactor to shut off[10] or a dam to open,[11] to a blackout of the air traffic control system that results in airplane crashes[12]—anticipate severe and widespread economic or physical damage. While none of these scenarios has thus far occurred, numerous smaller incidents happen regularly. Nevertheless, there is no settled definition for identifying these incidents as cyber-attacks,[13] much less as cyber-warfare. Only after governments widely accept a definition will analysts be able to develop coordinated policy recommendations and will countries be able to act multilaterally to address the growing threat posed by cyber-attacks. After describing some existing definitions, we offer a definition of cyber-attack that effectively encompasses the activity that lies at the heart of the concerns raised over cyber-attacks.

---

[9] Duncan B. Hollis, *Why States Need an International Law for Information Operations*, 11 LEWIS & CLARK L. REV. 1023, 1042 (2007).

[10] Vida Antolin-Jenkins, *Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places?*, 51 NAVAL L. REV. 132, 140 (2008).

[11] Barton Gellman, *Cyber Attacks by Al Qaeda Feared; Terrorists at Threshold of Using Internet as Tool of Bloodshed, Experts Say*, WASH. POST, June 27, 2002, at A01.

[12] General Accounting Office, Air Traffic Control: Weak Computer Security Practices Jeopardize Flight Safety (May 1998).

[13] As distinct from cyber-crime. *See* Part I.B.

1. Government Conceptions of Cyber-Attack

There have been two particularly prominent government-led efforts to understand the scope of the threat posed by cyber-attacks, one by the U.S. government and the other by the Russia- and China-led Shanghai Cooperation Organization. Perhaps not surprisingly, they have arrived at very different understandings of the problem.

The U.S. military has yet to offer an official definition of cyber-attack or cyber-warfare.[14] Instead, the Joint Chiefs of Staff have defined forms of warfare closely related to cyber-warfare. For example, the Joint Chiefs explain that "information warfare" includes operations "to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting [one's] own."[15] They define a sub-class of information warfare, computer network warfare, as:

> [T]he employment of Computer Network Operations (CNO) with the intent of denying adversaries the effective use of their computers, information systems, and networks, while ensuring the effective use of our own computers, information systems, and networks. These operations include Computer Network Attack (CNA), Computer Network Exploration (CNE), and Computer Network Defense (CND).[16]

---

[14] The Congressional Research Service does provide an official definition but it is not particularly specific: Cyber-warfare is "warfare waged in cyberspace. It can include *defending* information and computer networks, *deterring* information attacks, as well as *denying* an adversary's ability to do the same. It can include *offensive* information operations mounted against an adversary, or even *dominating* information on the battlefield." Steven A. Hildreth, *Cyberwarfare*, CONGRESSIONAL RESEARCH SERVICE, 16 (June 19, 2001). The Department of Defense's Strategy for Operating in Cyberspace utilizes the term "cyber threats" rather than cyber-attacks to describe the threats to cyberspace. *See* U.S. DEP'T OF DEF., DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE 2 (July 2011) [hereinafter DOD STRATEGY].

[15] JOINT CHIEFS OF STAFF, U.S. DEP'T OF DEF., JOINT PUB. 3-13, INFORMATION OPERATIONS, at ix (Feb. 13, 2006). [hereinafter JP 3-13] (listing five IO methods: (1) electronic warfare; (2) computer network operations, including computer network attacks; (3) psychological operations; (4) military deception; and (5) operational security).

[16] JEFFREY CARR, INSIDE CYBER WARFARE 176 (2010). Additionally, numerous commentators and scholars have offered their own similar definitions. Government security expert Richard A. Clarke defines cyber-war as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption." RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT 6 (2010). Former National Security Advisor and Central Intelligence Agency

Similarly, the U.S. National Research Council defines cyber-attack as "deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks."[17] Although the objective-based definitional approach taken by the United States is preferable, the complexity of these definitions partially explains the lack of uniformity within the government. Moreover, the definition fails to distinguish between a simple cyber-crime and a cyber-attack. A simpler, uniform definition would avoid ambiguity, overlap, and coverage gaps; facilitate a cleaner delineation between cyber-attack and cyber-crime; and promote greater inter-agency cooperation.

The Shanghai Cooperation Organization—a security cooperation group composed of China, Russia, and most of the former Soviet Central Asian republics, as well as observers including Iran, India, and Pakistan—has adopted a much more expansive means-based approach to cyber-attacks. The Organization has "express[ed] concern about the threats posed by possible use of [new information and communication] technologies and means for the purposes [sic] incompatible with ensuring international security and stability in both civil and military spheres."[18] It defines an "information war" as "mass psychologic[al] brainwashing to destabilize society and state, as well as to force the state to take decisions in the interest of an opposing party."[19] Moreover, it identifies the dissemination of information harmful to "social and political, social and economic systems, as well as spiritual, moral and cultural

("CIA") Director Michael Hayden defines cyber-war as the "deliberate attempt to disable or destroy another country's computer networks." Tom Gjelten, *Extending the Law of War into Cyberspace*, NPR.COM (Sept. 22, 2010), http://www.npr.org/templates/story/story.php?storyId=130023318.

[17] COMM. ON OFFENSIVE INFORMATION WARFARE, ET. AL., NAT'L RES. COUNCIL, TECHNOLOGY, POLICY LAW AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES (WILLIAM A. OWENS, ET. AL. EDS., 2009) [hereinafter NRC REPORT].

[18] Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security, 61st plenary meeting (Dec. 2, 2008) [hereinafter Shanghai Cooperation Agreement]. The distinction between this interpretation and that of the United States is understandable in light of Matthew Waxman's analysis of strategic differences in the cyber-attack context. As Waxman notes, "major state actors in this area are likely to have different views on legal line drawing because they perceive a different set of strategic risks and opportunities." Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE J. INT'L L. 421, 458-59 (2011).

[19] Shanghai Cooperation Agreement, Annex I, at 209.

spheres of other states" as one of the main threats to information security.[20]

Hence the Shanghai Cooperation Organization appears to have adopted an expansive vision of cyber-attacks to include the use of cyber-technology to undermine political stability. Commentators fear that this almost unrestricted definition represents an effort to justify censorship of political speech on the Internet.[21] This concern is particularly salient in light of recent government efforts to suppress political organizing using new media in Iran, Egypt, and elsewhere.

The distance between these two government-led understandings of cyber-attacks only serves to make clear the importance of specifying a clear definition of the problem to be faced. The next subsection takes on this task.

2. Recommended Definition

In this Article, we adopt a narrow definition of cyber-attack, one meant to focus attention on the unique threat posed by cyber-technologies:

A cyber-attack consists of any action taken to undermine the functions of a computer network for a political or national security purpose.

This subsection discusses each aspect of this definition to explain the reasoning behind the language and to clarify which activities it encompasses.

a. "A cyber-attack . . ."

Implicit in this term is the requirement that the conduct must be active: either offense or active defense.[22] Active defense includes "electronic counter-measures designed to strike attacking computer systems and shut down cyberattacks midstream."[23] Governments are likely to employ both active and passive defenses, and so it is crucial that the legal boundaries of both are well understood.[24]

---

[20] *Id.* at 203.

[21] *See, e.g.*, Tom Gjelten, *Seeing the Internet as an 'Information Weapon'*, NPR.com (Sep. 23, 2010), http://www.npr.org/templates/story/story.php?storyId=130052701; *see also infra* I.B.2.e.

[22] Measures of passive defense against cyber-attacks, such as virus scanning software or firewalls, are outside the scope of this definition.

[23] CARR, *supra* note 16, at 46.

[24] The U.S. government currently utilizes both active and passive defenses. *See* DOD STRATEGY, *supra* note 14.

b. ". . . consists of any action taken . . ."

A cyber-attack's means can include *any* action—hacking, bombing, cutting, infecting, and so forth—but the objective can only be to undermine or disrupt the function of a computer network. In this sense, we follow the U.S. objective-based approach rather than the means-based approach of the Shanghai Cooperation Organization.

There is no consistent strategy under international or domestic law for classifying different types of warfare. Some types of warfare are defined by their means, which is most often a weapon. Examples include kinetic warfare, biological warfare, chemical warfare, nuclear warfare, intelligence-based warfare, network-based warfare,[25] and guerilla warfare. Other types of warfare are defined by their objectives. "Objective" here means the direct target, rather than the long-range purpose. Examples include information warfare, psychological warfare, command and control warfare, electronic warfare, and economic warfare.

Because we define cyber-attack according to its objective, any means may be used to accomplish a cyber-attack. For this form of warfare or attack, a definition limited by objective rather than means is superior for three reasons. First, and most important, this type of definition is simply more intuitive. Using a computer network in Nevada to operate a predator drone for a kinetic attack in Pakistan is not a cyber-attack; rather, it is technologically advanced conventional warfare. Using a regular explosive to sever the undersea network cables that carry the information packets between continents, on the other hand, is a cyber-attack.[26] This view is consistent with that offered by the U.S. Department of Defense, which has identified kinetic attack as a strategy in "cyber offensive operations."[27]

Second, the objective-based approach is logical. Warfare traditionally functions in four domains—land, air, sea, and space—each of which is

[25] This is distinct from "network warfare," which is defined as "the employment of Computer Network Operations (CNO) with the intent of denying adversaries the effective use of their computers, information systems, and networks, while ensuring the effective use of our own computers, information systems, and networks." *Id.* at 176. Network-based warfare is any type of warfare that utilizes networks. Note a similar distinction between intelligence-based warfare (which describes the means) and information warfare (which describes the objective).

[26] *See* Antolin-Jenkins, *supra* note 10, at 138 ("[K]inetic weapons are certainly part of the cyber arsenal.").

[27] Joint Chiefs of Staff, National Military Strategy for Cyberspace Operations 15 (December 2006). A National Research Council report on "cyber offensive operations" excluded kinetic attacks on computer networks for the purposes of the report, but acknowledged that such attacks were realistic forms of cyber attack. NRC REPORT, *supra* note 17, at 12-19.

addressed by one of the full-time armed services.[28] With the rise of cyber-warfare, strategists have identified a fifth domain: cyberspace.[29] In response, the United States has created the U.S. Cyber Command, a subdivision of the joint services Strategic Command.[30] Although the Cyber Command is not a unique service, it coordinates the functional operations of the Army, Navy (and Marines), and Air Force. The armed services are traditionally organized by domain rather than by platform. The Army's function is to control land, not to drive tanks and fire land-based artillery; the Navy's function is to control the seas, not to operate boats and ships; and the Air Force's function is to control the skies, not to fly planes and drop bombs. Each service has access to whatever tools and weapons it deems necessary to control its domain: planes, boats, missiles, artillery, computer networks, and so forth. By the same logic, Cyber Command's mission is not to utilize computer networks for any objective, but to defend the ability to operate in cyberspace by any means.[31]

Third, a means-based definition poses serious risks that an objective-based definition avoids. By encompassing any activity that uses cyber-technology and jeopardizes stability, a means-based understanding of cyber-warfare can be used to constrain the expression of free speech and political dissent online.[32] The Shanghai Cooperation Organization's definition may have been designed to be means-based for precisely this reason.[33]

c. ". . . to undermine the function . . ."

The objective of a cyber-attack must be to undermine the *function* of a computer network. A computer network may be compromised in many

[28] Space is difficult to assign to the Army, Navy, or Air Force, but its proper classification is outside the scope of this paper.

[29] *See* DOD STRATEGY, *supra* note 14, at 5; *War in the Fifth Domain*, THE ECONOMIST, July 1, 2010, *available at* http://www.economist.com/node/16478792. The Joint Chiefs of Staff identify cyberspace as one of the "global commons," along with international waters, air space, and space. Joint Chiefs of Staff, *The National Military Strategy of the United States of America* (2004), *available at* http://www.strategicstudiesinstitute.army.mil/pdffiles/nms2004.pdf.

[30] William H. McMichael, *DoD Cyber Command Is Officially Online*, ARMYTIMES (May 22, 2010, 9:20 AM), http://www.armytimes.com/news/2010/05/military_cyber_command_052110; *see* Thom Shanker, *Cyberwar Chief Calls for Secure Computer Network*, N.Y. TIMES, Sept. 23, 2010.

[31] *See* DOD STRATEGY, *supra* note 14, at 5 ("[T]reating cyberspace as a domain is a critical organizing concept for DoD's national security missions. This allows DoD to organize, train, and equip for cyberspace as we do in air, land, maritime and space to support national security interests.").

[32] Gjelten, *supra* note 21.

[33] *Id.*

different ways. Syntactic attacks disrupt a computer's operating system, causing the network to malfunction.[34] Examples include "worms, viruses, Trojan horses and denial of service attacks."[35] The incident in Burma discussed in the opening to this Article constituted syntactic attack. In contrast, semantic attacks preserve the operating system but compromise the accuracy of the information it processes and to which it reacts.[36] As a result, "[a] system under semantic attack operates and will be perceived as operating correctly, . . . but it will generate answers at variance with reality."[37]

Cyber-attacks need not be limited to syntactic or semantic attacks.[38] In 2003, a security breach created numerous leaks of sensitive information from U.S. Department of Defense computers, which occurred over several months.[39] The Department has acknowledged that the majority of such incidents—collectively referred to as "Titan Rain"—were orchestrated by China as a method of cyber-espionage.[40] Another recent example of cyber-espionage occurred when China intruded into the network and copied the data of Google and other major Internet technology companies in 2010. The alleged purpose of the prolonged security breach ranged from theft of intellectual property to unlawful surveillance of human rights activists.[41] Recent revelations indicate that the cyber-exploitation may have been part of a larger espionage effort against American companies carried out over the course of the decade. More recently, the Department of Defense admitted that it suffered one of its worst cyber-espionage leaks in March 2011, when foreign hackers gained access to

[34] Antolin-Jenkins, *supra* note 10, at 139.
[35] *Id.*
[36] *Id.* at 140.
[37] MARTIN C. LIBICKI, WHAT IS INFORMATION WARFARE? 77 (1995).
[38] The U.S. cyber-operation in Iraq discussed below, for example, was neither syntactic nor semantic. Nevertheless, it constitutes a cyber-attack under this definition, as it did "undermine the function" of the secure email system by causing it to send an email from an unauthorized user.
[39] CLAY WILSON, CONG. RESEARCH SERV., RL32114, BOTNETS, CYBERCRIME, AND CYBER TERRORISM: VULNERABILITIES AND POLICY ISSUES FOR CONGRESS 12 (2008).
[40] *Id.*
[41] *A New Approach to China*, THE OFFICIAL GOOGLE BLOG (Jan. 12, 2010, 3:00 PM), http://googleblog.blogspot.com/2010/01/new-approach-to-china.html; *see also* James Glanz & John Markoff, *Vast Hacking by a China Fearful of the Web*, N.Y. TIMES, Dec. 4, 2010, *available at* http://www.nytimes.com/2010/12/05/world/asia/05wikileaks-china.html?_r=2&hp.

over 24,000 Pentagon files.[42] Meanwhile, the extent to which the United States is conducting similar activities is unknown.[43]

Although all of these incidents compromised the security of a computer network for the purpose of carrying out a military objective,[44] they do not meet this Article's definition of a cyber-attack. Mere cyber-espionage, or cyber-exploitation, does not constitute a cyber-attack, because neither of these concepts involves altering computer networks in a way that affects their current or future ability to function.[45] To "undermine the function" of a computer system, an actor must *do more than passively observe a computer network or copying data*, even if that observation is clandestine. The actor must affect the operation of the system or input something into the system, either by damaging the operating system or by adding false, misleading, or unwelcome information. Such activities may be criminal—as acts of corporate or political cyber-espionage—but are not cyber-*attacks*. In this respect, our definition reflects a common distinction between espionage and attacks in more traditional settings.

---

[42] Thom Shanker & Elisabeth Bumiller, *Hackers Gained Access to Sensitive Military Files*, N.Y. TIMES, at A6, July 15, 2011.

[43] *See* Jack Goldsmith, What is the Government's Strategy for the Cyber-exploitation Threat, Lawfareblog.com, Aug. 10, 2011.

[44] Michael Joseph Gross, *Enter the Cyber-dragon*, VANITY FAIR, Sept. 2011 (detailing these and other successful hacks of public and private systems).

[45] This Article adopts the following definition of cyber-espionage: "[T]he science of covertly capturing e-mail traffic, text messages, other electronic communications, and corporate data for the purpose of gathering national-security or commercial intelligence." Seymour M. Hersh, *The Online Threat: Should We Be Worried About a Cyber War?*, THE NEW YORKER, Nov. 1, 2010, *available at* http://www.newyorker.com/reporting/2010/11/01/101101fa_fact_hersh?. The Central Intelligence Agency (CIA) emphasizes that cyber-espionage does not fall under the umbrella of cyber-warfare, likely because the U.S. government—like many other governments—routinely engages in espionage over communications networks. Gjelten, *supra* note 16. Notably, the National Research Council draws a similar line. It distinguishes what it calls cyber-exploitation—which includes actions that merely gather information from the cyber-domain and is therefore related to, if perhaps somewhat broader than, cyber-espionage—from cyber-attack because "[t]he [law of armed conflict] presumes that a clear distinction can be drawn between the use of force and espionage, where espionage is avowedly not a use of force." NRC REPORT, *supra* note 17, at 22, § 1.6. Similarly, although the Department of Defense lists the stealing of intellectual property as a cyber threat, as military strength depends on economic vitality, such theft is not a cyber-attack as it does not undermine the ability of the network to function. *See* DOD STRATEGY, *supra* note 14, at 4.

d. ". . . of a computer network . . ."

A computer network is a system of computers and devices connected by communications channels. Frequently, this connection exists over the Internet, but there are also numerous closed networks, such as the secure networks employed by agencies of the U.S. government.

It is important to bear in mind that computers are now everywhere. The concept of a computer encompasses more than a simple desktop or laptop; it also includes the device that controls elevators and traffic lights, the program that regulates pressure on water mains, and many other ubiquitous appliances such as cell phones, televisions, and even washing machines.[46] The potential for widespread damage from a cyber-attack grows in tandem with the growth of systems controlled by computers.

e. ". . . for a political or national security purpose."

A political or national security purpose distinguishes cyber-attack from simple cyber-crime. Any aggressive action taken by a state actor in the cyber-domain necessarily implicates national security and is therefore a cyber-attack (where the action satisfies all the other elements of the definition), whether or not it rises to the level of cyber-warfare. Cyber-crime committed by a non-state actor for a political or national security purpose is a cyber-attack. On the other hand, cyber-crime that is not carried out for a political or national security purpose, such as Internet fraud, identity theft, and intellectual property piracy, does not fit this final element of a "cyber-attack" and is therefore mere cyber-crime.

There are numerous reasons for excluding non-political cyber-crimes (that is cyber-crimes not carried out for a political or national security purpose) from the definition of cyber-attack. First, such activities, while troubling, do not raise the same legal questions as activities that might breach public international law. The actions of the Kremlin Kids, private hackers who allegedly shut down the Georgian Internet during Russia's invasion of South Ossetia,[47] invoke legal doctrines surrounding state responsibility and terrorism[48] in a way that the actions of Onel de Guzman, a student who was

[46] CLARKE, *supra note* 16, at 70-74.
[47] *See infra* note 44 and accompanying text.
[48] The line drawn between simple cyber-crime and cyber-attack by private individuals is analogous to the line drawn between violent crime and terrorism. *See* 18 U.S.C. § 2331(1)(B) (2006) (defining terrorism according to its apparent political intentions); BLACK'S LAW

suspected of infecting tens of millions of computers in 2000 with the destructive but undirected "love bug virus,"[49] do not. Second, by corollary, cyber-crime presents unique legal questions that are not the focus of this Article.[50] Finally, a cleaner delineation between cyber-attacks that present threats to national security and purely private cyber-crime will clarify ownership of cyber-security needs among various government departments.

A political or national security purpose also denotes the public nature of the cyber-attacks without limiting the definition to state actors. This is important because, due to its low cost and the relative invulnerability of non-state actors to in-kind retribution, cyber-attacks are a particularly attractive weapon for terrorists and other non-state actors.[51] Because non-state actors may execute or may be the victim of cyber-attacks, the purpose, rather than the actor, must distinguish a cyber-attack from a simple cyber-crime. This definition does not distinguish between state and non-state actors. Rather, it identifies a legal framework that is compatible with existing law of war and international law distinctions between non-state and state actors.

Although this distinction is notable, it is not without risks. There is always a danger that cyber-regulations may be applied against individuals using technology for legitimate political dissent, which necessarily has a political purpose. While dissent is protected in the United States by the First Amendment, the use of cyberspace regulations to suppress dissent is a serious possibility in countries that do not have the same liberal democratic traditions, notably China and Russia.[52] Internet regulations in China are a troubling

---

DICTIONARY 1611 (9th ed. 2009) (defining terrorism as using violence "as a means of affecting political conduct").

[49] Mark Lander, *A Filipino Linked to "Love Bug" Talks About His License to Hack*, N.Y. TIMES, October 21, 2000, *available at* http://www.nytimes.com/2000/10/21/business/a-filipino-linked-to-love-bug-talks-about-his-license-to-hack.html.

[50] For example, the potentially global nature cyber-crime presents jurisdictional hurdles to comprehensive enforcement. While this Article advocates expanding the reach of criminal laws, *see infra* Part IV.A.1, it does not delve into the complexities of establishing extraterritorial jurisdiction.

[51] *See* NRC REPORT, *supra* note 17, at 20, §1.4 (on low cost); *id.* at 41 (on limited applicability of deterrence by threat of in-kind response); DOD STRATEGY, *supra* note 14, at 3 (discussing the power of small groups to cause significant harm due to the low barriers to entry for cyber-activity); Shanker & Bumiller, *supra* note 42 (noting that while most major efforts to penetrate military computer networks are still orchestrated by large rival nations, the technical expertise is certain to migrate to rogue states and nonstate actors).

[52] *See, e.g.*, Gjelten, *supra* note 21 (on Chinese and Russian efforts to control communication on the Internet).

testament to this fact.[53] As a foreign policy matter, the United States must ensure that any proposed domestic legislation (which may serve as a model for other countries) or international regime (which may be susceptible to multiple readings) clearly maintains online space for legitimate dissent while strengthening the legal tools to combat and punish cyber-attacks.[54] This definition seeks to keep legitimate dissent out of the category of cyber-attack by specifying that a cyber-attack's objective must be to undermine the function of a computer network. It would not include, for example, computer-based efforts to organize political protests.

The definition offered here adheres to the objective-based approach taken by the U.S. government, but it streamlines existing conceptions to facilitate uniformity. Moreover, by adding a "purpose," this definition enables policy-makers to distinguish between mere cyber-crime and cyber-attacks (that are, by definition, political in nature). Such a distinction is crucial to domestic and international efforts to implement cyber-security, since the legal approach to regular crime is distinct from the legal approaches to terrorism and warfare.

3. Cyber-Attack, Cyber-Crime, and Cyber-Warfare Compared

We summarize our definition of "cyber-attack" and the distinctions between "cyber-attack," "cyber-crime," and "cyber-warfare" in Figures 1 and 2.

---

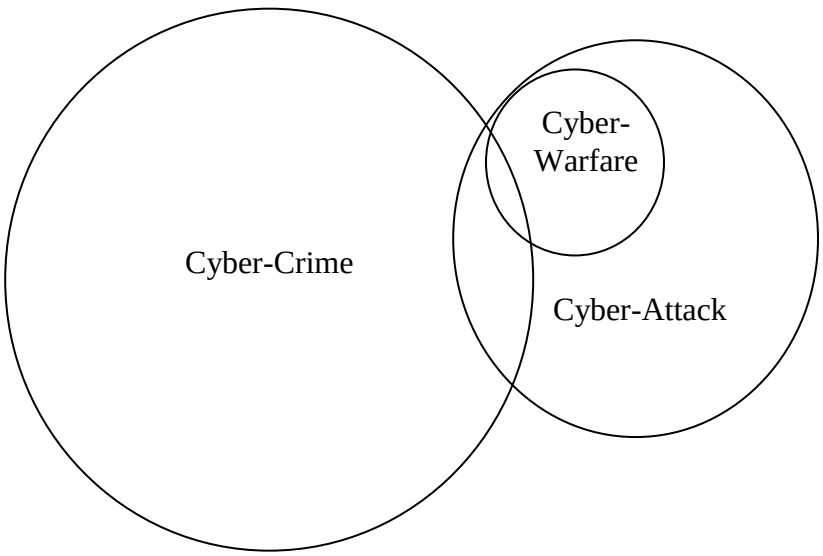
[53] China has also been embroiled in cyber-conflict with private entities as well—namely, Google and Yahoo. Since the early 2000's, the U.S.-based companies have been criticized for their cooperation with the Chinese government, both in policing internal dissidents and in censoring external information of a political nature. *See Yahoo 'Helped Jail China Writer,'* BBC NEWS (Sept. 7, 2005, 8:18 AM), http://news.bbc.co.uk/2/hi/4221538.stm; *Google Censors Itself for China*, BBC NEWS (Jan. 25, 2006, 8:45 AM), http://news.bbc.co.uk/2/hi/technology/4645596.stm. Pressure from the Chinese government for such cooperation comes in response to activity it labels as "cyber-attacks"—the dissemination of information that undermines civil and military stability. *See* Shanghai Cooperation Agreement, *supra* note 18.

[54] The White House's recent strategy paper on cyberspace addresses the danger that efforts to reduce cyber-attacks could stifle free speech. It notes that "the ability to seek, receive, and impart information and ideas through any medium and regardless of frontiers has never been more relevant" and urges that "exceptions to free speech in cyberspace must also be narrowly tailored." INTERNATIONAL STRATEGY FOR CYBERSPACE, WHITE HOUSE 5 (May, 2011), [hereinafter WHITE HOUSE CYBERSPACE STRATEGY] *available at* http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf. Protecting fundamental freedoms and privacy is one of the White House's seven high-level policy priorities for cyberspace, *id.*, at 23-24, and one of the three law enforcement policy priorities is to "[f]ocus cybercrime laws on combating illegal activities, not restricting access to the internet," *id.*, at 20.

FIGURE 1. ESSENTIAL CHARACTERISTICS OF DIFFERENT CYBER-ACTIONS

Type of Cyber-Action	Involves only non-state actors	Must be violation of criminal law, committed by means of a computer system	Objective must be to undermine the function of a computer network	Must have a political or national security purpose	Effects must be equivalent to an "armed attack," or activity must occur in the context of armed conflict
Cyber-Attack			√	√	
Cyber-Crime	√	√			
Cyber-Warfare			√	√	√

FIGURE 2: RELATIONSHIP BETWEEN CYBER-ACTIONS



In order to understand cyber-attack, it is important to appreciate the distinctions between cyber-attack and cyber-crime. Cyber-crime is a broad concept analytically distinct from cyber-attack. While, as with the concept of cyber-attack, there is no universally recognized definition of cyber-crime,[55] there are aspects of cyber-crime that are broadly recognized. In particular, cyber-crime is generally understood as the use of a computer-based means to commit an illegal act. One typical definition describes cyber-crime as "any crime that is facilitated or committed using a computer, network, or hardware device."[56] Cyber-crime, unlike the definition of cyber-attack proposed in this Article, is thus often defined by its means—that is, a computer system or network. As such, cyber-crime encompasses a very broad range of illicit activity. Among the priorities of the Department of Justice and FBI units addressing cyber-crime are fraudulent practices on the Internet, online piracy, storage and sharing of child pornography on a computer, and computer intrusions.[57] Unlike cyber-attacks, cyber-crimes need not undermine the target computer network (though in some cases they may do so), and most do not have a political or national security purpose. Finally, like all crimes, but unlike cyber-attacks, cyber-crimes are generally understood to be committed by

---

[55] *See, e.g.*, Sarah Gordon & Richard Ford, *On the Definition and Classification of Cybercrime*, J. COMPUTER VIROLOGY, no. 1, 2006, at 13, 13 ("Despite the fact that the word 'Cybercrime' has entered into common usage, many people would find it hard to define the term precisely."); Sylvia Mercado Kierkegaard, *International Cybercrime Convention* (2008), *available at* http://www.igi-global.com/viewtitlesample.aspx?id=7486 ("[T]here is still no accepted definition of what really constitutes cybercrime."); *see also* DEBRA LITTLEJOHN SHINDER & ED TITTEL, SCENE OF THE CYBERCRIME: COMPUTER FORENSICS HANDBOOK 16 (2002) ("[T]he definition of computer crime under state law differs, depending on the state.").

[56] Gordon & Ford, *supra* note 55, at 14. In addition, some proposed definitions are broad enough to include not only all crimes committed by means of a computer, but also any crime in any way involving a computer as means or target. *See, e.g.*, Shinder & Tittel, *supra* note 55, at 17 (referring to the Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders' broad definition of "computer-related crime," as compared to its narrower, means-based definition of "computer crime").

[57] *See generally* COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION, CRIMINAL DIVISION, U.S. DEPARTMENT OF JUSTICE, PROSECUTING COMPUTER CRIMES (2d ed. 2010), *available at* http://www.justice.gov/criminal/cybercrime/ccmanual/ccmanual.pdf; *Cyber Crime*, FBI, http://www.fbi.gov/about-us/investigate/cyber (last visited Sept. 23, 2011). The Council of Europe Convention on Cybercrime, similarly, covers a broad range of criminal activity committed by means of a computer, including "action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data." Council of Europe, ETS No. 185, Convention on Cybercrime, pmbl., Budapest (Nov. 23, 2001), entered into force July 1, 2004, *available at* http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

individuals, not states.[58]

Most cyber-crimes do not also constitute cyber-attack or cyber-warfare, as depicted in Figure 2. An act is only a cyber-crime when a non-state actor commits an act that is criminalized under state or international law. Consider the following three scenarios: First, a non-state actor commits an illegal act for a political or national security purpose and by means of a computer network but does *not* undermine that network. For example, an individual might commit a cyber-crime by expressing political dissent over the Internet where that dissent is illegal under state law. Similarly, an individual might commit a cyber-crime by hacking into a major bank's records with a national security or political purpose but without undermining the bank's system in the process. Second, a non-state actor commits an illegal act by means of a computer network—and undermines a computer network—but not for a political or national security purpose. Again consider the bank data hacker, who now manages to undermine the bank's online account system but whose only purpose is economic gain. This, too, would constitute a cyber-crime, but not a cyber-attack or cyber-warfare. Third, a non-state actor is engaged in illicit activity using a computer or network but does not undermine the function of a computer network and does not operate with a political or national security purpose. A person who transfers child pornography, for example, would commit a cyber-crime but not a cyber-attack, both because his actions do not undermine the function of a computer network and because he is not motivated by a political or national security purpose.

As shown in Figure 2, just as some cyber-crimes are neither cyber-attacks nor cyber-warfare, some cyber-attacks are neither cyber-crimes nor cyber-warfare. Two scenarios fall into this cyber-attack-only category. The first scenario includes attacks carried out by a state actor, outside the context of an armed conflict, provided its effects do not rise to the level of an armed attack. An example of this is the attack by Chinese government on the Falun Gong website in 2011.[59] Note that such attacks must still satisfy all elements of the cyber-attack definition, including undermining the function of a computer network for a political or national security purpose. As noted above, however, any act by a state actor automatically satisfies the political or national security purpose requirement.

The second cyber-attack-only scenario includes attacks by non-state actors that do not rise to the level of an armed attack and which do not constitute a cyber-crime, either because they have not been criminalized under

[58] While public officials may commit cyber-crimes while acting outside the scope of their authority, the actions of states, even if unlawful, are not considered to be crimes as such.
[59] *See supra* note 6 and accompanying text.

national or international law or because they do not use computer-based means. Practically speaking, it is unlikely for a private actor to purposefully[60] undermine the function of a computer network without also violating the law, but such gaps in the criminal law are conceptually possible. It is furthermore worth noting that a large majority of cyber-attacks would likely involve computer-based means, though such means are not necessary to cyber-attack under the definition proposed here.

While cyber-activity may constitute only cyber-crime or only cyber-attack, a substantial proportion of cyber-crimes are also cyber-attacks. The overlapping area between cyber-crime and cyber-attack seen in Figure 2 occurs when a non-state actor commits an illegal act by means of a computer network, undermines a computer network, *and* has a political or national security purpose. The consequences of this act would not rise to the level of an armed attack, or the activity would also constitute cyber-warfare. Note also that a state committing this very same act would not fall within this overlap, since only a non-state actor can commit a cyber-crime. Take, for example, a hypothetical group of individuals who hacked into the U.S. government's State Department server and shut it down out of disdain for the U.S. government. This instance would fall within the overlap between cyber-crimes and cyber-attacks given that a non-state actor committed the act, for a political or national security purpose, and it undermined a computer network.

Cyber-warfare is distinctive among the three cyber-categories considered here in that cyber-warfare *must* also constitute a cyber-attack. The overlapping area between cyber-attack and cyber-warfare (but not cyber-crimes) in Figure 2 includes two types of attacks. The first type includes attacks carried out by any actor in the context of an armed conflict, provided those actions could not be considered cyber-crimes, either because they do not constitute war crimes, or do not employ computer-based means, or both. The second type includes attacks carried out by a state actor, which produce effects equivalent to those of a conventional armed attack. Note that this use of force may be either lawful or unlawful; because the actor is a state actor, even unlawful actions do not constitute "cyber-crime."

Cyber-warfare can also constitute both cyber-attack and cyber-crime. The area of intersection between all three circles in Figure 2 includes two types of attacks carried out by a non-state actor. First, it includes attacks in the context of an existing armed conflict that undermine the function of a computer network for a political or national security purpose, violate the

[60] Because a cyber-attack must be "for a political or national security purpose," the only actions falling into this category would be purposeful. Thus, no *mens rea* element in a law would serve to exclude a cyber-attack from the zone overlapping with cyber-crime.

criminal law (for example, war crimes), and were committed by means of a computer system or network. Second, it includes attacks that produce effects equivalent to those of a conventional armed attack, undermine the function of a computer network for a political or national security purpose, and are violations of the criminal law committed by means of a computer system or network.

As summarized in these figures, then, a cyber-attack may be carried out by state or non-state actors, must involve active conduct, must aim to undermine the function of a computer network, and must have a political or national security purpose. Some cyber-attacks are also cyber-crimes, but not all cyber-crimes are cyber-attacks. Cyber-warfare, on the other hand, always meets the conditions of a cyber-attack. But not all cyber-attacks are cyber-warfare. Only cyber-attacks with effects equivalent to those of a conventional "armed attack," or occurring within the context of armed conflict, rise to the level of cyber-warfare. We say more about when this condition is met in Part II below.

B. Recent Cyber-Attacks

There are a variety of activities that fall within this Article's definition of cyber-attacks. The following—far from exhaustive—descriptions of cyber-incidents elucidate the variety and scope of recent cyber-attacks. They also introduce the wide-ranging challenges to regulating cyber-attacks.

1. Distributed Denial of Service Attacks

Distributed Denial of Service ("DDOS") attacks have been the most prevalent form of cyber-attack in recent years. In these attacks, coordinated botnets—collections of thousands of "zombie" computers hijacked by insidious viruses—overwhelm servers by systematically visiting designated websites. The attack in Burma, described above, was a DDOS attack, as was the attack on a Falun Gong Web site inadvertently aired on China Central Television. There are several other recent examples of such attacks.

After controversially moving a Soviet-era war memorial in April 2007, the densely wired[61] republic of Estonia suffered a DDOS attack. Such attacks often cause mere inconvenience, but this one nearly had life threatening

[61] Estonia has one of the highest network saturation rates in the world. RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT 13 (2010).

consequences—the emergency line to call for an ambulance or a fire truck was out of service for an hour.[62] Allegedly executed by networks of hackers,[63] authorities never officially attributed the attack to a state, but some suspect Russia's involvement due to the sophistication and scale of the attack.[64]

A similar fate befell Georgia in the summer of 2008, when the country found itself unable to communicate with the outside world over the Internet as Russian forces invaded South Ossetia.[65] Despite early speculations that the Russian government was behind the incident, it appears that the government may simply have been complicit as private hackers openly orchestrated the attack.[66]

Russians are certainly not the only source of DDOS attacks. In July 2009, a number of government and commercial websites in the United States and South Korea were shut down by a DDOS attack. Although South Korea quickly blamed North Korea,[67] the United States was more circumspect.[68] There remain some questions about where the attack originated. This serves to illustrate a common problem for cyber-attacks in general and DDOS attack in particular: By enlisting unsuspecting computers from around the world, botnets spin a web of anonymity around the attacker or attackers, making accurate attribution uniquely difficult.

2. Planting Inaccurate Information

---

[62] *Newly Nasty*, THE ECONOMIST, May 24, 2007, *available at* http://www.economist.com/node/9228757?story_id=9228757.

[63] Specifically, a youth movement (funded by the Russian government) later claimed responsibility for the attack. Noah Shachtman, *Kremlin Kids: We Launched the Estonian Cyber War*, WIRED (Mar. 11, 2009, 12:45 PM), http://blog.wired.com/defense/2009/03/pro-kremlin-gro.html.

[64] Jeffrey T.G. Kelsey, Note, *Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare*, 106 MICH. L. REV. 1427, 1429 (2008).

[65] *The Threat from the Internet: Cyberwar*, THE ECONOMIST, July 1, 2010, *available at* http://www.economist.com/node/16481504.

[66] Brian Krebs, *Report: Russian Hacker Forums Fueled Georgia Cyber Attacks*, WASH. POST SECURITY FIX BLOG (Oct. 16, 2008, 3:15 PM), http://voices.washingtonpost.com/securityfix/2008/10/report_russian_hacker_forums_f.html.

[67] Malcolm Moore, *North Korea Blamed for Cyber Attack on South Korea*, THE TELEGRAPH, July 8, 2009, *available at* http://www.telegraph.co.uk/news/worldnews/asia/southkorea/5778176/North-Korea-blamed-for-cyber-attack-on-South-Korea.html.

[68] Officials anonymously leaked qualified reports of U.S. suspicions that the attack emerged in North Korea. *U.S. Eyes N. Korea for 'Massive' Cyber Attacks*, MSNBC.COM (July 9, 2009, 3:31 AM), http://www.msnbc.msn.com/id/31789294/ns/technology_and_science-security.

Surreptitiously inputting inaccurate information in a computer system is another form of cyber-attack, known as a semantic attack. More sophisticated than the DDOS attack, a semantic attack causes the computer system to appear to operate normally, even as it fails.[69]

In 1999, for example, the United States developed a plan to feed false target data into the Serbian air defense command network, inhibiting Serbia's ability to target NATO aircraft.[70] This attack would have exploited the increasing reliance on computer networks that characterizes modern warfare. In the end, NATO forces abandoned the plan due to legal concerns about collateral damage.[71]

The Israeli Air Force employed a similar strategy on September 6, 2007 during its air strike against a nuclear facility in Syria. Israeli planes arrived undetected at their targets because of an earlier cyber-attack that compromised the Syrian air-defense system. The exact method of attack is unknown, but Israel apparently fed false messages to the radars, causing them to show clear skies on the night of the strike.[72]

Because these cyber-attacks frequently accompany, and facilitate, conventional attacks, attribution is less problematic. The difficulty here is in identifying when a cyber-attack has occurred, since the disruption remains hidden until its kinetic sequel.

3. Infiltrating a Secure Computer Network

For reasons explained above, cyber-espionage—stealing rather than planting information—is not included in most definitions of cyber-attack.[73] Once an attacker infiltrates a secure computer network, however, it can execute a variety of actions beyond passively harvesting intelligence. For example, the Stuxnet attack, in addition to being a semantic attack, targeted the secure computer networks at Iranian nuclear facilities for the purpose of disrupting the function of the nuclear facility.

Such an attack does not always destroy the computer network or the infrastructure it controls. In 2003, shortly before the invasion of Iraq, the United States infiltrated the Iraqi Defense Ministry email system to contact Iraqi officers with instructions for a peaceful surrender. The messages

---

[69] MARTIN C. LIBICKI, WHAT IS INFORMATION WARFARE? 77 (1995).
[70] William M. Arkin, *The Cyber Bomb in Yugoslavia*, WASHINGTONPOST.COM (Oct. 25, 1999), http://www.washingtonpost.com/wp-srv/national/dotmil/arkin.htm.
[71] Kelsey, *supra* note 64, at 1434-35.
[72] CLARKE & KNAKE, *supra* note 16, at 1-9.
[73] *See supra* text accompanying notes 34-37.

apparently worked: American troops encountered abandoned military equipment arranged in accordance with the email.[74] This cyber-attack was a "Command and Control Attack"—a term that includes any attack meant to interfere with the enemy's capacity to command and control its troops.

These incidents demonstrate that attacks need not arrive over the Internet, but may instead involve infiltrating separate, secure networks. These networks may include not only desktops and laptops, but the ubiquitous and unseen computing systems, such as industrial control systems, that facilitate modern life. Together, these examples also illustrate the growing number of cyber-attacks and the diversity of their forms and scope—making the project of crafting a legal approach to them all the more challenging. The next Part turns to examining when a cyber-attack rises to the level of "cyber-warfare" governed by the law of war—and when and how that law allows states to respond to such attacks.

II. LAW OF WAR AND "CYBER-WARFARE"

Although the term "cyber-warfare" has become part of common parlance, few have aimed to examine closely the scope of cyber-activity that might be governed by the law of war. In this Part, we aim to fill this gap by examining when a cyber-attack constitutes an armed attack under *jus ad bellum*—and thus can be accurately considered "cyber-warfare." We also examine how the laws governing conduct in the course of war—known as *jus in bello*—might apply to cyber-attacks. We do not attempt a detailed application of *jus ad bellum* and *jus in bello* to cyber-attacks, because such inquires are intensely fact-specific. Instead, we lay out the general types of cyber-attacks that would be governed by the law of war—and note how an attack's cyber-based nature complicates the traditional law of war analysis. We conclude that while the law of war provides useful guidelines for addressing some of the most dangerous forms of cyber-attack, the law of war framework ultimately addresses only a small slice of the full range of cyber-attacks.[75] Cyber-warfare is only a part of a much larger problem.

---

[74] CLARKE & KNAKE, *supra* note 16, at 9-10.

[75] Practitioners and scholars are divided on how easily the law of war can be applied to cyber-attacks. The Handbook guiding Navy, Marine, and Coast Guard operations, discussing information operations, states that "[l]egal analysis of intended wartime targets requires traditional law of war analysis." Dep't of the Navy, The Commander's Handbook on the Law of Naval Operations, § 8.11.1 (2007) [hereinafter Commander's Handbook]. Some scholars argue that "[t]he law of war targeting principles of military necessity, proportionality, and unnecessary suffering govern all uses of force, whatever means employed." Sean Watts,

It is worth noting at the outset that applying the existing law of war framework to cyber-attacks is extraordinarily challenging. The laws were, after all, written in the wake of World War II. Nothing was further from the minds of the drafters of the Geneva Convention than attacks carried out over a worldwide computer network. One particular challenge is how to address attacks that have no direct physical consequences. In Command and Control cyber-attacks, for example, the physical consequences do not result directly from the cyber-attack—instead, the cyber-attacks facilitate kinetic attacks. Perhaps for this reason, no state has ever claimed that any cyber-attack constitutes an "armed attack" giving rise to a right of self-defense under Article 51 of the U.N. Charter. Nor has any state to date argued that cyber-attacks generally constitute a prohibited use of force. The fact that such attacks are increasing in number and scope, however, suggests that there is a growing need for states to reach a consensus as to when a cyber-attack constitutes an armed attack or use of force. It also suggests that there may be a need for a more comprehensive legal framework to regulate activities—such as those causing widespread economic damage—that would not be governed by the law of war.[76]

We turn first to the most vital question under *jus ad bellum*—when would a cyber-attack rise to the level of an armed attack justifying self-defense under Article 51 of the U.N. Charter? As outlined in Figure 1 above, this Article concludes that the best test is whether a cyber-attack results in physical destruction—sometimes called a "kinetic effect"—comparable to a conventional attack. Arriving at this conclusion requires examining not only treaty text—which is quite general and vague—but also the meaning given to the text by state practice over time. Because an armed conflict has never begun solely in response to a cyber-attack, there is no state practice on what cyber-

---

Combatant Status and Computer Network Attack, 50 VA. J. INT'L L. 391, 425 (2010); *see also* Michael N. Schmitt, *Wired Warfare: Computer Network Attack and the* Jus in Bello, *in* COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW 187, 195 (Michael N. Schmitt & Brian T. O'Donnell eds., 2002) (arguing that existing norms remain intact, although a computer network attack offers new means to target non-military objectives); Major Eric Talbot Jensen, *Unexpected Consequences From Knock-On Effects: A Different Standard for Computer Network Operations?*, 18 AM. U. INT'L L. REV. 1145 (2003) (arguing that no new legal framework is necessary).

[76] Others argue that the law of war as it currently stands is insufficient and in need of revision in light of cyber-attacks. *See* Hollis, *supra* note 9, at 1028; 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).

attacks justify an armed response. Accordingly, the legal analysis here is necessarily speculative.

We turn next to applying the law of war once armed conflict has commenced, or *jus in bello*, to cyber-warfare. This body of law is less speculative, as there have been documented incidents of cyber-attacks in the context of an armed conflict. Even so, it is challenging to apply even widely accepted core *jus in bello* principles of proportionality and distinction to cyber-warfare. These challenges illustrate the importance of commencing an international dialogue on these issues to bring clarity to existing law of war principles in this context. They also demonstrate that the law of war alone cannot address the new challenges posed by cyber-attacks.

A. *Jus ad Bellum*

What law governs states' right to resort to armed force in self-defense against cyber-attacks? To answer this question, we proceed in three steps. First, we outline the general prohibition on the use or threat of force in international relations contained in Article 2(4) of the U.N. Charter. Second, we discuss the exceptions to that prohibition for collective security operations and self-defense, with particular attention to when a cyber-attack would justify resort to self-defense. Finally, we close by explaining the customary international law requirements of *jus ad bellum* necessity and proportionality and by detailing the limitations and problems of applying *jus ad bellum* requirements to cyber-attacks. We conclude that states may only use defensive armed force in response to a cyber-attack if the effects of the attack are equivalent to those of a conventional armed attack.

1. Governing Legal Principles

Article 2(4) of the U.N. Charter provides that member states "shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[77] This prohibition is complemented by a customary international law norm of non-intervention, which prohibits states from interfering in the internal affairs of other states.[78] The International Court of Justice ("ICJ") has held that, where

[77] U.N. Charter art. 2, para. 4.

[78] *See* Manila Declaration on the Peaceful Settlement of International Disputes, G.A. Res. 37/10, Annex, U.N. Doc. A/RES/37/10 (Nov. 15, 1982); Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States in

the interference takes the form of a use or threat of force, the customary international law norm of non-intervention is coterminous with Article 2(4).[79]

The precise scope of the international prohibition on the threat or use of force has been the subject of intense international and scholarly debate. Weaker states and some scholars have argued that Article 2(4) broadly prohibits not only the use of armed force, but also political and economic coercion. Nonetheless, the general consensus is that Article 2(4) prohibits only armed force.[80]

Discussions about cyber-attacks have the potential to reignite debates over the scope of Article 2(4).[81] Because it is much less costly to mount cyber-attacks than to launch conventional attacks, and because highly industrialized states are generally more dependent upon computer networks and are more vulnerable to cyber-attacks, cyber-attacks may prove to be a powerful weapon of the weak. This change in the cost structure of offensive capabilities may both increase the likelihood of cyber-attacks and change the political valence of different interpretations of Article 2(4)'s scope. Stronger states may begin to favor more expansive readings of Article 2(4) that prohibit coercive activities like cyber-attacks.[82] At present, however, the general consensus remains that Article 2(4) prohibits only physical armed force.

Accordance with the Charter of the United Nation, G.A. Res. 25/2625, U.N. Doc. A/RES/25/2625 (Oct. 24, 1970).

[79] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, para. 209 (June 27) ("[A]cts constituting a breach of the customary principle of non-intervention, will also, if they directly or indirectly involve the use of force, constitute a breach of the principle of non-use of force in international relations."). It is possible, however, that to the extent that cyber-attacks do not constitute a use of force, they may nevertheless violate the customary international law norm of non-intervention, as discussed below.

[80] Daniel B. Silver, *Computer Network Attack as a Use of Force Under Article 2(4) of the United Nations Charter*, *in* COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW, *supra* note 75, at 73, 80-82. The principal arguments for the prevailing view are: (1) that Article 2(4) was conceived against a background of efforts to limit unilateral recourse to armed force, not economic and political coercion; (2) that the *travaux preparatoires* show that the San Francisco Conference rejected a proposal that would have extended Article 2(4) to include economic sanctions; and (3) that the ICJ has held that financing armed insurrection does not constitute force, indicating that other economic measures that are even less directly related to armed violence would not constitute prohibited force either. *Id.* at 81. There remains some ambiguity, however, as to the extent to which Article 2(4) prohibits non-military physical force, such as flooding, forest fires, or pollution. *Id.*, at 82-83.

[81] *See* Waxman, *supra* note 18.

[82] Walter Sharp has advocated that the United States make precisely this kind of strategic interpretive move, arguing that a broad array of coercive cyber-activities should fall within Article 2(4)'s prohibition. WALTER GARY SHARP, SR., CYBERSPACE AND THE USE OF FORCE 129-33 (1999).

At the same time, there are preliminary indications that cyber-attacks as defined in this Article may violate the customary international law norm of nonintervention. First, states generally do not engage in cyber-attacks openly, but rather tend to try to hide their responsibility through technical means[83] and by perpetrating the attacks through non-state actors with ambiguous relationships with state agencies.[84] As Thomas Franck has observed, "Lying about facts . . . is the tribute that scofflaw governments pay to international legal obligations they violate."[85] In other words, the very fact that states attempt to hide their cyber-attacks may betray a concern that such attacks may constitute unlawful uses of force. Second, when states acknowledge that they have been victims of cyber-attack, they and their allies tend to denounce and condemn the attacks.[86] Third, in its common approach to cyber-defense, NATO has indicated that cyber-attacks trigger states parties' obligations under Article 4 of the NATO treaty,[87] which applies only when "the territorial integrity, political independence or security of any of the Parties is threatened."[88] The invocation of this provision strongly suggests that NATO member states believe that cyber-attacks violate the customary norm of nonintervention or a related international law norm.[89] Still, as the next Subsection explains, the fact that a cyber-attack is unlawful does not necessarily mean that armed force can be used in response.

2. Exceptions for Collective Security and Self-Defense

---

[83] *See* Matthew J. Sklerov, *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect their Duty to Prevent*, 201 MIL. L. REV. 1, 74-75 (2009).

[84] *See, e.g.*, CARR, *supra* note 16, at 29 ("Hacking attacks cloaked in nationalism are not only not prosecuted by Russian authorities, but they are encouraged through their proxies, the Russian youth organizations, and the Foundation for Effective Policy.").

[85] Thomas M. Franck, *Legitimacy After Kosovo and Iraq, in* INTERNATIONAL LAW AND THE USE OF FORCE AT THE TURN OF THE CENTURIES: ESSAYS IN HONOUR OF V. D. DEGAN 73 (V. Crnić-Grotić & M. Matulović eds., 2005).

[86] *See, e.g.*, Ian Traynor, *Russia Accused of Unleashing Cyberwar to Disable Estonia*, The Guardian, May 17, 2007, http://www.guardian.co.uk/world/2007/may/17/topstories3.russia (detailing the reactions by Estonian, EU, and NATO officials to a cyber-attack on Estonia).

[87] NATO Agrees on Common Approach to Cyber Defence, EURACTIV.COM, Apr. 4, 2008, *available at* http://www.euractiv.com/en/infosociety/nato-agrees-common-approachcyber-defence/article-171377.

[88] North Atlantic Treaty, Apr. 4, 1949, art. 4, 63 Stat. 2241, 34 U.N.T.S. 243, *available at* http://www.nato.int/cps/en/natolive/official_texts_17120.htm

[89] As noted below, however, NATO does not believe that cyber-attacks rise the level of armed attacks justifying self defense. *See infra* note 106 and accompanying text.

Article 2(4)'s blanket prohibition on the use or threat of force is subject to two exceptions: actions taken as part of collective security operations and actions taken in self-defense.

The first exception falls under Article 39 of the U.N. Charter. Article 39 empowers the Security Council to "determine the existence of any threat to the peace, breach of the peace, or act of aggression, and [to] make recommendations, or decide what measures shall be taken . . . to maintain or restore international peace and security."[90] The Security Council may employ "measures not involving the use of armed force"[91] and authorize "actions by air, sea, or land forces."[92] Collective security operations under Article 39 can be politically difficult, however, because they require authorization by the often deadlocked or slow-moving Security Council. Moreover, lawful collective security operations are easily identifiable and relatively uncontroversial. For all of these reasons, if the Security Council authorizes a use of force in response to, or in the form of, a cyber-attack, a state's lawful actions will likely be within the scope of that authorization.

The second exception to Article 2(4) is articulated in Article 51, which provides that "[n]othing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs."[93] Lawful self-defense is much harder to define and identify than lawful collective security operations. Indeed, in most armed conflicts, both sides claim to be acting in self-defense, and the international debates tend to focus on factual and political disputes rather than legal doctrine.[94] It is clear, however, that the critical question determining the lawfulness of self-defense is whether or not an armed attack has occurred. Many agree that a cyber-attack may rise to the level of an armed attack.[95]

The term "armed attack" is linguistically distinct from and has been interpreted to be substantively narrower than several other related terms in the

---

[90] U.N. Charter art. 39.
[91] *Id.* art. 41.
[92] *Id.* art. 42.
[93] *Id.* art. 51. For example, the White House's recent cyberspace strategy paper includes the right of self-defense as one of the norms that should guide conduct in cyberspace. *See* WHITE HOUSE CYBERSPACE STRATEGY, *supra* note 54, at 10.
[94] CHRISTINE GRAY, INTERNATIONAL LAW AND THE USE OF FORCE 95-96 (2004).
[95] *See, e.g.*, WHITE HOUSE CYBERSPACE STRATEGY, *supra* note 54, at 14 ("When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. All states possess an inherent right to self-defense, and we recognize that certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners.").

U.N. Charter.[96] For example, there may be acts that violate Article 2(4)'s prohibition on the use or threat of force that do not rise to the level of an armed attack and do not trigger the right of self-defense under Article 51. The ICJ has indicated that cross-border incursions that are minor in their "scale and effects" may be classified as mere "frontier incidents" rather than "armed attacks."[97] Instead, armed attacks must be of sufficient gravity to constitute "most grave forms of the use of force."[98] This does not leave states unable to respond to low-level violations of their sovereignty; even if they may not resort to defensive force, states may engage in retorsions or non-forceful countermeasures.[99] To the extent that cyber-attacks do not qualify as armed attacks triggering the right of self-defense, countermeasures could potentially take the form of responsive cyber-attacks (provided that they did not constitute a use of force in violation of treaty and customary international law and that the need to induce a return to compliance with international law still exists).[100]

Not every cyber-attack constitutes an armed attack. In scholarly debates over the application of *jus ad bellum* to cyber-attacks, three leading views have emerged to determine when a cyber-attack constitutes an armed

---

[96] *See* Yoram Dinstein, Computer Network Attack and Self-Defense, *in* COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW, *supra* note 75, at 100-01.

[97] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 ICJ 14, para. 195 (June 27); *cf.* Definition of Aggression, G.A. Res. 29/3314, Annex, art. 2, U.N. Doc. A/Res/29/3314 (Dec. 14, 1974) (determining that "[t]he First use of armed force by a State in contravention of the Charter shall constitute prima facie evidence of an act of aggression although the Security Council may . . . conclude that a determination that an act of aggression has been committed would not be justified in the light of other relevant circumstances, including the fact that the acts concerned or their consequences are not *of sufficient gravity*" (emphasis added)). Scholars generally agree that there is a gap between the prohibition on the use of force and the right of self-defense. *See, e.g.*, Dinstein, *supra* note 96, at 99, 100-01.

[98] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 ICJ 14, para. 191 (June 27).

[99] Retorsions are lawful unfriendly acts made in response to an international law violation by another state; countermeasures are acts that would be unlawful if not done in response to a prior international law violation. U.N. Int'l Law Comm'n Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries, ch. II, commentary *in* Report of the International Law Commission to the General Assembly, 56 U.N. GAOR, 53d Sess., Supp. No. 10, at 31,80, U.N. Doc. A/56/20 (2001) [hereinafter Draft Articles]. *See infra* Part III.A for a more detailed discussion of countermeasures.

[100] *See* OFFICE OF GEN. COUNSEL, DEP'T OF DEF., AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS (Nov. 1999), *reprinted in* COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW, *supra* note 75, at 459, 484-85 [hereinafter DOD Memo] ("If the provocation is not considered to be an armed attack, a similar response will also presumably not be considered to be an armed attack.").

attack that triggers the right of armed self-defense: the instrument-based approach, the target-based approach, and the effects-based approach.[101]

One scholar has given the moniker "instrument-based" to the classical approach to the armed attack inquiry.[102] Under this view, a cyber-attack alone will almost never constitute an armed attack for purposes of Article 51 "because it lacks the physical characteristics traditionally associated with military coercion"—in other words, because it generally does not use traditional military weapons.[103] This approach treats a cyber-attack as an armed attack only if it uses military weapons. For example, bombing computer servers or Internet cables could meet the requirements of an armed attack if the strike was of sufficient gravity.

The text of the U.N. Charter provides some support for the instrument-based approach, since Article 41 characterizes the "partial or complete interruption . . . of . . . telegraphic, radio, and other means of communication" as a "measure[] not involving the use of armed force."[104] The U.N. General Assembly's Definition of Aggression also implicitly supports the instrument-based view: it lists a number of acts that would constitute "aggression" under Article 39—a broader category than armed attack under Article 51—and all of them involve military weapons or force.[105] NATO has also signaled its agreement with this view; its new common approach to cyber-defense establishes that a cyber-attack will obligate member states to "consult" with one another under Article 4 of the NATO treaty, but a cyber-attack will not

---

[101] Once a state has been the victim of an armed attack, a further question arises as to against whom the state can respond. Where the armed attack is perpetrated by a state, this question is easily answered—self-defense may be directed against the perpetrating state. However, cyber-attacks may be perpetrated by non-state actors or by actors with unclear affiliations with state security agencies. Although some scholars argue that cyber-attacks (and conventional attacks) must be attributable to a perpetrating state in order for the victim state to take defensive action that breaches another state's territory, others—drawing on traditional jurisprudence on self-defense—argue that states possess the right to engage in self-defense directly against non-state actors if certain conditions are met. *See* Jordan J. Paust, *Self-Defense Targetings of Non-State Actors and Permissibility of U.S. Use of Drones in Pakistan*, 19 J. TRANSNAT'L L. & POL'Y (forthcoming 2010), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1520717 ("The vast majority of writers agree that an armed attack by a non-state actor on a state, its embassies, its military, or other nationals abroad can trigger the right of self-defense addressed in Article 51 of the United Nations Charter, even if selective responsive force directed against a non-state actor occurs within a foreign country.").

[102] Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885, 909 (1999); *see also* Hollis, *supra* note 9, at 1041.

[103] Hollis, *supra* note 9, at 1041.

[104] U.N. Charter art. 41.

[105] Definition of Aggression, *supra* note 97, art. 3.

constitute an armed attack that obligates member states to assist one another under Article 5 of the treaty.[106]

The instrument-based approach's chief advantage is simplicity of application, since uses of military weapons and force are relatively easy to identify. However, because cyber-attacks have the potential to cause catastrophic harm without employing traditional military weapons, most scholars have rejected the instrument-based approach to defining armed attacks as dangerously outdated.

Recognizing the fundamental inability of the instrument-based approach to account for harms not caused by conventional means, the target-based approach classifies as an armed attack any cyber-attack that targets a sufficiently important computer system.[107] The primary aim of this approach is to determine when a cyber-attack portends imminent and sufficient harm to justify the use of anticipatory self-defense in response.[108]

While the target-based approach has the benefit of allowing for aggressive protection of critical national systems, it broadly sanctions forceful self-defense, increasing the likelihood that cyber-conflicts will escalate into more destructive conventional armed conflicts.[109] A cyber-attack need only penetrate a critical system to justify a conventional military response that could start a physical, kinetic war. This approach could greatly harm the security of the international community by making war much more likely.

Finally, the effects-based approach classifies a cyber-attack as an armed attack based on the gravity of its effects. Steering a middle course between the instrument- and target-based views, the effects-based approach is the most promising and most widely accepted approach. Different versions of the effects-based approach may measure that gravity by reference to any of a variety of factors, from the sheer severity of the harm to the length of the

---

[106] North Atlantic Treaty, arts. 4, 5, 63, *supra* note 88; NATO Agrees on Common Approach to Cyber Defence, *supra* note 87.

[107] Walter Sharp, the leading proponent of this approach, argues that a cyber-attack constitutes an armed attack, and would grant the target the right to use force in self-defense, whenever it penetrates any critical national infrastructure system, regardless of whether it has yet caused any physical destruction or casualties. SHARP, *supra* note 82, at 129-30; *see also* Sean M. Condron, *Getting it Right: Protecting American Critical Infrastructure in Cyberspace*, 20 HARV. J.L. & TECH. 403, 415-16 (2007) (advocating a similar approach); Eric Talbot Jenson, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense*, 38 STAN. J. INT'L L. 207, 208-09 (2002) (same).

[108] Hollis, *supra* note 9, at 1041 n.73.

[109] Sklerov, *supra* note 83, 54 n.352 (criticizing the target-based approach for encouraging escalation and advocating an effects-based approach).

causal chain between the cyber-attack itself and the ultimate harm. But all versions of this approach share a common orientation towards the inquiry.

The problem with the effects-based approach, however, lies in articulating *ex ante* what types of effects justify self-defense.[110] Consider, for example, an attack on an air traffic control system, an attack that disables a regional electrical power grid an attack on the New York Stock Exchange or national financial networks, or the 2007 cyber-attack on prominent Estonian websites. Which of these cyber-attacks, if any, have effects large enough to be considered armed attacks justifying the use of defensive force in response? All of these attacks may cause small- or large-scale civilian deaths and infrastructure damage, but it would be difficult for the aggressor country to predict the outcome of any individual attack. Different versions of the effects-based approach may reach different conclusions for each of these examples.

Professor Michael Schmitt, the first proponent of the effects-based approach for determining when a cyber-attack should be considered an armed attack, argues that a cyber-attack's effects should be measured by reference to six factors: (1) severity, the type and scale of the harm; (2) immediacy, how quickly the harm materializes after the attack; (3) directness, the length of the causal chain between the attack and the harm; (4) invasiveness, the degree to which the attack penetrates the victim state's territory; (5) measurability, the degree to which the harm can be quantified; and (6) presumptive legitimacy, the weight given to the fact that, in the field of cyber-activities as a whole, cyber-attacks constituting an armed attack are the exception rather than the rule.[111] These factors are illuminating, but they call for such a wide-ranging inquiry that they may not provide sufficient guidance to decision makers.[112] In other words, different analysts applying this version of the effects-based approach might plausibly classify all or none of the examples listed above as armed attacks.

Daniel Silver, former General Counsel of the CIA and National Security Agency, argues instead that the key criterion determining when a cyber-attack constitutes an armed attack is the severity of the harm caused. A cyber-attack justifies self-defense "only if its foreseeable consequence is to

---

[110] This difficulty is aggravated by the reality that "the indirect effects" of cyber-attacks are often "more consequential" than the immediate ones. NRC REPORT, *supra* note 17, at 30.

[111] Schmitt, *supra* note 102, at 914-15.

[112] *See* Silver, *supra* note 80, at 89 (claiming that "examination of [Schmitt's] criteria suggests that virtually any event of [computer network attack] can be argued to fall on the armed force side of the line"); *see also* Jason Barkham, *Information Warfare and International Law on the Use of Force*, 34 N.Y.U.J. INT'L L. & POL. 57, 85-86 (2001) (criticizing Schmitt's use of presumptive legitimacy as a criterion, as well as Schmitt's assumption that policymakers will be able to engage in a thorough factual inquiry when responding to cyber-attacks).

cause physical injury or property damage and even then, only if the severity of those foreseeable consequences resembles the consequences that are associated with armed coercion."[113] Of course, foreseeability is a notoriously malleable and indeterminate legal requirement, since it is extremely difficult to specify in advance exactly how long a causal chain must stretch before it is no longer appropriate to find liability—particularly in the area of cyber-attacks. This test would treat an attack on the air traffic control system causing planes to crash as an armed attack and might treat an attack disabling a regional electrical grid as an armed attack. But it would not treat attacks on websites, or even mere penetration of critical computer systems, as armed attacks. Attacks on financial systems present a hard case for this approach—the analysis depends on whether one considers scrambled financial information to be "property damage."

It is also important to note that purpose of the attack is already accounted for in the definition of cyber-attack recommended herein—that is, that the attack must have been committed for a political or national security purpose. Therefore unintended national security consequences of an attack, should the attack not have had national or security purposes at the outset, would not be considered a cyber-attack or cyber-warfare under this definition.

This version of the effects-based approach provides the best balance between enabling states to adequately respond to catastrophic cyber-attacks and preventing states from resorting to armed force too easily. The test defines a small core of harmful cyber-attacks that rise to the level of an armed attack.[114] It also focuses the armed attack analysis on a limited set of criteria—particularly severity and foreseeability.[115]

3. Ad Bellum *Necessity and Proportionality*

In addition to overcoming Article 2(4)'s prohibition on the use of force, a state's use of armed force in response to a cyber-attack must also comply with the *jus ad bellum* principles of necessity and proportionality under customary international law. The principle of necessity requires that force must be used only as a last resort, when peaceful means, such as a diplomatic

[113] Silver, *supra* note 80, at 90-91.
[114] *Id.* at 92.
[115] The Department of Defense has signaled its approval of this approach. *See* DOD Memo, *supra* note 100, at 483 (arguing "the consequences are likely to be more important than the means used," and providing examples of cyber-attacks that would cause civilian deaths and property damage).

settlement, cannot achieve the state's overall aim.[116] Proportionality extends this logic, prohibiting force if the overall scope and intensity of force is excessive in relation to the state's actual or imminent danger.[117] The United States has acknowledged that these principles apply to military responses to cyber-attacks.[118]

While principles of necessity and proportionality are clear, applying those principles to state responses to cyber-attacks is challenging. Evaluating whether an invocation of self-defense complies with the principles of necessity and proportionality is difficult and fact-intensive even for conventional attacks, and cyber-attacks present hard new questions. For example, cyber-attacks rising to the level of armed attacks may require decision makers to devise ways of measuring harm to computer networks and its indirect effects against more conventional kinds of harm in order to determine what would constitute a lawful response.

This Section demonstrates that applying the existing *jus ad bellum* framework in the context of cyber-attacks is challenging—and can address only a small subset of the broad range of cyber-attacks. An *ad bellum* analysis will be relevant for regulating the use of or response to only cyber-attacks addressed by Security Council resolutions and which meet the standard for an armed attack giving rise to a right of self-defense. Part III of this Article explores other international legal regimes that may help to regulate cyber-attacks that do not fall within these narrow boundaries. First, however, the following Section describes the law of war framework governing cyber-attacks occurring in the context of an ongoing armed conflict.

B. *Jus in Bello*

---

[116] *See* R.Y. Jennings, *The* Caroline *and* McLeod *Cases*, 32 AM. J. INT'L L. 82, 89 (1938) (quoting Secretary of State Daniel Webster's letter to his British counterpart concerning the *Caroline* incident as follows: "It must be shown that admonition or remonstrance to the persons on board the *Caroline* was impracticable, or would have been unavailing . . . but that there was a necessity, present and inevitable, for attacking her . . . .").

[117] Robert D. Sloane, *The Cost of Conflation: Preserving the Dualism of Jus Ad Bellum and Jus in Bello in the Contemporary Law of War*, 34 YALE J. INT'L L. 47, 108-09 (2009) ("Ad bellum proportionality is . . . parasitic on ad bellum necessity . . . . An act is ad bellum disproportionate if the same ad bellum objective sought by force clearly could have been achieved by diplomacy or another nonviolent strategy at a roughly comparable, or even moderately greater, cost.").

[118] *See* WHITE HOUSE CYBERSPACE STRATEGY, *supra* note 54, at 14 ("[W]e will exhaust all options before military force whenever we can; will carefully weight the costs and risks of action against the costs of inaction; and will act in a way that reflects our values and strengthens our legitimacy, seeking broad international support whenever possible.").

Although a cyber-attack has never instigated an armed conflict, cyber-attacks have been used in wars in response to traditional provocations. This Section examines the relationship between traditional *jus in bello* requirements and cyber-attacks employed in armed conflicts. The novel conditions of cyber-warfare pose novel challenges to applying *jus in bello* principles of proportionality, distinction, and neutrality. Because cyber-attacks are often not immediately lethal or destructive and may cause only temporary incapacity of network systems, it may be hard to evaluate whether a cyber-attack is proportional. It can also be nearly impossible to distinguish between combatants, civilians directly participating in hostilities, civilians engaged in a continuous combat function, and protected civilians in the context of cyber-attacks. Finally, the ease of masking the source of a cyber-attack makes enforcement of neutrality duties complicated and expensive.

1. In Bello *Necessity*

Although the necessity of a cyber-attack may be difficult to evaluate, this difficulty arises from line-drawing debates that did not originate in cyber-warfare and are not unique to *in bello* cyber-attack. *In bello* necessity relates to the concrete military advantage to be gained from a specific hostile act. An individual cyber-attack may be unnecessary if it does not advance the military's objective.[119] While cyber-attacks must be necessary to be lawful, evaluating their *in bello* necessity does not present novel challenges.

2. In Bello *Proportionality*

The *in bello* proportionality requirement prohibits "[a]n attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated."[120] To

[119] In contrast, the *ad bellum* necessity analysis helps determine if non-forcible measures to abate a threat are inadequate, excusing an otherwise unlawful use of force.

[120] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol 1), art. 51(5)(b), June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Protocol Additional I]; *see also id.* art. 85(3)(b). An indiscriminate attack, defined by *excessive effect*, is not to be confused with an attack that does not discriminate amongst civilian and military objectives, which is defined by *objective*, and is prohibited by art. 85(3)(a). *See infra* Part II.B.3. Some scholars argue that, given the ability to avoid civilian casualties or damage to property and achieve the same military advantage, a state *must* do so. *See* DIMITRIOS DELIBASIS, THE RIGHT TO NATIONAL SELF-DEFENSE IN INFORMATION WARFARE OPERATIONS 268 (2007) (arguing that the "unmatched accuracy" of

conduct a *jus in bello* proportionality analysis, a military decision maker must weigh potential civilian casualties, destruction of civilian property, and the loss of indispensable civilian items against the benefit of achieving a military objective.[121] Unfortunately, due to the nature of harm they inflict, the proportionality of cyber-attacks poses unique challenges.

It is difficult to evaluate whether an attack would be proportional according to the relevant categories of "loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof," as the typical direct effects of cyber-attacks may be non-lethal or temporary, yet severe.[122] Furthermore, how should the temporary incapacity of critical systems be evaluated?[123] For example, a cyber-attack that effectively stops the transmission of information through the Internet might merely inconvenience the populace—or it might result in hospitals being unable to communicate vital information, leading to loss of life. An *in bello* proportionality analysis requires anticipating the probable consequences of an action, but that may be difficult, if not impossible, in the context of cyber-warfare. Just as cyber-attacks may change the understanding of an armed attack under Article 2(4),[124] cyber-attacks may also change the weight given to temporary or non-lethal consequences.

3. Distinction

---

information warfare means that cyber-attacks "practically nullif[y] the element of chance embodied in all military entanglements"); Dakota S. Rudesill, *Precision War and Responsibility: Transformational Military Technology and the Duty of Care Under the Laws of War*, 32 YALE J. INT'L L. 517, 535 (2007) (arguing that the United States might be held to heightened standard of care due to advances in military technology).

[121] Protocol Additional I, *supra* note 120, arts. 51(5)(b), 54, 57(2)(a)(iii). After deciding that the target is a military objective, the elements of the balancing test include "target selection, the means and methods chosen for the military strike, the lack of negligence in the execution of the military strike, and the determination of what constitutes the military advantage of a particular military strike." Randy W. Stone, *Protecting Civilians During Operation Allied Force: The Enduring Importance of the Proportional Response and NATO's Use of Armed Force in Kosovo*, 50 CATH. U. L. REV. 501, 522 (2001).

[122] Protocol Additional I, *supra* note 120, art. 57(2)(a)(iii).

[123] Similar questions arise in debates around non-lethal deployments of biological and chemical weapons, such as riot agents. *See* James D. Fry, *Gas Smells Awful: U.N. Forces, Riot-Control Agents, and the Chemical Weapons Convention*, 31 MICH. J. INT'L L. 475 (2010); Mirko Sossai, *Drugs as Weapons: Disarmament Treaties Facing the Advances in Biochemistry and Non-Lethal Weapons Technology*, 15 J. CONFLICT & SECURITY L. 5 (2010).

[124] *See supra* Part II.A.I, regarding debates over Article 2(4) in the context of cyber-attack.

The distinction requirement presents another large challenge in evaluating the *in bello* lawfulness of a cyber-attack.[125] This principle requires distinguishing between civilian and military personnel and restricting attacks to military objectives.[126] Additionally, military commanders must employ weapons that may be targeted accurately and must use this capability to distinguish between civilian and military objectives.[127] By extension, the law of war prohibits *in bello* cyber-attacks that are uncontrollable, unpredictable, or do not discriminate between civilian and military objectives.[128] Furthermore, Protocol Additional I prohibits attacks that deny the civilian population indispensable objects, such as food or water supplies.[129]

There are a few situations where the principle of distinction is easily applied to cyber-attacks, such as when the target is a military air traffic control system and the attack causes a troop transport to crash.[130] Similarly, there are some scenarios where it is easy to determine that a cyber-attack would be unlawful, since some objects—such as hospitals, museums, and places of worship—enjoy special protection even though they may offer military

---

[125] *See* DELIBASIS, *supra* note 120, at 274 (arguing that information warfare will likely run afoul of distinction and proportionality); Kelsey, supra note 64, at 1431 (2008) (arguing that cyber-attacks will often violate the principles of distinction and neutrality).

[126] Louise Doswald-Beck, *Some Thoughts on Computer Network Attack and the International Law of Armed Conflict*, *in* COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW, *supra* note 75, at 163, 166. Distinction also imposes responsibilities on combatants to identify themselves in order to facilitate distinction on the battlefield and to receive the protections that are due to combatants. *See* Watts, *supra* note 75, at 438-39. States also have a duty to facilitate distinction: "The application of this duty requires that personnel and equipment directly engaged in information warfare be located in facilities whose attack by kinetic weapons would not result in excessive collateral damage." Brown, *supra* note 75, at 192.

[127] *See* Jensen, *supra* note 75, at 1154. The ICJ has found that nuclear weapons may violate international humanitarian law if they cannot be used in a manner that distinguishes between civilians and military objectives. Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, para. 78 (Jul. 8).

[128] Military objectives are targets that meet two criteria: they serve a military purpose and their incapacitation conveys a definite advantage. Protocol Additional I, *supra* note 120, art. 52(2). For example, the first missile strikes of Operation Desert Storm in 1991 targeted Iraqi radar stations. Sean P. Kanuck, Recent Development, *Information Warfare: New Challenges for Public International Law*, 37 HARV. INT'L L.J. 272, 282 (1996). On distinction, *see* Doswald-Beck, *supra* note 126, at 168; Brown, *supra* note 75, at 195 (comparing malicious code, which is indiscriminate, to biological weapons). Schmitt also argues that indiscriminate weapons are unlawful, including in that category not only cyber-attacks that cannot distinguish civilian and military objects, but also those which cannot be limited to a military objective. Schmitt, *supra* note 75, at 201 (citing Protocol Additional I, *supra* note 120, art. 51(4)).

[129] Protocol Additional I, *supra* note 120, art. 54(2).

[130] *Id.* at 195.

advantage.[131] Cyber-attacks against the networks that manage these targets, like any other attack on these objects, would be unlawful.[132]

Aside from these traditionally protected objects, the distinction analysis will often be complicated in the context of a cyber-attack because the likely targets are used by a multiplicity of actors at once. Ninety-five percent of military communications use civilian networks at some stage,[133] so it is probable that civilian networks will be considered potential military targets.[134] As much of cyberspace is dual use—used by both the military and civilians—upholding the distinction requirement in cyberspace will become difficult.

In addition, civilian involvement in carrying out cyber-attacks raises questions about who can be targeted for participation in cyber-attacks and who can carry out cyber-attacks—questions that are challenging to evaluate under the distinction requirement and are ultimately beyond the scope of this Article.

a. Who May Lawfully Be Targeted in Cyber-Attacks?

Under the law of war, only three categories of individuals may be lawfully targeted: combatants, civilians directly participating in hostilities, and civilians acting in a continuous combat function. Civilians lose their right not to be targeted to the extent that they "participate directly in hostilities."[135] Furthermore, under recent guidance from the International Committee of the Red Cross, civilians who adopt a continuous combat function may also be targeted.[136] The unique characteristics of civilian contributions to cyber-attacks blur the line between direct participation, continuous combat function, and other types of involvement in the execution of hostilities.[137]

The civilian designer of a weapons system has traditionally not been thought of as a direct participant in hostilities. However, the programmer who works with military intelligence may tweak the code to carry out the intent of

---

[131] Protocol Additional I, *supra* note 120, art. 85(4)(d).
[132] Schmitt, *supra* note 75, at 200; Brown, *supra* note 75, at 199.
[133] Antolin-Jenkins, *supra* note 10, at 133.
[134] Jensen later argues that, given that military use of civilian infrastructure makes it a legitimate military target, the U.S. government has a duty to protect civilian networks from cyber-attacks. Eric Talbot Jensen, *Cyber Warfare And Precautions Against the Effects of Attacks*, 88 TEX. L. REV. 1533 (2010).
[135] Protocol Additional I, *supra* note 120, art. 51(3).
[136] INT'L COMM. OF THE RED CROSS, INTERPRETIVE GUIDANCE ON THE NOTION OF DIRECT PARTICIPATION IN HOSTILITIES UNDER INT'L LAW (2009) [hereinafter ICRC, INTERPRETIVE GUIDANCE], *available at* http://www.icrc.org/eng/assets/files/other/icrc_002_0990.pdf
[137] *See id.* (noting the challenge that private contractors and civilian employees pose to the definition of direct participation due to "geographic and organizational closeness").

the attack, right up until the moment of the attack.[138] The actions of such a civilian could conceivably be considered a "continuous function [that] involves the preparation, execution, or command of acts or operations amounting to direct participation in hostilities."[139] As a result, civilians involved in cyber-attacks might be regarded as performing tasks that might alter their status under the law of war, rendering them lawful targets of a counter-attack.[140]

b. Who May Lawfully Carry Out a Cyber-Attack?

In addition to the question of who may be targeted in a cyber-attack, the principle of distinction restricts how states constitute their cyber-fighting forces.[141] A state that sponsors use of force by individuals not in the regular armed forces may be breaching the law of war.[142] It is difficult to evaluate whether extensive but nonexclusive civilian involvement in a cyber-attack violates the law of war by encouraging the use of force by non-regular armed forces.

A current advantage of using non-regular forces to carry out cyber-attacks—namely, the ability to mask state involvement in the attack by including civilians—highlights the challenge that cyber-warfare poses to the principle of distinction. For example, Nashi—a pro-Kremlin youth group

---

[138] Watts, *supra* note 75, at 429.

[139] ICRC, INTERPRETIVE GUIDANCE, *supra* note 137, at 34.

[140] Geoffrey S. Corn, *Unarmed but How Dangerous? Civilian Augmentees, the Law of Armed Conflict, and the Search for a More Effective Test for Permissible Civilian Battlefield Functions*, 2 J. NAT'L SECURITY L. & POL'Y 257, 286-87 (2008). Although the principle that a civilian who directly participates in hostilities or who adopts a continuous combat function may be lawfully attacked is not in dispute, the status of a civilian who provides indispensable, contemporaneous assistance in cyber-attacks remains unresolved.

[141] Watts, *supra* note 75, at 423.

[142] *See* DELIBASIS, *supra* note 120, at 281. The allocation of responsibilities for cyber-warfare has been examined by the U.S. armed forces—the recently declassified Air Force cyberspace operations explains that National Guard members may only train for, but not carry out, cyber-attacks. *See* United States Air Force, Cyberspace Operations: Air Force Doctrine Document 3-12, at 29 (2010), *available at* http://www.e-publishing.af.mil/shared/media/epubs/AFDD3-12.pdf. Even though the United States has launched a new Cyber Command, the details of responsibility for defending against a cyber-attack are still being worked out. *See* Jim Garamone, *Official Details DOD Cybersecurity Environment*, AM. FORCES PRESS SERVICE (Oct. 20, 2010), http://www.defense.gov//News/NewsArticle.aspx?ID=61356 ("Government and private officials are grappling with basics such as what constitutes a cyber attack and who has responsibility to defend against threats."). The DoD strategy emphasizes partnering with the private sector to encourage innovation, incremental improvements, and workforce development, but says little about the nature of those collaborations. *See* DOD STRATEGY, *supra* note 14, at 10-11.

started by Vladimir Putin—has taken responsibility for the 2007 cyber-attacks against Estonia.[143] It has been alleged that by using Nashi as a "nominally independent" cyber-attacker, the business owners who fund the group may "ingratiate themselves with the regime," and the Russian government may plausibly deny involvement in the attack.[144]

A former Special Assistant for Law of War Matters of the Judge Advocate General, Lieutenant Colonel Geoffrey S. Corn, argues that the current law of war direct participation test is outdated.[145] He offers a new functional discretion test to determine who may carry out a cyber-attack based on whether "the exercise of discretion associated with this function [will] implicate [law of war] compliance."[146] Operating within a command relationship is his dispositive criterion for combatant status "because members of the armed forces are subject to responsible command, and they operate within a military hierarchy involving training, discipline, and unitary loyalty."[147] Corn argues that only individuals subject to command authority should be able to exercise discretion because the actions of those individuals can be imputed to their commanders.[148] Those commanders, in turn, could be subject to individual criminal liability for violating the law of war. This, Corn claims, would incentivize commanders to ensure that their forces are all complying with the law of war.[149] Civilians not subject to the compliance-enhancing mechanism of command authority may not engage in use of force if a good faith assessment indicates that there is a reasonable probability that their exercise of discretion would result in a violation of the law of war.[150]

---

[143] *See* Hollis, *supra* note 9, at 1024-25 (describing the attacks against Estonia); Shachtman, *supra* note 63.

[144] Shachtman, *supra* note 63.

[145] *See supra* note 137 and accompanying text.

[146] Corn, *supra* note 140, at 287. Corn emphasizes the importance of distinction and law of war compliance, for regular forces and for paramilitaries. *Id.* at 264-65. This functional test is different from Schmitt's consequences test, which focuses on whether the cyber-attack would cause foreseeable death, injury or destruction.

[147] Corn, *supra* note 140, at 287; *see also* Brown, *supra* note 75, at 191 (arguing that only armed forces should carry out cyber-attacks). *But see* SUSAN W. BRENNER, CYBERTHREATS: THE EMERGING FAULT LINES OF THE NATION STATE 199 (2009) (arguing that the rationale for excluding civilians was to protect them from retaliatory attack, but since civilian infrastructure is very likely to be attacked in cyber-warfare, this rationale for excluding civilians from combat is less persuasive).

[148] Corn, *supra* note 140, at 261.

[149] *Id.* at 274-75, 277. Problems arise if the commander is subject to responsibility for the actions of civilians over which he had no effective control. *Id.* at 277. A contractual relationship cannot replicate the compliance power of military discipline and extensive vicarious criminal liability. *Id.* at 278-79.

[150] *Id.* at 288.

Under this reasoning, if civilian contractors currently exercise discretion in cyber-attacks that implicate the law of war, the prohibition on state sponsorship of non-lawful combatants may require a change in the composition of cyber-forces.

4. Neutrality

A state may be neutral, either permanently, such as Switzerland, or for the duration of a specific conflict.[151] The principle of neutrality includes both rights and responsibilities: "[t]he principal right of the neutral nation is that of inviolability; its principal duties are those of abstention and impartiality. Conversely, it is the duty of a belligerent to respect the former and its right to insist upon the latter."[152]

A final challenge in evaluating the legality of an *in bello* cyber-attack is the fact that a cyber-attack may appear to, or may actually, originate from a neutral state.[153] Some scholars argue that neutral states are not obligated to stop belligerents from using their communications facilities, but they may not help belligerents build such facilities.[154] Others argue that neutral states that are unable or unwilling to stop an attack originating from their territory, including their information systems, may lawfully be targeted with disabling uses of force.[155]

Certain characteristics of cyber-attacks make the evaluation of the principle of neutrality unusually complex. Cyber-attacks may harness zombie computers located in one country to harm networks in another country—without the knowledge of any individual, much less the government—by masking their origin through a series of servers and computers. Such cyber-attacks are difficult to analyze under for the principle of neutrality for two reasons. First, a country may not know its computers are being used for a cyber-attack, and it therefore may not know its neutrality is threatened. Second, as the principle of neutrality determines lawful responses to attacks based on the identity of the origin country, the inability to attribute attacks to a certain state impedes the neutrality analysis.[156] However, it is also possible that

---

[151] *See* George K. Walker, *Information Warfare and Neutrality*, 33 VAND. J. TRANSNAT'L L. 1079, 1142 (2000) (on neutrality and information warfare).
[152] Commander's Handbook, *supra* note 75, para. 7.2.
[153] *See* BRENNER, *supra* note 147, at 9; *see also* Brown, *supra* note 75, at 208 (on rights and responsibilities of neutrality).
[154] *See* Doswald-Beck, *supra* note 126, at 176.
[155] *See* DELIBASIS, *supra* note 120, at 284; Commander's Handbook, *supra* note 75, para. 7.3.
[156] Shanker & Bumiller, *supra* note 42 ("Officials say the main challenge for the United States in a retaliatory cyberoperation is determining the attacker.").

political uncertainty about lawful responses to cyber-attack may be masquerading as an inability to attribute attacks; further clarity around the legal framework governing cyber-attacks may reduce barriers to attribution. While the political problems of attribution might contribute to the apparent difficulties of attribution, the issue of a country not knowing attacks are emanating from its borders remains.

Cyber-attacks present novel challenges for *jus in bello* principles. Most cyber-attacks create temporary incapacity with hard-to-estimate consequences, making it difficult to evaluate whether a cyber-attack is proportional. The dual-use nature of cyber infrastructure and the potential involvement of civilians in implementing cyber-attacks complicates distinguishing between civilians and combatants. Finally, the use of zombie computers and host servers raises questions regarding the rights and obligations of neutral states.

The existing law of war framework—including both *jus ad bellum* and *jus in bello*—provides some guidance for states seeking to respond to cyber-attacks. But it does not regulate the vast majority of cyber-attacks. Armed force is often an unlawful or otherwise inappropriate response to a cyber-attack. And as the incidents described in the introduction reveal, many harmful cyber-attacks do not constitute cyber-warfare. Yet the limits on the law of war do not necessarily mean that these cyber-attacks are unregulated. There are a variety of other legal frameworks that fill some of the gaps left by the law of war framework.

III. OTHER LEGAL FRAMEWORKS GOVERNING CYBER-ATTACKS

There are several existing legal frameworks in addition to the law of war that explicitly or implicitly regulate cyber-attacks. We begin our discussion of these other legal frameworks by describing the international law of countermeasures, which regulates how states may respond to international law violations that do not rise to the level of an armed attack justifying self-defense. Next, we outline the international legal regimes that directly regulate some elements of cyber-attacks. We then describe international legal regimes that indirectly govern some cyber-attacks by regulating the means through which those attacks are conducted. Finally, we examine U.S. domestic laws that could be used to address some cyber-attacks.

These other bodies of law offer victims of cyber-attacks useful tools for responding to attacks. Yet each individual tool has significant limits. Even taken together, the legal framework is piecemeal and incomplete. This should come as no surprise: Much of the law that applies to cyber-attacks was not

designed for this purpose and therefore addresses such attacks only tangentially. This Part sets the stage for reflections on legal reforms that would enable domestic and international law to more effectively regulate cyber-attacks.

A. Countermeasures

The customary international law of countermeasures governs how states may respond to international law violations that do not rise to the level of an armed attack justifying self-defense—including, implicitly, cyber-attacks. The Draft Articles on State Responsibility define countermeasures as "measures that would otherwise be contrary to the international obligations of an injured State *vis-à-vis* the responsible State, if they were not taken by the former in response to an internationally wrongful act by the latter in order to procure cessation and reparation."[157]

The international law of countermeasures does not define when a cyber-attack is unlawful. Instead it simply provides that when a state commits an international law violation, an injured state may respond with a reciprocal act.[158] As explained above, some cyber-attacks that do not rise to the level of an armed attack nonetheless violate the customary international law norm of nonintervention.[159] These violations may entitle a harmed state to use countermeasures to bring the responsible state into compliance with the law.

The Draft Articles lay out the basic customary international law principles regulating states' resort to countermeasures.[160] The Draft Articles provide that countermeasures must be targeted at the state responsible for the prior wrongful act and must be temporary and instrumentally directed to induce the responsible state to cease its violation.[161] Accordingly,

---

[157] Draft Articles, *supra* note 99, ch. II, commentary, para. 1. Traditionally, these acts were termed "reprisals," but this report follows the Draft Articles in using the more modern term "countermeasures." Reprisals now predominantly refer to forceful belligerent reprisals. *Id.* para. 3.

[158] States thus resort to countermeasures at their own risk. If the use of countermeasures does not comply with the applicable international legal requirements, the state may itself be responsible for an internationally wrongful act. *Id.* art. 49, commentary, para. 3.

[159] *See supra* Subsection II.A.1.

[160] Countermeasures are distinct from retorsions. Retorsions are acts that are unfriendly but lawful, such as limiting diplomatic relations or withdrawing from voluntary aid programs, and they always remain a lawful means for a State to respond to a cyber-attack or other international legal violation.

[161] Draft Articles, *supra* note 99, art. 49. Accordingly, the law of countermeasures does not specify how states may respond to international law violations by non-state actors. However, international law violations by non-state actors often lead to international law violations by

countermeasures cannot be used if the international law violation has ceased. Countermeasures also can never justify the violation of fundamental human rights, humanitarian prohibitions on reprisals, or peremptory international norms, nor can they excuse failure to comply with dispute settlement procedures or to protect the inviolability of diplomats.[162] Before resorting to countermeasures, the injured state generally must call upon the responsible state to cease its wrongful conduct, notify it of the decision to employ countermeasures, and offer to negotiate a settlement.[163] However, the injured state "may take such urgent countermeasures as are necessary to preserve its rights."[164] Countermeasures need not necessarily be reciprocal, but reciprocal measures are favored over other types because they are more likely to comply with the requirements of necessity and proportionality.[165]

In the cyber-attack context, an attacking state may violate its obligation not to intervene in another sovereign state through a harmful cyber-attack, and so the state that has been attacked may employ lawful countermeasures. The most important countermeasures in this context are so-called "active defenses," which attempt to disable the source of an attack; passive defenses, by contrast, such as firewalls, merely attempt to repel cyber-attacks.[166] Active defenses are a species of "reciprocal countermeasures," in which the injured state ceases obeying the same or a related obligation to the one the responsible state violated.

Before a state may use active defenses as a countermeasure, however, it must determine that an internationally wrongful act caused the state harm and identify the state responsible, as well as abide by other procedural requirements.[167] The time necessary to comply with these obligations may complicate states' efforts to deploy active defenses as a countermeasure against cyber-attacks, but the time lag should not render such measures

---

states. For example, if a non-state actor launches an attack on state A from state B's territory and state B is unwilling or unable to stop it, state B may violate an international law obligation to prevent its territory from being used for cross-border attacks. *See, e.g.*, Corfu Channel (Merits), 1949 I.C.J. 4, 22 (Apr. 9) (holding that states are obligated "not to allow knowingly its territory to be used for acts contrary to the rights of other States"). In the cyber-attack context, a state may commit an international law violation by allowing harmful cyber-attacks to be launched from its territory. *See* Sklerov, *supra* note 83, at 62-72.

[162] Draft Articles, *supra* note 99, art. 50.

[163] *Id.* art. 52.

[164] *Id.*

[165] *Id.* ch. II, commentary, paras. 4-5.

[166] DoD has recently made clear that it employs such "active cyber defense" to "detect and stop malicious activity before it can affect DoD networks and systems." DOD STRATEGY, *supra* note 14, at 7.

[167] *Id.* arts. 49-52.

ineffective. Identifying the state responsible may be difficult, but it will not always be an insurmountable technical and political problem. In addition, the Draft Articles have detailed provisions on when acts committed by non-state agents may be attributed to a state—for instance, when the state aids and assists the act with knowledge of the circumstances.[168] Furthermore, it is possible international norms will soon coalesce such that states have an obligation not only to refrain from committing cyber-attacks themselves, but also "not to allow knowingly its territory to be used for acts contrary to the rights of other States."[169] Indeed, there are some who believe states already have such an obligation.[170] Hence, this history of state practice indicates that countermeasures are warranted against most cyber-attacks so long they comply with the relevant procedural requirements and the principles of necessity and proportionality.

Countermeasures thus provide states with a tool for addressing cyber-attacks that do not rise to the level of an armed attack but nonetheless violate the customary international law norm of nonintervention. In such cases, countermeasures allow an injured state to respond to an attack with a reciprocal measure, with the goal of bringing an end to the unlawful activity.

Yet, there are significant limits to such measures. First and foremost, they require the identity of the attacker and the computer or network from which the attack originates to be accurately identified. Second, in order for a countermeasure to be effective, the attacking agent must find the countermeasure costly—ideally costly enough to encourage lawful behavior. If the attacker can readily relocate its operations, as is often possible in the context of cyber-attacks, the countermeasure may not impose a significant cost on the actor responsible for the attack. For this reason, countermeasures are likely to be more effective against state actors and less effective against non-state actors. Finally, there is a difficulty of designing a countermeasure to injure only the actor that perpetuated the wrongful attack. In particular, a countermeasure that disables a computer or network may be very well cause harm to those who have little or nothing to do with the original attacks—potentially making the state injured by the original attack into a perpetrator of an unprovoked attack against those who simply happen to share a network with the actor that generated the original attack. For these reasons, the customary law of countermeasures offers only a partial answer to the problem of cyber-attacks. We thus turn next to other international legal regimes that directly regulate cyber-attacks.

---

[168] *Id.* art. 16.
[169] Corfu Channel case (U.K. v. Albania), 1949 I.C.J. Rep. 4, 22 (Apr. 9) (Merits).
[170] *See, e.g.*, Sklerov, *supra* note 83, at 43.

B. International Legal Regimes That Directly Regulate Cyber-Attacks

While no comprehensive international legal framework currently governs all cyber-attacks, a patchwork of efforts provides some tools the United States and other countries can employ to control this growing threat. This Section surveys legal mechanisms created by the United Nations, NATO, the Council of Europe, the Organization of American States, and the Shanghai Cooperation Organization to directly regulate cyber-attacks. While both the Council of Europe and the Organization of American States have taken actions relating to cyber-crime—a category of activity that overlaps in part with cyber-attacks, as noted above—the increased computer network protection and regulations are also relevant to efforts to combat cyber-attacks. Collectively, these organizational measures demonstrate a growing interest in addressing this issue through common legal frameworks. Yet these efforts have fallen short of establishing a rigorous legal framework that can effectively govern all cyber-attacks.

1. The United Nations

There has been only limited U.N. action on the issue of cyber-security. The U.N. General Assembly has passed several related resolutions.[171] These resolutions, however, are vague and have not required any specific action by U.N. members.[172]

In August 1999, the United Nations sponsored an international meeting of experts in Geneva to better grasp the security implications of emerging information technologies.[173] A follow-up General Assembly resolution in 2002

[171] These resolutions have been based on the ongoing agenda item: "Developments in the field of information and telecommunications in the context of international security." *See, e.g.*, G.A. Res. 58/32, U.N. Doc. A/RES/58/32 (Dec. 8, 2003); G.A. Res. 59/61, U.N. Doc. A/RES/59/61 (Dec. 3, 2004); G.A. Res. 60/45, U.N. Doc. A/RES/60/45 (Jan. 6, 2006); G.A. Res. 61/54, U.N. Doc. A/RES/61/54 (Dec. 19, 2006); G.A. Res. 62/17, U.N. Doc. A/RES/62/17 (Jan. 8, 2008); G.A. Res. 63/37, U.N. Doc. A/RES/63/37 (Jan. 9, 2009); G.A. Res. 64/25, U.N. Doc. A/RES/64/25 (Jan. 14, 2010).

[172] This is equally true of the General Assembly's two related resolutions on the Creation of a Global Culture of Cybersecurity and the Protection of Critical Informational Infrastructures, G.A. Res. 58/199, U.N. Doc. No. A/RES/58/199 (Jan. 30, 2004), and Creation of a Global Culture of Cybersecurity and Taking Stock of National Efforts to Protect Critical Information Infrastructures, G.A. Res. 64/211, U.N. Doc. No. A/RES/64/211 (Mar. 17, 2010).

[173] G.A. Res. 57/53, U.N. Doc. A/RES/57/53 (Dec. 30, 2002).

called for further consideration and discussion of "information security."[174] The resolution also called for a new study of international informational security issues,[175] but little action resulted.[176] The United Nations also sponsored The World Summit on the Information Society to further consider issues including information security, but again with little result.[177]

The United Nations did take a step forward in July 2010, when government cyber-security specialists from fifteen countries—including major cyber-powers like the United States, China, and Russia—submitted a set of recommendations to the U.N. Secretary-General as "an initial step towards building the international framework for security and stability that these new technologies require."[178] The recommendations called for

> (i) Further dialogue among States . . .
> (ii) Confidence-building, stability and risk reduction measures . . . including exchanges of national views on the use of [information and communication technologies] in conflict;
> (iii) Information exchanges on national legislation and national information and communications technologies security strategies and technologies, policies and best practices;
> (iv) Identification of measures to support capacity-building in less developed countries;

---

[174] *Id.* at ¶ 1-2. The resolution called upon Member States to:

> promote further at multilateral levels the consideration of existing and potential threats in the field of information security, as well as possible measures to limit the threats emerging in this field . . . [and] . . . Invite[ed] all Member States to continue to inform the Secretary-General of their views and assessments on the following questions:
> (a) General appreciation of the issues of information security;
> (b) Definition of basic notions related to information security, including unauthorized interference with or misuse of information and telecommunications systems and information resources. . . .

Id.

[175] *Id.* ¶ 4.

[176] Similar exhortations appear in subsequent resolutions. *See* G.A. Res. 58/32,*supra* note 171, ¶ 4; G.A. Res. 59/61, *supra* note 171, ¶ 4; G.A. Res. 60/45, *supra* note 171, ¶ 4; G.A. Res. 61/54, *supra* note 171, ¶ 4; G.A. Res. 62/17, *supra* note 171, ¶ 4; G.A. Res. 63/37, *supra* note 171, ¶ 4; G.A. Res. 64/25, *supra* note 171, ¶ 4.

[177] G.A. Res. 60/252, U.N. Doc. A/RES/60/252 (Apr. 27, 2006).

[178] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, at 4, U.N. Doc. A/65/201 (July 30, 2010).

> (v) Finding possibilities to elaborate common terms and definitions . . . .[179]

Though vague, these recommendations represent real progress in overcoming a long impasse between the United States and Russia over how to address cyber-security issues. The cooperation may even suggest possibilities for a future multilateral treaty under the auspices of the United Nations, which Russia has been advocating for some time.[180] At the present, however, the role of the United Nations with respect to cyber-security remains largely limited to discussions and informational sharing.

2. NATO

NATO recently began to address the threat of cyber-attacks. NATO did little in response to the 2007 cyber-attack on Estonia, laying bare that it "lacked both coherent cyber doctrine and comprehensive cyber strategy."[181] On the heels of that attack,[182] NATO held its first meeting—the 2008 Bucharest Summit—to formally address cyber-attacks. This summit prompted the creation of two new NATO divisions focused on cyber-attacks: the Cyber Defence Management Authority and the Cooperative Cyber Defence Centre of Excellence.[183]

The Cyber Defence Management Authority aims to centralize cyber-defense capabilities across NATO members. Although little information is publicly available, the Authority is believed to possess "real-time electronic monitoring capabilities for pinpointing threats and sharing critical cyber intelligence in real-time"—with the goal of eventually becoming an operational war room for cyber-defense.[184] The Cooperative Cyber Defence

---

[179] *Id.* at 8.

[180] John Markoff, *Step Taken to End Impasse Over Cybersecurity Talks*, N.Y. TIMES, July 16, 2010, *available at* http://www.nytimes.com/2010/07/17/world/17cyber.html?_r=1.

[181] Rex B. Hughes, *NATO and Cyber Defence: Mission Accomplished?*, *ATLANTISCH PERSPECTIEF*, Apr. 2009, at 1, *available at* http://www.atlcom.nl/site/english/nieuws/wp-content/Hughes.pdf.

[182] This followed an October 2009 meeting of NATO defense ministers after which they called for the development of a NATO cyber defense policy. NATO Opens New Centre of Excellence on Cyber Defence, N. ATL. TREATY ORG. NEWS (May 14, 2008), http://www.nato.int/docu/update/2008/05-may/e0514a.html.

[183] Hughes, *supra* note 181. This is NATO's tenth COE, and is the only one focused solely on defending against and countering cyber-attacks. *See* Scott J. Shackelford, *Estonia Two-and-a-Half Years Later: A Progress Report on Combating Cyber Attacks*, J. INTERNET L. 5 (forthcoming), *available at* http://ssrn.com/abstract=1499849.

[184] Hughes, *supra* note 181, at 2.

Centre of Excellence aspires to "advance the development of long-term NATO cyber defence doctrine and strategy."[185] The North Atlantic Council, however, retains control of NATO cyber-policy and defense.[186] Despite some pressure from Eastern European countries, cyber-attacks still only activate Article 4 of the NATO treaty, which calls upon members to "consult together" in cases of cyber-attacks, but does not bind them to "assist" each other, as would be required under Article 5.[187]

Although NATO's creation of these two divisions signify concrete progress and recognition of the need for a more coherent cyber-strategy, concerns persist that "these teeth may not be sufficiently sharp to ward off any mischievous cyber bears or other e-adversaries seeking to compromise or destroy NATO digital assets deployed in either the Euro-Atlantic community or the 'near abroad.'"[188] NATO's cyber-plans and capabilities are still nascent.

3. Council of Europe

The Council of Europe has taken the most direct approach to regulating a subset of the cyber-security problem—in particular, cyber-crime—of any international organization to date. As the first international treaty on crimes committed using the Internet and other computer networks, the 2001 Council of Europe Convention on Cybercrime ("Cybercrime Convention") promulgated "a common criminal policy aimed at the protection of society against cybercrime," primarily through legislation and international cooperation.[189] The United States ratified the Convention in 2006.[190]

---

[185] *Id*.

[186] Defending Against Cyber Attacks, N. ATL. TREATY ORG. NEWS, Jan. 29, 2009, *available at* http://www.nato.int/issues/cyber_defence/index.html.

[187] North Atlantic Treaty, *supra* note 106, arts. 4, 5; *see also* NATO Agrees on Common Approach to Cyber Defence, *supra* note 106.

[188] Hughes, *supra* note 181, at 5.

[189] Council of Europe, ETS No. 185, Convention on Cybercrime, pmbl., Budapest (Nov. 23, 2001), entered into force July 1, 2004, *available at* http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm [hereinafter Cybercrime Convention]; *see also* Rasha AlMahroos, *Privacy on the Internet and in Organizational Database: Phishing for the Answer: Recent Developments in Combating Phishing*, 3 I/S: J. L. & POL'Y FOR INFO. SOC'Y 595, 613 (2008).

[190] The convention allows members of the Council of Europe and other invited states (among them the United States) to join the Convention. Declan McCullagh & Anne Broache, *Senate Ratifies Controversial Cybercrime Treaty*, CNET NEWS, (Apr. 4, 2006, 10:25), http://news.cnet.com/Senate-ratifies-controversial-cybercrime-treaty/2100-7348_3-6102354.html. As of November 2010, thirty countries have ratified the Convention on Cybercrime, and another 16 have signed but have not yet ratified it (including Australia, Japan,

Cyber-attacks implicate the Cybercrime Convention's offenses relating to confidentiality, integrity, and availability of computer data and systems—particularly illegal access, data interference, and system interference.[191] These rules, however, do not appear to apply to government actions, whether taken for law enforcement or national security purposes.[192] For example, Article 2 of the Convention requires that states adopt "legislative and other measures . . . to establish as criminal offenses under [their] domestic law, when committed intentionally, the access to the whole or any part of a computer system *without right*."[193] The Convention's accompanying "explanatory report" clarifies that the "without right" caveat allows for classic legal defenses, such as self-defense or necessity, but also "leaves unaffected conduct undertaken pursuant to lawful government authority"—including acts to "maintain public order, protect national security or investigate criminal offences."[194] This suggests that the Convention negotiators were aware of state interests in using cyber-attacks and sought to draft the agreement to permit such governmental action.

Nonetheless, the Cybercrime Convention may still impose limited constraints on the execution of cyber-attack operations by ratifying countries. Parties to the Convention have agreed to "co-operate with each other . . . to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data."[195] Although not explicit, this agreement to cooperate could limit the extent to which parties to the Convention could conduct cyber-attacks against other state parties, since that would undermine the overall intent of the agreement. It is unclear, however, what consequences or repercussions would result from such a breach of the Convention's intent and purpose by a state party.

For these reasons, the Convention—the most developed international legal framework directly regulating cyber-attacks—again addresses only a portion of the overall challenge. It is limited, in particular, both by its failure to regulate most attacks by state parties and by its largely regional membership. Yet it offers a starting point for thinking about a comprehensive international framework for regulating unlawful cyber-attacks.

---

and South Africa). Convention on Cybercrime, COUNCIL OF EUROPE, http://conventions.coe.int/Treaty/Commun/ ChercheSig.asp?NT=185&CM=&DF=&CL=ENG.

[191] Cybercrime Convention, *supra* note 189, arts. 2, 4, 5.

[192] *See* Arie J. Schaap, *Cyberwarfare Operations: Development and Use Under International Law*, 64 A.F. L. REV. 121, 171 (2009); Hollis, *supra* note 9, at 1052.

[193] Cybercrime Convention, *supra* note 189, art. 2 (emphasis added).

[194] Convention on Cybercrime: Explanatory Report, COUNCIL OF EUROPE, C.E.T.S. No. 185, para. 38 (Nov. 8, 2001), http://conventions.coe.int/Treaty/en/Reports/Html/185.htm.

[195] Cybercrime Convention, *supra* note 189, art. 23.

4. Organization of American States

The Organization of American States ("OAS") only recently began taking action to regulate cyber-attacks. In April 2004, the OAS approved a resolution stating that member states should "evaluate the advisability of implementing the principles of the Council of Europe Convention on Cybercrime (2001)" and should "consider the possibility of acceding to that convention."[196] The OAS also adopted a "Comprehensive Inter-American Cybersecurity Strategy," which aims, among other things, to adopt "cyber-crime policies and legislation that will protect Internet users and prevent and deter criminal misuse of computers and computer networks, while respecting the privacy and individual rights of Internet users."[197] To this end, the OAS agreed to deploy an Experts Group that will "provide technical assistance to member states in drafting and enacting laws that punish cyber-crime, protect information systems, and prevent the use of computers to facilitate illegal activity."[198] These experts only offer guidance; the OAS is not promulgating a set of uniform laws with which member states can combat cyber-crime and cyber-attacks.

At a January 2010 meeting, the OAS Working Group on Cyber-Crime recommended that members that had not already done so establish state bodies for investigating and prosecuting cyber-crimes and adopt domestic legislation criminalizing cyber-crime and enabling international cooperation to investigate and prosecute such crimes.[199] The Working Group pledged to review the progress made in implementing these measures at its next meeting.[200] The OAS has begun a useful regional conversation on joint strategies for battling the portion of cyber-attacks that constitute cyber-crime. Yet it has not yet developed a more active program for addressing cyber-attacks more generally.

5. Shanghai Cooperation Organization

---

[196] Organization of American States IV(8), AG/RES. 2040 (XXXIV-O/04) (June 8, 2004), http://www.oas.org/juridico/english/ga04/agres_2040.htm.

[197] Organization of American States, *A Comprehensive Inter-American Cybersecurity Strategy: A Multi-Dimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity*, Appendix A, adopted June 8, 2004, AG/RES. 2004 (XXXIV-O/04), *available at* http://www.oas.org/XXXIVGA/english/docs/approved_documents/adoption_strategy_combat_threats_cybersecurity.htm.

[198] *Id.* Appendix A.

[199] Sixth Meeting of the Working Group on Cyber-Crime, Jan. 21-22, 2010, Washington D.C., OEA/Ser.K/XXXIV, CIBER-VI/doc.4/10 rev. 1, *available at* http://www.oas.org/juridico/english/cyb_VIrec_en.pdf.

[200] *Id*, at para. 17.

The Shanghai Cooperation Organization also has taken significant preliminary steps toward cooperation in the cyber-security area. In its Yekaterinburg Declaration of June 16, 2009, "the SCO member states stress[ed] the significance of the issue of ensuring international information security as one of the key elements of the common system of international security."[201] The Organization presents a possible center of gravity in international legal action on cyber-attacks. As explained above, [202] the Organization has thus far adopted an expansive vision of cyber-attacks to include the use of cyber-technology to undermine political stability. As such, it represents a model that is likely to be at odds with that of Europe and the United States, which have sought to avoid regulations of cyber-activities that may interfere with the expression of political dissent.

As this Section demonstrates, international efforts to regulate cyber-attacks are still at an embryonic stage. With the possible exception of the Council of Europe's Convention on Cybercrime, most international agreements have not proceeded beyond the stage of discussing future strategies. Nonetheless, the widespread efforts demonstrate increasing interest in establishing a set of transnational regulations to address cyber-attacks. The diversity of approaches taken by these organizations also demonstrates that the central challenge—at least initially—will be defining the scope of the activity that should be addressed in an international agreement. Before we outline our recommendations for future efforts at directly regulating cyber-attacks, however, we first must complete the full existing legal picture by outlining the international regimes that indirectly regulate cyber-attacks and the domestic laws that address cyber-attacks.

C. International Legal Regimes That Indirectly Regulate Cyber-Attacks

Several international legal frameworks are not directly aimed at cyber-attacks but nonetheless regulate means that may be used in or may be a focus of a cyber-attack. These include, most notably, the international law governing telecommunications, aviation, space, and the law of sea. These legal regimes were largely formed prior to the emergence of cyber-attacks and therefore do not expressly regulate or prohibit cyber-attacks. Instead, these "means-based"

---

[201] Shanghai Cooperation Organization, Yekaterinburg Declaration of the Heads of the Member States of the Shanghai Cooperation Organization, Consulate General of Uzbekistan in New York City (July 9, 2009), *available at* http://www.uzbekconsulny.org/news/572/.

[202] *See infra* text accompanying notes 18-21.

frameworks implicate cyber-attacks only so long as an attack employs the particular means regulated by the agreement. For this reason, legal scholarship on cyber-security has suggested that these bodies of international law can be used to address cyber-attacks.[203] Yet we find, once again, that these existing legal regimes provide a patchwork of laws that are likely to apply to only a small number of harmful cyber-attacks.

1. International Telecommunications Law

Cyber-attacks that involve international wire or radio frequency communications may be subject to telecommunications law. Modern international telecommunications law is regulated by the International Telecommunications Union, the leading U.N. agency that establishes multinational standards for information and communication technology.[204] The Union's goal, as stated in its founding International Telecommunication Convention and International Telecommunication Constitution, is "the preservation of peace and the social and economic development of all countries . . . by means of efficient telecommunications services."[205] The International

[203] *See* Richard W. Aldrich, *The International Legal Implications of Information Warfare*, Airpower J. (Fall 1996), *available* at http://www.au.af.mil/au/awc/awcgate/au/aldrich.pdf; Jason Barkham, *Information Warfare and International Law on the Use of Force*, 34 N.Y.U.J. INT'L L. & POL. 57 (2001); Dimitrios Delibasis, *State Use of Force in Cyberspace for Self-Defence: A New Challenge for a New Century*, 8 PEACE CONFLICT DEV.: AN INTERDIS. J. (Feb. 2006), Bryan W. Ellis, *The International Legal Implications and Limitations of Information Warfare: What Are Our Options?*, U.S. ARMY WAR COLLEGE (Apr. 10, 2001), *available* at http://www.iwar.org.uk/law/resources/iwlaw/Ellis_B_W_A.pdf; Schaap, *supra* note 192; Scott J. Shackelford, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, 27 BERK. J. INT'L LAW 192 (2009); David Willson, *A Global Problem: Cyberspace Threats Demand an International Approach*, ISSA J. (Aug. 2009), *available* at http://www.issa.org/Library/Journals/2009/August?Wilson-A%20Global%20Problem.pdf; William Yurcik, *Information Warfare: Legal and Ethical Challenges of the Next Global Battleground*, Proceedings of The Second Annual Ethics and Technology Conference (June 6-7, 1997).

[204] CHARLES H. KENNEDY & M. VERONICA PASTOR, AN INTRODUCTION TO INTERNATIONAL TELECOMMUNICATIONS LAW 30-33 (1996). The International Telecommunications Convention is the founding charter that established the ITU. The International Telecommunications Union first began in 1865 as the International Telegraph Union and was founded in order to universalize telegraph services among mostly European nations. *Id.* at 30-32. It is based in Geneva, Switzerland, and its membership includes 192 member states and more than seven hundred sector members and associates. *About ITU*, INT'L COMM. UNION, http://www.itu.int/net/about/index.aspx (last visited Dec. 5, 2010). The full text of the Convention is available at *Basic Texts of ITU*, INT'L COMM. UNION http://www.itu.int/net/about/basic-texts/index.aspx (last visited Dec. 5, 2010).

[205] Constitution of the International Telecommunications Union, pmbl., Dec. 22, 1992,

Telecommunications Union enacts rules known as Administrative Regulations, which are treaties that bind all member parties; Radio Regulations, which also bind all parties; as well as non-binding Telecommunications Standards.[206] The Union mainly regulates the use of radio and telecommunication technologies in order to distribute them to member states in an efficient and equitable manner—for example, through developing methods of assigning rights to radio spectrums.[207]

International Telecommunication regulations apply to cyber-attacks that make use of electromagnetic spectrum or international telecommunications networks. For instance, broadcasting stations from one nation may not interfere with broadcasts of other states' services on their authorized frequencies.[208] Member states may cut off any non-state "private telecommunications that may appear dangerous to the security of the State or contrary to its laws, to public order or to decency"[209] or suspend international telecommunication services "either generally or only for certain relations and/or for certain kinds of correspondence, outgoing, incoming or in transit, provided that it immediately notifies such action to each of the other Member States through the Secretary-General."[210] Member states also must regulate against "harmful interference"[211] that "endangers the functioning of a radionavigation service or of other safety services or seriously degrades, obstructs or repeatedly interrupts a radiocommunication service"[212] and pursue all possible measures to ensure the secrecy of international correspondence, unless such secrecy would contravene their domestic laws or international conventions.[213]

Despite the above restrictions, international telecommunications law does not specifically prohibit the use of telecommunications for military purposes, such as cyber-attacks.[214] Article 48 states that "Member States retain their entire freedom with regard to military radio installations." The article

---

http://itu.int/net/about/basic-texts/index.aspx; International Telecommunications Convention pmbl., U.N. Doc. 26559, Nov. 6, 1982 [hereinafter ITU Constitution].

[206] KENNEDY & PASTOR, *supra* note 204, at 33.

[207] More information about the agency's work is available at *Committed to Connecting the World*, INT'L COMM. UNION, http://www.itu.int/en/pages/default.aspx (last visited Dec. 5, 2010); *see also The ITU Mission: Bringing the Benefits of ICT to All the World's Inhabitants*, INT'L COMM. UNION, http://www.itu.int/net/about/mission.aspx (last visited Dec. 5, 2010).

[208] ITU Constitution, *supra* note 205, art. 45.

[209] *Id.* art. 34.

[210] *Id.* art. 35.

[211] *Id.* art. 6.

[212] *Id.* annex.

[213] *Id.* art. 37.

[214] *Id.* art. 48(1).

requests that states limit such use: "Nevertheless, these installations must, so far as possible, observe . . . the measures to be taken to prevent harmful interference."[215] The International Telecommunications Union cautions against "harmful interference," but it allows for military transgressions of these regulations—without requiring a reporting mechanism or otherwise limiting its use. This exception might include within its scope cyber-attacks and possibly even cyber-warfare. In addition to this military exception, the International Telecommunication Union provisions have a second important limitation as a legal framework for regulating cyber-attacks: Violations of Union rules and regulations have only limited repercussions, given that the Union lacks enforcement and punitive mechanisms.[216]

2. Aviation Law

Cyber-attack operations that target or interfere with non-military aviation could implicate three major aviation regulations: the 1944 Chicago Convention on International Civil Aviation (Chicago Convention),[217] the 1971 Montreal Convention on the Suppression of Unlawful Acts Against Civil Aviation (Montreal Convention),[218] and the 1988 Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving Civil Aviation (Montreal

[215] *Id.* art. 48(2).

[216] The International Telecommunication Union's main "regulatory" body originally was the International Frequency Regulation Board (IFRB), which was formed "to manage the [radio frequency] spectrum internationally and to solve arising problems in a neutral manner." Wladyslaw Moron, *Radio Regulations Board (RRB): Its Place, Role and Functioning in the ITU*, ITU Doc. No. RRB10-1/4-E (Mar. 1, 2010), http://www.itu.int/ITU-R/information/promotion/e-flash/4/article7.html. Its founders envisioned it as a "cross between the Federal Communication Commission and the International Court of Justice." *Id.* (internal quotation marks omitted). This board, however, was never empowered to uphold its adjudicatory visions. *Id.* In 1994, the Radio Regulations Board subsumed the IFRB, aiming to act as an "independent interpreter and mediator" when dealing with non-compliance and sometimes conflicting interests of member states. *Id.* Even the Board, however, seems to function as more of a coordinating body rather than a regulatory one, seeing as it has no authority to enforce its decisions. *Id.* Furthermore, ITU resolutions are not considered legally binding. *See* STEPHEN GOROVE, DEVELOPMENTS IN SPACE LAW: ISSUES AND POLICIES 49 (1991) ("While states generally abide by ITU resolutions, they are not legally bound by them.").

[217] Convention on International Civil Aviation, Dec. 7, 1944, 61 Stat. 1180, [hereinafter Chicago Convention].

[218] Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation, Sept. 23, 1971, 24 U.S.T. 564 [hereinafter Montreal Convention].

Protocol).[219] For example, the disruption of air traffic control, the modification of flight passenger lists, or the addition of a name to a country's no-fly list all exemplify cyber-attacks that implicate aviation law.[220]

The 1944 Chicago Convention created a specialized UN agency tasked with coordinating and regulating international air travel.[221] It also established a set of rules on airspace, aircraft, navigation, registration, and safety.[222] The Convention stipulates that all states must show "due regard for the safety of navigation of civil aircraft."[223] Cyber-attack operations that target civilian flights, if launched by a government against another actor, could run counter to this Convention safeguard against interference with civilian flights. Such an operation would also run afoul of the 1984 amendment against using weapons targeting a civil aircraft in flight.[224] However, the Convention does allow member states to disregard the Convention during war or state emergencies, stating that "the provisions of this Convention shall not affect the freedom of action of any of the contracting States affected, whether as belligerents or as neutrals" in those two extreme circumstances.[225] State parties could legally disregard their obligations, and target civil aircraft in flight if acting during a war or state emergency, so long as the acting party "notifies the fact to the Council."[226]

The Montreal Convention outlines as unlawful specific conduct that could jeopardize the safety of civil aviation.[227] Article 1 states that a person commits a crime if he or she intentionally and unlawfully does or attempts to do a series of acts that would render an aircraft incapable of flight or would seriously endanger the safety of the aircraft while in flight, including through "destroy[ing] or damag[ing] air navigation facilities or interfer[ing] with their operation, . . . or communicat[ing] information which he [or she] knows to be false, thereby endangering the safety of an aircraft in flight."[228] This agreement would not seem to restrict any cyber-attack operations unless it rendered an

---

[219] Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, Feb. 24, 1988, 1589 U.N.T.S. 474 [hereinafter Montreal Protocol].
[220] Schaap, *supra* note 192, at 166.
[221] Chicago Convention, *supra* note 217, arts. 43, 44. The agency is called the International Civil Aviation Organization. *Id.*
[222] *Id.* pt. I.
[223] *Id.* art. 3(d).
[224] This 1984 amendment to the Chicago Convention "reaffirm[s] the principle of non-use of weapons against civil aircraft in flight." Protocol Relating to an Amendment to the Convention on International Civil Aviation, pmbl., May 10, 1984, 23 I.L.M. 705.
[225] Chicago Convention, *supra* note 217, art. 89.
[226] *Id.*
[227] Montreal Convention, *supra* note 218.
[228] *Id.* art. 1.

aircraft unable to fly (for example, by interfering with the aircraft's operating system) or endangered the safety of an aircraft in flight (for example, interfering with air traffic control communication or other aspects of aircraft navigation).

The Montreal Protocol extended the legal framework from civil aircraft in flight to "acts of violence which endanger or are likely to endanger the safety of persons at airports or which jeopardize the safe operation of such airports."[229] Article 2 states that a person commits a crime if he or she intentionally and unlawfully does or attempts to do any of the following while using a device, substance, or weapon:

> (a) performs an act of violence against a person at an airport serving international civil aviation which causes or is likely to cause serious injury or death; or
> (b) destroys or seriously damages the facilities of an airport serving international civil aviation or aircraft not in service located thereon or disrupts the services of the airport, if such an act endangers or is likely to endanger safety at that airport.[230]

This Protocol thereby prohibits any cyber-attacks that could undermine safety at an international airport, such as tampering with no-fly lists, passenger manifests, or an airport's computer network system. For these actions to be unlawful, however, they would have to endanger safety at the airport.

3. Law of Space

Cyber-attacks could implicate space law given that computer-operated satellites are integral to international telecommunications and military operations. Multiple scholars have proposed that treaties on outer space, the moon, and damage caused by space objects, as well as satellite regulations, could be used to regulate cyber-attacks.[231] Although relevant in terms of means employed, these particular treaties ultimately seem to have little relevance to the regulation of cyber-attacks. In light of their limited applicability, this

[229] Montreal Protocol, *supra* note 219, pmbl.
[230] *Id.* art. 2.
[231] Aldrich, *supra* note 203, at 20-24; Delibasis, *supra* note 203, at 15-17; LAWRENCE T. GREENBERG, SEYMOUR E. GOODMAN & KEVIN J. SOO HOO, INFORMATION WARFARE AND INTERNATIONAL LAW 8-9 (1998); Hollis, *supra* note 9, at 1051; Kanuck, *supra* note 128, at 276-279; Schaap, *supra* note 192, at 160-164. [no further information for Greenberg]

Section does not delve into the damage caused by space objects treaty[232] or the moon treaty.[233] Instead, it discusses the Treaty on Principles Governing the Activities in the Exploitation and Use of Outer Space and satellite regulations. None of these treaties, however, offer comprehensive avenues for regulating cyber-attacks.

The 1967 Outer Space Treaty provides for the free exploration of space but also prohibits the use of space for particular destructive purposes.[234] It stipulates that:

> States Parties to the Treaty undertake not to place in orbit around the Earth any objects carrying nuclear weapons or any other kinds of weapons of mass destruction, install such weapons on celestial bodies, or station such weapons in outer space in any other manner.
>
> The moon and other celestial bodies shall be used by all States

[232] The Convention on International Liability for Damage Caused by Space Objects lays out a set of procedures for determining state liability for activities in outer space. Article 2 states that "[a] launching State shall be absolutely liable to pay compensation for damage caused by its space object on the surface of the earth or to aircraft in flight." Convention on International Liability for Damage Caused by Space Objects, art 2, Mar. 29, 1972, 24 U.S.T. 2389, 961 U.N.T.S. 187. The Treaty defines damage as "loss of life, personal injury or other impairment of health; or loss of or damage to property of States or of persons, national or juridical, or property of international intergovernmental organizations." *Id.* art 1. It is unlikely, however, that the definition of damage or of space-object would apply to cyber-attacks.

[233] The Moon Treaty provides the international community with jurisdiction over all heavenly bodies, including the orbits around such bodies. Agreement Governing the Activities of States in Outer Space, on the Moon and Other Celestial Bodies, Dec. 5, 1979, 1363 U.N.T.S. 53, G.A. Res. 34/68, U.N. Doc. A34/46, 1979. The treaty refers to the "common heritage of mankind," reflecting a belief that all nations should share equitably in benefits derived from resources on the moon and other celestial bodies. *Id.* art. 11(1). The treaty also underscores that the moon should be used exclusively for peaceful purposes. *Id.* art. 3. Beyond this principle, however, the treaty offers little concrete means by which cyber-warfare could be regulated. Furthermore, the countries and organizations mainly engaged in space exploration, such as the United States, the European Union, Russia, China, Japan and India, have not ratified the treaty. As of December 19, 2008, only thirteen states had ratified and four signed the Moon Treaty. U.N. Office for Outer Space Affairs, *Status of International Agreements Relating to Activities in Outer Space as at 1 January 2010*, U.N. Doc. ST/SPACE/11/Rev.2/Add/3, *available at* http://www.unoosa.org/pdf/publications/ST_SPACE_11_Rev2_Add31E.pdf.

[234] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, Jan. 27, 1967, 18 U.S.T. 2410, 610 U.N.T.S. 205.

Parties to the Treaty exclusively for peaceful purposes.[235]

The Outer Space Treaty expressly permits certain military uses of space, such as earth-orbit military reconnaissance satellites, remote-sensing satellites, military global-positioning systems, and space-based aspects of an antiballistic missile system.[236] Because cyber-attacks will rarely be classified as causing mass destruction, it is unlikely that cyber-attacks could be properly characterized as prohibited by the treaty.[237]

Satellite regulations offer another potential avenue for cyber-attack regulation. The Agreement Relating to the 1971 International Telecommunications Satellite Organization (Telecommunications Satellite Organization)[238] and the Convention of the 1979 International Maritime Satellite Organization (Maritime Satellite Organization)[239] contain "peaceful purpose" provisions applicable to classes of satellites similar to the Outer Space Treaty. The regulations created by these organizations might appear to be more applicable, given that satellites are likely to have a role in cyber-attacks. Upon closer inspection, however, it is apparent that they too have little impact on the regulation of cyber-attacks. The Telecommunications Satellite Organization initially formed as an inter-governmental telecommunications satellite organization mandated to "carry forward on a definitive basis the design, development, construction, establishment, operation and maintenance of the space segment of the global commercial telecommunications satellite system,"[240] and was privatized in 2000.[241] Similarly, the Maritime Satellite Organization has largely ceased to represent inter-governmental interests.[242]

---

[235] *Id*. art. 4.
[236] Shackelford, *supra* note 203, at 219.
[237] Celestial bodies refer only to "natural bodies, such as the moon, asteroids, and planets, not to man-made satellites," the main means in outer space by which cyber-warfare could be conducted. *See also* Aldrich, *supra* note 203, at 20.
[238] Agreement Relating to the International Telecommunications Satellite Organization, "Intelsat," Aug. 20, 1971, 23 U.S.T. 3813 [hereinafter Telecommunications Satellite Agreement].
[239] Convention of the International Maritime Satellite Organization London, Sept. 3, 1976, 31 U.S.T. 1, [hereinafter INMARSAT].
[240] Telecommunications Satellite Agreement, *supra* note 238, art. 2.
[241] To "promote a more competitive global satellite services market," the Telecommunications Satellite Organization became a private company in 2000 named "INTELSAT." U.S. GOVERNMENT ACCOUNTABILITY OFFICE, TELECOMMUNICATIONS: INTELSAT PRIVATIZATION AND THE IMPLEMENTATION OF THE ORBIT ACT, 1 (2004), *available at* http://www.gao.gov/new.items/d04891.pdf.
[242] The Maritime Satellite Organization, originally founded as a non-profit international organization to establish a maritime satellite communications network, changed its name to

Consequently, neither organization is well situated to promulgate public regulations related to cyber-attacks.

4. Law of the Sea

The 1982 United Nations Convention on the Law of the Sea ("UNCLOS")—particularly Articles 19, 109, and 113—tangentially implicate cyber-attack operations at sea.[243] The Article 19 obligation allowing a vessel to exercise the right of innocent passage through a nation's territorial sea, so long as its activities are not "prejudicial to the peace, good order or security of the coastal State" is widely accepted to be not simply binding under the treaty but also as customary international law.[244] Activities prohibited by Article 19 include:

> (a) any threat or use of force against the sovereignty, territorial integrity or political independence of the coastal State, or in any other manner in violation of the principles of international law embodied in the Charter of the United Nations;

"International Mobile Satellite Organization" when it began to provide services to aircraft and portable users. JONATHAN HIGGINS, SATELLITE NEWSGATHERING, *What is IMSO?* 247-48 (2d. ed., 2007), http://www.imso.org/whatisimso_UK.asp. In 1999, the organization divided into two separate parts: most was converted into a commercial company, and a small group became the intergovernmental regulatory body, the International Mobile Satellite Organization (IMSO). *Id.* at 248. Through a private-public partnership, the IMSO oversees certain public satellite safety and security communication services provided by Inmarsat satellites.

[243] The United States has not ratified the Convention on the Law of the Sea, even though it has been abiding by the Convention since President Regan's 1983 Statement of Oceans Policy, and it signed the 1994 Agreement Relating to Implementation of Part XI. Nonetheless, many of the provisions of the Convention are considered binding on the U.S. and other countries as customary international law. Division for Ocean Affairs and the Law of the Sea, *Table Recapitulating the Status of the Convention and of Related Agreements, as at November 2010*, http://www.un.org/Depts/los/reference_files/status2010.pdf; Richard G. Lugar, *The Law of the Sea Convention: The Case for Senate Action* (May 4, 2004), http://www.brookings.edu/speeches/2004/0504energy_lugar.aspx (address at the Brookings Institution) (on the United States abiding by the Law of the Sea Convention).

[244] Rüdiger Wolfrum, President of the International Tribunal for the Law of the Sea, Statement to the International Tribunal for the Law of the Sea: Freedom of Navigation: New Challenges (Apr. 23, 2008), *available at* http://www.itlos.org/news/statements/Wolfrum/Singapore 32nd Oceans Conf. Freedom of Navigation ptg 23.04.08 BA.pdf, United Nations Convention on the Law of the Sea art. 19, Dec. 10, 1982, 21 I.L.M. 1261, 1833 U.N.T.S. 3 (1982) [hereinafter UNCLOS].

> . . .
> (c) any act aimed at collecting information to the prejudice of the defence or security of the coastal State;
> (d) any act of propaganda aimed at affecting the defence or security of the coastal State;
> . . .
> (k) any act aimed at interfering with any systems of communication or any other facilities or installations of the coastal State . . . .[245]

These regulations could be read to prohibit cyber-attacks that make use of computer systems on vessels that are at sea.

Similarly, Article 109 stipulates that all states should cooperate in suppressing unauthorized broadcasting from the high seas.[246] UNCLOS defines "unauthorized broadcasting" as "the transmission of sound radio or television broadcasts from a ship or installation on the high seas intended for reception by the general public contrary to international regulations, but excluding the transmission of distress calls."[247] Any person that broadcasts without proper authority is subject to prosecution.[248] Finally, Article 113 requires states to put in place domestic criminal legislation to punish willful damage to submarine cables.[249] These provisions provide some minimal legal protections against cyber-attacks that occur on or originate from the high seas.

Together, international law governing telecommunications, aviation, space, and the sea provide potentially effective tools for addressing some forms of cyber-attack that fall within their respective jurisdictions. Yet none provides a coherent mechanism for addressing cyber-attacks. Moreover, even taken as a whole, they offer only a patchwork of regulations that leave many harmful cyber-attacks unaddressed. Given that current international law provides limited and under-enforced mechanisms for regulating cyber-attacks, the following Section turns to consideration of how U.S. domestic law might be used to address cyber-attacks.

D. U.S. Domestic Law

---

[245] *Id.*
[246] *Id.*, art. 109.
[247] *Id.* art. 109(2).
[248] *Id.* art. 109(3). In particular, Article 109(3) states that prosecution may occur in "the court of: (a) the flag State of the ship; (b) the State of registry of the installation; (c) the State of which the person is a national; (d) any State where the transmissions can be received; or (e) any State where authorized radio communication is suffering interference." *Id.*
[249] *Id.* art. 113.

Domestic law—particularly domestic criminal law—offers an important tool for combating cyber-attacks, including those that cross international borders. Indeed, given the limited applicability of the law of war and other international legal frameworks, domestic laws addressing cyber-attacks are often the best available option. Unfortunately, the existing response to cyber-attack in the domestic law of the United States and other states has for the most part not been updated to address the novel modern challenges posed by cyber-attacks.[250] It is also severely limited by its lack of extraterritorial reach.

Although there is no U.S. federal statute that directly criminalizes cyber-attacks, the primary domestic legal tool for addressing cyber-attacks is criminal law.[251] At the federal level, criminal laws address fraud involving devices, computers, or e-mail;[252] malicious interference in communications lines, stations, or systems;[253] electronic communication interception;[254] illicit access to electronic communications and records;[255] and recording of dialing, routing, addressing, and signaling information.[256]

The majority of the existing criminal laws bearing on cyber-attack do not apply extraterritorially—that is, they do not reach criminal activity occurring outside the United States.[257] There are inherent limits to how much

---

[250] *See, e.g.*, Sklerov, *supra* note 83, at 6 ("Unfortunately, state responses to cyberattacks are governed by an anachronistic legal regime that impairs a state's ability to defend itself.").

[251] In addition to liability through criminal law, there have been some proposals for the use of tort law to allow for civil liability for cyber-attackers, or for intermediaries who are negligent in facilitating cyber-attack. *See, e.g.*, Michael D. Scott, *Tort Liability for Vendors of Insecure Software: Has the Time Finally Come?*, 67 MD. L. REV. 425 (2008); Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace* 31-32, 53-58, *available at* http://works.bepress.com/jay_kesan/4/. Such proposals face a number of serious challenges, however, including attribution and jurisdictional problems, and, for intermediaries, causation problems and a virtual "tax on technophobia, punishing those who do not know enough about protecting their personal computers." *Id*. at 32. Moreover, if software designers were held liable for leaving their products vulnerable to cyber-attack, software costs could increase substantially. *Id*

[252] 18 U.S.C. §§ 1029, 1030, 1037 (2006). 18 U.S.C. § 1030 is the codification of the Computer Fraud and Abuse Act.

[253] *Id*. § 1362.

[254] *Id*. §§ 2510-22.

[255] *Id.* §§ 2701-12.

[256] *Id*. §§ 3121-27.

[257] There is generally a presumption against extraterritorial application of federal law. *See* United States v. Cotten, 471 F.2d 744, 750 (9th Cir. 1973). Nevertheless, "Congress has the authority to enforce its laws beyond the territorial boundaries of the United States," and may do so by evidence of its intent as gauged through statutory interpretation. Equal Opportunity

of the problem domestic law can reach, since domestic law can only be enforced against individuals that are within the jurisdiction of domestic law enforcement. There are, however, some exceptions to that rule. For example, the criminal statute banning access device fraud, as amended by the USA PATRIOT Act of 2001, provides that:

> Any person who, outside the jurisdiction of the United States, engages in any act that, if committed within the jurisdiction of the United States, would constitute an offense under . . . this section, shall be subject to the fines, penalties, imprisonment, and forfeiture provided in this title if—
>
> (1) the offense involves an access device issued, owned, managed, or controlled by a[n] . . . entity within the jurisdiction of the United States; and
> (2) the person transports, delivers, conveys, transfers to or through, or otherwise stores, secrets, or holds within the jurisdiction of the United States, any article used to assist in the commission of the offense or the proceeds of such offense or property derived therefrom.[258]

The statute banning computer fraud was also amended as part of the USA PATRIOT Act to provide for extraterritorial applicability.[259] Both of these statutes may serve as useful models for extending extraterritorial application to other domestic laws related to cyber-attack.

Several recent legislative efforts in the United States tackle pieces of the cyber-attack threat not addressed by criminal law. These include the

---

Empl. Comm. v. Arabian American Oil Co., 499 U.S. 244, 248 (1991) (internal citations omitted). In certain cases, extraterritorial reach may also be extended without explicit or implied Congressional authorization based on detrimental effects in the United States. *See* United States v. Muench, 694 F.2d 28, 33 (2d Cir. 1982) ("The intent to cause effects within the United States . . . makes it reasonable to apply to persons outside United States territory a statute which is not extraterritorial in scope.").

[258] 18 U.S.C. § 1029 (2006); U.S. DEP'T OF JUSTICE, PROSECUTING COMPUTER CRIMES 94 (Scott Eltringham ed., 2007), *available at* http://www.justice.gov/criminal/cybercrime/ccmanual/index.html.

[259] 18 U.S.C. § 1030 (2006) ("[T]he term 'protected computer' [to which this statute applies] means a computer . . . which is used in interstate or foreign commerce or communications, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States."); U.S. DEP'T OF JUSTICE, PROSECUTING COMPUTER CRIMES, *supra* note 258, at 94.

Cybersecurity Enhancement Act;[260] the Executive Cyberspace Authorities Act of 2010;[261] the Rockefeller-Snowe Cybersecurity Act;[262] the International Cyberspace and Cybersecurity Coordination Act of 2010;[263] and the Protecting Cyberspace as a National Asset Act of 2010.[264] The most widely-discussed of these efforts has been the Protecting Cyberspace as a National Asset Act, co-written by Senators Lieberman, Collins, and Carper, which was introduced in the Senate and the House in June 2010.[265] The bill builds on the military's recent establishment of the United States Cyber Command[266] by proposing the establishment of an Office of Cyberspace Policy in the White House and a National Center for Cybersecurity and Communications in the Department of Homeland Security.[267] The bill also addresses a wide range of related cyber-security matters, including cyber-security definitions and federal information security management provisions.[268]

The bill has become caught up in a vigorous debate over the proper role of the government in regulating cyberspace. Dubbed the "kill switch bill" by opponents, the bill came to be seen as an effort to grant the president emergency powers over certain Internet communications.[269] Had it passed into law, the bill would likely have put in place more checks on the president's power to respond to cyber-emergencies than currently exist. The bill has since been reintroduced in amended form, but has not yet proceeded to a vote on the Senate floor.[270] This debate offers an important lesson for reformers: Any future law must clearly indicate what activities are to be covered, put in place a transparent and high bar for emergency measures, and address well-founded concerns that efforts to strengthen cyber-security might simultaneously weaken

---

[260] H.R. 4061, 111th Cong. (2010).
[261] H.R. 5247, 111th Cong. (2010).
[262] S. 773, 111th Cong. (2009).
[263] S. 3193, 111th Cong. (2010).
[264] S. 3480, 111th Cong. (2010); H.R. 5548, 111th Cong. (2010).
[265] *Id.*
[266] William H. McMichael, *DoD Cyber Command Is Officially Online*, ARMY TIMES (May 22, 2010), http://www.armytimes.com/news/2010/05/military_cyber_command_052110/.
[267] S. 3480, *supra* note 264; H.R. 5548, *supra* note 264.
[268] *Id.*
[269] *See* Emelie Rutherford, *Senate Committee OKs Cybersecurity Bill on Majority Leader's Radar*, DEFENSE DAILY, June 25, 2010, *available at* http://www.defensedaily.com/publications/dd/10568.html. The bill has since been reintroduced with changes meant to prevent the government from using a "kill switch" to shut of internet service as a political tool. Diane Bartz, Reid Pushes U.S. Republicans for Cybersecurity Bill, Reuters (July 27, 2011), *available at* http://www.reuters.com/article/2011/07/27/congress-cybersecurity-idUSN1E76Q1M320110727.
[270] *See id.*

the free and open access to modern technology for those engaging in political speech and organizing.

Other domestic legal efforts to address cyber-attacks are either based in criminal law or have focused on building up U.S. defensive capabilities, but none of the recent legislative efforts that might strengthen defensive capacity against cyber-attack has yet been made into law. Moreover, the existing domestic law framework is insufficient for addressing the larger global problem.[271] In particular, the lack of extraterritorial effect in most of the criminal laws that do exist to counter cyber-attacks severely limits their ability to reach those initiating such attacks, who are often located outside the United States. The next Part of this Article offers recommendations for remedying the substantial limitations of the current domestic law framework, as well as the international legal framework for addressing cyber-attack.

IV. NEW LAW FOR CYBER-ATTACKS

Cyber-attacks present a new and growing threat—one that current international and domestic law is not prepared to meet. The law of war, often cited as the relevant body of law to address cyber-attacks in fact offers a basis for responding only to those cyber-attacks that amount to an armed attack. Other existing international legal frameworks offer only embryonic or piecemeal protection. U.S. domestic law is potentially a powerful tool for battling cyber-attacks, but it has not yet addressed the challenge directly. And to the extent it provides some remedy for cyber-attacks, it is restricted by jurisdictional limits on its reach.

To begin to fill the gaps left by existing law, we recommend two types of legal reform—domestic and international—aimed at addressing these shortcomings.[272] The domestic law reforms are twofold: First, the United States should take steps to add extraterritorial applicability to criminal laws bearing on cyber-attack. Second, the United States should utilize limited

---

[271] *See* JOHNSON & SPECTOR, *supra* note 264, at 3.

[272] We focus here on potential legal reforms. In addition to legal reform, government should (and has) put in place programs to work with the private sector to address cyber-attack threats. Indeed, the Obama Administration has recognized that "ensuring the resilience of our networks and information systems requires collective and concerted national action that spans the whole of government, in collaboration with the private sector and individual citizens." WHITE HOUSE CYBERSPACE STRATEGY, *supra* note 54, at 13. The U.S. Department of Defense has also suggested that there may be a need for "incentives or other measures . . . to promote private sector participation." DOD STRATEGY, *supra* note 14, at 9. The legal reforms outlined here are meant to compliment such cooperative measures, not substitute for them.

counter-measures, as appropriate, to combat cyber-attacks that do not rise to the level of armed attacks under the law of war.

Though these domestic measures will address elements of the problem of cyber-attacks, getting at the root of the international problem of cyber-attack will require international solutions. We therefore recommend an international cyber-treaty with two central aims. First, such an agreement should provide a definition of cyber-attacks and cyber-warfare. The transnational conversation leading to such a treaty should serve to limit and define the cyber-attacks to which states may respond with force. Second, the treaty should empower states to engage in international cooperation in evidence collection and criminal prosecutions of individuals involved in transnational cyber-attacks. Meeting this second aim will likely be a longer-term project, but it will offer the only truly effective solution to the inherently international problem of cyber-attacks.

A. Battling Cyber-Attacks at Home

1. Extend the Extraterritorial Reach

There are a number of existing and proposed domestic laws that may play a role in combating cyber-attacks. As noted above, the most prevalent of these today—and likely for the foreseeable future—are the numerous criminal statutes regulating harmful cyber-activity outside the context of armed conflict. However, only a small number of these criminal laws provide for explicit extraterritorial reach.[273] Limitations on the extraterritorial reach of domestic laws can make them of relatively little use in combating cyber-attacks, which nearly always cross international boundaries.

To remedy this limitation, domestic criminal statutes may be amended to give them extraterritorial reach. This relatively simple change could play a valuable role in increasing the United States' ability to take action against those initiating cyber-attacks affecting the United States from outside U.S. territory. Other states might reciprocate by making their own criminal statutes pertaining to cyber-attacks extraterritorial as well, greatly increasing global enforcement.

Even if domestic criminal laws that apply to cyber-attacks obtain extraterritorial application, there will also be jurisdictional hurdles. It may be difficult, for example, to gain custody of accused cyber-criminals operating abroad, particularly if they are not U.S. citizens or operate in countries that do not have extradition treaties with the United States. Strengthened extradition

[273] *See supra* Part III.D.

relationships around the world would complement increasing extraterritorial application of domestic law.

The United States and other countries could also make efforts to explicitly criminalize aspects of cyber-attacks in the United States that fall outside the scope of the law of war and are not already criminalized under existing domestic or international law. This measure would ideally be taken in coordination with other countries after the negotiation and ratification of an international treaty addressing this issue, as recommended below. But, in the absence of such an international agreement, it is still possible for the United States to use domestic law to more effectively counter cyber-attacks not already criminalized by domestic law.

2. Use Countermeasures To Increase the Options Available To Respond to Cyber-Attacks

Although the international law of countermeasures has played a minimal role in legal debates around cyber-attacks thus far, as detailed above, it nonetheless offers an extremely useful legal framework for states seeking to respond to a cyber-attack. The United States and other countries should begin to develop a policy as to what types of countermeasures are legally and strategically appropriate for different types of cyber-attacks.

As noted in the discussion of *jus ad bellum* above,[274] the vast majority of cyber-attacks do not rise to the level of an armed attack. But armed self-defense is not the only manner in which states can respond to cyber-attacks. Provided that the initial cyber-attack violates an international obligation of the perpetrating state, the victim state is entitled under customary international law to employ limited, proportional countermeasures designed to induce the perpetrating state to resume compliance with international norms and to stop conducting (or allowing) cyber-attacks from its territory.[275]

Active defenses are the most commonly discussed type of countermeasure that might be employed in response to a cyber-attack, but they are only one option among many. The key limit on what international obligations a victim state may violate as a countermeasure is proportionality—that is, the countermeasure must not be disproportionate to the injury suffered by the victim state.[276] Moreover, the goal of countermeasures must be to enable a return to the status quo ante, where both the perpetrating and victim states complied with all of their relevant duties towards one another.

---

[274] *See supra* Part II.A.
[275] *See* Draft Articles, *supra* note 99, art. 49.
[276] *See id.* art. 51.

Countermeasures must be temporary and designed such that once the cyber-attacks stop, the countermeasure may stop as well and normal international relations can resume.[277]

The Draft Articles on State Responsibility express a preference for reciprocal countermeasures, but this is not a requirement.[278] Still, the closer the relationship between the obligation the victim state breaches as a countermeasure and the obligation the perpetrating state initially breached, the more likely the countermeasure is to be proportional and therefore lawful.[279] The United States and other countries should consider in advance what international obligations it has toward likely cyber-aggressor states that relate to telecommunications, cyberspace, and similar fields, since these are the most promising areas for countermeasures. States could develop a policy regarding the types of countermeasures available to them in response to particular types of cyber-attacks.

B. A Cyber-Attack Treaty

Changes in domestic law and policy, such as adding extraterritorial applicability to criminal laws and planning for the use of countermeasures, are valuable legal responses to the threat of cyber-attack. Yet "cyberspace is a network of networks that includes thousands of internet service providers across the globe; no single state or organization can maintain effective cyber defenses on its own."[280] Given the transnational nature of the challenge, international cooperation is likely to be necessary to provide a solution commensurate to the problem.[281]

---

[277] *See id.* art. 49.
[278] *See id.*, ch. 2 commentary, para. 5.
[279] *Id.*
[280] DOD STRATEGY, *supra* note 14, at 9.
[281] We are not the first to propose a cyber-attack treaty. Russia has for some time been proposing a treaty banning cyber-attack, though that proposal focuses on activity quite different from that addressed in the Council of Europe agreement. *See, e.g.*, John Markoff & Andrew E. Kramer, *U.S. and Russia Differ on a Treaty for Cyberspace*, N.Y. TIMES, June 27, 2009, *available at* http://www.nytimes.com/ 2009/06/28/world/28cyber.html ("Russia favors an international treaty along the lines of those negotiated for chemical weapons and has pushed for that approach at a series of meetings . . . and in public statements."); CLARKE & KNAKE, CYBER WAR, *supra* note 16, at 268-71 (arguing for a Cyber War Limitations Treaty); *cf.* Jack Goldsmith, *Cybersecurity Treaties: A Skeptical View*, *available at* http://media.hoover.org/sites/default/files/documents/ FutureChallenges_Goldsmith.pdf (offering a skeptical take on the possibility of a cyber-security treaty). Yet the shape of our proposed agreement is quite different—beginning with securing a shared agreement on the activity meant to be prohibited.

The United States has already committed itself to working "with like-minded states to establish an environment of expectations or norms of behavior, that ground foreign and defense polices and guide international partnerships."[282] While the development of international norms is useful, it will not provide governments and private actors with the clarity of a codified definition of cyber-attack or written guidelines on how states should respond to certain types of challenges. For this reason, we recommend that the international community create a multilateral agreement. The agreement should have two central features. First, it must offer a shared definition of cyber-attack and which cyber-attacks constitute armed attack—"cyber-warfare"—under the U.N. Charter.[283] Second, it should offer a framework for more robust international cooperation in evidence collection and criminal prosecution of those participating in cross-national cyber-attacks. That framework should be attentive to the challenges of over-criminalization, maintaining room for individuals to use the Internet and related technologies to engage in lawful dissent. Such a treaty would serve both international aims and national interests of participating countries.[284]

1. Define Cyber-Attack and Cyber-Warfare

Any international resolution defining when a cyber-attack rises to the level of an armed attack should follow the effects-based approach described above.[285] In other words, a cyber-conflict should be defined to escalate into a conventional conflict only if the cyber-attack causes physical injury or property damage comparable to a conventional armed attack. Although the framework of *jus in bello* is of limited usefulness in evaluating the lawfulness of cyber-attacks because of its ambiguities, it would not be appropriate for this definitional treaty to attempt to articulate the content of *jus in bello* norms for cyber-attack. Rather, the *jus in bello* challenges articulated above—such as proportionality of non-lethal or temporary harm and the definition of direct participation for civilians working alongside military cyber-attackers—are likely to be clarified through state practice. In any resolution or agreement on cyber-attacks, but especially in the Security Council, the international

[282] WHITE HOUSE CYBERSPACE STRATEGY, *supra* note 54, at 9. The United States is currently prepared to build bilateral and multilateral partnerships, to work with regional organizations, and to collaborate with the private sector. *See id.* at 12.

[283] It is worth noting again that cyber-attacks that do constitute use of force under the law of war are already covered by *jus in bello* principles, which may be more clearly defined over time in the cyber-attack context through state practice. *See also supra* Part IV.C.2.

[284] *See* WHITE HOUSE CYBERSPACE STRATEGY, *supra* note 54, at 7.

[285] *See supra* Part II.A.2.

community should ensure that the accepted definition of cyber-attack does not quell legitimate dissent and other legitimate expressive activities in cyberspace.

Adopting a clear definition of cyber-warfare and cyber-attack could be concluded in the context of a comprehensive treaty or as an independent agreement in anticipation of more broad-based future cooperation. As a starting point, a defining declaration would provide predictability on the answer to the question of whether a state is initiating an armed conflict and whether retaliation in self-defense is warranted.[286] A defining declaration would also provide a reference point for the extraterritorial criminal laws described in Part IV.A and would provide content that could be incorporated into a later, more comprehensive international treaty. [287]

2. International Cooperation on Evidence Collection and Criminal Prosecution

The definition of cyber-warfare and cyber-attack outlined above provides a common understanding of cyber-attack that individual countries could incorporate into their own domestic criminal legislation. This strategy has been applied, for example, in the international effort to battle bribery: the OECD Bribery Convention provides a definition of bribery that state parties

---

[286] The White House predicts that shared understanding about norms of acceptable cyber-behavior will bring "predictability to state conduct, helping prevent the misunderstandings that could lead to conflict." WHITE HOUSE CYBERSPACE STRATEGY, *supra* note 54, at 9. As a result, the strategy commits the United States to take the lead in building consensus on norms of cyber-behavior. *Id.* at 18.

[287] A defining declaration was also the starting point of another successful effort to criminalize loathsome conduct. Before the Convention Against Torture was adopted by the U.N. General Assembly in 1984, Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, Dec. 10, 1984, S. Treaty Doc. No. 100-20 (1988), 1465 U.N.T.S. 85, *available at* http://www2.ohchr.org/english/law/cat.htm [hereinafter CAT], the General Assembly adopted the Declaration Against Torture. CHRIS INGELSE, THE UN COMMITTEE AGAINST TORTURE: AN ASSESSMENT 69-70 (2001). The Declaration described consensus on key elements of the definition of torture. (These included "the infliction of severe physical or mental pain or suffering," intentional infliction of pain and suffering, the action or sanction of a public official, and conduct that serves a proscribed purpose, "such as obtaining information or a confession. *Id.* at 70.) The Declaration provided much of the substance that later was incorporated into the Convention Against Torture, which has been ratified by 147 states, including the United States. *See* Status, Convention Against Torture And Other Cruel, Inhuman Or Degrading Treatment Or Punishment, (last visited Apr. 10, 2011)**.** In fact, the Swedish draft of the Convention, which formed the basis of the negotiations, used the exact text of the definition of torture from the Declaration. *Id.* at 74. Unfortunately, the draft Sweden submitted to the 34th Session, E/CN.4/1285, is not available on the U.N. Documents database.

then integrate into national legislation forbidding the practice.[288] Under the Bribery Convention, "signatories pledged to criminalize and prosecute the bribery of foreign public officials."[289] The thirty-eight state parties have passed implementing legislation.[290] A defining declaration on cyber-attack could similarly provide the content for domestic criminal legislation targeting the practice.

In addition to such loose coordination, an international treaty addressing cyber-attacks should provide for more extensive cooperation among states on evidence collection and criminal prosecution of those involved in cyber-attacks. A useful starting point for building a universal treaty is the Council of Europe Convention on Cybercrime, described in Part III.B.3, which provides for harmonized regulation of a wide range of cyber-crimes, many of which might be utilized in cyber-attacks. This treaty remains largely limited to Europe (though the United States has ratified the agreement) and it does not address all cyber-attacks that a comprehensive agreement would ideally regulate.[291] Nonetheless, it provides a framework from which a more comprehensive agreement might begin.

Building on the framework established in the Council of Europe Convention, the new agreement should require parties to pass domestic laws banning the cyber-attack-related conduct prohibited under the treaty, so as to harmonize laws across states. The agreement could begin with the information-sharing program suggested above, layering on additional mechanisms for fostering cooperation in identifying and stopping the sources of cyber-attacks through criminal law enforcement agencies.

---

[288] Organisation for Economic Co-operation and Development, Convention on Combating Bribery of Foreign Public Officials in International Business Transactions, Dec. 18, 1997, 37 I.L.M. 1 (1998) [hereinafter OECD Bribery Convention].

[289] Developments in the Law, *Extraterritorial Law and International Norm Internalization*, 124 HARV. L. REV. 1280, 1285 (2011); *see* Bribery Convention, *supra* note 288, art 1(1) ("Each Party shall take such measures as may be necessary to establish that [bribery] is a criminal offence under its law").

[290] OECD Anti-Bribery Convention: National Implementing Legislation, OECD, (last visited Apr. 10, 2011), http://www.oecd.org/document/30/0,3746,en_2649_34859_2027102_1_1_1_1,00.html. Unfortunately, it appears that few countries have actually been enforcing the domestic anti-bribery provisions. *See* Developments in the Law, *Extraterritorial Law and International Norm Internalization*, 124 HARV. L. REV. 1280, 1285 (2011).

[291] Convention on Cybercrime, *Chart of Signatures and Ratifications*, COUNCIL OF EUROPE (last visited Nov. 30, 2010), http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG. Canada, Japan, and South Africa are the other non-European signatories, but the United States is the only one of the four that has ratified the Convention. *Id.*

Member states should also be granted access to cyber-related information that would not be available to non-members. Information sharing would not only give states an incentive to commit to limiting their resort to armed force, but it might also aid states in identifying the source of cyber-attacks. This technical challenge—a fundamental limitation of the legal framework governing cyber-attack—is essentially a problem of information. The more information that is available to states regarding sources and locations of cyber-threats, the easier it will be to prevent cyber-attacks. International cooperation in information-sharing could be an extremely valuable complement to other regulation of cyber-attack.

Finally, consistent with the Tunis Commitment[292] and Agenda,[293] a treaty could provide a foundation that would allow more technologically-developed countries to assist less-developed ones in responding to shared cyber threats. As the recent White House Cyberspace Strategy memo observed,

> Enhancing national-level cybersecurity among developing nations is of immediate and long-term benefits [to the United States and all nations], as more states are equipped to confront threats emanating from within their borders and in turn, build confidence in globally interconnected networks and cooperate across borders to combat criminal misuse of information technologies. It is also essential to cultivating dynamic, international research communities able to take on next-generation challenges to cybersecurity.[294]

Any country's cyber-security can be compromised by its allies' security gaps,[295] therefore any attempt to prevent cyber-attacks must include some efforts to improving the defenses of other countries as well.

Establishing common legal standards for cyber-attacks creates a danger of over-criminalization that could be used to quash legitimate dissent in some signatory states.[296] Any new universal treaty must therefore ensure that criminalization of cyber-attacks is not used to limit legitimate dissent. So long

---

[292] World Summit on the Information Society, Tunis Commitment, http://www.itu.int/wsis/docs2/tunis/off/7.html (last visited Aug. 14, 2011).

[293] World Summit on the Information Society, Tunis Agenda for the Information Society, http://www.itu.int/wsis/docs2/tunis/off/6rev1.html (last visited Aug. 14, 2011).

[294] WHITE HOUSE CYBERSPACE STRATEGY, *supra* note 54, at 15.

[295] Shanker & Bumiller, *supra* note 42 (The United States' allies are "all over the map" on cyber-security issues, according to James Lewis, an expert on computer network warfare at the Center for Strategic and International Studies.).

[296] *See supra* text accompanying notes 18-21.

as cyber-attacks are carefully defined, as proposed at the outset of this Article, this problem should be largely preventable.

There remain other significant challenges that will have to be overcome in the effort to achieve a comprehensive cyber-treaty.[297] First and foremost, it will be necessary to bridge fairly substantial divides between the United States and other leading cyber-powers that have a more expansive view of what activity ought be criminalized through international cooperation. Russia, for example, has been promoting an international agreement banning cyber-attack for some time,[298] but the character of the perceived threat it seeks to address is quite different in character from that addressed by the Council of Europe Convention on Cybercrime. In addition, a comprehensive treaty will have to address difficulties of appropriate verification.[299] Nonetheless, the effort is necessary. As General Keith Alexander, chief of the new U.S. Cyber Command, recognized earlier this year, "[w]e do have to establish the lanes of the road" for what cyber-activities governments can and cannot pursue."[300]

* * *

The emergence of Stuxnet last year heralded a new era for cyber-attacks. Although the damage it caused was apparently limited to the Iranian nuclear program at which it was aimed, the vulnerabilities it revealed were immense. By the time it was discovered, Stuxnet had wormed its way into computer networks around the world, including, by some estimates, nearly half of those running electric utilities.[301]

---

[297] Indeed, some have suggested a successful treaty may be nearly impossible to achieve, at least in the short term. *See, e.g.*, Waxman, *supra* note 18, at 425-26 ("[N]ot only do certain features of cyber-activities make international legal regulation very difficult, but major actors also have divergent strategic interests that will pull their preferred doctrinal interpretations and aspirations in different directions, impeding formation of a stable international consensus."); Goldsmith, *supra* note 43, at 12 ("This paper has argued that the fundamental clash of interests concerning the regulation of electronic communications, the deep constraints the United States would have to adopt to receive reciprocal benefits in a cybersecurity treaty, and the debilitating verification problems will combine to make it unfeasible to create a cybersecurity treaty that purports to constrain governments."). For a dissenter's view on the appropriate international response to cyber-attack, see Duncan B. Hollis, *An E-SOS for Cyberspace*, 52 HARV. INT'L L.J. 373 (2011) (arguing for a duty to assist cyber-threat victims, rather than regulation of bad cyber-actors).

[298] *See* Markoff & Kramer, *supra* note 281.

[299] *See* Goldsmith, *supra* note 43, at 10-12.

[300] Siobhan Gorman, *U.S. Backs Talks on Cyber Warfare*, WALL ST. J., June 4, 2010, *available at* http://online.wsj.com/article/SB10001424052748703340904575284964215965730.html.

[301] *Id.*

Cyber-attacks on vital infrastructure are already becoming widespread. Cyber-security professionals report that the computer infrastructure has become more vulnerable even in just the past year.[302] And yet, while the threat of cyber-attacks has rapidly grown, the response has not kept pace. This Article has shown that both the U.S. government and the international community at large have thus far largely failed to update the legal framework for responding to cyber-attacks. To face the new and growing threats, governments continue to rely on limited and piecemeal bodies of law not designed to meet modern threats.

It is past time to begin a conversation about the scope of the threat posed by cyber-attacks and the best ways to meet it. By expanding the reach of domestic law abroad and developing a system for utilizing limited countermeasures, where appropriate, the United States can expand its capacity to battle this new threat. Yet the United States is restricted in what it can accomplish alone. Cyber-attacks are quintessentially transnational—often designed by authors in multiple countries, run through networks across the world, undermining a computer system in a country where those designing the attack have never set foot. This global threat may only be effectively met by a global solution—by the international community working together to design a new law for cyber-attacks.

[302] Mark Clayton, *Security Lags Cyberattack Threats in Critical Industries, Report Finds*, CHRISTIAN SCIENCE MONITOR (April 20, 2011) (citing a global survey of 200 computer security professionals working in critical infrastructure industries, "In the Dark: Crucial Industries Confront Cyberattacks").