The Law of Cyber-Attack

Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue & Julia Spiegel*

Cyber-attacks have become increasingly common in recent years. Capable of shutting down nuclear centrifuges, air defense systems, and electrical grids, cyber-attacks pose a serious threat to national security. As a result, some have suggested that cyber-attacks should be treated as acts of war. Yet the attacks look little like the armed attacks that the law of war has traditionally regulated. This Article examines how existing law may be applied—and adapted and amended—to meet the distinctive challenge posed by cyber-attacks. It begins by clarifying what cyber-attacks are and how they already are regulated by existing bodies of law, including the law of war, international treaties, and domestic criminal law. This review makes clear that existing law effectively addresses only a small fraction of potential cyber-attacks. The law of war, for example, provides a useful framework for only the very small number of cyber-attacks that amount to an armed attack or that take place in the context of an ongoing armed conflict. This Article concludes that a new, comprehensive legal framework at both the domestic and international levels is needed to more effectively address cyber-attacks. The United States could strengthen its domestic law by giving domestic criminal laws addressing cyber-attacks extra-territorial effect and by adopting limited, internationally permissible countermeasures to combat cyber-attacks that do not rise to the level of armed attacks or that do not take place during an ongoing armed conflict. Yet the challenge cannot be met by domestic reforms alone.

Copyright © 2012 California Law Review, Inc. California Law Review, Inc. (CLR) is a California nonprofit corporation. CLR and the authors are solely responsible for the content of their publications.

* Gerard C. and Bernice Latrobe Smith Professor of International Law, Yale Law School; law clerk, Judge Mark Kravitz (D. Conn.); J.D., Yale Law School, 2012; J.D., Yale Law School, 2012; J.D., Yale Law School, 2012; Associate, Arnold & Porter LLP; 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. We thank participants in the George Washington University School of Law Symposium on the Future of Cyber-Warfare and in the Harvard National Security Journal and Harvard University National Security & Law Association Annual Symposium for their very helpful comments and suggestions.

International cooperation will be essential to a truly effective legal response. New international efforts to regulate cyber-attacks must begin with agreement on the problem—which means agreement on the definition of cyber-attack, cyber-crime, and cyber-warfare. This would form the foundation for greater international cooperation on information sharing, evidence collection, and criminal prosecution of those involved in cyber-attacks—in short, for a new international law of cyber-attack.

INTRODUCTION

In 2010, 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.[1]

A few months later, a so-called "distributed denial of service" attack took the entire population of Burma off the Internet immediately preceding the country's first national election in twenty years.[2] Observers suspect that the military junta in Burma coordinated the attack to shut down the Internet and thereby restrict the free flow of information,[3] but American public officials

1. The seeds for this attack were apparently sown 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 spread that Iran's uranium enriching capabilities had been diminished. *The Stuxnet Worm: A Cyber-Missile Aimed at Iran?*, 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 et al., *Israeli Tests Called Crucial in Iran Nuclear Setback*, N.Y. TIMES, Jan. 16, 2011, at A1. Stuxnet is the first computer virus known to be capable of specifically targeting and destroying industrial systems such as nuclear facilities and power grids. Fildes, *supra*.

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

3. *See id.*

have resisted blaming the attack on the government, even as they have criticized the election.[4]

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 website based in Alabama.[5] This revelation followed on the heels of a report by the McAfee cyber-security company suggesting 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.[6]

What law governs these attacks? Some have referred to these and similar attacks as "cyber-warfare," suggesting that the law of war might apply.[7] Yet the attacks look little like the armed conflict 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

4. *See, e.g.*, Barack Obama & Michelle 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.

5. Ellen Nakashima & William Wan, *China's Denials on Cyberattacks Undercut*, WASH. POST, Aug. 24, 2011, at A12.

6. David Barboza & Kevin Drew, *Security Firm Sees Global Cyberspying*, N.Y. TIMES, Aug. 3, 2011, at A11. This was not the first suggestion of a program of cyber-attacks 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 Eunjung Cha & Ellen Nakashima, *Google Attack Part of Vast Campaign; Targets Are of Strategic Importance to China, Where Scheme Is Thought to Originate*, WASH. POST, Jan. 14, 2010, at A1.

7. *See, e.g.*, RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT 6 (2010); Stephen Dycus, *Congress's Role in Cyber Warfare*, J. NAT'L SECURITY L. & POL'Y 155, 162 (2010) ("Cyber warfare, as that term is used here, refers to conflicts that utilize cyber or electronic weapons either offensively or defensively, or both."); *Understanding Cyber Warfare*, LAWS.COM, http://cyber.laws.com/cyber-warfare (last visited Apr. 18, 2012).

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

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 demonstrates how existing law is deficient and what needs to be done to improve it. Although such 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 regulating 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 policing cyber-attacks through law. Examining existing law leads to a clear conclusion: a new, comprehensive legal framework is needed to address cyber-attacks.

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. This may seem a mundane task, but it is a critical starting point for any reform effort. To that end, we 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.[9]

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 first apply *jus ad bellum*—the law governing a state's right to resort to armed force—to cyber-attacks. We conclude that most cyber-attacks do not rise to the level of an armed attack and thus do not justify the use of armed force in response. "Cyber-warfare" is thus a term properly used only to refer to the small subset of cyber-attacks that do constitute armed attacks or that occur in the context of an ongoing armed conflict. 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. With the scope of cyber-warfare clear, we then explore how *jus in bello*—the law governing conduct in an armed conflict—applies.

9. This definition differs from that currently applied by the U.S. Cyber Command, which uses the term "Cyber Attack" to apply only to attacks that cause physical damage to property or injury to persons. E-mail from Gary D. Brown, Col. U.S. Airforce, Staff Judge Advocate, U.S. Cyber Command to author (May 15, 2012 10:07AM) (on file with author). Our terminology allows differentiation between those attacks that are covered by the law of armed conflict (which we call cyber-warfare) and those that violate the norm of nonintervention but are not covered by the law of armed conflict (which we call cyber-attack).

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 the 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—namely, codifying clear definitions of cyber-warfare and cyber-attack and providing guidelines for international cooperation on evidence collection and criminal prosecution—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,[10] to a false message that causes a nuclear reactor to shut off[11] or a dam to open,[12] to a blackout of the air traffic control system that results in airplane crashes[13]—anticipate severe and widespread economic or physical damage. While none of these scenarios has thus far occurred, numerous cyber-incidents occur regularly.[14] Nevertheless, there is no settled definition for identifying these incidents as cyber-attacks,[15] much less as cyber-warfare. The absence of a shared definition has made it difficult for analysts from different countries to develop coordinated policy recommendations and for governments to engage in coordinated action. Hence the technical project of defining cyber-attack is an important first step toward addressing the growing threat posed by cyber-attacks. After describing some existing definitions, we offer a definition that effectively encompasses the activity that lies at the heart of the concerns raised by cyber-attacks.[16]

1. Existing Conceptions of Cyber-Attack

Existing definitions of "cyber-attack" and related terms vary widely. Perhaps one of the most widely cited definitions comes from government security expert Richard A. Clarke, who 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."[17] Similarly, former NSA and CIA director Michael Hayden has spoken of cyber-war as the "deliberate attempt to disable or destroy another country's computer networks."[18] These definitions, however, do not distinguish between a cyber-crime, cyber-attack, and cyber-war.[19] As a result, they are open to a dangerously broad application of the war framework in the cyber context.[20] In addition, Clarke's definition is too narrow

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

11. Vida M. Antolin-Jenkins, *Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places?*, 51 NAVAL L. REV. 132, 140 (2005).

12. 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 A1.

13. U.S. GEN. ACCOUNTING OFFICE, AIR TRAFFIC CONTROL: WEAK COMPUTER SECURITY PRACTICES JEOPARDIZE FLIGHT SAFETY (May 1998).

14. *See, e.g.*, *infra* Part I.B (providing recent examples of cyber-attacks).

15. As distinct from cyber-crime. *See infra* Part I.B.

16. In Part IV of this Article, we explore methods by which the U.S. government and other governments can adopt the proposed definition or a similar, uniform definition.

17. CLARKE & KNAKE, *supra* note 7, at 6; *see, e.g.*, *More Than Firewalls: Three Challenges to American Cyber Security*, ASYMMETRIC THREAT (Aug. 2011), http://asymmetricthreat.net/docs/snapshot2011_08.pdf (citing Clarke's definition); *Understanding Cyber Warfare*, *supra* note 7.

18. Tom Gjelten, *Extending the Law of War to Cyberspace*, NAT'L PUB. RADIO (Sept. 22, 2010), http://www.npr.org/templates/story/story.php?storyId=130023318 (last visited Apr. 18, 2012).

19. *See infra* Part I.A.3 for a discussion of the importance and mechanics of distinguishing between the concepts of cyber-attack and cyber-crime.

20. *See infra* Part II.A for a detailed exploration of *jus ad bellum* as it applies to cyber-attacks.

in one respect: it limits the definition to attacks perpetrated by *nation-states*, thereby excluding entirely plausible scenarios in which attacks are carried out by non–state actors.

Technical experts have proposed more limited definitions. For example, in his famous and prescient 1995 work on information warfare, Martin Libicki limits cyber-warfare to semantic attacks—digital assaults that cause systems to seem to operate normally, when in fact they generate "answers at variance with reality."[21] This approach excludes the broad range of potential threats to a country's national security that target cyber-infrastructure but do not meet the requirements of a semantic attack. These threats have the same capacity to inflict harm on computer systems or networks, and thus any definition of cyber-attack that excludes them is necessarily incomplete.

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 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. Perhaps not surprisingly, they have arrived at very different understandings of the problem.

Shortly after establishing the United States Cyber Command, the Joint Chiefs of Staff published a lexicon in 2011 for military use in cyber-operations, which included the first official military definition of cyber-attack. It defines a cyber-attack as:

> A hostile act using computer or related networks or systems, and intended to disrupt and/or destroy an adversary's critical cyber systems, assets, or functions. The intended effects of cyber attack are not necessarily limited to the targeted computer systems or data themselves—for instance, attacks on computer systems which are intended to degrade or destroy infrastructure or C2 capability. A cyber attack may use intermediate delivery vehicles including peripheral devices, electronic transmitters, embedded code, or human operators. The activation or effect of a cyber attack may be widely separated temporally and geographically from the delivery.[22]

A key feature of this approach is that it limits "cyber-attacks" to those hostile acts that are intended to harm critical cyber systems—thus restricting the definition based on the objective of the attack.[23]

---

21. MARTIN C. LIBICKI, WHAT IS INFORMATION WARFARE? 77 (1995).

22. Gen. James E. Cartwright, Memorandum for Chiefs of the Military Servs., Commanders of the Combatant Commands, Dirs. of the Joint Staff Directories on Joint Terminology for Cyberspace Operations 5 (Nov. 2011).

23. Alternative views of cyber-attack and cyber-warfare preceded this announcement in policy circles in the United States. In 2001, the Congressional Research Service defined cyber-warfare as "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*

The Shanghai Cooperation Organization, by contrast, has adopted a 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."[24] 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."[25] Moreover, it identifies the dissemination of information harmful to "social and political, social and economic systems, as well as spiritual, moral and cultural spheres of other states" as one of the main threats to information security.[26]

Hence the Shanghai Cooperation Organization appears to have adopted an expansive vision of cyber-attacks that includes the use of cyber-technology to undermine political stability. Commentators fear that this definition represents an effort to justify censorship of political speech on the Internet.[27] This concern is particularly salient in light of recent government efforts to suppress political organizing using new media in Iran, Egypt, and elsewhere.[28]As the Internet is increasingly utilized as a forum for exchange of ideas and political organization, such suppression threatens human rights.

---

information operations mounted against an adversary, or even *dominating* information on the battlefield." STEVEN A. HILDRETH, CONG. RESEARCH SERV., CRS REPORT FOR CONGRESS: CYBERWARFARE 16 (2001). In 2009, the U.S. National Research Council, an independent organization in Washington, D.C., defined 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." NAT'L RESEARCH COUNCIL, TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 1 (William A. Owens et al. eds., 2009) [hereinafter NRC REPORT].

24. 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).

25. SHANGHAI COOPERATION AGREEMENT, Annex I, at 209.

26. *Id.* at 203.

27. *See, e.g.*, Tom Gjelten, *Seeing the Internet as an 'Information Weapon,'* NAT'L PUB. RADIO (Sept. 23, 2010), http://www.npr.org/templates/story/story.php?storyId=130052701; *see also infra* Part I.A.2.e.

28. *See, e.g.*, Saeed Kamali Dehghan, *Iran Clamps Down on Internet Use*, GUARDIAN (Jan. 5, 2012), http://www.guardian.co.uk/world/2012/jan/05/iran-clamps-down-internet-use; Matt Richtel, *Egypt Halts Most Internet and Cell Service, and Scale of Shutdown Surprises Experts*, N.Y. TIMES, Jan. 29, 2011, at A13; Sal Gentile, *Gadhafi Regime "Turns Off the Tap" on Libya's Internet*, *Live Blog: Libya Revolts*, PBS (Mar. 4, 2011, 6:46 PM), http://www.pbs.org/wnet/need-to-know/the-daily-need/libya-revolts-a-live-blog/7679/.

The distance between these two government-led understandings of cyber-attacks demonstrates 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.[29] Active defense includes "electronic countermeasures designed to strike attacking computer systems and shut down cyber-attacks midstream."[30] Governments are likely to employ both active and passive defenses—and the two are often designed to work in tandem[31]—but the passive defense cannot on its own amount to a cyber-attack.[32]

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

A cyber-attack may be carried out by means of *any* action—hacking, bombing, cutting, infecting, and so forth—but to be a cyber-attack it must aim to undermine or disrupt the function of a computer network. In this respect, this Article adopts the U.S. objective-based approach rather than the means-based approach of the Shanghai Cooperation Organization.

Warfare may be classified on the basis of the means of attack. For example, warfare may be classified as kinetic (conventional, physical) warfare, biological warfare, chemical warfare, nuclear warfare, intelligence-based warfare, network-based warfare,[33] or guerilla warfare. Warfare may also be

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

30. JEFFREY CARR, INSIDE CYBER WARFARE 46 (2010).

31. Active defense may be triggered by passive activities. For example, a routine virus scan that identifies a virus and then eliminates it switches from passive (scanning) to active (elimination).

32. The U.S. government currently utilizes both active and passive defenses. *See* U.S. DEP'T OF DEF., DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE (2011) [hereinafter DOD STRATEGY].

33. 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." NRC REPORT, *supra* note 23, at 165. 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).

defined by its objective. "Objective" here means the direct target, rather than the long-range purpose, of the action. Examples include information warfare, psychological warfare, command and control warfare,[34] electronic warfare, and economic warfare.

Because we define cyber-attack according to its objective ("to undermine the functions of a computer network for a political or national security purpose"), any means may be used to accomplish a cyber-attack. Defining cyber-attack 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.[35] 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.[36]

Second, the objective-based approach is logical. Warfare traditionally functions in four domains—land, air, sea, and space—each of which is addressed by one of the full-time armed services.[37] With the rise of cyber-warfare, strategists have identified a fifth domain: cyberspace.[38] In response, the United States has created the U.S. Cyber Command, a subdivision of the joint services Strategic Command.[39] Although the Cyber Command is not a

---

34. "Command and control warfare" includes any attack meant to interfere with the enemy's capacity to command and control its troops. *See* GEORGE J. STEIN, INFORMATION ATTACK: INFORMATION WARFARE IN 2025, at 2 (1996), *available at* http://csat.au.af.mil/2025/volume3/vol3ch03.pdf. The Department of Defense defines command and control as

> [t]he exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission.

Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, Joint Chiefs of Staff (Nov. 2010), *available at* http://www.dtic.mil/ doctrine/new_pubs/jp1_02.pdf.

35. *See* Antolin-Jenkins, *supra* note 11, at 138 ("[K]inetic weapons are certainly part of the cyberwar arsenal.").

36. CHAIRMAN OF THE JOINT CHIEFS OF STAFF, U.S. DEP'T OF DEFENSE, NATIONAL MILITARY STRATEGY FOR CYBERSPACE OPERATIONS 15 (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 23, at 12–19.

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

38. *See* DOD STRATEGY, *supra* note 32, at 5; *War in the Fifth Domain*, ECONOMIST (July 1, 2010), 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, NATIONAL MILITARY STRATEGY OF THE UNITED STATES OF AMERICA 5 (2004).

39. 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/;

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.[40]

Third, an objective-based approach avoids unnecessarily limiting Internet speech, thereby avoiding the serious risks posed by a means-based definition. 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.[41] The Shanghai Cooperation Organization's definition may have been designed to be means-based in part for this reason.[42]

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 different ways. Syntactic attacks disrupt a computer's operating system, causing the network to malfunction.[43] Examples include "worms, viruses, [and] Trojan horses."[44] The incident in Burma, discussed in the opening to this Article, constituted a syntactic attack. In contrast, semantic attacks preserve the operating system but compromise the accuracy of the information it processes and to which it reacts.[45] 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."[46] The Stuxnet attack described above was, in part, a semantic attack because the nuclear plant appeared to be operating normally even as it was malfunctioning.[47]

---

see Thom Shanker, *Cyberwar Chief Calls for Secure Computer Network*, N.Y. TIMES, Sept. 24, 2010, at A1.

40. *See* DOD STRATEGY, *supra* note 32, 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.").

41. *See* Gjelten, *supra* note 27.

42. *See id.*; SHANGHAI COOPERATION AGREEMENT, *supra* note 24.

43. Antolin-Jenkins, *supra* note 11, at 139.

44. *Id.*

45. *Id.* at 140.

46. LIBICKI, *supra* note 21, at 77.

47. Cyber-attacks need not be limited to syntactic or semantic attacks. The U.S. cyber-operation in Iraq discussed below, for example, was neither syntactic nor semantic. Nevertheless, it

By contrast, neither cyber-espionage nor cyber-exploitation constitutes a cyber-attack because these concepts do not involve altering computer networks in a way that affects their current or future ability to function.[48] For example, in 2003, a security breach created numerous leaks of sensitive information from U.S. Department of Defense computers, which occurred over several months.[49] 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.[50] Another recent example of cyber-espionage occurred when hackers operating from China copied data from 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.[51] Subsequent developments imply that at least one purpose of the attack—dubbed "Operation Aurora"—was to monitor U.S. government officials' emails.[52] 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 over 24,000 Pentagon files.[53] Meanwhile, the extent to which the United States is conducting similar activities is unknown.[54]

---

constitutes a cyber-attack under this Article's definition, as it did "undermine the function" of the secure email system by causing it to send an email from an unauthorized user.

48. 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?* NEW YORKER (Nov. 1, 2010), http://www.newyorker.com/reporting/2010/11/01/101101fa_fact_hersh?. The former director of 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 18. 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 23, at 22, § 1.6.

49. CLAY WILSON, CONG. RESEARCH SERV., BOTNETS, CYBERCRIME, AND CYBERTERRORISM: VULNERABILITIES AND POLICY ISSUES FOR CONGRESS 14 (2008).

50. *Id.*

51. *A New Approach to China*, 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, *State's Secrets Day 7; Vast Hacking by a China Fearful of the Web*, N.Y. TIMES, Dec. 4, 2010, at A1.

52. *See, e.g.*, Amir Efrati & Siobhan Gorman, *Google Mail Hack Is Blamed on China*, WALL ST. J., June 2, 2011, at A1; Wyatt Andrews, *China Google Hacker's Goal: Spying on U.S. Govt*, CBS NEWS (June 2, 2011), http://m.cbsnews.com/fullstory.rbml?catid=20068474&feed_id=0&videofeed=36 (last visited Apr. 19, 2012).

53. Thom Shanker & Elisabeth Bumiller, *After Suffering Damaging Cyberattack, the Pentagon Takes Defensive Action*, N.Y. TIMES, July 15, 2011, at A6.

54. *See* Jack Goldsmith, *What Is the Government's Strategy for the Cyber-Exploitation Threat?*, LAWFARE BLOG (Aug. 10, 2011, 10:58 PM), http://www.lawfareblog.com/2011/08/what-is-the-government%E2%80%99s-strategy-for-the-cyber-exploitation-threat/ (last visited Apr. 19, 2012).

Although all of these incidents of cyber-espionage compromised the security of a computer network for the purpose of carrying out a military objective,[55] they did not "undermine the function" of a computer system and thus were not cyber-attacks as defined here. To "undermine the function" of a computer system, an actor must *do more than passively observe a computer network or copy data*, even if that observation is clandestine. The actor must affect the operation of 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 they are not cyber-*attacks*. In this respect, our definition reflects a common distinction between espionage and attacks in more traditional settings.

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

A cyber-attack must target a computer network, where a computer network is defined as 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 devices that control elevators and traffic lights, regulate pressure on water mains, and are ubiquitous in appliances such as cell phones, televisions, and even washing machines.[56] The potential for widespread damage from a cyber-attack grows in tandem with the spread of computers to nearly every facet of human activity.

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. A cyber-crime committed by a non–state actor for a political or national security purpose is a cyber-attack. On the other hand, a cyber-crime that is not carried out for a political or national security purpose, such as most instances of Internet fraud, identity theft, and intellectual property piracy, does not fit this final element of a "cyber-attack" and is therefore mere cyber-crime.

55. *See* Michael Joseph Gross, *Enter the Cyber-Dragon*, VANITY FAIR, Sept. 2011, *available at* http://www.vanityfair.com/culture/features/2011/09/chinese-hacking-201109 (detailing these and other successful hacks of public and private systems).

56. CLARKE & KNAKE, *supra* note 7, at 70–74.

There are at least two important reasons for excluding nonpolitical 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,[57] invoke legal doctrines surrounding state responsibility and terrorism[58] in a way that the actions of Onel de Guzman, a student who was suspected of infecting tens of millions of computers in 2000 with the destructive but undirected "love bug virus,"[59] do not. Second, 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 their 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.[60] 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 the First Amendment protects dissent in the United States, the use of cyberspace regulations to suppress dissent is a serious possibility in

57. *See* Noah Shachtman, *Kremlin Kids: We Launched the Estonian Cyber War*, WIRED (Mar. 11, 2009, 12:45 PM), http://www.wired.com/dangerroom/2009/03/pro-kremlin-gro/ (last visited Apr. 19, 2012); *infra* Part I.B.1.

58. 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 international terrorism according to its apparent political intentions); BLACK'S LAW DICTIONARY 1611 (9th ed. 2009) (defining terrorism as using violence "as a means of affecting political conduct").

59. Mark Landler, *A Filipino Linked to 'Love Bug' Talks About His License to Hack*, N.Y. TIMES, Oct. 21, 2000, at C1.

60. *See* NRC REPORT, *supra* note 23, 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 32, 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 53 (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 non–state actors).

countries that do not have the same liberal democratic traditions.[61] Internet regulations in China are a troubling testament to this fact.[62] 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.[63] 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 adopts the objective-based approach taken by the U.S. government, but it adds a "purpose" requirement that enables policy-makers to distinguish between mere cyber-crime and cyber-attacks. Such a distinction is crucial to domestic and international efforts to implement cyber-security, because it more effectively tailors the legal approach to the threat posed and focuses resources on true national security threats.

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 Table 1 and Figure 1.

61. *See, e.g.*, Gjelten, *supra* note 27 (on Chinese and Russian efforts to control communication on the Internet).

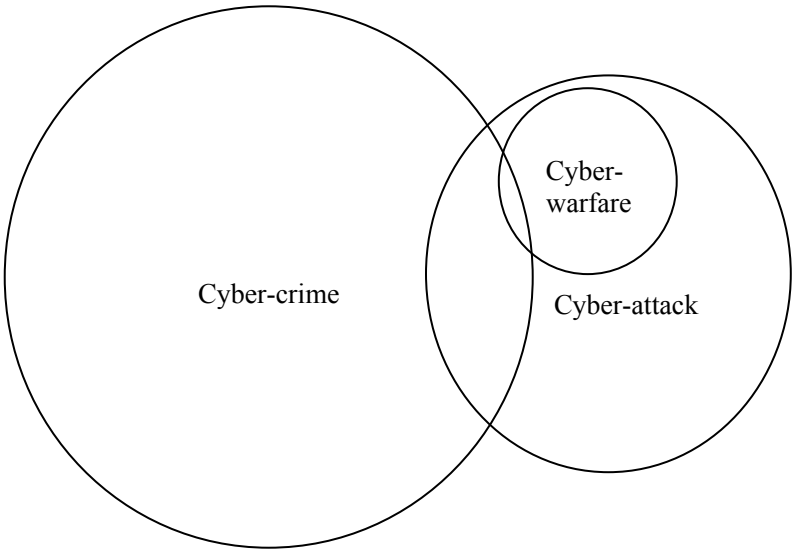
62. China has also been embroiled in cyber-conflict with private entities as well—namely, Google and Yahoo. Since the early 2000s, the U.S.-based companies have been criticized for their cooperation with the Chinese government, both in policing internal dissidents and in censoring external information 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 24.

63. 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." OFFICE OF THE PRESIDENT, INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD 5 (2011) [hereinafter WHITE HOUSE CYBERSPACE STRATEGY]. 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.

TABLE 1: Essential characteristics of different cyber-actions

	Type of cyber-action		
	Cyber-attack	*Cyber-crime*	*Cyber-warfare*
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			√

FIGURE 1: 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,[64]

64. *See, e.g.*, Sarah Gordon & Richard Ford, *On the Definition and Classification of Cybercrime*, 2 J. COMPUTER VIROLOGY 13, 13 (2006) ("Despite the fact that the word 'Cybercrime' has entered into common usage, many people would find it hard to define the term precisely."); Sylvia

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."[65] 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.[66] 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 individuals, not states.[67] While the distinction between cyber-crime and cyber-attack is important, we acknowledge that it often will not be readily apparent at the moment of the cyber-event whether it is one or the other (or both)—in part because the identity and purpose of the actor may not be apparent. Such uncertainty counsels in favor of an immediate response that would be appropriate to either cyber-crime or a cyber-attack.

Most cyber-crimes do not also constitute cyber-attack or cyber-warfare, as depicted in Figure 1. An act is only a cyber-crime when a non–state actor commits an act that is criminalized under domestic or international law.

Mercado Kierkegaard, *International Cybercrime Convention*, IGI GLOBAL, http://www.igi-global.com/viewtitlesample.aspx?id=7486 (last visited Apr. 6, 2012) ("[T]here is still no accepted definition of what really constitutes cybercrime."); *see also* DEBRA LITTLEJOHN SHINDER, SCENE OF THE CYBERCRIME: COMPUTER FORENSICS HANDBOOK 16 (Ed Tittel ed., 2002) ("[T]he definition of computer crime under state law differs, depending on the state.").

65. Gordon & Ford, *supra* note 64, 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 a means or a target. *See, e.g.*, SHINDER, *supra* note 64, 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").

66. *See generally* COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION, CRIMINAL DIVISION, U.S. DEP'T OF JUSTICE, PROSECUTING COMPUTER CRIMES (2d ed. 2010); *Cyber Crime*, FBI, http://www.fbi.gov/about-us/investigate/cyber (last visited Apr. 21, 2012). 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." Convention on Cybercrime, Council of Europe, E.T.S. No. 185, pmbl., Nov. 23, 2001 (entered into force July 1, 2004), *available at* http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm [hereinafter Cybercrime Convention].

67. Therefore, under our definition, 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.

Consider the following three scenarios, each of which includes a cyber-crime that is not a cyber-attack:

First, a non–state actor commits an illegal act for a political or national security purpose 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 domestic 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 the actions do not undermine the function of a computer network and because he or she is not motivated by a political or national security purpose.

As shown in Figure 1, 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 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 is the attack by the Chinese government on the Falun Gong website in 2011.[68] 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 national or international law or because they do not use computer-based means. Practically speaking, it is unlikely for a private actor to purposefully[69] undermine the function of a computer network without also violating the law,

68. *See* Nakashima & Wan, *supra* note 5.

69. Because a cyber-attack must be "for a political or national security purpose," the only actions falling into this category would be purposeful.

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 1 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. State Department's 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 1 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 necessarily constitute "cyber-crime."

Cyber-warfare can also constitute both cyber-attack and cyber-crime. The area of intersection between all three circles in Figure 1 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 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 Table 1 and Figure 1, 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 examples of recent cyber-incidents—though far from exhaustive—demonstrate the variety and scope of recent cyber-attacks. They also introduce the wide-ranging challenges to regulating such 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 website inadvertently aired on China Central Television. There are several other recent examples of such attacks—a few of which we describe here to provide a sense of the varied ways in which such attacks may be carried out.

After controversially moving a Soviet-era war memorial in April 2007, the densely wired[70] Republic of Estonia suffered a DDOS attack. Such attacks often cause mere inconvenience, but this one nearly had life threatening consequences—the emergency line to call for an ambulance or a fire truck was out of service for an hour.[71] Allegedly executed by networks of hackers,[72] authorities never officially attributed the attack to a state, but some suspect Russia's involvement due to the sophistication and scale of the attack.[73]

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.[74] Despite early speculation that the

70. Estonia has one of the highest network saturation rates in the world. CLARKE & KNAKE, *supra* note 7, at 13.

71. *Newly Nasty: Defences Against Cyberwarfare Are Still Rudimentary. That's Scary*, ECONOMIST (May 24, 2007), http://www.economist.com/node/9228757?story_id=9228757 (last visited Apr. 19, 2012).

72. Specifically, a youth movement (funded by the Russian government) later claimed responsibility for the attack. Shachtman, *supra* note 57.

73. 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).

74. *The Threat from the Internet: Cyberwar: It Is Time for Countries to Start Talking About Arms Control on the Internet*, ECONOMIST (July 1, 2010), http://www.economist.com/node/16481504 (last visited Apr. 19, 2012).

Russian government had planned the incident, it now appears likely that the government simply stood by as private hackers openly orchestrated the attack.[75]

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,[76] the United States was more circumspect.[77] There remain some questions about where the attack originated. This serves to illustrate a common problem for cyber-attacks in general and DDOS attacks 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

Another form of cyber-attack is a semantic attack, in which the attacker surreptitiously inputs inaccurate information in a computer system. More sophisticated than the DDOS attack, a semantic attack causes the computer system to appear to operate normally, even as it fails.[78]

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.[79] 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.[80]

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.[81]

Because these cyber-attacks frequently accompany and facilitate conventional attacks, attribution is less problematic. The difficulty here is in

75. 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.

76. Malcolm Moore, *North Korea Blamed for Cyber Attack on South Korea*, TELEGRAPH (July 8, 2009), http://www.telegraph.co.uk/news/worldnews/ asia/southkorea/5778176/North-Korea-blamed-for-cyber-attack-on-South-Korea.html.

77. 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.

78. LIBICKI, *supra* note 21, at 77.

79. William M. Arkin, *The Cyber Bomb in Yugoslavia*, WASH. POST (Oct. 25, 1999), http://www.washingtonpost.com/wp-srv/national/dotmil/arkin.htm.

80. Kelsey, *supra* note 73, at 1434–35.

81. CLARKE & KNAKE, *supra* note 7, at 1–9.

identifying when a cyber-attack has occurred, since the disruption remains hidden until its kinetic sequel.

3. Infiltrating a Secure Computer Network

Once an attacker infiltrates a secure computer network she can execute a variety of actions.[82] 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 apparently worked: American troops encountered abandoned military equipment arranged in accordance with the email.[83] 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 that make the project of crafting a legal approach to them all the more challenging. The next Part examines 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 inquiries are intensely fact specific. Instead, we lay out the general types of cyber-attacks that would be governed

82. For reasons explained above, cyber-espionage—stealing rather than planting information—is not included in most definitions of cyber-attack. *See supra* text accompanying notes 43–46.

83. CLARKE & KNAKE, *supra* note 7, at 9–10.

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.[84] Cyber-warfare is only a part of a much larger problem.

It is worth noting at the outset that applying the existing law of war framework to cyber-attacks is extraordinarily challenging. The key treaties governing conduct in war, the Geneva Conventions, were last revised in the wake of World War II. Nothing was further from the minds of the drafters of the Geneva Conventions than attacks carried out over a worldwide computer network. One unanticipated challenge is how to address attacks that have little or no direct physical consequences, but that nonetheless cause real harm to national security. Perhaps for this reason, thus far no state has claimed that a 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 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. In the absence of agreement, the increase in attacks heightens the possibility that states might respond to a cyber-attack with conventional military means.[85] The rise in attacks also creates a more pressing 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.[86]

---

84. 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, 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, *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 nonmilitary objectives); 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).

85. This is not mere speculation. The Department of Defense issued a report in late 2011 in which it declared that the United States reserves the right to respond to cyber-attacks using "all necessary means—diplomatic, informational, military, and economic." DEP'T OF DEFENSE, CYBERSPACE POLICY REPORT: A REPORT TO CONGRESS PURSUANT TO THE NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2011, SECTION 934, at 2 (2011).

86. 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 10, at 1027–28; Davis Brown, *A Proposal for an*

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 indicated in Table 1 above, we conclude that the best test of when a cyber-attack is properly considered cyber-warfare is whether the attack results in physical destruction—sometimes called a "kinetic effect"—comparable to a conventional attack. Arriving at this conclusion requires examining not only the Charter's text—which is quite general and vague—but also the meaning given to that text by state practice and interpretation over time. Because an armed conflict has never begun solely as a result of a cyber-attack, there is no state practice on what cyber-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, paying 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: Prohibition on Use of Force and Intervention in Internal Affairs

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

International Convention to Regulate the Use of Information Systems in Armed Conflict, 47 HARV. INT'L L.J. 179 (2006).

territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[87] This prohibition is complemented by a customary international law norm of nonintervention, which prohibits states from interfering in the internal affairs of other states.[88] The International Court of Justice ("ICJ") has held that, where the interference takes the form of a use or threat of force, the customary international law norm of nonintervention is coterminous with Article 2(4).[89]

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 consensus is that Article 2(4) prohibits only armed force.[90]

Discussions about cyber-attacks have the potential to reignite debates over the scope of Article 2(4).[91] 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.[92]

---

87. U.N. Charter art. 2, para. 4.

88. *See* G.A. Res. 37/10, U.N. Doc. A/RES/37/10 (Nov. 15, 1982); G.A. Res. 25/2625, U.N. Doc. A/RES/25/2625 (Oct. 24, 1970).

89. 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 nonintervention 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 cyber-attacks do not constitute a use of force, they may nevertheless violate the customary international law norm of nonintervention, as discussed below.

90. 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 73, 80–82 (Michael N. Schmitt & Brian T. O'Donnell eds., 2002). 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 nonmilitary physical force, such as flooding, forest fires, or pollution. *Id.* at 82–83.

91. *See* Waxman, *supra* note 24.

92. 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).

Cyber-attacks may also violate the customary international law norm of nonintervention, as defined by a growing record of state practice and opinion juris. First, states generally do not engage in cyber-attacks openly, but rather try to hide their responsibility by camouflaging attacks through technical means[93] and by perpetrating the attacks through non–state actors with ambiguous relationships to state agencies.[94] As Thomas Franck has observed, "[l]ying about facts . . . is the tribute scofflaw governments pay to international legal obligations they violate."[95] 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.[96] 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,[97] which applies only when "the territorial integrity, political independence or security of any of the Parties is threatened."[98] 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.[99] 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

Article 2(4)'s blanket prohibition on the nonconsensual 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

93. *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., Fall 2009, at 1, 74–75.

94. *See, e.g.*, CARR, *supra* note 30, 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 associations, and the Foundation for Effective Policy.").

95. Thomas M. Franck, *Legitimacy After Kosovo and Iraq*, *in* INTERNATIONAL LAW AND THE USE OF FORCE AT THE TURN OF CENTURIES: ESSAYS IN HONOUR OF V.D. DEGAN 69, 73 (Vesna Crnić-Grotić & Miomir Matulović eds., 2005).

96. *See, e.g.*, Ian Traynor, *Russia Accused of Unleashing Cyberwar to Disable Estonia*, GUARDIAN (May 16, 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).

97. *NATO Agrees Common Approach to Cyber Defence*, EURACTIV.COM (Apr. 4, 2008), http://www.euractiv.com/en/infosociety/nato-agrees-common-approach-cyber-defence/article-171377.

98. North Atlantic Treaty, art. 4, Apr. 4, 1949, 63 Stat. 2241, 34 U.N.T.S. 243.

99. As noted below, however, NATO does not believe that cyber-attacks rise to the level of armed attacks justifying self defense. *See NATO Agrees Common Approach to Cyber Defence*, *supra* note 97; *infra* Part II.A.2.

recommendations, or decide what measures shall be taken . . . to maintain or restore international peace and security."[100] The Security Council may employ "measures not involving the use of armed force"[101] and authorize "action by air, sea, or land forces."[102] Collective security operations under Article 39 can be politically difficult, however, because they require authorization by the often deadlocked or slow-moving Security Council.

The second exception to Article 2(4) is codified 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."[103] Lawful self-defense can be harder to define and identify than lawful collective security operations. Indeed, in many 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.[104] It is clear, however, that the critical question determining the lawfulness of self-defense is whether or not an armed attack has occurred. A cyber-attack must rise to the level of an armed attack for a state to respond lawfully under Article 51.[105]

The term "armed attack" is linguistically distinct from several other related terms in the U.N. Charter and has been interpreted to be substantively narrower than them.[106] 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 hence 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 incident[s]" rather than "armed attacks."[107] Instead, to qualify as armed attacks sufficient to justify a

100. U.N. Charter art. 39.

101. *Id.* art. 41.

102. *Id.* art. 42.

103. *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. WHITE HOUSE CYBERSPACE STRATEGY, *supra* note 63, at 10.

104. CHRISTINE GRAY, INTERNATIONAL LAW AND THE USE OF FORCE 95–96 (2d ed. 2004).

105. *See, e.g.*, WHITE HOUSE CYBERSPACE STRATEGY, *supra* note 63, 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.").

106. *See* Yoram Dinstein, *Computer Network Attacks and Self-Defense*, *in* COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW 99, 100–01 (Michael N. Schmitt & Brian T. O'Donnell eds., 2002).

107. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, ¶ 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) [hereinafter Definition of Aggression] (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

response under Article 51, attacks must constitute "most grave forms of the use of force."[108] Where they may not resort to defensive force under Article 51 (because an attack does not rise to the level of an "armed attack"), states may be permitted to respond with retorsions or nonforceful countermeasures within carefully proscribed legal limits.[109] As described in more detail in Part III.A, such countermeasures might include responses in cyberspace.[110]

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 attack that triggers the right of armed self-defense: the instrument-based approach, the target-based approach, and our preferred approach: the effects-based approach.[111]

One scholar has given the moniker "instrument-based" to the classical approach to the armed attack inquiry.[112] 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.[113] This approach treats a cyber-attack as an armed

---

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 106, at 99, 100–01.

108. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, ¶ 191 (June 27).

109. 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, Rep. of the Int'l Law Comm'n, U.N. GAOR, 53d Sess., Supp. No. 10, U.N. Doc. A/56/10 (2001), at 31, 80 [hereinafter Draft Articles]. *See infra* Part III.A for a more detailed discussion of countermeasures.

110. *See* OFFICE OF GEN. COUNSEL, DEP'T OF DEF., AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS (1999), *reprinted in* COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW 459, 484–85 [hereinafter DOD MEMO] (Michael N. Schmitt & Brian T. O'Donnell eds., 2002) ("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.").

111. 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 237, 238–39 (2010) ("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.").

112. 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 10, at 1041.

113. Hollis, *supra* note 10, at 1041.

attack only if it uses military weapons. Bombing computer servers or Internet cables could meet the requirements of an armed attack, for example, 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 "complete or partial interruption of . . . telegraphic, radio, and other means of communication" as a "measure[] not involving the use of armed force."[114] 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.[115] 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 constitute an armed attack that obligates member states to assist one another under Article 5 of the treaty.[116]

The chief advantage of the instrument-based approach 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.[117] The primary aim of this approach is to determine when a cyber-attack portends imminent harm sufficient to justify the use of anticipatory self-defense in response.[118]

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

114. U.N. Charter art. 41.

115. *See* Definition of Aggression, *supra* note 107, art. 3.

116. North Atlantic Treaty, *supra* note 98, arts. 4, 5, 63; *NATO Agrees Common Approach to Cyber Defence*, *supra* note 97.

117. 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 92, 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 Jensen, *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).

118. Hollis, *supra* note 10, at 1041 n.73.

destructive conventional armed conflicts.[119] 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 undermine 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 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.[120] 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 best-known 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.[121] These factors are illuminating, but they call for such a wide-ranging

119. *See* Sklerov, *supra* note 93, at 56 n.352 (criticizing the target-based approach for encouraging escalation and advocating an effects-based approach).

120. 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 23, at 19.

121. Schmitt, *supra* note 112, at 914–15; *see also* Sean P. Kanuck, *Recent Development: Information Warfare: New Challenges for Public International Law*, 37 HARV. INT'L L.J. 272, 290 (1996) ("Each suspect activity could be reviewed for its effects on other states, and sanctioned accordingly.").

inquiry that they may not provide sufficient guidance to decision makers.[122] 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 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."[123] Under this test, a cyber-attack on the air traffic control system causing planes to crash would be regarded as an armed attack because it is foreseeable that such an attack would cause loss of life and substantial property damage. But a cyber-attack on a website or mere penetration of a critical computer system generally would not, unless it caused physical injury or property damage. A cyber-attack on financial systems presents a harder case for this approach—the analysis would depend on whether the attack was found to have caused substantial damage to property.

It is important to note that the purpose of the attack is already accounted for in the definition of cyber-attack recommended herein: the attack must have been committed for a political or national security purpose. Therefore a cyber-attack that has unforeseen national security consequences would not be considered a cyber-attack, much less cyber-warfare.

This final 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.[124] It also focuses the armed attack analysis on a limited set of criteria—particularly severity and foreseeability.[125]

122. *See* Silver, *supra* note 90, 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 policy makers will be able to engage in a thorough factual inquiry when responding to cyber-attacks).

123. Silver, *supra* note 90, at 90–91.

124. *See id.* at 92.

125. The Department of Defense has signaled its approval of this approach. *See* DOD MEMO, *supra* note 110, 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).

3. Ad Bellum *Necessity and Proportionality*

A state's use of armed force in response to a cyber-attack must not only conform with U.N. Charter and customary international law limits on the use of armed force, but it 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 settlement, cannot achieve the state's overall aim.[126] 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.[127] The United States has acknowledged that these principles apply to military responses to cyber-attacks.[128]

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.

Applying the existing *jus ad bellum* framework in the context of cyber-attacks is challenging. Moreover, the framework only applies to the small subset of cyber-attacks that are addressed by Security Council resolutions or that constitute an armed attack, giving rise to a right of self-defense under Article 51. As a result, only a small number of cyber-attacks are properly considered "cyber-warfare," to which the laws of war apply. 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 legal framework governing cyber-attacks during an ongoing armed conflict.

---

126. *See, e.g.*, 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 . . . .").

127. *See* 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.").

128. *See* WHITE HOUSE CYBERSPACE STRATEGY, *supra* note 63, at 14 ("[W]e will exhaust all options before military force whenever we can; will carefully weigh 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.").

B. Jus in Bello

Although a stand-alone cyber-attack has never instigated an armed conflict, cyber-attacks have been used in wars in response to traditional provocations or to prepare the way for an imminent conventional attack. This Section examines the relationship between traditional *jus in bello* requirements and cyber-attacks employed in the course of conventional armed conflicts. The novel conditions of cyberspace can pose challenges to applying *jus in bello* principles of necessity, 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 difficult 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. We briefly address each challenge in turn.

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-attacks. *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.[129] 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."[130] To

129. In contrast, the *ad bellum* necessity analysis helps determine if nonforcible measures to abate a threat are inadequate, excusing an otherwise unlawful use of force.

130. 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 article 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 information warfare "practically nullifies 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

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.[131]

Due to the nature of harm they inflict, the proportionality of cyber-attacks poses unique challenges. It can be 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 nonlethal or temporary, yet severe.[132] In particular, how should the temporary incapacity of critical systems be evaluated?[133] A cyber-attack that effectively stops the transmission of information through the Internet might merely inconvenience the populace, but it might also have more severe consequences. For example, it might cause hospitals to be unable to communicate vital information, leading to loss of life. An ex ante *in bello* proportionality analysis for a DDOS attack may therefore carry a much greater degree of uncertainty than would a conventional attack. An *in bello* proportionality analysis requires anticipating the probable consequences of an action, but additional uncertainty will make that analysis much more difficult in the cyber context. As a result, cyber-attacks may change the weight given to temporary consequences, and may force states to confront more uncertainty than they typically face in making decisions about the legality of planned attacks.

3. Distinction

The principle of distinction—which requires states to distinguish civilian and military personnel and restrict attacks to military objectives[134]—presents

L. 517, 535 (2007) (arguing that the United States might be held to heightened standard of care due to advances in military technology).

131. Protocol Additional I, *supra* note 130, 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).

132. Protocol Additional I, *supra* note 130, art. 57(2)(a)(iii).

133. Similar questions arise in debates around nonlethal 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).

134. Louise Doswald-Beck, *Some Thoughts on Computer Network Attack and the International Law of Armed Conflict*, *in* COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW 163, 166 (Michael N. Schmitt & Brian T. O'Donnell eds., 2002). 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 84, at 438–39. States also have a duty to facilitate distinction: "The application of this duty requires that personnel and

another legal challenge.[135] Under this principle, military commanders must employ weapons that can target accurately and must use this capability to distinguish between civilian and military objectives.[136] By extension, the law of war prohibits *in bello* cyber-attacks that are uncontrollable, unpredictable, or do not discriminate between civilian and military objectives.[137] Furthermore, Additional Protocol I prohibits attacks that deny the civilian population indispensable objects, such as food or water supplies.[138]

There are situations where the principle of distinction is easily applied to cyber-attacks. For example, a cyber-attack that targets a military air traffic control system and only causes a troop transport to crash would comply with the principle of distinction.[139] Other cyber-attacks would clearly violate the principle of distinction—for example, an attack on the civilian banking sector or on hospitals, museums, or places of worship.[140] Cyber-attacks against the networks that manage these targets, like any other attack on these objects, would be unlawful.[141]

Such cases are easy, but cyberspace offers many much more difficult ones. 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,[142] so it is possible that civilian networks could be attractive military targets.[143] Because much of cyberspace is dual use—used by both the

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 86, at 192.

135. *See* DELIBASIS, *supra* note 130, at 274 (arguing that information warfare will likely run afoul of distinction and proportionality); Kelsey, *supra* note 73, at 1431 (arguing that cyber-attacks will often violate the principles of distinction and neutrality).

136. *See* Jensen, *supra* note 84, 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, ¶ 78 (Jul. 8).

137. 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 130, art. 52(2). For example, the first missile strikes of Operation Desert Storm in 1991 targeted Iraqi radar stations. Kanuck, *supra* note 121, at 282. On distinction, *see* Doswald-Beck, *supra* note 134, at 165–71; Brown, *supra* note 86, 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 84, at 201 (citing Protocol Additional I, *supra* note 130, art. 51(4)).

138. Protocol Additional I, *supra* note 130, art. 54(2).

139. Schmitt, *supra* note 84, at 196 ("Military equipment and facilities . . . are clearly military objectives.").

140. *See, e.g.*, Protocol Additional I, *supra* note 130, art. 85(4)(d).

141. Schmitt, *supra* note 84, at 200; Brown, *supra* note 86, at 199.

142. Antolin-Jenkins, *supra* note 11, at 133.

143. 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-

military and civilians—upholding the distinction requirement in cyberspace can be more challenging than it is in a conventional context.

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

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 "take a direct part in hostilities."[144] Furthermore, under customary international law affirmed by the International Committee of the Red Cross, civilians who adopt a continuous combat function may also be targeted.[145] These rules are familiar in the post-9/11 context. Yet the unique characteristics of civilian contributions to and participation in cyber-attacks threaten to blur the line between direct participation, continuous combat function, and other types of involvement in the execution of hostilities.[146]

The civilian designer of a weapons system has traditionally not been treated as a direct participant in hostilities. However, the programmer who works with military intelligence may tweak the code to enable the attack, right up until the moment of the attack.[147] The actions of such a civilian—particularly of a civilian who regularly engages in such activity—could be considered a "continuous function [that] involves the preparation, execution, or command of acts or operations amounting to direct participation in hostilities."[148] As a result, civilians involved in cyber-attacks might be regarded as performing tasks that alter their status under the law of war, rendering them lawful targets of a counterattack.[149]

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

attacks. Eric Talbot Jensen, *Cyber Warfare and Precautions Against the Effects of Attacks*, 88 TEX. L. REV. 1533 (2010).

144. Protocol Additional I, *supra* note 130, art. 51(3).

145. INT'L COMM. OF THE RED CROSS, INTERPRETIVE GUIDANCE ON THE NOTION OF DIRECT PARTICIPATION IN HOSTILITIES UNDER INTERNATIONAL HUMANITARIAN LAW 16 (2009), *available at* http://www.icrc.org/eng/assets/files/other/icrc_002_0990.pdf [hereinafter ICRC, INTERPRETIVE GUIDANCE].

146. *See id.* at 37 (noting the challenge that private contractors and civilian employees pose to the definition of direct participation due to "geographic and organizational closeness").

147. Watts, *supra* note 84, at 429.

148. ICRC, INTERPRETIVE GUIDANCE, *supra* note 145, at 34.

149. 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 SEC. 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.

forces.[150] A state that sponsors use of force by civilians may be placing those civilians outside the protections they enjoy under the law of armed conflict, and may be undermining the principle of distinction between combatants and civilians.[151]

Despite the legal consequences, there are many reasons to think states will be tempted to use civilians in the cyber context. First, civilians may possess technical expertise that governments do not. Second, by using civilians to carry out cyber-attacks, states can mask their own involvement in such operations.[152] For example, Nashi—a pro-Kremlin youth group started by Vladimir Putin—has taken responsibility for the 2007 cyber-attacks against Estonia.[153] It has been alleged that Russian business owners fund Nashi to carry out cyber-attacks favored by the Russian government. The business owners "ingratiate themselves with the regime," and the Russian government may plausibly deny involvement in the attack.[154]

A former Special Assistant for Law of War Matters of the Judge Advocate General, Lieutenant Colonel Geoffrey S. Corn, argues that the current direct participation test is outdated.[155] 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."[156] Operating within a command relationship is the dispositive criterion for combatant status "because members of the armed forces are subject to responsible command, and they operate within a military hierarchy

150. Watts, *supra* note 84, at 420.

151. *See* DELIBASIS, *supra* note 130, 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 document explains that National Guard members may train for, but not carry out, cyber-attacks. *See* U.S. AIR FORCE, CYBERSPACE OPERATIONS: AIR FORCE DOCTRINE DOCUMENT 3-12, at 29 (2010), *available at* http://www.fas.org/irp/doddir/usaf/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 SERV. (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 32, at 10–11.

152. States that do so may not only deny those civilians the protections due to civilians under the laws of war, but may also be guilty of perfidy themselves. *See* Protocol Additional I, *supra* note 130, art. 37.

153. *See* Hollis, *supra* note 10, at 1024–25 (describing the attacks against Estonia); Shachtman, *supra* note 57.

154. Shachtman, *supra* note 57.

155. *Cf. supra* note 146 and accompanying text.

156. Corn, *supra* note 149, 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.

involving training, discipline, and unitary loyalty."[157] Corn argues that only individuals subject to command authority should be able to exercise discretion that could result in a law of armed conflict violation, because the actions of those individuals are within a command and discipline structure that can prevent and punish violations.[158] Under this reasoning, states may not employ civilian contractors to carry out activities where they will exercise discretion that implicates the law of armed conflict.

4. Neutrality

A final challenge in evaluating the legality of an *in bello* cyber-attack is the fact that a cyber-attack may appear to originate, or may actually originate, from a neutral state.[159] A state may be neutral, either permanently, such as Switzerland, or for the duration of a specific conflict.[160] The principle of neutrality includes both rights and responsibilities: "The 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."[161]

Scholars hold differing views regarding neutral states' obligations to guard against the use of their facilities by belligerents. Some argue that neutral states are not obligated to stop belligerents from using their communications facilities, but they may not help belligerents build such facilities.[162] Others argue that neutral states that are unable or unwilling to stop an unlawful attack originating from their territory, including their information systems, may lawfully be targeted for the purpose of stopping the unlawful attack.[163] They claim that states have an obligation not only to refrain from committing cyber-attacks themselves, but also "not to allow knowingly [their] territory to be used for acts contrary to the rights of other States."[164]

157. Corn, *supra* note 149, at 287; *see also* Brown, *supra* note 86, 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).

158. Corn, *supra* note 149, at 261.

159. *See* BRENNER, *supra* note 157, at 131–32 (noting the difficulty of identifying attackers in the cyber-threat context); *see also* Brown, *supra* note 86, at 208 (on rights and responsibilities of neutrality).

160. *See* George K. Walker, *Information Warfare and Neutrality*, 33 VAND. J. TRANSNAT'L L. 1079, 1141–42 (2000) (discussing neutrality and information warfare).

161. COMMANDER'S HANDBOOK, *supra* note 84, ¶ 7.2 (noting also that "[t]his customary law has, to some extent, been modified by the Charter of the United Nations").

162. *See* Doswald-Beck, *supra* note 134, at 176.

163. *See* DELIBASIS, *supra* note 130, at 284; COMMANDER'S HANDBOOK, *supra* note 84, ¶ 7.3.

164. Corfu Channel Case (U.K. v. Albania) (Merits), 1949 I.C.J. 4, 22 (Apr. 9). *See, e.g.*, Sklerov, *supra* note 93, at 43.

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.[165] Such cyber-attacks pose challenges to analysis under 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, the principle of neutrality determines lawful responses to attacks based on the identity of the origin country. Consequently, the inability to attribute attacks to a certain state impedes the neutrality analysis.[166] However, it is also possible that 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 possibility remains that a country may not know attacks are emanating from its borders.

The existing law of war framework—both *jus ad bellum* and *jus in bello*—provides some guidance, albeit incomplete and imperfect, for states seeking to determine the scope of permissible offensive and defensive cyber-attacks. But it does not regulate the vast majority of cyber-attacks. Most cyber-attacks do not rise to the level of an armed attack or take place in the context of an armed conflict. Consequently, they do not implicate the law of war. Yet this does not necessarily mean that these cyber-attacks are unregulated. As the next Part shows, 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 with what is potentially the most important such framework—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.

165. Goldsmith, *supra* note 54, at 10–12.

166. Shanker & Bumiller, *supra* note 53 ("Officials say the main challenge for the United States in a retaliatory cyberoperation is determining the attacker.").

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. 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."[167]

The international law of countermeasures does not define when a cyber-attack is unlawful. Indeed, the Draft Articles do not directly address cyber-attacks at all. The law simply provides that when a state commits an international law violation, an injured state may respond with a countermeasure.[168] 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.[169] These violations of international law 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.[170] 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.[171] Accordingly, countermeasures cannot

167. Draft Articles, *supra* note 109, at 128. 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.*

168. 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.* at 130.

169. *See supra* Part II.A.1.

170. 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.

171. Draft Articles, *supra* note 109, at 129. 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 states. For

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.[172]

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.[173] However, in some situations, the injured state "may take such urgent countermeasures as are necessary to preserve its rights."[174] 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.[175]

Under the customary law of countermeasures, an attacking state that violates its obligation not to intervene in another sovereign state through a harmful cyber-attack may be subject to lawful countermeasures by the injured state. Such countermeasures might go beyond "passive defenses" that aim to repel cyber-attacks (such as firewalls), and constitute "active defenses," which attempt to disable the source of an attack.[176] Active defenses—if properly designed to meet the requirements of necessity and proportionality—might be considered a form of "reciprocal countermeasures," in which the injured state ceases obeying the same or a related obligation to the one the responsible state violated (in this case, the obligation of nonintervention).

Before a state may use active defense 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 restrictions.[177] The countermeasures must be designed, for example, to induce the wrongdoing state to comply with its obligations. The Draft Articles also have detailed provisions regarding when acts committed by non–state agents may be

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 Case (U.K. v. Albania) (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 93, at 62–72.

172. Draft Articles, *supra* note 109, at 131.

173. *Id.* at 135.

174. *Id.*

175. *Id.* at 129.

176. 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 32, at 7.

177. Draft Articles, *supra* note 109, at 129–34.

attributed to a state—for instance, when the state aids and assists the act with knowledge of the circumstances.[178]

While countermeasures provide states with a valuable tool for addressing cyber-attacks that do not rise to the level of an armed attack, countermeasures are far from a panacea. 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 targeted actor must find the countermeasure costly—ideally costly enough to cease its unlawful behavior. If the target can easily relocate its operations, as is often possible in the cyber context, 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, it can be difficult to design a countermeasure that injures only the actor that perpetuated the legally wrongful attack. In particular, a countermeasure that disables a computer or network may very well cause harm to those who have little or nothing to do with the unlawful attacks. This could have the perverse effect of making the state injured by the original attack a perpetrator of an unlawful attack against those who simply happen to share a network with the actor that generated the original attack, or whose computers were used as pawns without its knowledge or acquiescence. Together, these challenges can lead a system that relies too heavily on active countermeasures to spin out of control. As a result, 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.

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 thus far fallen short of establishing a rigorous legal framework that can effectively govern all cyber-attacks.

178. *Id.* at 65.

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.[179] These resolutions, however, are vague and have not required any specific action by U.N. members.[180]

In August 1999, the United Nations sponsored an international meeting of experts in Geneva to better grasp the security implications of emerging information technologies.[181] A follow-up General Assembly resolution in 2002 called for further consideration and discussion of "information security."[182] The resolution also called for a new study of international informational security issues,[183] but little action resulted.[184] The United Nations sponsored a two-phase summit in 2003 and 2005 called the World Summit on the Information Society, but again with little concrete result.[185]

The United Nations did take a step forward in July 2010, when government cyber-security specialists from fifteen countries—including major

179. 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).

180. 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).

181. G.A. Res. 54/49, at 2, U.N. Doc. A/RES/54/49 (Dec. 23, 1999).

182. *Id.* ¶ 1. 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] . . . [i]nvite[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. ¶¶ 1-3.

183. *Id.* ¶ 4.

184. Similar exhortations appear in subsequent resolutions. *See* G.A. Res. 58/32, *supra* note 179, ¶ 4; G.A. Res. 59/61, *supra* note 179, ¶ 4; G.A. Res. 60/45, *supra* note 179, ¶ 4; G.A. Res. 61/54, *supra* note 179, ¶ 4; G.A. Res. 62/17, *supra* note 179, ¶ 4; G.A. Res. 63/37, *supra* note 179, ¶ 4; G.A. Res. 64/25, *supra* note 179, ¶ 4.

185. *See* WORLD SUMMIT ON THE INFORMATION SOCIETY: GENEVA 2003–TUNIS 2005, http://www.itu.int/wsis/index.html (last visited Apr. 21, 2012) (compiling conference documents and follow-up documents, including annual "outcome documents"); G.A. Res. 60/252, ¶ 11, U.N. Doc. A/RES/60/252 (Apr. 27, 2006) ("*Urges* Member States, relevant United Nations bodies and other intergovernmental organizations, as well as non-governmental organizations, civil society and the private sector, to contribute actively, inter alia by initiating actions, where appropriate, to the implementation and follow-up of the outcomes of the Geneva and Tunis phases of the Summit.").

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."[186] 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;
v. Finding possibilities to elaborate common terms and definitions . . . .[187]

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.[188] 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.[189] At present, however, the role of the United Nations with respect to cyber-security remains largely limited to discussions and information 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."[190] On the heels of that attack,[191] NATO held its first meeting—the 2008 Bucharest

186. U.N. Secretary-General, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, 4, U.N. Doc. A/65/201 (July 30, 2010).

187. *Id.* at 8.

188. Historically Russia and the United States have expressed conflicting views on cyber-security as it relates to sovereignty and political dissent as well as international cooperation. *See, e.g.*, TIM MAURER, CYBER NORM EMERGENCE AT THE UNITED NATIONS: AN ANALYSIS OF THE ACTIVITIES AT THE UN REGARDING CYBER-SECURITY 1, 17, 25, 27, 47 (2011) (describing the contrasting views of the two countries).

189. John Markoff, *Step Taken to End Impasse over Cybersecurity Talks*, N.Y. TIMES, July 17, 2010, at A7.

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

191. This followed an October 2007 meeting of NATO defense ministers during 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.

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.[192]

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.[193]

The Cooperative Cyber Defence Centre of Excellence aspires to "advance the development of long-term NATO cyber defence doctrine and strategy."[194] The North Atlantic Council, however, retains control of NATO cyber-policy and defense.[195] Despite strong pressure from Eastern European countries, cyber-attacks are still considered to activate only 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.[196]

Although NATO's creation of these two divisions signifies 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.'"[197] NATO's cyber-plans and capabilities are still nascent.

3. Council of Europe

The Council of Europe[198] has taken the most direct and concrete 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

192. Hughes, *supra* note 190. 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 Three Years Later: A Progress Report on Combating Cyber Attacks*, J. INTERNET L., Feb. 2010, at 22.

193. Hughes, *supra* note 190.

194. *Id.*

195. *Defending The Networks: The NATO Policy on Cyber Defence*, N. ATL. TREATY ORG. (2011), http://www.nato.int/nato_static/assets/pdf/pdf_2011_09/20111004_110914-policy-cyberdefence.pdf ("The NATO Policy on Cyber Defence reiterates that any collective defence response is subject to decisions of the North Atlantic Council.").

196. North Atlantic Treaty, *supra* note 98, arts. 4, 5; *see also NATO Agrees Common Approach to Cyber Defence*, *supra* note 97 ("The competencies of the [Cyber Defence Management Authority] will fall exclusively on Article 4 of the North Atlantic Treaty.").

197. Hughes, *supra* note 190.

198. Founded in 1949, the Council of Europe aims to promote cooperation amongst its forty-seven European member states.

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.[199] The United States ratified the Convention in 2006.[200]

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.[201] These rules, however, do not appear to apply to government actions, whether taken for law enforcement or national security purposes.[202] 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*."[203] 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."[204] This suggests, as Duncan Hollis and others have argued, that the Convention negotiators were aware of state interests in using cyber-attacks and sought to draft the agreement to permit such governmental action.[205]

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

199. Cybercrime Convention, *supra* note 64, pmbl.; *see also* Rasha AlMahroos, *Phishing for the Answer: Recent Developments in Combating Phishing*, 3 I/S: J. L. & POL'Y FOR INFO. SOC'Y 595, 613 (2008) ("The Council of Europe's Convention on Cybercrime . . . is the first and only international treaty that deals explicitly with cybercrime.").

200. The convention allows members of the Council of Europe and other states that participated in its elaboration (among them the United States) to join the Convention. Cybercrime Convention, *supra* note 66, at ch. IV; Declan McCullagh & Anne Broache, *Senate Ratifies Controversial Cybercrime Treaty*, CNET, (Aug. 4, 2006, 11:25 AM), http://news.cnet.com/Senate-ratifies-controversial-cybercrime-treaty/2100-7348_3-6102354.html. As of January 2012, thirty countries have ratified the Convention on Cybercrime, and another sixteen have signed but have not yet ratified it (including Australia, Japan, and South Africa). *Convention on Cybercrime*, TREATY OFFICE, COUNCIL OF EUROPE, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=28/10/2010&CL=ENG (last visited Apr. 21, 2012).

201. Cybercrime Convention, *supra* note 66, arts. 2, 4, 5.

202. *See* Arie J. Schaap, *Cyber Warfare Operations: Development and Use Under International Law*, 64 A.F. L. REV. 121, 171 (2009) ("However, [the Cybercrime Convention's] rules do not apply to government activities, whether for law enforcement or national security purposes."); Hollis, *supra* note 10, at 1052 ("[The Cybercrime Convention's] rules, however, do not apply to government activities, whether for law enforcement or national security purposes.").

203. Cybercrime Convention, *supra* note 66, art. 2 (emphasis added).

204. Council of Eur., *Convention on Cybercrime: Explanatory Report*, 109th Sess., ¶ 38 (Nov. 8, 2001), *available at* http://conventions.coe.int/Treaty/en/Reports/Html/185.htm.

205. Hollis, *supra* note 10.

concerning criminal offences related to computer systems and data."[206] 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—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 designing a comprehensive international framework for regulating unlawful cyber-attacks.

4. Organization of American States

The Organization of American States ("OAS"), representing thirty-five states from the Americas,[207] only recently began taking preliminary 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."[208] The OAS also adopted a "Comprehensive Inter-American Cybersecurity Strategy," which aims, among other things, to adopt "cybercrime 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."[209] 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 cybercrime, protect information systems, and prevent the use of computers to facilitate illegal activity."[210] 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

206. Cybercrime Convention, *supra* note 66, art. 23.

207. The OAS aims for its member states to achieve "an order of peace and justice, to promote their solidarity, to strengthen their collaboration, and to defend their sovereignty, their territorial integrity, and their independence." Charter of the Organization of American States art. 1, *available at* http://www.oas.org/dil/treaties_A-41_Charter_of_the_Organization_of_American_States.htm.

208. Organization of American States, AG/RES. 2040 (XXXIV-O/04), at ch. IV, ¶ 8 (June 8, 2004), *available at* http://www.oas.org/juridico/english/ga04/agres_2040.htm.

209. Organization of American States, AG/RES. 2004 (XXXIV-O/04), at app. A, (June 8, 2004), *available at* http://www.oas.org/XXXIVGA/english/docs/approved_documents/adoption_strategy_combat_threats_cybersecurity.htm.

210. *Id.*

criminalizing cyber-crime and enabling international cooperation to investigate and prosecute such crimes.[211] The Working Group pledged to review the progress made in implementing these measures at its next meeting.[212] The OAS has thus begun a useful regional conversation on joint strategies for battling the portion of cyber-attacks that constitute cyber-crime, but it has not yet developed a more active program for addressing cyber-attacks more generally.

5. Shanghai Cooperation Organization

The Shanghai Cooperation Organization, an intergovernmental mutual security organization founded in 2001 by China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan,[213] has taken significant preliminary steps toward cooperation in the cyber-security area. In its Yekaterinburg Declaration of June 16, 2009, "[t]he 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."[214] The Organization presents a possible center of gravity in international legal action on cyber-attacks. As explained above,[215] the Organization has thus far adopted an expansive understanding of cyber-attacks that includes 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 Western Europe and the United States, which have sought to avoid regulations of cyber-activities that may interfere with the expression of political dissent.[216]

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 existing legal picture by outlining the

211. Organization of American States, Sixth Meeting of the Working Group on Cyber-Crime, Recommendations, Jan. 21–22, 2010, OEA/Ser.K/XXXIV, CIBER-VI/doc.4/10 rev. 1, ¶¶ 1–2, *available at* http://www.oas.org/juridico/english/cyb_VIrec_en.pdf.

212. *Id.* ¶ 17.

213. These six countries are the only members of the SCO, though others are able to participate as observer states, dialogue partners, and guest attendees. More information on the SCO can be found here: http://www.fmprc.gov.cn/eng/topics/sco/t57970.htm.

214. CONSULATE GEN. OF UZB. IN N.Y.C., YEKATERINBURG DECLARATION OF THE HEADS OF THE MEMBER STATES OF THE SHANGHAI COOPERATION ORGANISATION, (July 9, 2009), http://www.uzbekconsulny.org/news/572/.

215. *See supra* text accompanying notes 24–27.

216. MAURER, *supra* note 188.

international regimes that indirectly regulate cyber-attacks as well as 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.[217] 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" frameworks can be used to address a cyber-attack only if the attack employs the particular means regulated by the agreement.[218] Hence the international regimes that indirectly regulate cyber-attacks provide a patchwork of laws that are likely to apply to only a small portion of harmful cyber-attacks.

1. 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

217. While a number of countries have recognized Internet access as a human right, we do not discuss it here, due to its diffuse and currently unenforceable status. *See, e.g.*, David Meyer, *European 'Internet Freedom' Law Agreed*, ZDNET (Nov. 5, 2009, 1:11 PM), http://www.zdnet.co.uk/news/networking/2009/11/05/european-internet-freedom-law-agreed-39860587/. It therefore would not offer an alternate governing legal framework for cyber-attack with any practical significance. Moreover, the right to access the Internet does not implicate one of the key elements of our proposed cyber-attack definition: a national security or political purpose.

218. *See* Richard W. Aldrich, *The International Legal Implications of Information Warfare*, AIRPOWER J., Fall 1996, at 99, 109, *available* at http://www.au.af.mil/au/awc/awcgate/au/aldrich.pdf ("[M]ost of the law to which legal scholars are looking for guidance was developed, in many cases, decades before information warfare concepts were envisioned."); Barkham, *supra* note 122, at 95–96 (discussing existing treaty regimes that could be used to regulate information warfare); Dimitrios Delibasis, *State Use of Force in Cyberspace for Self-Defence: A New Challenge for a New Century*, PEACE, CONFLICT & DEV.: AN INTERDISC. J., Feb. 2006, at 1; BRYAN W. ELLIS, THE INTERNATIONAL LEGAL IMPLICATIONS AND LIMITATIONS OF INFORMATION WARFARE: WHAT ARE OUR OPTIONS? 3–4 (Apr. 10, 2001) (USAWC Strategy Research Project) (explaining how a network attack may implicate existing international telecommunications law); Schaap, *supra* note 202, at 160–70 (discussing other treaties and conventions that could impact cyber warfare operations, including the International Outer Space Law, International Telecommunications Law, and International Aviation Law); Scott J. Shackelford, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, 27 BERKELEY J. INT'L L. 191, 250–51 (2009) ("To the extent that cyber attacks are below the threshold of an armed attack, provisions of space law, nuclear non-proliferation, UNCLOS, and communications law, all have a role to play in crafting a functioning legal regime."); David Willson, *A Global Problem: Cyberspace Threats Demand an International Approach*, ISSA J., Aug. 2009, at 12, *available* at http://www.issa.org/Library/Journals/2009/August/Willson-A%20Global%20Problem.pdf; William Yurcik, *Information Warfare: Legal & Ethical Challenges of the Next Global Battleground*, *in* PROCEEDINGS OF THE SECOND ANNUAL ETHICS AND TECHNOLOGY CONFERENCE 1 (1997).

multinational standards for information and communication technology.[219] The Union's stated aim is "the preservation of peace and the economic and social development of all States . . . by means of efficient telecommunications services."[220] The International 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 nonbinding Telecommunications Standards.[221] The Union 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.[222]

International Telecommunication regulations may be used to address 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.[223] Member states may cut off any nonstate private telecommunications that "may appear dangerous to the security of the State or contrary to its laws, to public order or to decency"[224] 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."[225] Member states also must regulate against "harmful interference"[226] that "endangers the functioning of a radionavigation service or of other safety services or seriously degrades, obstructs or repeatedly interrupts a radiocommunication service"[227] and pursue all possible measures to ensure the secrecy of international correspondence,

219. 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 ITU 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 193 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 Apr. 21, 2012). 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 Apr. 21, 2012).

220. Constitution of the International Telecommunications Union, pmbl., Dec. 22, 1992, *available at* http://itu.int/net/about/basic-texts/index.aspx [hereinafter ITU Constitution]; *see also* International Telecommunications Convention, Nov. 6, 1982, U.N. Doc. 26559.

221. KENNEDY & PASTOR, *supra* note 219, at 33.

222. 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 Apr. 21, 2012); *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 Apr. 21, 2012).

223. ITU Constitution, *supra* note 220, art. 45.

224. *Id.* art. 34.

225. *Id.* art. 35.

226. *Id.* art. 6.

227. *Id.* annex. (definition of "harmful interference").

unless such secrecy would contravene their domestic laws or international conventions.[228]

Despite the above restrictions, international telecommunications law does not specifically prohibit the use of telecommunications for military purposes, such as cyber-attacks. Article 48 states that "Member States retain their entire freedom with regard to military radio installations."[229] The article requests that states limit such use: "Nevertheless, these installations must, so far as possible, observe . . . the measures to be taken to prevent harmful interference."[230] 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 possesses little enforcement or punitive capacity.[231]

2. Aviation Law

Cyber-attack operations that target or interfere with nonmilitary aviation could implicate three major aviation regulations: the 1944 Chicago Convention on International Civil Aviation (Chicago Convention),[232] the 1971 Montreal Convention for the Suppression of Unlawful Acts Against Civil Aviation

228. *Id.* art. 37.

229. *Id.* art. 48(1).

230. *Id.* art. 48(2).

231. The International Telecommunication Union's main "regulatory" body originally was the International Frequency Registration 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*,*'* INT'L TELECOMM. UNION (Mar. 1, 2010), http://www.itu.int/ITU-R/information/promotion/e-flash/4/article7.html (last visited Apr. 21, 2012). 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 noncompliance and sometimes conflicting interests of member states. *Id.* Even the Board, however, does not have full regulatory authority, since it can only issue recommendations when cases of "harmful interference" arise. *The International Telecommunication Union (ITU): Structure*, ENCYCLOPEDIA OF THE NATIONS, http://www.nationsencyclopedia.com/United-Nations-Related-Agencies/The-International-Telecommunication-Union-ITU-STRUCTURE.html#b (last visited Apr. 21, 2012). 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.").

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

(Montreal Convention),[233] and the 1988 Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation (Montreal Protocol).[234] 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.[235]

The 1944 Chicago Convention created a specialized U.N. agency tasked with coordinating and regulating international air travel.[236] It also established a set of rules on airspace, aircraft, navigation, registration, and safety.[237] The Convention stipulates that all states must show "due regard for the safety of navigation of civil aircraft."[238] Cyber-attack operations that target civilian flights, if launched by a government against another actor, could run counter to this Convention's 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.[239] However, the Convention does allow a member state to derogate from the Convention's obligations during war or state emergencies,[240] so long as the state "notifies the fact to the Council."[241]

The Montreal Convention outlines as unlawful specific conduct that could jeopardize the safety of civil aviation.[242] 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."[243] This agreement would not seem to restrict any cyber-attack operations unless it rendered an 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).

---

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

234. 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].

235. Schaap, *supra* note 202, at 166.

236. Chicago Convention, *supra* note 232, arts. 43, 44. The agency is called the International Civil Aviation Organization. *Id.*

237. *Id.* pt. I.

238. *Id.* art. 3(d).

239. 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.

240. Chicago Convention, *supra* note 232, art. 89.

241. *Id.*

242. Montreal Convention, *supra* note 233.

243. *Id.* art. 1.

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."[244] 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.[245]

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.

3. Law of Space

Given that computer-operated satellites are integral to international telecommunications and military operations, cyber-attacks could implicate space law. 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.[246] Treaties related to the damage caused by space objects[247] or the moon[248] are clearly inapplicable to cyber-

244. Montreal Protocol, *supra* note 234, pmbl.

245. *Id.* art. 2.

246. Aldrich, *supra* note 218, at 20–24; Delibasis, *supra* note 218, at 15–17 (discussing how the law of space is applicable to cyber-warfare); LAWRENCE T. GREENBERG ET AL., INFORMATION WARFARE AND INTERNATIONAL LAW 8–9 (1998) ("Space law, though, leaves ample room for information warfare."); Hollis, *supra* note 10, at 1051 ("[B]ecause information infrastructures frequently use outer space to relay communications or collect data, space law may affect [information operations]."); Schaap, *supra* note 202, at 160–69 (discussing international outer space law, international telecommunications law, and international aviation law as legal regimes that states should consider in developing cyber-warfare operations).

247. 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 Convention 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, natural 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.

248. The Moon Treaty grants the international community 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. The treaty refers to

attacks as we have defined them, and therefore we do not discuss them here. Instead, we focus on satellite regulations and the Treaty on Principles Governing the Activities in the Exploitation and Use of Outer Space. We conclude, however, that these treaties also have little promise for the regulation of cyber-attacks.

The 1967 Outer Space Treaty provides for the free exploration of space and prohibits the use of space for particular destructive purposes.[249] 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 Parties to the Treaty exclusively for peaceful purposes.[250]

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.[251] Because cyber-attacks are unlikely to cause mass destruction of the kind contemplated in the treaty, it is unlikely that cyber-attacks could be properly characterized as prohibited by the treaty.[252]

Satellite regulations offer another potential avenue for cyber-attack regulation. The Agreement Relating to the 1971 International Telecommunications Satellite Organization ("Telecommunications Satellite Organization")[253] and the Convention of the 1979 International Maritime Satellite Organization ("Maritime Satellite Organization")[254] contain "peaceful purpose" provisions applicable to satellites similar to the Outer Space Treaty.

---

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, and Japan, have not ratified the treaty. As of January 1, 2011, only thirteen states had ratified and four signed the Moon Treaty. U.N. Office for Outer Space Affairs, Comm. on the Peaceful Uses of Outer Space, *Status of International Agreements Relating to Activities in Outer Space*, U.N. Doc. ST/SPACE/11/Rev.2/Add/3 (2011).

249. 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.

250. *Id.* art. 4.

251. Shackelford, *supra* note 218, at 219.

252. Celestial bodies "refers 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. Aldrich, *supra* note 218, at 20.

253. Agreement Relating to the International Telecommunications Satellite Organization, "INTELSAT," Aug. 20, 1971, 23 U.S.T. 3813 [hereinafter Telecommunications Satellite Agreement].

254. Convention of the International Maritime Satellite Organization London, Sept. 3, 1976, 31 U.S.T. 1 [hereinafter INMARSAT].

However, despite the fact that satellites are likely to have a role in cyber-attacks, these treaties have little utility in regulating attacks. The Telecommunications Satellite Organization, which initially formed as an intergovernmental body mandated to "carry forward . . . the design, development, construction, establishment, operation and maintenance of the space segment of the global commercial telecommunications satellite system,"[255] was privatized in 2000.[256] Similarly, the Maritime Satellite Organization has largely ceased to represent intergovernmental interests.[257] 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 implicates cyber-attack operations at sea.[258] The article 19 obligation, which allows a vessel the right of innocent passage through another nation's territorial sea so long as its activities are not "prejudicial to the peace, good order or security of the coastal State,"[259] is widely accepted as customary international law.[260] Activities prohibited by article 19 include

255. Telecommunications Satellite Agreement, *supra* note 253, art. 2.

256. To "promote a more competitive global satellite services market," the Telecommunications Satellite Organization became a private company in 2000 named "Intelsat." U.S. GOV'T ACCOUNTABILITY OFFICE, TELECOMMUNICATIONS: INTELSAT PRIVATIZATION AND THE IMPLEMENTATION OF THE ORBIT ACT 1 (2004).

257. The Maritime Satellite Organization, originally founded as a nonprofit international organization to establish a maritime satellite communications network, changed its name to "International Mobile Satellite Organization" when it began to provide services to aircraft and portable users. JONATHAN HIGGINS, SATELLITE NEWSGATHERING 247–48 (2d ed. 2007). In 1999, the organization divided into two separate parts: most 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.

258. United Nations Convention on the Law of the Sea, art. 19, Dec. 10, 1982, 1833 U.N.T.S. 3 [hereinafter UNCLOS]. 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 United States and other countries as customary international law. Div. for Ocean Affairs and the Law of the Sea, *Table Recapitulating the Status of the Convention and of the Related Agreements, as at 20 September 2011*, http://www.un.org/Depts/los/reference_files/status2010.pdf; Senator Richard G. Lugar, The Law of the Sea Convention: The Case for Senate Action, Address at the Brookings Institution (May 4, 2004), *available at* http://www.brookings.edu/speeches/2004/0504energy_lugar.aspx (discussing the United States abiding by the Law of the Sea Convention).

259. UNCLOS, *supra* note 258, art. 19(1).

260. RÜDIGER WOLFRUM, FREEDOM OF NAVIGATION: NEW CHALLENGES (2008), *available at* http://www.itlos.org/fileadmin/itlos/documents/statements_of_president/wolfrum/freedom_navigation_080108_eng.pdf.

> (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;
>
> . . .
>
> (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 . . . .[261]

These regulations, particularly part (k), 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.[262] 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."[263] The prohibition could extend to a cyber-attack that compromises the computer network that operates a ship's broadcast system.[264] Similarly, article 113 requires states to put in place "laws and regulations necessary" to punish willful damage to submarine cables, including damage caused by a cyber-attack.[265] Thus, by prohibiting actions that undermine the functioning of communications systems at sea, 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 forms of cyber-attack within specific contexts. Yet this patchwork of regulations fails to provide a complete or coherent mechanism for addressing all forms of cyber-attacks. Given the limits of current international law, the following Section considers how U.S. domestic law might be used to address cyber-attacks.

---

261. UNCLOS, *supra* note 258, art. 19(2).

262. *Id.* art. 109(1).

263. *Id.* art. 109(2).

264. *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.*

265. *Id.* art. 113.

D. U.S. Domestic Law

Domestic law offers an important tool for combating cyber-attacks, including those that cross international borders. Because many cyber-attacks are also cyber-crimes,[266] domestic criminal law is particularly relevant. Unfortunately, existing domestic law largely fails to directly address the novel modern challenges posed by cyber-attacks,[267] and is severely limited by its lack of extraterritorial reach.

Although there is no U.S. federal statute that directly criminalizes cyber-attacks,[268] there is extensive federal criminal law that offers an important legal tool for addressing cyber-attacks.[269] At the federal level, criminal laws address fraud involving devices, computers, or email;[270] malicious interference in communications lines, stations, or systems;[271] electronic communication interception;[272] illicit access to electronic communications and records;[273] and recording of dialing, routing, addressing, and signaling information.[274]

The majority of existing criminal laws bearing on cyber-attack do not apply extraterritorially—that is, they do not reach criminal activity occurring outside the United States.[275] There are, however, some exceptions to that

266. *See supra* Part I.A.3 and Figure 1.

267. *See, e.g.*, Sklerov, *supra* note 93, at 6 ("Unfortunately, state responses to cyberattacks are governed by an anachronistic legal regime that impairs a state's ability to defend itself.").

268. As this Article went to print, several cyber-security bills had been proposed but none passed. *See* Brendan Sasso, *Senate Dems Modifying Cybersecurity Bill to Pick Up GOP Votes*, HILLICON VALLEY (May 6, 2012), http://thehill.com/blogs/hillicon-valley/technology/225607-senate-dems-revamping-cybersecurity-bill-; Ellen Nakashima, *On Hill, Imagining a Cyberattack on New York*, WASH. POST CHECKPOINT WASHINGTON (Mar. 9, 2012), http://www.washingtonpost.com/blogs/checkpoint-washington/post/officials-use-nyc-blackout-scenario-to-sell-senators-on-cyber-attack-legislation/2012/03/09/gIQA9Z530R_blog.html.

269. In addition to criminal liability, there have been proposals for the use of tort law against cyber-attackers or intermediaries who negligently facilitate 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 1, 31–32 (2011) (unpublished research paper) (available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1979857). Such proposals face a number of serious challenges, however, including attribution and jurisdictional problems, *id.* at 30, 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.*

270. 18 U.S.C. §§ 1029, 1030, 1037 (2006). 18 U.S.C. § 1030 is the codification of the Computer Fraud and Abuse Act.

271. *Id.* § 1362.

272. *Id.* §§ 2510–2522.

273. *Id.* §§ 2701–2712.

274. *Id.* §§ 3121–3127.

275. 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. EEOC v. Arabian Am. 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

general rule. For example, the criminal statute banning access device fraud, as amended by the USA PATRIOT Act of 2001, provides that

> [a]ny 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.[276]

The statute banning computer fraud was likewise amended as part of the USA PATRIOT Act to provide for extraterritorial applicability.[277] Both of these statutes may serve as useful models for extending extraterritorial application to other domestic laws related to cyber-attack.

In addition, several recent legislative efforts tackle pieces of the cyber-attack threat not addressed by U.S. criminal law. These include the Cybersecurity Enhancement Act;[278] the Executive Cyberspace Authorities Act of 2010;[279] the Rockefeller-Snowe Cybersecurity Act;[280] the International Cyberspace and Cybersecurity Coordination Act of 2010;[281] and the Protecting Cyberspace as a National Asset Act of 2010.[282]

The most widely discussed of these efforts has been the Protecting Cyberspace as a National Asset Act, cowritten by Senators Lieberman, Collins, and Carper, which was introduced in the Senate and the House in June 2010.[283] The bill builds on the military's recent establishment of the U.S. Cyber

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 expressly extraterritorial in scope.").

276. 18 U.S.C. § 1029 (2006); U.S. DEP'T OF JUSTICE, PROSECUTING COMPUTER CRIMES, *supra* note 65, at 94, 115.

277. 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 communication, 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 66, at 5.

278. H.R. 4061, 111th Cong. (2010).

279. H.R. 5247, 111th Cong. (2010).

280. S. 773, 111th Cong. (2009).

281. S. 3193, 111th Cong. (2010).

282. S. 3480, 111th Cong. (2010); H.R. 5548, 111th Cong. (2010).

283. S. 3480; H.R. 5548.

Command[284] by proposing the establishment of two new administrative bodies: (1) an Office of Cyberspace Policy in the White House, charged with developing and coordinating a national strategy to increase the security and resiliency of cyberspace; and (2) a National Center for Cybersecurity and Communications within the Department of Homeland Security, designed to "enable automated and continuous monitoring of any information collected" and "use [of] the information to enhance the risk-based security of the Federal information infrastructure."[285] The bill also addresses a wide range of related cyber-security matters, including definitions and federal information security management provisions.[286]

The bill sparked a vigorous debate over the proper role of the government in regulating cyberspace. Opponents dubbed the proposed regulation the "kill switch bill," seeing it as an effort to grant the president emergency powers over certain Internet communications.[287] However, had it passed into law, the bill would likely have established more checks on the president's power to respond to cyber-emergencies than currently exist.[288] Its authors amended and reintroduced the bill, but it has made little progress toward a vote on the Senate floor.[289] It has since been superseded by alternative proposals, none of which has yet won the approval of Congress.[290]

This debate offers an important lesson for advocates of cyber-attack regulation: any future law must clearly indicate what activities are to be covered, place a high and transparent bar on emergency measures, and address well-founded concerns that efforts to strengthen cyber-security might simultaneously weaken 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 developing U.S. defensive capabilities. However, none of the recent legislative efforts that might strengthen defensive capacity against cyber-attack have yet been made into law. Moreover, the existing domestic law framework is insufficient for addressing the larger global

284. McMichael, *supra* note 39.

285. S. 3480; H.R. 5548.

286. S. 3480; H.R. 5548.

287. *See* Emelie Rutherford, *Senate Committee OKs Cybersecurity Bill on Majority Leader's Radar*, DEFENSE DAILY (June 25, 2010), http://findarticles.com/p/articles/mi_6712/is_61_246/ai_n54561980/ (last visited Apr. 22, 2012). The bill has since been reintroduced with changes meant to prevent the government from using a "kill switch" to shut off Internet service as a political tool. *Id.*; *see also* Diane Bartz, *Reid Pushes US Republicans for Cybersecurity Bill*, REUTERS (July 27, 2011, 5:09 PM), http://www.reuters.com/article/2011/07/27/congress-cybersecurity-idUSN1E76Q1M320110727.

288. *See, e.g.*, Rutherford, *supra* note 287 (describing congressional "frustration . . . that people have misconstrued a provision related to the president's emergency powers to take over communications networks" when "[t]he president already has this authority, . . . and the bill would restrict when he can use it").

289. *See id.*; Bartz, *supra* note 287.

290. *See supra* note 268.

problem.[291] In particular, the lack of extraterritorial reach of most criminal laws that apply to cyber-attacks severely limits their ability to reach those initiating such cyber-attacks, who are often located outside the United States. The next Part offers recommendations for remedying the substantial limitations of both the domestic and international legal frameworks for addressing cyber-attack.

IV.
NEW LAW FOR CYBER-ATTACKS

Cyber-attacks present a new and growing threat—one that current international and domestic laws are not yet fully prepared to meet. The law of war offers a basis for responding only to those cyber-attacks that amount to an armed attack or that take place in the context of an ongoing armed conflict. Other existing international legal frameworks offer only embryonic or piecemeal protection. U.S. domestic law, though potentially a powerful tool for battling cyber-attacks, has not yet addressed the challenge directly, and what remedies exist are in many cases restricted by jurisdictional limits.

To begin to fill the gaps in existing law, we propose legal reform on both domestic and international levels.[292] Our recommended domestic law reforms are twofold. First, the United States should add extraterritorial applicability to criminal laws bearing on cyber-attack. Second, the United States should utilize limited countermeasures, as appropriate, to combat cyber-attacks that do not rise to the level of armed attacks under the law of war.

These domestic measures will address elements of the problem, but getting at the root of the global cyber-attack challenge 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 that limits the cyber-attacks to which states may respond with force. Second, the treaty should empower states to cooperate in evidence collection and criminal prosecution of individuals involved in transnational cyber-attacks. While this second aim will likely be a longer-term project, it offers the only truly effective solution to the inherently international problem of cyber-attacks.

---

291. *See* Andy Johnson & Kyle Spector, *Deterring Cyber War: A U.S.-Led Cybersecurity Summit*, THIRD WAY 3 (Oct. 2010), *available at* http://content.thirdway.org/publications/343/Third_Way_Idea_Brief_-_Deterring_Cyber_War-A_US-Led_Cybersecurity_Summit.pdf (last visited Apr. 22, 2012).

292. We focus here on potential legal reforms. In addition to legal reform, government should coordinate with the private sector to address cyber-attack threats. Indeed, the Obama administration has recognized that "[e]nsuring 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 63, 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 32, at 9. The legal reforms outlined here are meant to compliment such cooperative measures, not substitute for them.

A. Battling Cyber-Attacks at Home

1. Extend the Extraterritorial Reach of Domestic Law

As noted above, a number of existing and proposed domestic laws may play a role in combating cyber-attacks, including numerous criminal statutes regulating harmful cyber-activity outside the context of armed conflict.[293] It is important to recall that domestic criminal law alone cannot regulate cyber-attacks because not all cyber-attacks are defined as cyber-crimes. But many cyber-attacks—including those involving non–state actors and computer-based means—are also cyber-crimes that fall within the ambit of domestic criminal law.[294] Unfortunately, only a small number of existing criminal laws that might govern cyber-attacks explicitly provide for extraterritorial reach.[295]

To remedy this limitation, legislators could amend domestic criminal statutes to give them extraterritorial reach. If other states reciprocate by making their own criminal statutes pertaining to cyber-attacks extraterritorial as well, this could greatly increase global enforcement.[296] Indeed, increased domestic enforcement through extraterritorial application will be much more successful and legitimate if it takes place in concert with the creation of an international treaty that establishes basic shared standards regarding cyber-attacks.

Even if domestic criminal laws that apply to cyber-attacks extend across borders, jurisdictional hurdles will likely hamper enforcement by any individual state. It may be difficult, for example, for the United States 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. Thus, strengthened extradition relationships around the world would complement increased extraterritorial application of domestic law. Though dramatic improvement in extradition relationships may not be immediately feasible given that extradition treaties, which are negotiated on a bilateral basis, take substantial time and effort to negotiate and pass, such relationships could help effectuate the prosecution of many crimes resulting from increasing globalization including drug, weapon, and human trafficking, and transnational white-collar crime.[297] Thus, the United States should prioritize the development of these relationships moving forward.

Further, the United States, and the global community in general, should endeavor to explicitly criminalize aspects of cyber-attacks that fall outside the

293. *See supra* Part III.D.

294. *See supra* Part I.A.3.

295. *See supra* Part III.D.

296. This extraterritorial reach would not regulate cyber-actions taken by governments but rather those of individuals and other non–state actors.

297. *See generally* John T. Soma, et al., *Transnational Extradition for Computer Crimes: Are New Treaties and Laws Needed?*, 34 HARV. J. ON LEGIS. 317 (1997) (discussing the limitations of current extradition treaties and proposing potential reforms).

scope of existing domestic or international law, including the law of war. In the present absence of an international cyber-crime agreement, it is possible for the United States to more effectively counter cyber-attacks through carefully crafted and narrowly framed domestic law.

2. Countermeasures in Response to Cyber-Attacks

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

As noted in the discussion of *jus ad bellum* above, the vast majority of cyber-attacks do not rise to the level of an armed attack.[298] 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 necessary and 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.[299]

While active defense is the most commonly discussed type of countermeasure that might be employed in response to a cyber-attack, it is only one option among many.[300] A key limit to a legally permissible countermeasure is that it must be proportional to the injury suffered by the victim state.[301] Moreover, countermeasures must be designed to enable a return to the status quo ante, in which both the perpetrating and victim states comply with their relevant legal duties towards one another.[302] Countermeasures must be temporary so that once the cyber-attacks stop, the countermeasure may stop as well and normal international relations may resume.[303]

The Draft Articles on State Responsibility express a preference for reciprocal countermeasures, but this is not a requirement.[304] Still, the closer the relationship between the breach and countermeasure the more likely the countermeasure is to be proportional and therefore lawful.[305] The United States should consider in advance what international obligations it has toward likely cyber-aggressor states that it might lawfully revoke in case of an unlawful

298. *See supra* Part II.A.
299. *See* Draft Articles, *supra* note 109, art. 49.
300. *See* Sklerov, *supra* note 93, at 2 n.5 (comparing active and passive defenses).
301. *See* Draft Articles, *supra* note 109, art. 51.
302. *See id.* art. 49(1).
303. *See id.* art. 49.
304. *See id.* pt. 3, ch. 2, cmt., ¶ 5.
305. *Id.*

cyber-attack. Indeed, the United States could develop a policy regarding the types of countermeasures legally available in response to particular types of cyber-attacks.

B. A Cyber-Attack Treaty

Changes in domestic law and policy, such as adding extraterritorial reach to criminal laws and planning for the use of countermeasures, are valuable legal responses to the threat of cyber-attack. Yet to truly address the cyber-attack challenge, international coordination will be necessary.[306] The scope of the problem is global, and the solution must be as well. As the U.S. Department of Defense has explained, "cyberspace is a network of networks that includes thousands of ISPs [internet service providers] across the globe; no single state or organization can maintain effective cyber defenses on its own."[307]

The United States has developed a Cyberspace Strategy that emphasizes 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."[308] 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 with two central features. First, it must offer a shared definition of cyber-crime, cyber-attack, and cyber-warfare.[309] Second, it should offer a framework for more robust international cooperation in information sharing, evidence collection, and criminal prosecution of those participating in cross-national cyber-attacks. That framework should be attentive to the challenges of overcriminalization, maintaining room for individuals to use the Internet and related technologies to engage in lawful dissent.[310]

---

306. As discussed in Part III.B, there have already been several efforts to create a cyber-attack treaty. *See* CLARKE & KNAKE, *supra* note 7, at 268–71 (arguing for a Cyber War Limitations Treaty); *cf.* JACK GOLDSMITH, CYBERSECURITY TREATIES: A SKEPTICAL VIEW (2011) (offering a skeptical take on the possibility of a cyber-security treaty). Russia has for some time been proposing a treaty banning cyber-attack. *See, e.g.*, John Markoff & Andrew E. Kramer, *U.S. and Russia Differ on Treaty for Cyberspace*, N.Y. TIMES, June 28, 2009, at A1 ("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 . . . ."). Yet the shape of the agreement proposed here is quite different—it begins with securing a shared agreement on the activity meant to be prohibited.

307. DOD STRATEGY, *supra* note 32, at 9.

308. WHITE HOUSE CYBERSPACE STRATEGY, *supra* note 63, 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.

309. 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 II.B.

310. *See* WHITE HOUSE CYBERSPACE STRATEGY, *supra* note 63, at 7.

1. Define Cyber-Attack and Cyber-Warfare

The first aim of a cyber-attack treaty regime should be to develop a shared definition of cyber-attack, cyber-crime, and cyber-warfare. These definitions could serve as the foundation for domestic criminal legislation targeting cyber-attacks and cyber-crime as well as more extensive international cooperation. A similar strategy has been used, for example, in the international effort to battle bribery: the OECD Bribery Convention provides a definition of bribery that state parties then integrate into national legislation forbidding the practice.[311] Under the Bribery Convention, "signatories pledged to criminalize and prosecute the bribery of foreign public officials."[312] The thirty-eight state parties have then used that shared definition as the basis for domestic implementing legislation.[313]

We have proposed a definition of cyber-attack that would include any action taken to undermine the function of a computer network for a political or national security purpose. An appropriate definition of cyber-crime would include any violation of criminal law by non–state actors, committed by means of a computer system. Finally, cyber-warfare should be defined as a cyber-attack that causes physical injury or property damage comparable to a conventional armed attack.

States could adopt a clear definition of cyber-attack, cyber-crime, and cyber-warfare in the context of a comprehensive binding treaty, nonbinding declaration, or through independent agreements in anticipation of more broad-based future cooperation. Even a stand-alone nonbinding defining declaration could provide an important starting point for future cooperation if it provides a definition that is later incorporated into a more comprehensive international treaty.[314] Such a document could offer much-needed clarity on when cyber-

311. Convention on Combating Bribery of Foreign Public Officials in International Business Transactions, Dec. 18, 1997, 37 I.L.M. 4 (1998) [hereinafter OECD Bribery Convention]. Under the Convention, the "Offense of Bribery of Foreign Public Officials" is defined as

> intentionally to offer, promise or give any undue pecuniary or other advantage, whether directly or through intermediaries, to a foreign public official, for that official or for a third party, in order that the official act or refrain from acting in relation to the performance of official duties, in order to obtain or retain business or other improper advantage in the conduct of international business.

Id. art. 1(1).

312. *Developments in the Law – Extraterritoriality*, 124 HARV. L. REV. 1226, 1285 (2011); *see* OECD Bribery Convention, *supra* note 311, art 1(1) ("Each Party shall take such measures as may be necessary to establish that [bribery] is a criminal offence under its law.").

313. *OECD Anti-Bribery Convention: National Implementing Legislation*, ORG. FOR ECON. CO-OPERATION & DEV., http://www.oecd.org/document/30/0,3746,en_2649_34859_2027102_1_1_1_1,00.html (last visited Apr. 21, 2012). Unfortunately, it appears that few countries have actually been enforcing the domestic antibribery provisions. *See Developments in the Law*, *supra* note 312, at 1285.

314. The idea that a nonbinding, defining declaration can provide a basis for negotiating a subsequent binding treaty is illustrated by the successful U.N. effort to criminalize torture and other cruel, inhuman, or degrading treatment. Before the Convention Against Torture was adopted by the U.N. General Assembly in 1984, the General Assembly adopted the Declaration Against Torture. Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, Dec.

attacks amount to an armed conflict that warrants self-defense,[315] and could offer a common reference point for subsequent domestic criminal legislation.

Even an agreement limited to common definitions will likely face challenges.[316] In particular, 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 to be criminalized through international cooperation, including some forms of legitimate political dissent.[317] As noted earlier, Russia and other members of the Shanghai Cooperation Organization have been promoting an international agreement banning cyber-attack for some time,[318] but their focus differs greatly from that of the United States and much of Europe in the cyber-attack arena.[319] A key challenge of this first stage agreement will thus be to find common ground with major cyber-powers without expanding the definition of cyber-attack in ways that would quell free speech and democratic political organization.

2. International Cooperation on Evidence Collection and Criminal Prosecution

Once states develop a shared definition of cyber-attacks, cyber-crime, and cyber-warfare, the next step is more extensive cooperation among states on

---

10, 1984, 1465 U.N.T.S. 85 [hereinafter CAT]; CHRIS INGELSE, THE UN COMMITTEE AGAINST TORTURE: AN ASSESSMENT 73 (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 149 states, including the United States. *See* Status, Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (last visited Nov. 8, 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. INGELSE, *supra*, at 74. Unfortunately, the draft Sweden submitted to the 34th Session, E/CN.4/1285, is not available on the U.N. Documents database.

315. 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 63, 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.

316. Indeed, some have suggested that a successful treaty may be nearly impossible to achieve, at least in the short term. *See, e.g.*, Waxman, *supra* note 24, 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 306, 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).

317. *See supra* text accompanying notes 21–26.

318. *See* Markoff & Kramer, *supra* note 306.

319. *See supra* text accompanying notes 24–26.

information sharing, evidence collection, and criminal prosecution of those involved in cyber-attacks. A useful starting point for building such a 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. 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.[320] Nonetheless, it provides a framework from which a more comprehensive agreement might begin.

Building on this framework, 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 information-sharing, layering on additional mechanisms for fostering cooperation in identifying and stopping the sources of cyber-attacks through criminal law enforcement agencies. International cooperation in information sharing could be an extremely valuable complement to other regulation of cyber-attacks.[321]

Member states could agree to share access to cyber-related information with other member states. That information would not be available to nonmembers or to states that fail to comply with the treaty's core obligations. Offering privileged access to information to member states in good standing would provide states with an incentive to participate in and comply with the treaty regime.[322]

Finally, consistent with the Tunis Commitment[323] and Agenda,[324] a treaty could encourage 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 benefit [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

320. *Convention on Cybercrime, Chart of Signatures and Ratifications*, COUNCIL OF EUR. (last visited Apr. 21, 2012), http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&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.*

321. Information sharing in this context was endorsed by a group of experts from countries as diverse as the United States, China, and Russia in a 2010 report to the U.N. Secretary-General. *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, *supra* note 186, at 8.

322. This proposal aims to harness the power of outcasting to build a strong treaty regime. *See* Oona Hathaway & Scott J. Shapiro, *Outcasting: The Enforcement of Domestic and International Law*, 121 YALE L. J. 252 (2011).

323. *Tunis Commitment*, WORLD SUMMIT ON THE INFO. SOC'Y (Nov. 18, 2005), http://www.itu.int/wsis/docs2/tunis/off/7.html (last visited Apr. 21, 2012).

324. *Tunis Agenda for the Information Society*, WORLD SUMMIT ON THE INFO. SOC'Y (Nov. 18, 2005), http://www.itu.int/wsis/docs2/tunis/off/6rev1.html (last visited Apr. 21, 2012).

> 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.[325]

Because any country's cyber-security can be compromised by its allies' security gaps, a collective attempt to prevent cyber-attacks must include efforts to improve the defenses of partner countries as well.[326]

Another challenge to any comprehensive cyber-attack treaty is the difficulty of verifying where cyber-attacks originate.[327] Uncertainty in tracing and attributing a cyber-attack "makes retaliation for breach much harder for any president or general to order."[328] Yet while verification of a cyber-attack's origin is difficult, even those who have expressed skepticism about the short-term feasibility of a cyber-treaty acknowledge that it is not impossible. As Jack Goldsmith has put it, "Sometimes traceback and related forensic tools can provide good-enough attribution."[329] Indeed, while negotiations on the treaty are underway, states should continue a parallel technical effort to enhance their capacities to trace the source of cyber-attacks.

As General Keith Alexander, chief of the new U.S. Cyber Command, explained earlier this year when reopening negotiations with Russia on this issue, "We do have to establish the lanes of the road" for what cyber-activities governments can and cannot pursue.[330] Establishing those lanes is the necessary first step to addressing the challenge of cyber-attacks. Only once they are in place will verification challenges become salient.

CONCLUSION

The emergence of Stuxnet in 2010 heralded a new era for cyber-attacks. Although its damage was apparently limited to the Iranian nuclear program it was designed to attack, it revealed how vulnerable even nation-states are to cyber-attacks. Indeed, by the time it was discovered, Stuxnet had wormed its way into computer networks around the world.

Cyber-attacks on vital infrastructure are already becoming widespread. Cyber-security professionals report that the computer infrastructure has become more vulnerable even in just a year.[331] And yet, while the threat of cyber-

---

325. WHITE HOUSE CYBERSPACE STRATEGY, *supra* note 63, at 15.

326. Shanker & Bumiller, *supra* note 53 (noting that 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).

327. *See* GOLDSMITH, *supra* note 306, at 10–12.

328. *Id.* at 11.

329. *Id.* at 10.

330. Siobhan Gorman, *U.S. Backs Talks on Cyber Warfare*, WALL ST. J., June 4, 2010, at A3.

331. Mark Clayton, *Security Lags Cyberattack Threats in Critical Industries, Report Finds*, CHRISTIAN SCI. MONITOR (Apr. 20, 2011), http://www.csmonitor.com/USA/2011/0420/Security-lags-cyberattack-threats-in-critical-industries-report-finds (citing a global survey of 200 computer security

attacks has rapidly grown, the response has not kept pace. This Article has shown that both the U.S. government and the international community have thus far largely failed to update legal frameworks that might respond to cyber-attacks. To face new and growing threats, governments continue to rely on limited and piecemeal bodies of law not designed to meet the challenge of cyber-attacks.

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. The United States should expand the reach of domestic law abroad and develop a system for utilizing limited countermeasures where appropriate to respond to certain types of cyber-attacks. Yet the United States is restricted in what it can accomplish alone. Cyber-attacks are often transnational—designed by authors in multiple countries, run through networks across the world, and used to undermine computer systems in countries 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.

professionals working in critical infrastructure industries, "In the Dark: Crucial Industries Confront Cyberattacks").