California Law Review

Volume 101 | Issue 4 Article 4

8-1-2013

Navigating Jus Ad Bellum in the Age of Cyber Warfare

Reese Nguyen

Link to publisher version (DOI)
http://dx.doi.org/https://doi.org/10.15779/Z38QZ4J

Navigating *Jus Ad Bellum* in the Age of Cyber Warfare

Reese Nguyen*

The last decade has witnessed the heightened destructive potential of cyber attacks; correspondingly, cyberspace has become the new battlefield for nation-states in conflict. Yet jus ad bellum*—the body of international law governing legitimate use of force—provides little guidance about the legality of a cyber attack or when such an attack becomes an act of war justifying resort to responsive force. This Comment provides a new analytical framework for addressing that question. It begins by clarifying definitional ambiguities in the literature on cyber attack, setting forth a definition that focuses on computer networks as the* instruments*, rather than* objects*, of attack. It examines the technical concepts and considerations that influence the use-of-force analysis and animate the evaluation of potential analytical frameworks. It then discusses the governing* jus ad bellum *standards and critiques the leading approaches to assessing cyber attacks under these standards. This Comment departs from the traditional and accepted models of inquiry, drawing on cyber security research to propose a framework centered on cyber-physical systems that addresses cyber attacks under the laws of just war.*

Introduction.. 1080
I. The Definition of Cyber Attack.. 1085
A. Problems with an Object-Based Definition of Cyber Attack........ 1086
B. An Instrument-Based Definition of Cyber Attack 1088
II. Cyber Attacks: Contours and Technology.. 1091
A. Anatomy of a Cyber Attack... 1092

* Associate, Keker & Van Nest LLP; J.D., University of California, Berkeley, School of Law, 2012; B.A., Yale University, 2005. Thanks to Michael B. Taylor for the many engaging conversations on these topics, to John C. Yoo for helpful comments on initial drafts, and to the editors and staff of the *California Law Review* for their valuable suggestions and editing. All errors are my own.

B. The Cyber Attack Arsenal 1093

1. Penetration Attacks 1093

2. Denial-of-Service Attacks 1097

C. Cyber Attack's Challenges 1098

1. Scope of Effects 1098

2. Unpredictability 1102

3. Reversible Damage 1103

4. Anonymity and the Problem of Attribution 1104

D. An Evolving Cyberspace 1106

1. Cyber-Physical Convergence and Network Connectivity...... 1106

2. Vulnerabilities, Revisited 1108

III. *Jus Ad Bellum*: Use of Force and Armed Attack 1111

A. *Jus Ad Bellum* 1112

1. Use of Force 1113

2. Armed Attack 1115

3. Cyber Attack Analogies 1116

B. Leading Approaches 1117

1. Instrument-Based Approach 1117

2. Target-Based Approach 1119

3. Effects-Based Approach 1121

C. A New Approach: Force as Intentional Damage to Cyber-Physical Systems 1124

Conclusion 1129

INTRODUCTION

As societal dependence on computing technology has increased dramatically over the last several decades,[1] so too has the attractiveness of computers and networks as military targets for nation-states in conflict.[2] At the

[1] *See* Edward Skoudis, *Evolutionary Trends in Cyberspace*, *in* CYBERPOWER AND NATIONAL SECURITY 147, 166–69 (Franklin D. Kramer et al. eds., 2009) (describing global trends in technological development and Internet use).

[2] *See* Lesley Swanson, *The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict*, 32 LOY. L.A. INT'L & COMP. L. REV. 303, 305 (2010) ("As modern society increasingly relies on global and domestic information structures, these structures tend to become targets during war and other hostilities."); *cf.* JEFFREY CARR, INSIDE CYBER WARFARE 161–77 (2d ed. 2012) (examining military doctrines for cyber warfare in the Russian Federation, the People's Republic of China, and the United States and noting that "[o]ver 120 nations are engaged in developing [cyber warfare] capability").

Cyber attacks on U.S. federal government systems, for example, increased in number from approximately 30,000 reported to the United States Computer Emergency Readiness Team (US-CERT) in 2009 to 41,776 reported in 2010. OFFICE OF MGMT. & BUDGET, EXECUTIVE OFFICE OF THE PRESIDENT, FISCAL YEAR 2010 REPORT TO CONGRESS ON THE IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT OF 2002, at 12–13 (2011), *available at* http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/FY10_FISMA.pdf. In 2011, the number grew to 43,889. OFFICE OF MGMT. & BUDGET, EXECUTIVE OFFICE OF THE PRESIDENT, FISCAL YEAR 2011 REPORT TO CONGRESS ON THE IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY same time, the sophistication and capabilities of those who seek to exploit these technologies as weapons have continued to rise.[3] Taken together, these trends underscore the enormous potential for determined hackers to mount campaigns of widespread, devastating damage, not only against legitimate military targets and installations, but also against civilian lives and property, as well as critical national infrastructures essential to modern survival.

As a weapon for warfare between nation-states, cyber attacks strain traditional international law notions about the use of force. The United Nations Charter, which prohibits the unauthorized use of force except in response to an armed attack,[4] was drafted and adopted during an era in which warring nations inflicted physical damage on their adversaries primarily through kinetic attack: the bombs and bullets delivered by artillery and rifles that are the mainstay of conventional military combat.[5] Although the Charter does not define what constitutes a "use of force" or an "armed attack," decades of state practice and International Court of Justice (ICJ) application have provided some measure of clarity with regard to the traditional modes of war—aerial bombardment, ground assault, missile strikes, and other territorial incursions.[6] In the realm of cyber attacks, the definitional boundaries remain blurred: international law provides little direct guidance as to when a cyber attack rises to the level of force or armed attack.[7]

Consider, for example, the Chinese military program of systematic cyber attacks. This program of assault on corporate and government computer networks in the United States, Canada, South Korea, Taiwan, and Vietnam over

MANAGEMENT ACT OF 2002, at 16 (2012), *available at* http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy11_fisma.pdf. Between 1988 and 2003, the total number of cyber incidents reported by third parties within the United States grew from 6 to 137,529. ROBERT J. TURK, US-CERT CONTROL SYSTEMS SECURITY CENTER, CYBER INCIDENTS INVOLVING CONTROL SYSTEMS INL/EXT-05-0671, at 3–4 (2005), *available at* http://www.inl.gov/technicalpublications/documents/3480144.pdf.

[3] *Cf.* HOWARD F. LIPSON, CERT COORDINATION CENTER, TRACKING AND TRACING CYBER-ATTACKS: TECHNICAL CHALLENGES AND GLOBAL POLICY ISSUES CMU/SEI-2002-SR-009, at 10 (2002), *available at* http://www.sei.cmu.edu/reports/02sr009.pdf (illustrating the correlation between growing attack sophistication and rising intruder technical knowledge between 1980 and 2000).

[4] U.N. Charter, art. 2, para. 4; art. 51.

[5] The Charter of the United Nations was signed on June 26, 1945, and came into force on October 24, 1945. U.N. Charter, Introductory Note.

[6] *See generally* A. MARK WEISBURD, USE OF FORCE: THE PRACTICE OF STATES SINCE WORLD WAR II (1997) (explaining that the writings of the ICJ and other commentators have demonstrated that the general practice of states creates a body of "customary international law" that imposes legal obligations limiting interstate war under the U.N. Charter).

[7] *See Nomination of LTG Keith B. Alexander, USA, to be General and Director, National Security Agency/Chief, Central Security Service/Commander, U.S. Cyber Command: Hearing Before the S. Comm. On Armed Services*, 110th *Servs.*, 111th Cong. (2010) (Statement of Keith Alexander, Nominee, Commander, U.S. Cyber Command) ("There is no international consensus on a precise definition of a use of force, in or out of cyberspace. Consequently, individual nations may assert different definitions, and may apply different thresholds for what constitutes a use of force.").

the last several years[8] has resulted in the theft of hundreds of terabytes of data.[9] This type of hacking is unlikely to be seen as an act of war and more likely to be seen as espionage,[10] which is neither condoned nor condemned under international law.[11] But how should international law treat the cyber attack that does more than steal information—the cyber attack that plants software giving the attacker remote command over computers that control critical infrastructures such as power grids,[12] or the cyber attack that shuts down access to government and banking websites nationwide?[13] Under what framework should a nation's policy makers and military decision makers assess the legal status of these varied attacks when crafting the appropriate response?

The case of the Stuxnet virus illustrates some of the difficulties of applying the existing law of war framework in the age of cyber warfare. In 2010, the Stuxnet worm, a self-replicating computer virus targeting computers that regulate automated physical processes,[14] took control of Iran's nuclear centrifuges at Natanz and caused about one-fifth of them to spin out of control and self-destruct.[15] Iran's uranium enrichment operations halted, resulting in an estimated several years of delay in the country's nuclear arms development program.[16] Responsibility for Stuxnet has been attributed to Israel and the United States.[17]

In effect, Stuxnet produced physical damage of the Iranian nuclear facility comparable to that caused by the 1981 and 2007 Israeli air strikes that

[8] *See* David E. Sanger et al., *Chinese Army Unit Is Seen as Tied to Hacking Against U.S.*, N.Y. TIMES (Feb. 18, 2013), www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html. China has denied responsibility for the attacks, alleging that nearly two-thirds of the more than 100,000 cyber attacks on Chinese military websites per month originate in the United States. *See id.*; Paul Mozur, *China Alleges Cyberattacks Originated in U.S.*, WALL ST. J. (Feb. 28, 2013), http://online.wsj.com/article/SB10001424127887323293704578331832012056800.html.

[9] MANDIANT INTELLIGENCE CENTER, APT1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS 3 (2013), *available at* http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

[10] *See* Lt. Col. Geoffrey B. Demarest, *Espionage in International Law*, 24 DENV. J. INT'L L. & POL'Y 321, 347 (1996) (explaining that although espionage is "an unfriendly act," it does not violate international law).

[11] *See* Christopher D. Baker, *Tolerance of International Espionage: A Functional Approach*, 19 AM. U. INT'L L. REV. 1091, 1092 (2004).

[12] U.S. President Barack Obama alluded to this type of attack in his 2013 State of the Union address. President Barack Obama, Remarks by the President in the State of the Union Address (Feb. 12, 2013) ("Now our enemies are also seeking the ability to sabotage our power grid, our financial institutions, our air traffic control systems.").

[13] The country of Estonia experienced this type of cyber attack in 2007. *See* discussion *infra* Part III.B–C.

[14] Thomas M. Chen, Editor's Note, *Stuxnet, the Real Start of Cyber Warfare?*, 24 IEEE NETWORK, 2, 2–3 (2010).

[15] William J. Broad, John Markoff & David E. Sanger, *Israeli Test on Worm Called Crucial in Iran Nuclear Delay*, N.Y. TIMES, Jan. 16, 2011, at A1.

[16] *Id.*

[17] David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. TIMES, June 1, 2012, at A1.

destroyed partially-constructed nuclear reactors in Baghdad[18] and Syria.[19] Yet few nation-states or commentators have explicitly asserted that Stuxnet constituted an illegal use of force or armed attack.[20] Israel and the United States, moreover, may have created the Stuxnet worm in order to disable Iran's nuclear facility while avoiding the risk of war, or at least the international condemnation, that could result from a preemptive, overt military strike.[21] But should damage and disruption caused internally by malicious computer code be treated any differently under the laws of war than that caused externally, for example, by bombs?

This threshold inquiry is crucial to regulating violence between states. Because the UN Charter prohibits the unauthorized use of force except in response to an armed attack, a state must be able to quickly assess whether a cyber attack is an "armed attack" justifying responsive force. It must also know whether a cyber attack would constitute a "use of force" not rising to the level of an armed attack, but nonetheless illegal and subject to condemnation or sanctions under international law. These questions are important to both the country considering using force (to predict the potential consequences) and the country under attack (to assess the legality of potential responses).

Scholars have advanced three main approaches for addressing when a cyber attack crosses the threshold to be considered use of force or an armed attack under *jus ad bellum*, the international law principles governing the resort to force:[22] the first, the instrument-based approach, looks to the form of weapon used to perpetrate an attack, asking whether the attack possesses the "physical characteristics traditionally associated with military coercion;"[23] the second, the target-based[24] or "strict liability" approach,[25] automatically treats any cyber

[18] *See Israel Bombs Baghdad Nuclear Reactor*, BBC NEWS (June 7, 1981), *available at* http://news.bbc.co.uk/onthisday/hi/dates/stories/june/7/newsid_3014000/3014623.stm.

[19] *See* David E. Sanger & Mark Mazzetti, *Israel Struck Syrian Nuclear Project, Analysts Say*, N.Y. TIMES, Oct. 14, 2007, at A1.

[20] *See* David P. Fidler, *Was Stuxnet an Act of War? Decoding a Cyberattack*, 9 IEEE SECURITY & PRIVACY 56, 57–59 (2011) ("Nation-states have been curiously quiet about Stuxnet . . . [A]lthough Stuxnet caused serious damage to Iranian centrifuges through exploitation of cyber-controlled physical systems, states—including Iran—haven't denounced this incident as an illegal use of force or armed attack, even though such damage caused by conventional, kinetic means would have triggered such accusations.").

[21] Broad et al., *supra* note 15.

[22] The law of war is divided into two primary substantive areas, *jus ad bellum* and *jus in bello*. CARR, *supra* note 2, at 48. *Jus ad bellum* principles govern the transition from peace to war, dictating when a nation-state may lawfully use force against another nation-state. *Id. Jus in bello*, which regulates wartime conduct, is based upon the Geneva humanitarian laws that protect specific classes of war victims and the Hague laws that regulate the overall means and methods of combat. Chris af Jochnick & Roger Normand, *The Legitimation of Violence: A Critical History of the Laws of War*, 35 HARV. INT'L L.J. 49, 52 (1994).

[23] *See* Duncan B. Hollis, *Why States Need an International Law for Information Operations*, 11 LEWIS & CLARK L. REV. 1023, 1041 (2007); Sean P. Kanuck, *Information Warfare: New Challenges for Public International Law*, 37 HARV. INT'L L.J. 272, 289 (1996).

[24] *See* Hollis, *supra* note 23.

attack against critical national infrastructure as an armed attack because of the potential for severe consequences if such systems are disabled;[26] and the third, the effects- or consequences-based model, focuses on the overall effect of the cyber attack on the victim state, looking to factors such as severity, immediacy, and directness of harm in order to assess whether the consequences of the cyber attack are of sufficient gravity to render it a use of force or armed attack.[27]

This Comment argues that none of the three primary approaches proposed in the scholarship provide an analytical framework that offers both principled and concrete guidance for assessing cyber attacks under *jus ad bellum*, particularly given the challenges that are unique to this novel form of weaponry. Cyber attacks straddle the boundary lines of the use-of-force analysis described above, confounding application by analogy in weaving a path that falls as easily on one side of demarcation as the other. This Comment aims to deconstruct some of the fallacies that plague the current approaches, demonstrating that none of these models are fully satisfactory to address the difficulties cyber attacks pose for the law of war.

Building on the strengths of each of the three major approaches, this Comment aims to provide a model that is both analytically sound and prospectively useful. It draws from computer science and cyber security research to propose that cyber attacks constitute "armed attack" when they are aimed at causing irreversible disruption or physical damage to a cyber-physical system (CPS), which is a physical system monitored or controlled by computers. Such systems include, for example, electrical grids, antilock brake systems, or a network of nuclear centrifuges. However, if the intended disruption or damage is trivial, or the cyber attack is aimed at causing disruption or damage to computers or networks that do not monitor or control physical systems, the action could be considered an illegal "use of force" or an "armed attack" justifying responsive force, depending on the gravity of the intended or reasonably foreseeable consequences.

This CPS-focused approach resolves many of the rigidity problems of the instrument- and target-based approaches, as well as the malleability problems of the multifactor effects-based approach. At the same time, the CPS-focused approach remains true to one of the primary goals of the UN Charter: to prevent the types of catastrophic, devastating harms that destabilize countries and threaten international peace and security.

[25] *See* David E. Graham, *Cyber Threats and the Law of War*, 4 J. NAT'L SECURITY L. & POL'Y 87, 91 (2010).

[26] *See* WALTER GARY SHARP, SR., CYBERSPACE AND THE USE OF FORCE 129–30 (1999); Sean M. Condron, *Getting It Right: Protecting American Critical Infrastructure in Cyberspace*, 20 HARV. J.L. & TECH. 404, 415–22 (2007); Eric T. Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense*, 38 STAN. J. INT'L L. 207, 228–31 (2002).

[27] *See* 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, 914–15 (1999).

This Comment proceeds as follows: Part I begins by offering an important threshold distinction between the use of computers and computer networks as *instruments* of attack and computers and networks as the *objects* of attack, a distinction that is absent in the literature on cyber attack. Part I critiques the standard definitions, clarifies the instrument/object distinction, and sets out a simple, instrument-based definition for the purposes of the argument. Part II lays out the technical concepts and considerations that influence the use-of-force boundary for cyber attacks and will animate the evaluation of potential analytical frameworks. Part III discusses the governing *jus ad bellum* standards, critiques the leading approaches to assessing cyber attacks under these standards, and proposes a novel framework for analyzing whether a particular instance of cyber attack constitutes a use of force or armed attack under international law.

I.
THE DEFINITION OF CYBER ATTACK

Defining "cyber attack" is a crucial starting point for analyzing the status of cyber attacks under international laws of war. Not only do scholars routinely use terms such as "information warfare,[28] "cyber warfare,"[29] "cyber threats,"[30] "computer network attack,"[31] "cyber operations,"[32] and "information operations"[33] interchangeably with "cyber attacks," they often do so without reference to any particular definition or limitation on scope. They do this, perhaps relying on an intuitive definition, or acting under the assumption that there exists a prevailing standard definition. Such an assumption would be erroneous. In particular, the literature on cyber attack reveals two predominant understandings of the term: some speak of the use of computers and computer networks as *instruments* of attack, and some speak of computers and networks as the *objects* of attack.

These differing conceptions of cyber attack are problematic because they render ambiguous the nature of the operative term "cyber," creating uncertainty in any use-of-force or armed attack analysis. This is particularly evident when one considers the current leading models for such inquiry, models which themselves employ instrumentality, target, and effects as their analytical

[28] *See, e.g.*, Jason Barkham, *Information Warfare and International Law on the Use of Force*, 34 N.Y.U. J. INT'L L. & POL. 57, 57 n.1 (2001) (using the term "Information Warfare" while noting that the terms "cyberwarfare," "cyberattack," and "computer network attack" are "often used interchangeably in the literature").

[29] *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).

[30] *E.g.*, SUSAN W. BRENNER, CYBERTHREATS: THE EMERGING FAULT LINES OF THE NATION STATE (2009).

[31] *See, e.g.*, Schmitt, *supra* note 27.

[32] *See, e.g.*, Michael N. Schmitt, *Cyber Operations and the* Jus Ad Bellum *Revisited*, 56 VILL. L. REV. 569 (2011).

[33] *See, e.g.*, Hollis, *supra* note 23.

foundation. Furthermore, before there can be a discussion about whether a cyber attack falls within these categories, there must be a baseline understanding of what a cyber attack is. That definition will affect the assessment of how valuable a legal framework is (How coherent is the framework? Is it comprehensive? Does it provide a way for state actors to categorize the types of cyber attacks that are most difficult to characterize under international law?). It thus matters greatly whether the term "cyber" describes computers and computer networks as the modes of attack or the objects of attack.

A. Problems with an Object-Based Definition of Cyber Attack

Scholars and policy makers who undertake the task of explicitly defining cyber attack most often do so with reference to computers and networks as the objective, with the word "cyber" characterizing the *object* under attack. In a comprehensive report on U.S. cyber attack capabilities published in 2009, the U.S. National Research Council defined cyber attack as "the use of deliberate actions—perhaps over an extended period of time—to alter, disrupt, deceive, degrade, or destroy adversary computer systems or networks or the information and/or programs resident in or transiting these systems or networks."[34] Until recently,[35] although it did not use the term cyber attack, the U.S. military put forth nearly identical language for "computer network attack": "[o]perations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves."[36] Although the military now uses updated terminology, scholars often cite to or adopt the U.S. military's definition, and the National Research Council likely drew upon it to craft its own, slightly more precise definition.[37] This definition leaves the means or instrumentality of the actions or operations undefined. Instead, it

[34] COMM. ON OFFENSIVE INFO. WARFARE, NAT'L RES. COUNCIL, TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 80 (William A. Owens et al. eds., 2009) [hereinafter NRC CYBERATTACK REPORT].

[35] In 2011, the U.S. Joint Chiefs of Staff developed a joint cyber operations lexicon for use as a "starting point" for updating terminology used in all cyber-related documents as they come up for review. Memorandum from Gen. James E. Cartwright, Vice Chairman of the Joint Chiefs of Staff, to Chiefs of the Military Servs., Commanders of the Combatant Commands, and Dirs. of the Joint Staff Directorates 1 (Nov. 2011), *available at* http://www.nsci-va.org/CyberReferenceLib/2010-11-Joint%20Terminology%20for%20Cyberspace%20Operations.pdf.

[36] JOINT CHIEFS OF STAFF, JOINT PUBLICATION 3-13: JOINT DOCTRINE FOR INFORMATION OPERATIONS (Oct. 9, 1998), *available at* http://www.c4i.org/jp3_13.pdf.

[37] *See, e.g.*, 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 74, 75–76 (Michael N. Schmitt & Brian T. O'Donnell eds., 2002) (adopting the Joint Chiefs' definition "for the sake of convenience" while noting that the definition "sweeps too broadly to be truly useful . . . as a tool of legal analysis"); Jensen, *supra* note 26, at 208 n.3 (using the Joint Chiefs' definition); Schmitt, *supra* note 27, at 888 (same). *But cf.* Condron, *supra* note 26, at 404 n.4 ("[A] cyber attack would refer to an attack using a computer system or network or an attack against a computer system or network.").

focuses on computer systems or networks as the target of an attack conducted through any means.

Commentators proposing their own definitions focus similarly on the object of attack. One has defined cyber war as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption,"[38] and another has defined cyber attack as "any action taken to undermine the function of a computer network for a political or national security purpose."[39] Rather than characterizing the mode of the attack, which is left open, these definitions use the word "cyber" to refer to the *object* of the attack (for example, "actions taken to disrupt or destroy computers and computer networks"). This usage is inadequate because it is at once overbroad, outmoded, and misleading.

The standard definitions for the term "cyber attack" do not qualify the actions or operations that fall under their purview, leading to broad interpretations of the types of actions included. Although computers can be, and often are used to execute attacks targeting other computers, bombs can also destroy computer facilities or transmission lines, and electromagnetic pulse energy can be manipulated to overwhelm computer circuitry or jam communications.[40] Computers and computer networks hold no special legal status relative to other potential targets for destruction,[41] so a missile strike against a computer facility poses no difficult question for international law. Therefore, an analytical framework for assessing the legality of a modern cyber attack need not encompass these more traditional types of attacks, and the framework's value as a policy tool is unaffected by whether or not it addresses these types of attacks.

In addition to encompassing too broad a conception of the mode of attack, the existing definitions also offer a view of the object of attack that is too narrow in light of technological progression. Microprocessors are increasing in performance while decreasing in size and cost.[42] As these chips increase in power, they are also becoming increasingly interconnected through networks.[43]

[38] *See* CLARKE & KNAKE, *supra* note 29.

[39] *See* Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CALIF. L. REV. 817, 821 (2012).

[40] A congressional commission on the threat of electromagnetic pulse (EMP) weapons found that "a high-altitude nuclear burst could emit electromagnetic energy powerful enough to permanently disable many U.S. critical infrastructure computers, and . . . as U.S. military weapons and control systems become more complex, they may be increasingly vulnerable to the effects of EMP." CLAY WILSON, CONG. RES. SERV., HIGH ALTITUDE ELECTROMAGNETIC PULSE (HEMP) AND HIGH POWER MICROWAVE (HPM) DEVICES: THREAT ASSESSMENTS 1 (2008); *see also id.* at 4, 8.

[41] *See generally* Hathaway et al., supra note 39 (proposing a comprehensive cyber attack treaty to address the absence of international law governing cyber attacks).

[42] *See* Skoudis, *supra* note 1, at 148. Processors are also increasing in size: according to Moore's Law, the number of transistors on a microprocessor will roughly double every two years. *Id.* at 149. This increase in chip density leads to increased processor performance and lower cost over time. *Id.*

[43] *Id.*

These trends will facilitate the incorporation of networked computing technology into more and more physical infrastructure, systems, and products—most electrically powered devices will eventually possess some cyberspace functionality.[44] As a result, the target of a cyber attack on a computer network will often be these physical components with which the cyber aspect is tightly interwoven, rather than the network itself.[45] Stuxnet, for example, was not employed in order to disrupt or destroy the programmable logic controllers that regulated Iran's nuclear centrifuges; the objective was to disrupt or destroy the centrifuges themselves.[46] Rather than destroying the computer, this type of cyber manipulation treats the target computer as conduit for an attack on the physical target. A definition centered on the damage to the computer is thus a poor fit.

B. An Instrument-Based Definition of Cyber Attack

The standard definitions create confusion and inconsistency because "cyber attack" intuitively connotes a mode of attack.[47] Thus, rather than defining "cyber attack" by the *object* of attack, it makes more sense to define the term by the *instrument* of attack. Under this reading, the term "cyber attack" may describe the use of cyber operations as a weapon or form of attack, with the word "cyber" characterizing the mode of assault. Just as an "air assault" denotes a military attack using aircraft,[48] or as an "amphibious assault" denotes an assault by land and sea executed on a hostile shore,[49] a "cyber attack" can denote an attack executed by means of a computer or computer network.[50] Here, a cyber attack is an *instrument* or *method* of attack, a *weapon* or *capability* that is used to effectuate a particular objective.

[44] *Id.* at 148.

[45] *See, e.g.*, Broad et al., *supra* note 15 (Stuxnet "was designed to send Iran's nuclear centrifuges spinning wildly out of control.")

[46] *See id.*

[47] An older definition, still used by some, referred to cyber attacks as "computer network attacks," which were often defined as attacks on computer networks. *See* CHAIRMAN OF THE JOINT CHIEFS OF STAFF, *supra* note 36, at GL-5. Scholars writing in this area over the last decade have abandoned the use of "computer network attacks" in favor of the more fashionable prefix "cyber-." *Compare* Schmitt, *supra* note 27, *and* Jensen, *supra* note 26 *with* Schmitt, *supra* note 32, *and* Eric T. Jensen, *Sovereignty and Neutrality in Cyber Conflict*, 35 FORDHAM INT'L L.J. 815 (2012).

[48] JOINT CHIEFS OF STAFF, DEPARTMENT OF DEFENSE DICTIONARY OF MILITARY AND ASSOCIATED TERMS 5 (Apr. 15, 2013), *available at* http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf ("air assault – The movement of friendly assault forces by rotary-wing aircraft to engage and destroy enemy forces or to seize and hold key terrain.").

[49] *Id.* at 14 ("amphibious assault – The principal type of amphibious operation that involves establishing a force on a hostile or potentially hostile shore.").

[50] *Cyber Definition*, MERRIAM-WEBSTER.COM, http://www.merriam-webster.com/dictionary/cyber (last visited May 17, 2013) ("of, relating to, or involving computers or computer networks (as the Internet)").

Scholars often distinguish cyber attack from "kinetic attack," or conventional physical attack.[51] They may do so, for example, by juxtaposing "cyber-attack capabilities, such as inserting malicious computer code" with "kinetic military force,"[52] or by comparing "cyber manipulation of information" to "kinetic attack."[53] This understanding of cyber attack runs parallel to U.S. Department of Defense usage of the term "cyberspace operations," an analogous formulation defining cyberspace operations as "[t]he employment of cyberspace capabilities where the primary purpose is to achieve military objectives in or through cyberspace."[54] The military lexicon may also soon be updated to include "cyber attack," defined 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."[55] This usage conforms with our intuitive sense of "cyber" as referring to the means of attack.

In a discussion of cyber attacks and *jus ad bellum*, construing cyber attack as an instrument of attack, rather than an object of attack, makes sense. The language of *jus ad bellum* relies upon concepts such as scope, duration, and intensity in speaking of the use of force, armed attack, and aggression.[56] These are all concepts bearing more on the type of force exerted against a target than the character of the target attacked. I propose therefore to define cyber attack as a hostile act using computer or related networks or systems to cause disruption or destruction for a political or national security objective. Under this construction, a cyber attack is hostile (as such is the nature of attack) and *uses computers or their networks* to conduct the attack, but leaves open what type of *disruption or damage* it may cause. The attack is constrained only by its political or national security objective, which distinguishes a cyber attack

[51] *See, e.g.*, Commander Todd C. Huntley, *Controlling the Use of Force in Cyber Space: The Application of the Law of Armed Conflict During a Time of Fundamental Change in the Nature of Warfare*, 60 NAVAL L. REV. 1, 11 (2010) ("While such activity may not present an immediate threat to the national security of the [United States] such as that posed by kinetic, physical attacks or cyber attacks that result in destruction of systems and networks, the long-term threat could be even greater."); Jensen, *supra* note 26, at 235 ("Adding to the difficulty, [computer network attacks] can be more problematic to characterize than conventional kinetic weapons.").

[52] 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, 431 (2011) ("Offensive cyber-attack capabilities, such as inserting malicious computer code to take down public or private information systems or functions that rely on them, bear some similarities to kinetic military force, economic coercion, and subversion.").

[53] Graham, *supra* note 25, at 91 ("For example, using th[e effects-based] approach, a cyber manipulation of information across a state's banking and financial institutions significantly disrupting commerce within that state would be viewed as an armed attack. That is, while such an action would bear no resemblance to a kinetic attack, the overall damage that this manipulation of information would cause to the victim state's economic wellbeing would warrant it being equated with an armed attack.").

[54] JOINT CHIEFS OF STAFF, *supra* note 48, at 77.

[55] Memorandum from Gen. James E. Cartwright, *supra* note 35, at 5.

[56] *See* CARR, *supra* note 2, at 58.

subject to international law from a cyber crime subject to domestic law.[57] This definition offers a clearer alternative to existing definitions by specifying that only attacks using computer systems instrumentally, or as the means of attack, will be considered cyber attacks. And in leaving undefined the specific object of the attack, it takes into account a broader range of targets. As the line between cyber and physical is increasingly blurred, it becomes important to include attacks using computers against physical targets within a legal framework governing cyber attacks.

By limiting the effects of a cyber attack to "disruption or damage," this definition also excludes cyber exploitation,[58] or cyber espionage. Cyber exploitation actions and operations do not disturb the normal functioning of a computer system; instead, they leverage cyber capabilities to obtain confidential information otherwise inaccessible to the attacker.[59] These passive intrusions are often referred to as "weapons" of cyber warfare in the media,[60] but they do not rise to the level of belligerence required for war. Because they are a type of espionage, and because they lack an element of force,[61] these activities are legal under international law,[62] even during peacetime.[63] In cyberspace, however, it may be more difficult to actually distinguish a

[57] *Cf.* BRENNER, *supra* note 30, at 29–70 (discussing more precise categories, including cybercrime, cyberterrorism, weapons of mass destruction, weapons of mass distraction, weapons of mass disruption, and cyberwarfare).

[58] *See* Herbert S. Lin, *Offensive Cyber Operations and the Use of Force*, 4 J. NAT'L SECURITY L. & POL'Y 63, 63 (2010) (distinguishing "cyber attack" from "cyberexploitation."). The NRC Cyberattack Report similarly excludes cyber exploitation from its definition of cyber attack. *See* NRC CYBERATTACK REPORT, *supra* note 34, at 10–11.

[59] Lin, *supra* note 58, at 63–64.

[60] *See, e.g.*, Nicole Perlroth, *Virus Infects Computers Across Middle East*, N.Y. TIMES BITS BLOG (May 28, 2012, 3:10 PM), http://bits.blogs.nytimes.com/2012/05/28/new-computer-virus-looks-like-a-cyberweapon/ (describing Flame, a virus that "grabb[ed] images of users' computer screens, record[ed] their instant messaging chats . . . record[ed] their audio conversations and monitor[ed] their keystrokes and network traffic," and Duqu, a virus that also "performed reconnaissance" as "major Internet weapon[s]" and quoting a security expert who stated that Flame "pretty much redefines the notion of cyberwar and cyberespionage").

[61] Roger D. Scott, *Territorially Intrusive Intelligence Collection and International Law*, 46 A.F. L. REV. 217, 223–24 (1999) (noting that "[p]articular forms of espionage, for example by ships, submarines, or aircraft, may raise issues of national self-defense" because they may be perceived as a threat of armed aggression).

[62] *See* Hague Convention (IV) Respecting the Laws and Customs of War on Land, Annex (Regulations), Oct. 18, 1907, art. 24, 36 Stat. 2295, 1 Bevans 643, *reprinted in* DOCUMENTS ON THE LAWS OF WAR (Adam Roberts & Richard Guelf eds., 2d ed. 1989).

[63] *See* Vienna Convention on Diplomatic Relations, Apr. 18, 1961, 500 U.N.T.S. 95; SHARP, *supra* note 26, at 123 (describing state practice as specifically recognizing a right to engage in espionage as an inherent part of foreign relations); Scott, *supra* note 61, at 217 ("[W]hile the surreptitious penetration of another nation's territory to collect intelligence in peacetime potentially conflicts with the customary principle of territorial integrity, international law does not specifically prohibit espionage"). However, espionage is generally illegal under the domestic law of most states. *Id.* at 217–18; *see, e.g.*, Espionage Act of 1917, 18 U.S.C. §§ 792–99 (1990).

permissible act of cyber espionage from a use of cyber force,[64] a complication that can accordingly blur the conceptual and legal distinction between espionage and attack.[65] Exploration of this boundary is beyond the scope of this Comment,[66] which assumes for the purpose of discussion that the nature of a cyber intrusion can be determined with some certainty, as is frequently the case.[67]

Note that this Comment seeks not to provide a comprehensive definition of cyber attack (indeed, the term may rightfully connote different things to different parties and in different contexts). Instead, by identifying and clarifying the definitional ambiguities in the literature, it presents a reasoned justification for rejecting the prevailing definitions in favor of a computer-as-weapon approach for the following discussion.

II.
CYBER ATTACKS: CONTOURS AND TECHNOLOGY

The previous discussion narrowed and clarified the initial scope of our inquiry. Before asking how cyber attacks should be treated under the laws of war, we needed to broadly define what a cyber attack is and is not. This Part explores the mechanisms and technology behind cyber attacks and the particular features of cyber attacks that complicate the application of the laws of war as they have been applied to traditional weaponry. This Part first describes the basic structure of a cyber attack, then introduces the major categories and most common forms of cyber attacks. It then explores the aspects of cyber attacks that distinguish them from conventional military attacks, including the challenges that cyber attacks pose for *jus ad bellum* analysis.

[64] Cyber attacks and cyber espionage use the same technical methodology that begins with exploitation of a system vulnerability. *See infra* Part II.A.

[65] *Cf.* Lin, *supra* note 58, at 84 ("Although espionage has not traditionally been regarded as a use of force, some analysts argue that cyberexploitations against sensitive military or intelligence sites conducted over an extended period and in large volume constitute a demonstration of hostile intent that may indeed violate U.N. Charter provisions prohibiting the use of force.").

[66] For a discussion of issues regarding attack attribution, see BRENNER, *supra* note 30, at 71–126; *cf.* Robert D. Williams, *(Spy) Game Change: Cyber Networks, Intelligence Collection, and Covert Action,* 79 GEO. WASH. L. REV. 1162 (2011) (exploring the distinction between intelligence collection and covert action in cyberspace).

[67] *See, e.g.*, Nicole Perlroth, *Researchers Find Clues in Malware,* N.Y. TIMES, May 31, 2012, at B1 (stating that the Stuxnet virus was "designed to attack industrial control systems," while the Flame and Duqu viruses were designed to assist in information gathering operations).

A. Anatomy of a Cyber Attack

A cyber attack consists of two major components: exploitation of the target's vulnerabilities and delivery of payload.[68] Vulnerabilities are weaknesses that facilitate the attack; they involve a system's susceptibility or flaw,[69] an access path for reaching that flaw,[70] and an attacker's capability to exploit the flaw.[71] The term "payload" describes the actions that can be executed once the vulnerability has been exploited.[72]

Virtually any system may have flaws or other characteristics that render it insecure and susceptible to attack. These may be design or implementation defects introduced inadvertently or intentionally into software,[73] hardware, or the seams between software and hardware.[74] Alternatively, an attacker may masquerade as an authorized user to exploit communications channels, other authorized users and operators, or service providers.[75] The attacker may access these vulnerabilities remotely through networks,[76] or locally through close access, such as insertion of data-carrying external media (such as USB thumb drives), local software or hardware installation (compromised third-party security software), or elsewhere in the system supply chain (during design, development, testing, production, distribution, or maintenance).[77] Nation-states have special advantages that make them particularly capable of exploiting flaws,[78] including special access to source code[79] or hardware components in the supply chain, and resources to invest in cyber operations research or to bankroll the services of hackers-for-hire.[80]

[68] *See* NRC CYBERATTACK REPORT, *supra* note 34, at 83. The NRC Report provides a useful analogy: "In a non-cyber context, a vulnerability might be an easily pickable lock in the file cabinet. Access would be an available path for reaching the file cabinet. . . . The payload is the action taken by the intruder after the lock is picked." *Id.*

[69] *Id.*

[70] *Id.* at 86.

[71] *Cf.* CLARKE & KNAKE, *supra* note 29, at 147–49 (comparing the cyber war strength of the United States, Russia, China, Iran, and North Korea in terms of cyber offense and defense capabilities and cyber dependence).

[72] NRC CYBERATTACK REPORT, *supra* note 34, at 88.

[73] Software has become increasingly susceptible because of its rapid growth in both volume and complexity. *Id.* at 84. These upward trends increase the probability of flaws, and consequently, increase potential opportunities for attack. *See* Skoudis, *supra* note 1, at 156–57.

[74] *See* NRC CYBERATTACK REPORT, *supra* note 34, at 360–67.

[75] *Id.* at 85–86.

[76] *See* JOSEPH MIGGA KIZZA, COMPUTER NETWORK SECURITY AND CYBER ETHICS 62 (2002).

[77] *See* NRC CYBERATTACK REPORT, *supra* note 34, at 87, 102–04. The hundreds of software and hardware components in modern computing technology are manufactured and assembled in countries throughout the world, by companies in North America, Europe, and primarily Asia. Each step in this supply chain is a gateway for the introduction of inadvertent or intentional vulnerabilities. *See* CLARKE & KNAKE, *supra* note 29, at 86–88.

[78] *See* NRC CYBERATTACK REPORT, *supra* note 34, at 93.

[79] *See id.* at 84.

[80] *See* CHARLES G. BILLO & WELTON CHANG, INST. FOR SECURITY TECH. STUD., CYBER WARFARE: AN ANALYSIS OF THE MEANS AND MOTIVATIONS OF SELECTED NATION STATES 107

After an attacker identifies system susceptibilities and access points, he then exploits them to deliver a payload, or the intended malicious action. The payload may include inserting, deleting, altering, or copying data (including code) as well as reproducing and retransmitting itself or self-destructing.[81] It may also be programmed to activate at a certain date and time or when certain conditions are met.[82] If the attacker is able to access the payload through a communications channel, the attacker can remotely update the payload by revising or replacing its instructions.[83] As a result, a computing device may malfunction or report inaccurate information, provide implanted data or information under the guise of authenticity, or fail to be available to its authorized users.[84] If the computer is closely integrated with physical components, the payload can also have physically destructive consequences.

B. The Cyber Attack Arsenal

Cyber attacks come in a number of forms, which fall into two main categories: penetration attacks, which involve intrusion into a system,[85] and denial-of-service (DoS) attacks, which interrupt the services of a system.[86] These methods and their most common incarnations—viruses, worms, Trojans, and bots—are briefly described here. Because the different types of cyber attacks may be treated differently under the various frameworks for assessing the legality of an attack, it is useful to have an understanding of how the most commonly used cyber weapons operate. As this Section describes, cyber weapons that are penetration attacks may have the most destructive potential, while even the most severe denial-of-service attacks are unlikely to cause physical harm.

1. Penetration Attacks

Penetration attacks exploit system vulnerabilities to intrude into a computer system, access its resources, and deliver the intended payload.[87] If the attacker is able to directly penetrate the system, either accessing it locally through security vulnerabilities in a local area network or remotely through an

(2004) (noting that "Russian intelligence services have a history of employing hackers against the United States"); Siobhan Gorman, *Alert on Hacker Power Play*, WALL ST. J., Feb. 21, 2012, at A3 (describing White House discussions about scenarios "in which a foreign government developed the attack capability and outsourced it to a group like Anonymous [a loose affiliation of hackers], or . . . a U.S. adversary like al Qaeda hired hackers to mount a cyberattack").

[81] *See* NRC CYBERATTACK REPORT, *supra* note 34, at 88–89.

[82] *Id.*

[83] *Id.* at 88.

[84] *Id.* at 111–12.

[85] *See* KIZZA, *supra* note 76, at 67.

[86] *Id.* at 48.

[87] *See id.* at 62.

unencrypted wireless network, the attacker can directly access and alter files for a variety of objectives.[88]

One of these objectives may be the implantation of malicious computer code, or malware. Malware "is code or software that is specifically designed to damage, disrupt, steal, or in general inflict some other 'bad' or illegitimate action on data, hosts, or networks."[89] Malware can infect computer systems by exploiting operating system, network device, or software vulnerabilities.[90] It can also trick users into activating the malware by opening an email attachment, downloading a file, viewing an image, or visiting a website.[91] In contrast to direct system penetration, malware does not require immediate direction from the individual attacker to execute hostile actions—the code automatically executes and either replicates through user action or self-propagates, and can thus spread to and attack a much broader range of systems much more quickly than through an attacker's direct manipulation.[92] The speed of malware transmission has increased as network connectivity has grown worldwide,[93] but transmission speed is also affected by the length of time the malware can replicate undetected—if unnoticed, malware may continue to exploit hidden vulnerabilities in the absence of antivirus security patching.[94]

Malware's common forms are likely familiar to the modern computer user, at least in name: viruses, worms, Trojans, and bots.[95] The word "virus" is Latin in derivation, meaning "poison."[96] For centuries it was used only medically to describe a foreign agent that injected itself into the human body, using that body as its host to multiply and spread to other bodies.[97] The term was appropriated to describe malicious computer code that similarly infects a computer system. The malicious code attaches itself to software, using that

[88] *See id.*

[89] *What is the Difference: Viruses, Worms, Trojans, and Bots?*, CISCO SYSTEMS, http://www.cisco.com/web/about/security/intelligence/virus-worm-diffs.html (last visited May 17, 2013) [hereinafter CISCO SYSTEMS].

[90] *Id.*

[91] *Id.*

[92] *See id.*

[93] *See, e.g.*, Guanhua Yan et al., *Malware Propagation in Online Social Networks: Nature, Dynamics, and Defense Implications, in* ASIACCS 2011: PROCEEDINGS OF THE 6TH ACM SYMPOSIUM ON INFORMATION, COMPUTER AND COMMUNICATIONS SECURITY, *available at* http://www.cs.uml.edu/~glchen/papers/socialworm-asiaccs11.pdf (describing the expansion of online social networks as a popular communication infrastructure and the corresponding increase in malware targeting such networks); MCAFEE LABS, MCAFEE THREATS REPORT: FIRST QUARTER 2012, 4–5, http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2012.pdf (reporting on the increase in mobile malware attacks, including malware exploiting the Android mobile phone platform and mobile text messaging).

[94] *See* KIZZA, *supra* note 76, at 67. A security patch is a software update that fixes vulnerabilities that have been discovered. MARK CIAMPA, SECURITY+ GUIDE TO NETWORK SECURITY FUNDAMENTALS 82 (3d ed. 2009).

[95] *See* CISCO SYSTEMS, *supra* note 89.

[96] KIZZA, *supra* note 76, at 63.

[97] *See id.*

software to execute its payload to alter or damage the computer, self-replicate, and spread to other computers[98] when the host file or program to which the virus is attached is intentionally transferred from one computer to another.[99]

Trojans are slight variations on this basic model, differing primarily in the manner in which the malware is spread. Like its namesake, the Trojan Horse, a Trojan "is a harmful piece of software that looks legitimate."[100] Trojans hide within common, trusted files and programs and require that the user invite the malware in by executing these files on their systems.[101] Trojans do not self-replicate, unlike true viruses and worms.[102]

Worms, like viruses, spread through self-replication; however, worms have a different transmission mechanism. While viruses "require the spreading of an infected host file," worms are a type of "standalone software" that replicates independently of a host file or user action.[103] Worms use the computers they infect to seek out other computers to infect: "A worm enters a computer through a vulnerability in the system and takes advantage of file-transport or information-transport features on the system, allowing it to travel unaided."[104] This feature of self-propagation allows worms to spread much more quickly than viruses.[105]

Bots and botnets, yet another category of malware, have been identified as one of the biggest threats to Internet stability and security today.[106] They are particularly powerful tools in the cyber arsenal because they allow an attacker, or "botmaster," to leverage the capabilities of a virtual army of compromised computers surreptitiously enlisted into the bot network, or "botnet," through the use of viruses, Trojans, and worms.[107] The attacker can remotely control these botnets, which consist of hundreds or hundreds of thousands of individual bot, or "zombie," computers through Internet commands.[108] A continuous broadband connection facilitates a communications channel between the

[98] *See id.*

[99] *See* CISCO SYSTEMS, *supra* note 89.

[100] *Id.*

[101] *Id.*

[102] *Id.*

[103] *Id.*

[104] *Id.*

[105] Justin Balthrop et al., *Technological Networks and the Spread of Computer Viruses,* 304 SCIENCE 527 (2004).

[106] *See* JOHN R. VACCA, NETWORK AND SYSTEM SECURITY, at xxx (2010) (describing botnets as "one of the biggest threats to the Internet today" and the source of "[m]ost spam, DDoS attacks, spyware, click fraud, and other [cyber] attacks").

[107] *See* CLAY WILSON, CONG. RESEARCH SERV., RL32114, BOTNETS, CYBERCRIME, AND CYBERTERRORISM: VULNERABILITIES AND POLICY ISSUES FOR CONGRESS 5 (2008).

[108] *Id.*; *see also* Evan Cooke et al., *The Zombie Roundup: Understanding, Detecting, and Disrupting Botnets, in* SRUTI'05: PROCEEDINGS OF THE STEPS TO REDUCING UNWANTED TRAFFIC ON THE INTERNET WORKSHOP (2005), *available at* http://www.eecs.umich.edu/fjgroup/pubs/botnets-sruti05.pdf.

botmaster and his zombie-bots,[109] which may initially sense and probe their immediate environment, examine system files, and relay the information to the botmaster.[110] With the benefit of this information, the botmaster can then upgrade that merely investigatory payload to a destructive payload specifically tailored to the target system.[111] The botmaster also has the flexibility to direct the entire botnet to perform the same action, or assign different bots to perform different actions.[112]

Attackers increasingly use botnets for cyber attacks, not only because of their attack capabilities, but also because of their relative anonymity. An attacker need not have designed the botnet and enlisted the bots himself; botmasters readily make their botnets and technical services available for a fee.[113] The zombie-bots, which are usually infected computers belonging to innocent users around the world, serve as further attack intermediaries that provide a buffer between the botmaster and his targets and conceal the source of attack.[114] Most botnets appearing to date have been organized hierarchically, with a common centralized architecture in which the botmaster sends commands to command-and-control servers that forward the commands to the bots in the network.[115] Recently, however, botnets using a peer-to-peer protocol[116] have emerged, which may make botnets increasingly impervious to defensive measures that rely on shutting down the command-and-control

[109] NRC CYBERATTACK REPORT, *supra* note 34, at 92. The connection need not be constant or immediate for the bots to accept commands; they may execute their initial payload and relay any information or accept new commands once the connection is reestablished. *See id.* at 95.

[110] *Id.* at 96.

[111] *Id.*

[112] *Id.* at 94–95.

[113] WILSON, *supra* note 107, at 5. Wilson cites the example of Jeanson Ancheta, "a 21-year-old hacker and member of a group called the 'Botmaster Underground,' . . . [who] made tens of thousands [of] dollars renting his 400,000-unit 'botnet herd' to other companies that used them to send out spam, viruses, and other malicious code on the Internet." *Id.* at 5. Botnets are also available for rent from their owners for $200–$300 per hour. *Id.* at 6; *see also Cybersecurity: Assessing the Immediate Threat to the United States: Hearing Before the Subcomm. on Nat'l Sec. Homeland Def. and Foreign Operations of the H. Comm. on Oversight and Gov't Reform*, 112th Cong. 27 (2011) (prepared statement of James A. Lewis, Director, Technology and Public Policy Program, Center for Strategic and International Studies) ("The future will be the "'commoditization' of advanced attack techniques that will enable a range of groups to consider cyber attack as an option.").

[114] *See* NRC CYBERATTACK REPORT, *supra* note 34, at 94.

[115] *See* Julian B. Grizzard et al., *Peer-to-Peer Botnets: Overview and Case Study, in* HOTBOTS'07: PROCEEDINGS OF THE FIRST WORKSHOP ON HOT TOPICS IN UNDERSTANDING BOTNETS, (2007), *available at* http://static.usenix.org/event/hotbots07/tech/full_papers/grizzard/grizzard.pdf (noting that peer-to-peer architecture is "beginning to appear" and requires no centralized coordination point); Ping Wang et al., *An Advanced Hybrid Peer-to-Peer Botnet*, *in* HOTBOTS'07: PROCEEDINGS OF THE FIRST WORKSHOP ON HOT TOPICS IN UNDERSTANDING BOTNETS, (2007), *available at* http://static.usenix.org/event/hotbots07/tech/full_papers/wang/wang.pdf.

[116] *See* Grizzard, *supra* note 115, at 2 ("A peer-to-peer network is a network in which any node in the network can act as both a client and a server.").

servers.[117] With a peer-to-peer architecture, such a botnet would be difficult to defeat because the control nodes would be decentralized; even if one node were taken offline, the botnet would continue to operate under the attacker's command.[118]

2. Denial-of-Service Attacks

Aside from the penetration attack, the other main category of cyber attack is the DoS attack. In contrast to penetration attacks, DoS attacks do not modify or destroy computer system resources.[119] Instead, they disrupt the system by diminishing its functionality. Large-scale DoS attacks can bring a system down, making it completely inaccessible to legitimate users.[120] DoS attacks work by "flood[ing] a specific target with bogus requests for service, thereby exhausting the resources available to the target to handle legitimate requests for service and thus blocking others from using those resources."[121] Since attacks coming from a single source can easily be blocked by denying all requests from that source, attackers employ botnets to conduct distributed denial-of-service (DDoS) attacks from multiple machines.[122] Because the requests in a DDoS attack are dispersed among a diversity of users rather than concentrated at any one source, the server is unable to distinguish between attacker-bots and legitimate users attempting to access the computer.[123] The attacks cannot therefore be easily blocked simply by denying requests from any single source.[124]

DDoS attacks were initially regarded as "nuisance attacks" that "simply interrupt the services of the system."[125] However, as the size of such attacks has grown and societal dependence on technology has risen, they have increased in their potential to inflict significant damage. For example, in a 2007 DDoS attack against Estonia, an estimated one million zombie computers were used as part of several coordinated botnets, each controlling tens of thousands of bot computers that flooded the websites of government, media, and financial organizations.[126] The attack rendered the sites inaccessible for hours at a

[117] *See id.* at 1 ("Presently, the centralized characteristic of botnets is useful to security professionals because it offers a central point of failure for the botnet. In the near future, we believe attackers will move to more resilient architectures [such as] . . . peer-to-peer based architectures.").

[118] *See id.* (explaining that peer-to-peer networks contain no centralized coordination point that can be incapacitated, and that if one node is taken offline the network continues to operate).

[119] KIZZA, *supra* note 76, at 76.

[120] *See id.*

[121] NRC CYBERATTACK REPORT, *supra* note 34, at 95.

[122] *See id.*

[123] *See id.*

[124] *See id.*

[125] *See* KIZZA, *supra* note 76, at 48; *see also* CLARKE & KNAKE, *supra* note 29, at 13.

[126] BRENNER, *supra* note 30, at 2–4.

time.[127] Some described the attack as particularly "crippling" because Estonia relies heavily on information technology.[128] As such dependence increases across society, the impact of large-scale DDoS attacks is also likely to grow.

C. Cyber Attack's Challenges

The drafters of the UN Charter may not have foreseen that computer code could one day be exploited for purposes so destructive that the attacks might be classified as war. However, it is not simply the novelty of the technology at issue that perplexes the application of law in this context. Cyber attacks challenge traditional notions of warfare because, compared to traditional weapons, worms, viruses, and botnets may have a scope of impact that is potentially far broader; their effects may be highly unpredictable; their payload may often be reversible; and they may be difficult to attribute to a particular source. This Part explores these factors, which will animate the discussion of *jus ad bellum* legal frameworks in Part III.

1. Scope of Effects

As Part I noted, the destructive objective of a cyber attack often does not center on direct damage or disruption to the computer system or network itself, but on the cyber attack's indirect effects.[129] The attack may have the immediate aim of flooding a web server, modifying or deleting code that the system runs, or altering data stored on the computer. But the larger objective of launching the cyber attack will often be its effects on the systems or devices controlled by the targeted computer or on the human decision making that depends on information contained within or processed by the targeted computer.[130] Stuxnet, for example, was not so much an attack on the Natanz facility's programmable logic controllers, or the SCADA (supervisory control and data acquisition) software running on them, but on the centrifuges these computer systems controlled.[131] By damaging the centrifuges, the attack compromised Iran's uranium enrichment capabilities, slowing the progress of its nuclear weapons development program.[132]

[127] Christopher Rhoads, *Cyber Attack Vexes Estonia, Poses Debate*, WALL ST. J. (May 18, 2007), http://online.wsj.com/article/SB117944513189906904.html.

[128] WILSON, *supra* note 107, at 7.

[129] NRC CYBERATTACK REPORT, *supra* note 34, at 80 ("Direct or immediate effects are effects on the computer system or network attacked. Indirect or follow-on effects are effects on the systems and/or devices that the attacked computer system or network controls or interacts with, or on the people that use or rely on the attacked computer system or network.").

[130] *Id.*

[131] *See* Chen, *supra* note 14, at 2 (stating that unlike previous attacks that were aimed at computer systems, Stuxnet attempted to take control of physical infrastructure.).

[132] *See* Sanger & Mazzetti, *supra* note 19 (noting that the attacks caused 1,000 of 5,000 centrifuges Iran was using to purify uranium to temporarily stop functioning).

What matters is not so much the fact that cyber attacks have indirect effects, but instead that these effects are removed from the actors and acts that caused them. Any attack, cyber or kinetic, will likely carry with it indirect effects in multiple degrees;[133] in either form of attack, nation-state attackers will seek out consequences that advantageously bear on their political or national security goals. In this way, the cyber attack effects chain might well resemble that of a kinetic attack. The difference is a cyber attack's origin. Where traditional military attacks often require risk of physical harm to the attacker or investment in sophisticated, resource-heavy weapons-development programs, there is a disconnect between the acts required to launch cyber attacks and the magnitude of their potential effects. Only a snippet of code, for example, can delete an entire hard drive.[134] Cyber attacks are also weapons in their developmental infancy,[135] so their power as a tool for warfare, while real, is still largely hypothetical. As a result, the scope of disruption and damage is potentially wider, the risk of collateral damage potentially steeper, and the uncertainty of consequences potentially greater.

The unrestrained scope of cyber attacks is due in part to the self-propagating and nondiscriminating nature of these attacks. As we have seen, cyber attacks are often conducted through the use of botnets and malware, engaging malicious computer code that automatically replicates itself and infects other systems rapidly and without discrimination. In January 2003, the Sapphire (or Slammer) worm spread worldwide via Internet-connected computers, doubling in size every 8.5 seconds and infecting at least seventy-five thousand computers, or more than 90 percent of vulnerable hosts within ten minutes.[136] And in 2008 and 2009, the Conficker worm infected an estimated five million or more personal computers in over two hundred countries, enlisting the compromised computers into a massive botnet.[137] Conficker has not yet caused any damage beyond nuisance spam, but it remains lurking in millions of computers, occasionally checking in with its command-and-control center for updates with latent destructive potential.[138] Unlike a

[133] For example, bombing a stock exchange would surely have as significant indirect effects on the stability of financial systems and markets and the people who rely on them, as would the deletion or erasure of data in the computers systems controlling the stock market exchange.

[134] Eight characters, to be precise. The UNIX command "rm –rf /" will automatically delete all files, directories, and subdirectories. *See* ARNOLD ROBBINS, UNIX IN A NUTSHELL 174 (4th ed. 2005).

[135] The first Internet worm was released in November 1988, the work of Robert T. Morris, a Cornell graduate in computer science. *See* Hilarie Orman, *The Morris Worm: A Fifteen-Year Perspective*, 1 IEEE SECURITY & PRIVACY, Sept.–Oct. 2003, at 35.

[136] *See* DAVID MOORE ET AL., COOPERATIVE ASS'N FOR INTERNET DATA ANALYSIS, THE SPREAD OF THE SAPPHIRE/SLAMMER WORM (Jan. 2003), *available at* http://www.caida.org/publications/papers/2003/sapphire/sapphire.html.

[137] *See* John Markoff, *Defying Experts, Rogue Code Lurks in World's Computers*, N.Y. TIMES, Aug. 27, 2009, at A1.

[138] *See* Mark Bowden, *The Enemy Within*, THE ATLANTIC, June 2010, at 72.

directed kinetic attack, such a worm cannot be geographically contained. It operates by exploiting a system vulnerability, like those in computers running the Microsoft SQL Server (as with the Sapphire worm), or the Windows operating system (as with Conficker), which may be present in individual computer systems and networks worldwide.[139] And even where the malware is intended to infect only a closed network or is highly selective in its targeted systems (Stuxnet, for example, targeted only a particular programmable logic controller made by Siemens on vulnerable Windows computers),[140] even a chance circumstance or minor coding error can result in global propagation.[141]

The same features of cyber attacks that lead to their unrestrained scope also create the potential for such an attack to result in similarly unrestrained damage to systems beyond the intended attack target.[142] In the course of its rapid propagation, for example, the Sapphire worm took down servers in South Korea, the suspected target of the attack,[143] but its consequences were more wide-ranging. Sapphire also disrupted internet services in Thailand, Japan, Malaysia, the Philippines, and India;[144] disconnected a city's 911 emergency service and caused problems for thirteen thousand Bank of America ATMs in the United States;[145] postponed a Canadian national election;[146] and cancelled airline flights.[147] Researchers studying Sapphire stated that, "if the worm had carried a malicious payload, had attacked a more widespread vulnerability, or had targeted a more popular service, the effects would likely have been far

[139] *See, e.g.*, MOORE ET AL., *supra* note 136.

[140] *See* Chen, *supra* note 14, at 2.

[141] *See, e.g.*, Orman, *supra* note 135, at 37 (describing the "overly aggressive" and "rampant" behavior of the Morris Worm); Sanger *supra* note 17 ("In the summer of 2010, shortly after a new variant of the [Stuxnet] worm had been sent into Natanz, it became clear that the worm, which was never supposed to leave the Natanz machines, had broken free. . . . An error in the code . . . had led it to spread to an engineer's computer when it was hooked up to the centrifuges. When the engineer left Natanz and connected the computer to the Internet, the American- and Israeli-made bug failed to recognize that its environment had changed. It began replicating itself all around the world.").

[142] *See* NRC CYBERATTACK REPORT, *supra* note 34, at 122 ("[I]n analyzing the possible effects of a cyberattack, there may be no good analog to the notion of a lethal radius within which any target will be destroyed. When computer systems are interconnected, damage to a computer at the NATO Defense College in Italy can propagate to a computer at the U.S. Air Force Rome Laboratory in New York – and whether or not such a propagation occurs depends on a detail as small as the setting on a single switch, or the precise properties of every device connected at each end of the link, or the software characteristics of the link itself.").

[143] *See* John McCormick, *Lock IT Down: Sapphire/Slammer Worm Attacks SQL Server and the Internet*, TECHREPUBLIC (Jan. 28, 2003, 8:00 AM), http://www.techrepublic.com/article/lock-it-down-sapphireslammer-worm-attacks-sql-server-and-the-internet/1058309.

[144] *See Virus-like Attack Hits Web Traffic*, BBC NEWS, (Jan. 25, 2003), http://news.bbc.co.uk/2/hi/technology/2693925.stm.

[145] *See* Bruce Schneier, *Blaster and the Great Blackout*, SALON (Dec. 16, 2003), http://www.salon.com/2003/12/16/blaster_security.

[146] *See* Editorial, *Shielding Cyber-Space*, L.A. TIMES (Feb. 15, 2003), http://articles.latimes.com/2003/feb/15/opinion/ed-cyber15.

[147] *See id.*

more severe."[148] Malware generally delivers its payload automatically and without direction from its originator.[149] Under these circumstances, the attacker cannot scale back or halt the extent of damage once the malware is released—the damage spreads as surely as the virus or worm spreads—and an attack on systems in South Korea becomes an attack on systems in Thailand and Japan, Canada and the United States.

By the same token, a cyber attack targeting military cyber resources easily becomes an attack on civilian cyber resources. An estimated 98 percent of U.S. Government communications, both classified and unclassified, travel over civilian networks and systems.[150] The vast majority of computer hardware and software used by the U.S. Government, including its information security products, is also procured from and serviced by civilian companies.[151] And the military is increasingly dependent on commercial off-the-shelf (COTS) software.[152] These trends enhance the risk of collateral damage even in a cyber attack aimed specifically at military objectives, as such an attack can easily spread to civilian systems carrying the same vulnerabilities.[153] As one author explains, "what may seem a precisely targeted disabling of a software module on a military computer may have profound consequences on civilian computers that happen, unknown to attackers, to use that same module."[154]

[148] MOORE ET AL., *supra* note 136.

[149] See *supra* Part II.B.1.

[150] Eric Talbot Jensen, *Cyber Warfare and Precautions Against the Effects of Attacks*, 88 TEX. L. REV. 1533, 1534, 1542 (2010) (citing Michael McConnell, Former Dir. of Nat'l Intelligence, Keynote Address at the Texas Law Review Symposium: Law at the Intersection of National Security, Privacy, and Technology (Feb. 4, 2010)).

[151] *Id.* at 1543–44.

[152] "COTS software refers to software which is not specifically developed for military or governmental use, and is instead purchased 'as is' from an external vendor." Luke Ho & Anthony Atkins, *Security of Software Outsourcing in Military and Government Agencies*, *in* PROCEEDINGS OF THE IADIS INTERNATIONAL CONFERENCE ON WWW/INTERNET 347, 348 (2005). Ho and Atkins describe examples of increased COTS software-related use by the military as including "the Aegis Weapon System which incorporates an entirely COTS advanced processing architecture . . . and the Airborne Warning and Control System (AWACS) mission computer upgrade involving COTS operating system software" as well as the "increasing trend in the adaptation of COTS game software for military simulation." *See id.*

[153] Though not a focus of this Comment, reliance on civilian companies to supply and service government and military cyber resources implicates the *jus in bello* requirement of distinction between civilian and military targets, as it "brings the premises and objects used by these civilian companies potentially within the [legal] targeting options of an attacking enemy as well." Jensen, *supra* note 150, at 1544; *see also* Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) art. 58, *opened for signature* Dec. 12, 1977, 1125 U.N.T.S. 3, 29 [hereinafter Geneva Protocol Additional] (requiring that parties in conflict protect civilians within their control from the destructive effects of military operations).

[154] Neil C. Rowe, *Ethics of Cyber War Attacks*, *in* CYBER WARFARE AND CYBER TERRORISM 105, 107 (Lech J. Janczewski & Andrew M. Colarik eds., 2008).

2. Unpredictability

Even the first-order effects of a cyber attack can be highly unpredictable. The designer of the first Internet worm, Robert T. Morris, created the worm without malicious intent, "to try to discover how large the Internet was at the time."[155] The Morris worm, as a result of a coding design error, replicated far more quickly than intended and produced a DoS attack against the entire Internet (which also resulted in an estimated $10 million to $100 million in damage).[156]

Although malware propagated by nation-states in a cyber attack is likely to be narrowly tailored to meet its military objectives, even code containing strict controls on timing and conditions of attack, or possessing a communications channel with a command-and-control center that can update the payload, can have errors in coding or implementation that produce uncertain results.[157] Indeed, compared to other forms of (legitimate) software, malware is more likely to have coding or implementation bugs because of the inherent inadequacy of pre-deployment testing. The malware's targeted environment often is not and cannot be accurately reproduced before the malware is released. And in contrast to kinetic attacks, cyber attacks require intelligence information that is difficult to obtain through traditional intelligence methods (such as remote photo reconnaissance).[158] These uncertainties amplify the likelihood that a cyber attack will have unintended or unanticipated consequences.[159]

The Stuxnet worm demonstrates the degree of unpredictability latent in cyber attacks. Although intricately designed and carefully executed, Stuxnet was not impervious to coding error, despite having been tested on American-built replicas of Iran's P-1 centrifuges at several of the U.S. Energy Department's national laboratories.[160] But the replicas were simply that—replicas, approximations based on some P-1 centrifuges the United States had purchased from Libya in 2003.[161] According to the U.S. National Research Council, "[t]he smallest change in the configuration and interconnections of an IT system can result in completely different system behavior," and a cyber

[155] JEREMY FAIRCLOTH & CHRIS HURLEY, 2 PENETRATION TESTER'S OPEN SOURCE TOOLKIT 520 (2007).

[156] *Id.* at 520–21. As one commenter noted, he "should have tried it on a simulator first." *Id.* at 521.

[157] Another risk on the horizon that would create uncertainty is that as malware code development progresses, a computer virus, like its biological counterpart, may eventually be able to evolve new functionalities and change its behavior autonomously. *See* DIMITRIS ILIOPOULOS ET AL., PROCEEDINGS OF VIRUS BULLETIN CONFERENCE, DARWIN INSIDE THE MACHINES: MALWARE EVOLUTION AND THE CONSEQUENCES FOR COMPUTER SECURITY 187 (2008), *available at* http://arxiv.org/pdf/1111.2503v1.pdf.

[158] NRC CYBERATTACK REPORT, *supra* note 34, at 49.

[159] *Id.*

[160] *See supra* note 141 and accompanying text.

[161] Sanger & Mazzetti, *supra* note 19.

attack's effects on a system "may be driven by the behavior and actions of the human system operator and the specific nature of that system as well as the intrinsic characteristics of the cyberweapon involved."[162]

The exact conditions at Iran's Natanz nuclear plant were unknown, and once Stuxnet was released, a programming error allowed the worm, meant to be confined to the plant, to spread to an engineer's computer, and then around the world.[163] Fortunately, Stuxnet had a very narrowly targeted payload, executing only on machines running Siemens software, interfaced with a programmable logic controller connected to a certain kind of machinery, and under specific conditions.[164] But less carefully tailored malware could have attacked control systems globally, irreversibly damaging physical infrastructure in a number of countries with catastrophic results.

3. Reversible Damage

Cyber attacks are notable because their direct effects, unlike those of kinetic attacks, are often temporary or reversible.[165] As opposed to undoing the damage of an exploded missile, additions, deletions, and modifications to code caused by penetration attacks and malware can usually be reversed. And lost or corrupted electronic data can often be restored, as contemporary norms of electronic data storage dictate redundancy; backup copies of important data are made so that originals can be recovered after a data loss event. For DoS attacks, the loss of access is temporary as well; as soon as the attacker stops flooding the computer system with requests for service, normal service can resume.[166] The computer system or network usually emerges unscathed.

It is the indirect effects of a cyber attack that are generally irreversible, and producing irreversible damage is often the objective of a cyber attack.[167] For instance, while the most common cases of DoS attacks will result in simple annoyance or inconvenience, with users unable to access a website for hours or days, a DoS attack on an emergency response service can prevent people from getting timely assistance, and a DoS attack on a hospital can disrupt the provision of medical service.[168] While data can be recovered or system access

[162] NRC CYBERATTACK REPORT, *supra* note 34, at 122.

[163] Sanger & Mazzetti, *supra* note 19.

[164] *See* Michael Joseph Gross, *A Declaration of Cyber-War*, 53 VANITY FAIR, Apr. 2011, at 152.

[165] *See* Martin Libicki, *Pulling Punches in Cyberspace*, *in* PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR U.S. POLICY 123, 124, 129 (2010), *available at* http://cs.brown.edu/courses/csci1800/sources/lec19/Libicki.pdf.

[166] See *supra* Part II.B.2.

[167] NRC CYBERATTACK REPORT, *supra* note 34, at 113.

[168] For example, in 2005, a botnet attacked a Seattle hospital, shutting down computers in the intensive care unit and causing operating room doors and doctors' pagers to malfunction. *See* Susan W. Brenner, *"At Light Speed": Attribution and Response to Cybercrime/Terrorism/Warfare*, 97 J. Crim. L. & Criminology 379, 397–98 (2007). In this particular case, these results were unintentional—

restored, delay or disruption in health care services can result in death or irreversible bodily harm to those whose life or wellness depends on the timely provision of medical care.

Compared to DoS, malware has even more power to cause the indirect effect of permanent loss, as computers control many components of critical infrastructure and industrial processes. Malware can change pressure in gas lines to cause fires and explosions, shut down cooling systems so that generators overheat, open a dam's spillway to flood neighboring communities,[169] and direct nuclear centrifuges to malfunction and self-destruct. The prospect of an attacker using a computer to remotely destroy physical infrastructure is no longer a purely theoretical doomsday exercise, plausible in concept but unrealistic in practice: the Stuxnet worm demonstrated that a malware infection can cause large-scale, tangible damage. While "[p]revious cyberattacks had effects limited to other computers," said Michael V. Hayden, the former chief of the Central Intelligence Agency, "[Stuxnet] is the first attack of a major nature in which a cyberattack was used to effect physical destruction."[170]

4. Anonymity and the Problem of Attribution

As others have explored,[171] attributing a cyber attack to a particular source is one of the most significant challenges for policing such attacks, as cyber attacks can be perpetrated with a degree of anonymity orders of magnitude beyond that of a kinetic attack. In the context of force, armed attack, and aggression by nation-states, a kinetic attack can almost always be easily traced to a geographical source: the country that authorized the attack, owns the weapons used to conduct the attack, and whose distinctive national insignias adorn the uniforms and equipment used in the attack.[172] As one scholar has noted, "the approaches we use to identify attackers implicitly assume territorially-based activity in the physical world."[173] But in cyberspace, the

the botmaster was attempting to use the botnet to install adware on computers—so the attack was brief; hospital staff were able to work around the problems, so the attack did not cause lasting damage. *Id.* at 397.

[169] *See* Charles Jaeger, *Cyberterrorism and Information Security*, *in* GLOBAL PERSPECTIVES ON INFORMATION SECURITY: LEGAL, SOCIAL, AND INTERNATIONAL ISSUES 127, 130 (Hossein Bidgoli ed., 2009) (describing several potentially lethal acts of cyber terrorism).

[170] Sanger & Mazzetti, *supra* note 19.

[171] *See, e.g.*, BRENNER, *supra* note 30, at 71–161 (discussing both attack attribution and attacker attribution); JEFFREY HUNKER ET AL., INST. FOR INFO. INFRASTRUCTURE PROT., ROLE AND CHALLENGES FOR SUFFICIENT CYBER-ATTACK ATTRIBUTION, (Jan. 2008), *available at* http://www.thei3p.org/docs/publications/whitepaper-attribution.pdf; LIPSON, *supra* note 3, 1–23 (explaining the difficulty with tracking and tracing cyber attackers); David D. Clark & Susan Landau, *Untangling Attribution*, 2 HARV. NAT'L SEC. J. 323 (2011); Duncan B. Hollis, *An e-SOS for Cyberspace*, 52 HARV. INT'L L.J. 373, 397–403 (2011).

[172] *See* BRENNER, *supra* note 30, at 128.

[173] Brenner, *supra* note 168, at 409.

territorial point of attack origin is not only inconclusive, but often misleading—assuming the attack can even be accurately traced to its origin. These facts make cyber attack attribution particularly problematic.

Information on the Internet is carried in packets of data that contain source and destination Internet Protocol (IP) addresses, identifying from where the packet came and where it is headed.[174] But because these packets are often transmitted without mechanisms to authenticate their origin, the source IP address can easily be forged, or "spoofed," to conceal the sender's identity.[175] Thus, spoofing allows an attacker to hide his location and makes it difficult for others to accurately trace a cyber attack to its source. More complex cyber attacks that require a two-way communications channel do not rely on IP spoofing (which would prevent a reply from reaching the sender) but rely on a chain of intermediaries.[176] For example, botmasters create command-and-control centers that direct the bot army. These centers act as barriers that shield the originator of the attack from detection, while the innocent computer systems drafted into the botnet serve at the front lines of attack.

Although technical attribution may be difficult, the origin of an attack may still be identified. IP addresses are not the sole source of attribution. Investigators can also consider information from political sources, such as a nation's intelligence agencies and diplomatic representatives; other technical signatures, such as similarity to malware with known origin or the use of identical programming languages and distinctive coding sequences; and temporal proximity to other coercive or aggressive actions that can be attributed to a particular source.[177] But even if the computer or server of origin is identified, further complications remain. A nation-state may deny culpability entirely, ascribing responsibility for the cyber attack to individual criminals or hacktivists. In response, some scholars have proposed that states should bear responsibility for cyber attacks that originate within their territory,[178] or where the state provides sanctuary for the attackers.[179] This is an approach analogous to the one taken by the United States to justify its invasion of Taliban-controlled Afghanistan, which harbored the Islamic militant group Al Qaeda

[174] *See* Clark & Landau, *supra* note 171, at 326.

[175] *See* KIZZA, *supra* note 76, at 41.

[176] *See* Clark & Landau, *supra* note 171, at 327.

[177] NRC CYBERATTACK REPORT, *supra* note 34, at 140–41; Hollis, *supra* note 171, at 399–400.

[178] *See, e.g.*, Graham, *supra* note 25, at 92–93 (seeking to impute responsibility to states for attacks originating from that state's territory); Scott J. Shackelford, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, 27 BERKELEY J. INT'L L. 192, 231–34 (2009).

[179] *See* Graham, *supra* note 25, at 94–96 ("Thus, a sanctuary state's benign indifference to cyber attacks continuously launched from within its borders, its failure to investigate and prosecute those responsible, and its refusal to cooperate with the efforts of victim states to deter such attacks leave it vulnerable to charges of imputed responsibility for these actions.").

that was responsible for the 9/11 World Trade Center and Pentagon attacks.[180] In short, although determining the source of a cyber attack may occasionally be problematic, attribution to a state actor is often quite possible.[181]

This Comment assumes for the purposes of discussion that, based on these techniques or otherwise, responsibility for a cyber attack can been attributed to a state actor.

D. An Evolving Cyberspace

Technology tends to innovate more quickly than cyber security solutions can support, leaving emergent information systems and technologies especially vulnerable to attack. Two long-standing computing trends, in particular, have both increased opportunities for would-be attackers and raised the stakes of potential attacks. First, improvements in processor design and performance have facilitated integration of computer systems and physical processes, allowing the cyber system to automate, control, and monitor the physical components. Second, the rapid proliferation of broadband and wireless networks has fueled unprecedented interconnectivity. Together, they also amplify the danger of modern cyber attacks. This Section explores these two highly significant areas of development, which provide the foundation for the cyber-physical system-oriented approach to the *jus ad bellum* framework that this Comment proposes.

1. Cyber-Physical Convergence and Network Connectivity

In 2001, the National Research Council (NRC) asserted that "[i]nformation technology is on the verge of another revolution."[182] This revolution is driven by continuing reductions in the size and cost of microprocessors, reductions which enable the embedding of computing technology in other devices.[183] According to the NRC, "networked systems of

[180] The test under international law is that the state to which an attack might be attributed must have been "unwilling or unable" to suppress the threat. *See* Ashley S. Deeks, *"Unwilling or Unable": Toward a Normative Framework for Extraterritorial Self-Defense*, 52 VA. J. INT'L L. 483 (2012).

[181] *Cf. Department of Defense Authorization for Appropriations for Fiscal Year 2014 and the Future Years Defense Program: Hearing Before the S. Comm. on Armed Servs.*, 113th Cong. (2013) (prepared statement of Gen. Keith B. Alexander, Commander U.S. Cyber Command), *available at* http://www.armed-services.senate.gov/statemnt/2013/03%20March/Alexander%2003-12-13.pdf ("State actors continue to top [Cyber Command's] list of concerns. We feel confident that foreign leaders believe that a devastating attack on the critical infrastructure and population of the United States by cyber means would be correctly traced back to its source and elicit a prompt and proportionate response.").

[182] COMM. ON NETWORKED SYS. OF EMBEDDED COMPUTERS ET AL., NAT'L RES. COUNCIL, EMBEDDED, EVERYWHERE: A RESEARCH AGENDA FOR NETWORKED SYSTEMS OF EMBEDDED COMPUTERS 1 (2001) [hereinafter NRC EMBEDDED SYSTEMS REPORT].

[183] *See* Marjory S. Blumenthal & David D. Clark, *The Future of the Internet and Cyberpower*, *in* CYBERPOWER AND NATIONAL SECURITY 206, 213 (Franklin D. Kramer et al. eds., 2009); Skoudis, *supra* note 1, at 148; *see also supra* note 42 and accompanying text.

embedded computers . . . have the potential to change radically the way people interact with their environment by linking together a range of devices and sensors that will allow information to be collected, shared, and processed in unprecedented ways."[184]

In a sense, the information technology revolution the NRC predicted is well underway, as most computers in use today are components of such embedded systems.[185] The "embedded systems" terminology has given way to the more modern term "cyber-physical systems" (CPS), which emphasizes the link to physical systems.[186] But the concept is, in essence, unchanged: CPS are "physical and engineered systems whose operations are monitored, coordinated, controlled and integrated by a computing and communication core"—systems involving an "intimate coupling between the cyber and physical."[187] Cyber-physical systems can expand the capabilities of the physical world by enhancing safety, efficiency, consistency, and reliability. Forms of CPS are already employed in a broad range of civil and national security applications: automotive electronics (e.g., air bag control systems, antilock braking systems, engine control systems, and global positioning satellite systems); avionics (e.g., flight control systems and anti-collision systems);[188] health and medical equipment (e.g., pacemakers); industrial automation (e.g., manufacturing, fabrication, and power generation); and critical infrastructure control (e.g., energy management systems and supervisory control and data acquisition (SCADA) systems that monitor and control oil and gas pipelines, electrical power grids, and water treatment and distribution).[189] So integral are cyber-physical systems to the future of industrial and technological development that the National Science Foundation has identified CPS as a top

[184] NRC EMBEDDED SYSTEMS REPORT, *supra* note 182, at 1.

[185] CPS STEERING GROUP, CYBER-PHYSICAL SYSTEMS EXECUTIVE SUMMARY 1 (Mar. 6, 2008), *available at* http://iccps2012.cse.wustl.edu/_doc/CPS-Executive-Summary.pdf; *cf.* Stefan Savage, *In Planning Digital Defenses, the Biggest Obstacle Is Human Ingenuity*, N.Y. TIMES, Dec. 6, 2011, at D10, http://www.nytimes.com/2011/12/06/science/stefan-savage-girding-for-digital-threats-we-havent-imagined-yet.html (explaining that computer attacks such as the Stuxnet worm are "a particularly troubling precedent because computing capabilities are now embedded in virtually every aspect of our lives").

[186] *See* PETER MARWEDEL, EMBEDDED SYSTEM DESIGN: EMBEDDED SYSTEMS FOUNDATIONS OF CYBER-PHYSICAL SYSTEMS, at xiii (2d ed. 2011).

[187] Ragunathan Rajkumar et al., *Cyber-Physical Systems: The Next Computing Revolution*, *in* PROCEEDINGS OF THE 47TH DESIGN AUTOMATION CONFERENCE 731, 731 (2010). More precisely:

> [A CPS is a system] in which computation/information processing and physical processes are so tightly integrated that it is not possible to identify whether behavioral attributes are the result of computations (computer programs), physical laws, or both working together; where functionality and salient system characteristics are emerging through the interaction of physical and computational objects; in which computers, networks, devices and their environments in which they are embedded have interacting physical properties, consume resources, and contribute to the overall system behavior.

CPS STEERING GROUP, *supra* note 185, at 8.

[188] MARWEDEL *supra* note 186, at 1.

[189] Blumenthal & Clark, *supra* note 183, at 215.

national priority for federal research and development.[190] Combined with the underlying trend of smaller, faster, and less expensive computer chips, this recent focus on and investment in CPS research will serve as catalyst for increasing cyber-physical integration and CPS ubiquity.

As computers have become more tightly interwoven with the physical world, they have also become increasingly interconnected in networks. Between 1993 and 2003, the number of Internet hosts (users) grew from approximately 1.3 million to 171.6 million.[191] Over the last decade, that number has multiplied five-fold; as of July 2012, over 908.6 million computers were connected to the Internet.[192] More people, devices, and applications can connect to the Internet due to widespread deployment of broadband services enabling connectivity at faster speeds.[193] The proliferation of wireless technology is also transforming communications technology, as untethering computers from wired connections makes them available for use in a wider variety of applications.[194] But while increased networking has resulted in a host of societal benefits, it has also made cyber-physical systems vulnerable to cyber attacks.

2. Vulnerabilities, Revisited

Cyber-physical systems may make particularly attractive targets for cyber attacks precisely because such attacks have the ability to cause physical devastation. The attacker arrives silently, unseen, and with the power to order devices to self-destruct. As computers become more pervasive, interconnected, complex, and tightly linked with physical components, creating networked cyber-physical systems out of previously purely mechanical devices, the number and variety of potential targets multiply.

Similar to trends elsewhere in computing technology, modern cyber-physical control systems are using increasingly complex software with greater

[190] PRESIDENT'S COUNCIL OF ADVISORS ON SCI. & TECH., EXEC. OFFICE OF THE PRESIDENT, LEADERSHIP UNDER CHALLENGE: INFORMATION TECHNOLOGY R&D IN A COMPETITIVE WORLD 32 (Aug. 2007), *available at* http://www.nsf.gov/geo/geo-data-policies/pcast-nit-final.pdf. In 2010 the President's Council of Advisors on Science and Technology called for continued federal investment in CPS research for its scientific and technological importance and its potential impact on sectors critical to U.S. security and competitiveness. PRESIDENT'S COUNCIL OF ADVISORS ON SCI. AND TECH., EXEC. OFFICE OF THE PRESIDENT, DESIGNING A DIGITAL FUTURE: FEDERALLY FUNDED RESEARCH AND DEVELOPMENT IN NETWORKING AND INFORMATION TECHNOLOGY, at xiii (Dec. 2010), *available at* http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-nitrd-report-2010.pdf; *see also Funding: Cyber-Physical Systems*, NAT'L SCI. FOUND., http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=503286 (last visited May 17, 2013) (soliciting CPS-related project proposals).

[191] *ISC Domain Survey*, INTERNET SYSTEMS CONSORTIUM, http://www.isc.org/services/survey/ (last visited June 16, 2013).

[192] *Id.*

[193] *See* Skoudis, *supra* note 1, at 150.

[194] *Id.* at 152.

functionalities[195]—a complexity prone to generate more flaws and vulnerabilities.[196] In contrast to the proprietary systems of the past, control systems today incorporate commodity information technology components, such as COTS software,[197] which render these control systems subject to the same vulnerabilities present in widely available commercial software and hardware.[198] Furthermore, computer systems that operate different infrastructures may have a number of interdependencies; a cyber attack on one system may have unpredictable, cascading downstream effects.[199]

Because SCADA systems perform vital control functions for national critical infrastructure, health care devices, weapons systems, and industrial processes, they are often closed, or "air-gapped," keeping them isolated from remote access.[200] But even where air-gapped, the systems are hardly secure from attack.[201] For example, cyber attackers have been able to overcome air-gapped industrial process systems by sabotaging SCADA software intercepted along the supply chain to cause gas pipelines to explode.[202] Another group of cyber attackers exploited employee inside access by planting malware-infected USB drives to cause nuclear centrifuges to self-destruct.[203] For many control systems, however, exploiting a vulnerability may not require direct access; today, such control systems are often remotely accessible through local area networks or the Internet.[204] In Australia, Russia, and Poland, hackers have

[195] Alvaro A. Cárdenas et al., *Research Challenges for the Security of Control Systems*, *in* HOTSEC'08: PROCEEDINGS OF THE 3RD USENIX WORKSHOP ON HOT TOPICS IN SECURITY 6 (2008), *available at* http://static.usenix.org/event/hotsec08/tech/full_papers/cardenas/cardenas.pdf.

[196] Skoudis, *supra* note 1, at 156–57.

[197] *See supra* note 152 and accompanying text.

[198] *See* Cárdenas et al., *supra* note 195; *see also* William D. O'Neil, *Cyberspace and Infrastructure*, *in* CYBERPOWER AND NATIONAL SECURITY 113, 147, 166–169 (Franklin D. Kramer et al. eds., 2009). Systems using proprietary components are less attractive targets because they are installed on a relatively small number of unique systems. Time spent searching for security vulnerabilities in a COTS product may reap more rewards for the attacker, as the COTS software may be running on a large number of computers or embedded in many systems. *See* WILSON, *supra* note 107, at 18 n.76.

[199] *See* WILSON, *supra* note 107, at 22 n.79.

[200] *See* GABRIEL WEIMANN, TERROR ON THE INTERNET: THE NEW ARENA, THE NEW CHALLENGES 149 (2006).

[201] *See* Cárdenas, *supra* note 195.

[202] During the Cold War, an American covert operation sabotaged the SCADA system of a Soviet gas pipeline, causing it to "go haywire, after a decent interval, to reset pump speeds and valve settings to produce pressures far beyond those acceptable to pipeline joints and welds." *War in the Fifth Domain*, THE ECONOMIST (Jul. 1, 2010), http://www.economist.com/node/16478792 ?story_id=16478792 (quoting the memoirs of a former Air Force secretary, Thomas Reed). The operation resulted in "the most monumental non-nuclear explosion and fire ever seen from space." *Id.*

[203] *See supra* Part II.B. *But see* WEIMANN, *supra* note 200, at 149 (arguing that "the current threat posed by cyberterrorism has been exaggerated" because there have been no instances of cyberterrorism yet, and U.S. defense systems are air-gapped).

[204] *See* WILSON, *supra* note 107, at 18; *Protecting SCADA Systems with Air Gaps Is a Myth*, INFOSECISLAND (May 21, 2012), http://www.infosecisland.com/blogview/21388-Protecting-SCADA-Systems-with-Air-Gaps-is-a-Myth.html (citing statements of SCADA security expert, Eric Byres, that the idea of "air-gapping" is a myth because "SCADA systems inherently need to be networked to

launched remote-access cyber attacks to flood a sewage treatment plant, seize control of natural gas pipelines, and derail trains.[205] And in the United States, researchers at the Idaho National Laboratory of the U.S. Department of Energy demonstrated that a targeted, remote-access cyber attack against an electrical power network could physically damage generators.[206] Although there have yet to be cyber attacks on U.S. critical infrastructure, hackers from China, Russia, and other countries have successfully penetrated the U.S. electrical grid for reconnaissance and left malware that could cause infrastructure damage.[207]

Potentially catastrophic damage from a cyber attack on a cyber-physical system is not confined to attacks on critical infrastructure; an attack that compromises any safety-critical CPS can have dire consequences. An attacker could remotely access the processing control systems of food or pharmaceuticals manufacturers to modify the formulas, contaminating common food products or altering the ingredient proportions to lethal levels.[208] An attacker could also sabotage medical devices, such as computerized insulin pumps and implantable cardiac defibrillators.[209] In one experiment, researchers were able to penetrate the wireless local area network of a suburban hospital using multiple attack vectors, exploiting the access points to launch a DDoS attack and plant malware.[210] Another recent experiment demonstrated weaknesses in the electronic control systems of popular vehicles: researchers over one thousand miles away were able to "adversarially control a wide range of automotive functions and completely ignore driver input—including disabling the brakes, selectively braking individual brakes on demand, [and] stopping the engine."[211] These experiments prove that cyber-physical systems are vulnerable. And with computers embedded in more and more common products, a cyber attack can cause physical harm in previously unforeseen ways.

function properly due to their demand for large quantities of monitoring information"); Skoudis, *supra* note 1, at 162 (noting that SCADA systems "are managed via maintenance ports that use the same technologies as the Internet, and even isolated SCADA systems sometimes communicate with laptop PCs that also connect to the Internet from time to time").

[205] *See* Cárdenas, *supra* note 195, at 2.

[206] Chen-Ching Liu et al., *Intruders in the Grid*, IEEE POWER & ENERGY MAGAZINE, Jan.–Feb. 2012, at 58.

[207] Siobhan Gorman, *Electricity Grid in U.S. Penetrated by Spies*, WALL ST. J., Apr. 8, 2009, at A1.

[208] *See* Jaeger, *supra* note 169, at 130–31.

[209] Lui Sha et al., *Cyber-Physical Systems: A New Frontier, in* PROCEEDINGS OF THE 2008 IEEE INTERNATIONAL CONFERENCE ON SENSOR NETWORKS, UBIQUITOUS, AND TRUSTWORTHY COMPUTING (2008).

[210] *See* Randall K. Nichols, *Wireless Information Warfare, in* GLOBAL PERSPECTIVES ON INFORMATION SECURITY GLOBAL PERSPECTIVES ON INFORMATION SECURITY: LEGAL, SOCIAL, AND INTERNATIONAL ISSUES 750–63 (Hossein Bidgoli ed., 2009).

[211] Karl Koscher et al., *Experimental Security Analysis of a Modern Automobile, in* PROCEEDINGS OF THE 2010 IEEE SYMPOSIUM ON SECURITY AND PRIVACY 1 (2010), *available at* http://www.autosec.org/pubs/cars-oakland2010.pdf.

III.
JUS AD BELLUM: USE OF FORCE AND ARMED ATTACK

Cyber attacks are a new form of weapon, one without precedent in international law. No treaties or conventions—domestic or international—explicitly address cyber attacks, and the text of the U.N. Charter sheds no light on whether and when such attacks constitute acts of war. Additional Protocol I to the 1949 Geneva Conventions does make clear that *jus ad bellum*[212] principles governing the legality of a nation's recourse to force would, as with any other new weapon, apply to cyber attacks,[213] but it is similarly silent about when and how.

Absent direct law or state practice, nations have historically responded to innovations in weaponry by developing new regulatory regimes, amending the law to accommodate the new weapons, or extending existing law.[214] According to a number of scholars, the *jus ad bellum* analysis is insufficient, and a comprehensive international law governing the treatment of cyber attacks is necessary to address the complex challenges that cyber attacks present.[215] For the near future, however, international cooperation on a treaty or revising the law of war appears unlikely, as there are fundamental differences among the world's major cyber-powers about the scope of activities that should be prohibited under an international cyber attack agreement.[216] It may be decades

[212] *See supra* note 22 and accompanying text.

[213] *See* Geneva Protocol Additional, *supra* note 153, at art. 36, 1125 U.N.T.S. at 21 ("In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party.").

[214] *See* Hollis, *supra* note 23, at 1037.

[215] *See, e.g.*, Hathaway et al., *supra* note 39, at 880 (proposing an international cyber attack treaty that would clarify definitions and "offer a framework for more robust international cooperation in information sharing, evidence collection, and criminal prosecution of those participating in cross-national cyber-attacks"); Hollis, *supra* note 23 (arguing that a new international regime is necessary to regulate information warfare); Shackelford, *supra* note 178, at 248–50 (urging the "adoption of a comprehensive treaty dealing exclusively with cyber security"). *But see* Eric Talbot Jensen, *Unexpected Consequences from Knock-On Effects: A Different Standard for Computer Network Operations?*, 18 AM. U. INT'L L. REV. 1145, 1149 (2003) (rejecting proposals for new cyber attack agreements as "unnecessary" where commanders can "apply the traditional analysis . . . to ensure that they correctly apply this new technology during armed conflict"); *cf.* Arthur K. Cebrowski, *CNE and CNA in the Network-Centric Battlespace: Challenges for Operators and Lawyers*, 76 INT'L L. STUD. SERIES, U.S. NAVAL WAR C. 1, 6 (2002) ("We must be cautious not to advocate new law regarding information warfare without understanding its moral, legal, and practical implications."); Philip A. Johnson, *Is It Time for a Treaty on Information Warfare?*, 76 INT'L L. STUD. SERIES, U.S. NAVAL WAR C. 439, 439 (2002).

[216] *See* Tom Gjelten, *Seeing the Internet as an 'Information Weapon,'* NPR (Sept. 23, 2010), http://www.npr.org/templates/story/story.php?storyId=130052701 (describing differences in perspectives on cyberwar and cyber-arms control between the United States and Russia and asserting that "continuing disagreements over the definition of cyberweapons are likely to complicate any effort to reach international agreement on a broad cyber disarmament accord"). The Shanghai Cooperation Organization, a mutual security organization consisting of China, Russia, and four Central Asian

before an official international treaty can be achieved.[217] Given the rising threat of cyber attacks as a weapon of warfare, it will be necessary to develop a coherent analytical framework under *jus ad bellum*.

Furthermore, because the modern understanding of *jus ad bellum* derives from the U.N. Charter and customary international law, these sources remain the starting point for guiding future state practice vis-à-vis cyber attacks.[218] For its deterrent and normative effects, determining the legality of cyber attacks under these authorities matters. It is to these principles that this Comment now turns. This Section describes international law concerning the use of force and armed attack, and discusses its applicability to cyber attacks. It then summarizes how scholars have determined when a cyber attack constitutes force or an armed attack. It next identifies the limitations of these approaches. Finally, it proposes a new framework under which to analyze these issues.

A. Jus Ad Bellum

International law specifies when a country is prohibited from using force against another country. As a general rule, Article 2(4) of the U.N. Charter prohibits member states from employing "the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations."[219] The references to "territorial integrity" and "political independence" are not constraints on this provision; rather, it proscribes *any* threat of force or use of force against another state not otherwise permitted by special exception in the Charter.[220] Although the U.N. Charter is binding only on member states, the prohibition has been generally accepted and followed by the international

nations—as well as observer nations including Iran, India, Pakistan, and Afghanistan—has adopted a broad definition for "information war." *See id.* The accord defines "information war" to include the undermining of "political, economic, and social systems," as well as "mass psychologic [sic] brainwashing" and the "dissemination of information 'harmful to the spiritual, moral and cultural spheres of other states.'" *Id.* (quoting the Shanghai Cooperation Organization accord). The United States takes a more restrictive approach, which would not permit information controls that may lead to political censorship, and has opposed Russian efforts at the United Nations to pass a cyber disarmament treaty that would limit Internet communication. *See id.*

[217] *See* David Tubbs et al., *Technology and Law: The Evolution of Digital Warfare*, 76 INT'L L. STUD. SERIES, U.S. NAVAL WAR C. 7, 17 (2002) (asserting that "[a]n international consensus on a comprehensive regulation of State activities in cyberspace is very unlikely"). It was not until twenty-three years after the United States detonated two nuclear bombs over Hiroshima and Nagasaki in 1945 that the Nuclear Non-Proliferation Treaty was signed. Treaty on the Non-Proliferation of Nuclear Weapons, *opened for signature* July 1, 1968, 21 U.S.T. 483, 729 U.N.T.S 161 (entered into force May 3, 1970).

[218] CARR, *supra* note 2, at 49.

[219] U.N. Charter, art. 2, para. 4. Article 2, paragraph 3 further buttresses the prohibition on force by requiring the peaceful settlement of international disputes. *Id.* art. 2, para. 3 ("All Members shall settle their international disputes by peaceful means in such a manner that international peace and security, and justice, are not endangered.").

[220] Schmitt, *supra* note 32, at 571.

community.[221] As such, it represents customary international law, binding on all states regardless of U.N. membership.[222] Whether a particular act is a "threat or use of force" is a threshold matter bearing on the legality of that act.

International law provides exceptions that permit a state to use force against another state. The primary exception is self-defense in response to an armed attack.[223] This "inherent right of individual or collective self-defen[s]e" is customary international law, codified in Article 51 of the Charter. Article 51 affirms that the Charter requires no Security Council approval before a state may respond to protect itself.[224] Whether a particular act is an "armed attack" bears on the legality of a victim-state's responsive measures: force is permissible only under the narrow circumstances in which another state has used such gravity of force that it constitutes an "armed attack."[225]

Thus, the fundamental questions for *jus ad bellum* analysis of cyber attacks are: When does a cyber attack constitute an illegal "use of force" under international law? And under what circumstances does it rise to the level of an "armed attack" justifying responsive force in self-defense? These two terms are neither synonymous nor well defined.

1. Use of Force

The paradigm examples at the core of Article 2(4) are relatively clear; at either end of the spectrum, it is apparent what *is* force and what *is not* force. Although Article 2(4) does not define "force," "force" encompasses "armed force," examples of which are cited in the U.N. Charter. Article 42 allows the U.N. Security Council to use conventional military weapons in "demonstrations, blockade, and other operations by air, sea, or land forces" should it find that measures *not* involving the use of armed force are

[221] CARR, *supra* note 2, at 49; Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14 109–10 (June 27) ("[A]cts constituting a breach of the customary principle of non-intervention will also, if they directly or indirectly involve the use of force, constitute a breach of the principle of non-use of force in international relations."). The principle of non-intervention prohibits states from intervening in the internal affairs of other states. *See* Manila Declaration on the Peaceful Settlement of International Disputes, G.A. Res. 37/10, Annex, U.N. Doc. A/RES/37/10 (Nov. 15, 1982); Declaration on Principles of International Law Concerning Friendly Relations and Cooperation Among States in Accordance with the Charter of the United Nations, G.A. Res. 25/2625, U.N. Doc. A/RES/25/2625 (Oct. 24, 1970).

[222] Nicar. v. U.S., 1986 I.C.J. at 109–10.; Statute of the International Court of Justice art. 38, June 26, 1945, 59 Stat. 1055, 3 Bevans 1153.

[223] U.N. Charter, art. 51 ("Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security."). The only other exception in the Charter permits a state to use force when authorized by the U.N. Security Council. *Id.* arts. 39, 41, 42 (permitting the U.N. Security Council to authorize the use of military force to restore international peace and security in response to a threat to or breach of peace or act of aggression).

[224] *Id.* art. 51.

[225] *See id.* art. 51; art. 2, para. 4.

inadequate.[226] Furthermore, the Preamble to the Charter states that the United Nations' mission is "to save succeeding generations from the scourge of war, which twice in our lifetime has brought untold sorrow to mankind" and "to ensure . . . that armed force shall not be used, save in the common interest."[227] These statements reflect the international sentiment that led to Article 2(4)'s prohibition on force: a desire to eliminate unilateral recourse to armed force in the aftermath of the World War II.[228] At minimum, then, "force" includes the type of conventional "armed force" used during the First and Second World Wars.

While traditional military force clearly constitutes "use of force" under the U.N. Charter, other actions that might be considered "force" under a broad, literal interpretation clearly do not. The Charter's legislative history and subsequent U.N. resolutions' drafting history indicate that force does *not* include political or economic coercion. During the drafting of the Charter, some states proposed that the Article 2(4) include economic sanctions,[229] but those proposals ultimately failed.[230] The Western powers sought to confine Article 2(4) to the use of military force and allow the customary international law of non-intervention to govern other actions.[231] Subsequent attempts to include political and economic sanctions under the prohibition on force also failed.[232] Thus, unfavorable trade decisions or severing diplomatic or economic relations are not prohibited force.[233] State practice supports these understandings: the United States, among other nations, has used forms of economic and political coercion since the early days of the Charter largely without legal challenge.[234] Based on state practice, it is also widely accepted that force does not encompass space-based surveillance, boycotts, and espionage.[235] The boundary, therefore, falls somewhere in the wide gray expanse between exercises of traditional forms of military power and soft power coercion or passive intrusions.

[226] *See id.* art. 42.

[227] *Id.* at preamble.

[228] *See* Edward Gordon, *Article 2(4) in Historical Context*, 10 YALE J. INT'L L. 2711 (1985); Silver, *supra* note 37, at 81.

[229] *See* Doc. 2, G/7(e)(4), 3 U.N.C.I.O. Docs. 251, 252–53 (May 6, 1945) (Brazilian amendment proposals).

[230] *See* Silver, *supra* note 37, at 81.

[231] *See* Derek W. Bowett, *Economic Coercion and Reprisals by States*, 13 VA. J. INT'L L. 1 (1972).

[232] *Id.*; *see* G.A. Res. 25/2625, *supra* note 221; Declaration on the Enhancement of the Effectiveness of the Principle of Refraining from Threat or Use of Force in International Relations, G.A. Res. 42/22, Annex, U.N. Doc. A/RES/42/22 (Nov. 18, 1987).

[233] Economic sanctions are considered to be distinct from blockades. *See* Schmitt, *supra* note 32, at 574 n.19. The latter is considered to be armed force because it is enforced by military force, while the former is not a use of force under Art. 2(4). *Id.*

[234] *See* Tom J. Farer, *Political and Economic Aggression in Contemporary International Law*, *in* THE CURRENT LEGAL REGULATION OF THE USE OF FORCE 121, 126 (1986).

[235] Lin, *supra* note 58, at 72–73.

2. Armed Attack

The meaning of "armed attack" in Article 51 is likewise ambiguous, but it is clear that not all force under Article 2(4) rises to the level of an armed attack. In *Nicaragua v. United States*, the seminal case interpreting Articles 2(4) and 51 of the U.N. Charter,[236] the International Court of Justice (ICJ) held that minor "transborder incursions into the territory" of another state and "the provision of arms to the opposition in another state" were insufficient to constitute an armed attack justifying self-defense.[237] Arming and training guerilla rebels seeking to overthrow another country's government was "a prima facie violation" of the prohibition on force,[238] the court stated, but merely supplying financial assistance to those rebels did not amount to a use of force.[239] Decided in 1986, the *Nicaragua* case was the ICJ's first in-depth examination of the substance of international law on the use of force.[240] Yet the court declined to explicitly define "use of force" or "armed attack," or to address what would constitute permissible responsive action, if any, when force falls short of armed attack.[241]

Similarly, the ICJ did not answer these questions in *Democratic Republic of the Congo v. Uganda*, but it did provide an additional data point for understanding armed attack.[242] In that case, the ICJ rejected Uganda's claim of self-defense under Article 51,[243] finding that Uganda had not been under attack by Democratic Republic of the Congo (DRC) forces.[244] The court held that cross-border attacks by anti-Ugandan rebel groups from within DRC territory were insufficiently connected to the DRC government to justify Uganda's use of force.[245] Again, the ICJ declined to elaborate on what actions by non-traditional forces would constitute armed attack that would permit a forceful defensive response.[246] In international law, then, there is little concrete guidance—only a handful of examples showing only what *is* and what *is not* armed attack.

[236] *See* TOM RUYS, 'ARMED ATTACK' AND ARTICLE 51 OF THE UN CHARTER: EVOLUTIONS IN CUSTOMARY LAW AND PRACTICE 7 (2010).

[237] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, 119–20 (June 27).

[238] *Id.* at 118.

[239] *Id.* at 118–19.

[240] *See* RUYS, *supra* note 236, at 7–8.

[241] *See* Military and Paramilitary Activities in and Against *Nicaragua* (Nicar. v. U.S.), 1986 I.C.J. 14 (June 27).

[242] *See* Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), 2005 I.C.J. 168.

[243] *Id.* at 223.

[244] *Id.* at 222–23.

[245] *Id.*

[246] *Id.* at 223.

3. Cyber Attack Analogies

Cyber attacks do not succumb to easy analogy, nor has any international court attempted to so analogize. Like a missile, which would clearly meet the threshold of armed attack, a cyber attack using malware to infect an adversary's cyber-physical weapons system can launch remotely, physically destroy the system, and cause collateral damage to civilian property; but unlike a missile, there is no physical invasion of territory and little risk of human death or injury. Or like a biological agent,[247] a computer virus can arrive unseen, cause undetected contamination to the food supply, and result in widespread public alarm; but unlike a biological agent, the effect on the food supply is indirect—the malware targets the computer controlling or monitoring the food processing system, the malfunctioning of which causes the contamination. Or like an economic sanction, a DDoS attack can cause economic harm, disrupting a state's ability to freely engage in trade; but unlike an economic sanction, a DDoS attack may unilaterally prevent the victim-state from engaging in trade with any other state, not just the country that initiated the attack.

Yet even where the analogies run more parallel, such as when a nation provides funding and resources to third-party hackers for the purpose of launching cyber attacks against another nation, some characteristics of cyber attacks pull the conclusions about force in the opposite direction. For instance, cyber attacks are often the work of hired hackers, but state funding for a cyber attack involves different motives, incentives, and deterrents than for funding a conventional armed attack perpetrated by the third party. In determining the United States' responsibility for assisting the actions of armed insurgents against Nicaragua, the ICJ drew the use-of-force line at providing monetary assistance: arming and training the contras constituted force,[248] but funding them did not.[249] Perhaps one reason for this distinction is the connection between the means provided and the ends achieved—arms and training promotes no other purpose but to facilitate the rebels' use of force, whereas monetary assistance can be used in other ways. In either case, force is its own deterrent; the physical nature of such an attack puts the aggressor at risk of injury and death. For cyber attacks, these deterrents are virtually non-existent. Individuals launching cyber assaults can do so remotely, without risking their

[247] The U.N. Charter does not address chemical or biological weapons. However, the 1925 Geneva Protocol, in effect at the time the U.N. Charter was drafted, explicitly prohibits the use of chemical and biological weapons. *See* Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare, June 17, 1925, 26 U.S.T. 571. This complete prohibition on the use of chemical and biological weapons, regardless of circumstance, strongly suggests that the Charter contemplated that the use of such weapons would constitute armed attack.

[248] Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), 2005 I.C.J. 168, 246–47.

[249] *Id.* at 247.

personal safety, using little more than a personal computer.[250] With little danger and no risk of bodily harm at stake, a hacker with just an ounce of patriotism is far more likely to act as a cyber mercenary, and thus a state may more easily enlist the services of a hacker than a traditional mercenary.

Heterogeneous in form and varied in scope, nature, and intensity, cyber attacks require a highly fact-specific *jus ad bellum* analysis, one attuned to the major challenges that cyber attacks present for war and international relations. The following Section explores the strengths and weaknesses of the major approaches to providing a framework for that analysis.

B. Leading Approaches

Scholars addressing the status of cyber attacks under *jus ad bellum* have advanced three approaches to deciding when a cyber attack becomes a use of force or an armed attack. First, the instrument-based approach looks to the form of weapon used to perpetrate an attack, asking whether the attack possesses the "physical characteristics traditionally associated with military coercion."[251] Second, the target-based,[252] or "strict liability,"[253] approach automatically treats any cyber attack against critical national infrastructure as an armed attack because of the potential for severe consequences if such systems are disabled.[254] Third, the effects- or consequences-based model focuses on the overall effect of the cyber attack on the victim state, looking to factors such as severity, immediacy, and directness of harm to assess whether the consequences of the cyber attack are of sufficient gravity to render it a use of force or armed attack.[255] Each of these models has significant flaws that fail to account for many of the characteristics distinguishing cyber attacks from the conventional military arsenal.

1. Instrument-Based Approach

According to the instrument-based approach, force is assessed in relation to the instrumentality, or type of weaponry, used. The more analogous a new weapon is to conventional forms of military force, the more likely its operation will constitute a "use of force" or "armed attack." This view derives from a textualist reading of the U.N. Charter. Although Articles 2(4) and 51 do not define these terms, elsewhere the Charter provides examples for related concepts, which provide a guiding basis for this view. Articles 39–49 set out the parameters for the U.N. Security Council's response to threats to the peace,

[250] Criminal charges by domestic law enforcement are possible but are less visceral and more removed than physical assault.

[251] *See* Hollis, *supra* note 23, at 1041; *see also* Kanuck, *supra* note 23, at 289.

[252] *See* Hollis, *supra* note 23.

[253] *See* Graham, *supra* note 25, at 91.

[254] *See* Condron, *supra* note 26 at 419; Jensen, *supra* note 26, at 229.

[255] *See* Schmitt, *supra* note 27, at 914–15.

breaches of the peace, or acts of aggression. In this context, the Charter uses the terms "use force," "armed force," and "armed forces" interchangeably.[256] It specifies that "armed force" is "action by air, sea, or land forces," which includes "demonstrations, blockade, and other operations by air, sea, or land forces,"[257] but *not* "complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations."[258] It would appear that force means traditional, military armed force to the exclusion of other forms of coercion. The U.N. Resolution on the Definition of Aggression confirms this view: aggression includes armed invasions, port blockades, bombardments, and armed violations of territory—all actions involving physical force and physical territory.[259] The instrument-based approach looks to the principles of *ejusdem generis* (of the same kind, class, or nature) and *noscitur a sociis* (a word is known by the company it keeps) to conclude that a cyber attack, by definition, cannot be force or armed attack because the instrument used—computer code—is neither physical nor a form of conventional military force.

While the strength of the instrument-based view lies in its ease of administration, it lacks logical justification. Under this view, the legality of an attack rests on whether the method or implement used falls on one side or another of two false dichotomies: physical/non-physical and conventional-military/non-conventional-military. The instrument-based view differentiates based on the nature of the assault, regardless of the consequences. A naval blockade against a country is explicitly regarded as armed force under the Charter,[260] while a trade embargo against that country is not, although it may have virtually equivalent effects.[261] The argument from this camp relates to the physical coercion the blockade involves, a seemingly greater threat to national sovereignty than purely legal trade restrictions. Yet by restricting "force" to only its most conventional forms under international law, this approach is rigid and inflexible. Further, it ignores new forms of violence until there is international agreement on their status—a process that can take decades.

[256] *See* U.N. Charter, art. 41 ("The Security Council may decide what measures not involving the use of *armed force* are to be employed to give effect to its decisions.") (emphasis added); *id.* art. 44 ("When the Security Council has decided to *use force* it shall, before calling upon a Member not represented on it to provide *armed forces* in fulfillment of the obligations assumed under Article 43, invite that Member, if the Member so desires, to participate in the decisions of the Security Council concerning the employment of contingents of that Member's armed forces.") (emphasis added); *id.* art. 46 ("Plans for the application of *armed force* shall be made by the Security Council with the assistance of the Military Staff Committee.") (emphasis added).

[257] U.N. Charter, art. 42.

[258] *Id.* art. 41.

[259] *See* Definition of Aggression, G.A. Res. 29/3314, Annex, art. 2, U.N. Doc. A/RESRes/29/3314 (Dec. 14, 1974).

[260] *See* U.N. Charter, art. 42.

[261] *See* U.N. Charter, art. 41 ("The Security Council may decide what measures not involving the use of armed force are to be employed . . . . These may include complete or partial interruption of economic relations.").

In the same vein, an information embargo, in which a state with disproportionate control over telecommunications satellites and networks unilaterally cuts off another state's access,[262] would also fall short of illegal force. The same would be true of a more direct cyber attack on another state's communications networks.[263] Under the instrument-based approach, Stuxnet would not be considered "force" because it was malware rather than a missile; nor would the DDoS attacks against Estonia's information systems be considered "force" because a botnet was used. Under this view, the acts that define warfare remain frozen in 1945 terms. Cyber attacks that destroy electrical power grids and oil and gas pipelines; disrupt emergency response communications systems; and cause weapons systems, automobile safety systems, and medical devices to malfunction do not trigger U.N. scrutiny and opprobrium, or a nation's right to use force in self-defense, merely because malware, not a bomb, caused the damage. Given the increasingly significant role computer networks have assumed, these inconsistencies and dangerous exceptions to international law illustrate the shortcomings of the instrument-based approach.

2. Target-Based Approach

As the name suggests, the target-based view frames its legality analysis not around the instrumentality used to execute the attack, but around the status of the attack's target. The proponents of this approach typically privilege critical infrastructure with special status, regarding any cyber attack against such infrastructure as an "armed attack" sufficient to trigger a nation's right to self-defense, including anticipatory self-defense.[264] Countries may define their own critical infrastructure in different ways. In the United States, Congress has defined "critical infrastructure" to mean "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[265] The White House has identified sixteen critical infrastructure

[262] Kanuck, *supra* note 23, at 289.

[263] *See* U.N. Charter, art. 41 ("The Security Council may decide what measures not involving the use of armed force are to be employed . . . . These may include complete or partial interruption of . . . rail, sea, air, postal, telegraphic, radio, and other means of communication.").

[264] *See* SHARP, *supra* note 26, at 129–31 (arguing that if cyber espionage targets one of the "sensitive systems that are critical to a state's vital national interests," that state has the presumptive right to use necessary and proportional force in anticipatory self defense); Jensen, *supra* note 26, at 229 ("[T]he law should evolve to recognize a nation's inherent right of self-defense, including anticipatory self-defense, against a [computer network attack] focused on critical national infrastructure, even if that [computer network attack] does not constitute an armed attack."); *cf.* Condron, *supra* note 26, at 419 ("The nation should initially presume any cyber attack on the critical infrastructure of the United States is a national security threat rather than a criminal activity, at least until federal authorities neutralize the threat and determine that the activity is actually criminal in nature.").

[265] Critical Infrastructure Protection Act of 2001, 42 U.S.C. § 5195c(e) (2006).

sectors falling within this rubric, including food and agriculture, banking and finance, commercial facilities, communications, healthcare, and transportation systems.[266]

Like the instrument-based approach, the target-based approach benefits from ease of administrability. Assuming adequate attribution, any cyber attack targeting critical infrastructure systems will justify self-defense. Indeed, any cyber intrusion into these systems, including cyber espionage, would permit a state to respond with defensive force regardless of the attack's actual effect. Although this strict liability approach reflects the importance of critical infrastructure to national security and the severe consequences that could result from a targeted cyber attack, it is dangerously overbroad. It assumes that any critical infrastructure network penetration demonstrates hostile intent and that for any such penetration, the "necessity of . . . self-defence is instant, overwhelming, and leav[es] no choice of means, and no moment for deliberation."[267]

Indeed, the target-based approach touches on a major challenge of analyzing cyber attacks under international laws of war: that "[a] state's penetration of another state's information infrastructure may be espionage, a pre-attack exploration, or an actual attack in progress that has not yet manifested itself."[268] But by categorizing all cyber intrusions into critical infrastructure as acts of war, the target-based approach puts the United States at war with China, Russia, and a number of other countries that have already penetrated U.S. infrastructure systems for unknown purposes.[269] Some scholars have argued that treating all infrastructure penetrations as justifying self-defense would have a strong deterrent effect.[270] But it is unlikely that states would accede to this approach given the prevalence of state-sponsored cyber

[266] *See* PRESIDENTIAL POLICY DIRECTIVE 21: CRITICAL INFRASTRUCTURE, SECURITY AND RESILIENCE, THE WHITE HOUSE (Feb. 12, 2013), *available at* http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil [hereinafter PRESIDENTIAL POLICY DIRECTIVE 21]. The sixteen sectors are food and agriculture; financial services; chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; governmental facilities; healthcare and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water. *See also* CRITICAL INFRASTRUCTURE SECTORS, U.S. DEPT. OF HOMELAND SECURITY, http://www.dhs.gov/critical-infrastructure-sectors (last visited May 28, 2013).

[267] 2 JOHN BASSETT MOORE, A DIGEST OF INTERNATIONAL LAW § 217, at 412 (quoting then-U.S. Secretary of State Daniel Webster concerning the 1837 *Caroline* case). This is known as the *Caroline* doctrine, which is the basis for justification of preemptive self-defense. For more information about the *Caroline* case, see generally Christopher Greenwood, *The Caroline*, Max Planck Encyclopedia of Public International Law (Apr. 2009), *available at* http://www.mpepil.com/sample_article?id=/epil/entries/law-9780199231690-e261&recno=12&.

[268] SHARP, *supra* note 26, at 128.

[269] *See, e.g.*, Gorman, *supra* note 80.

[270] *See* Jensen, *supra* note 26, at 228.

espionage and its similarities to other forms of espionage and surveillance that have long been permitted by state practice under international law.[271]

In addition, using the term "critical infrastructure" may be both over- and underinclusive, which could allow a state to frame a cyber intrusion as a use of force justifying self-defense according to convenience. The sixteen critical infrastructure sectors identified by the White House, for example, are so comprehensive as to be all-encompassing. They cover not only core infrastructure (including energy, defense, and transportation), but also less essential services and facilities (such as commercial facilities).[272] Under this definition, seemingly any cyber intrusion other than those targeting an individual's personal computer would permit responsive force, regardless of how benign or reversible the payload. Here, not only would the Stuxnet worm have permitted Iran to use force against the United States in self-defense, but the Duqu and Flame reconnaissance viruses, specifically designed for data-mining and information theft, would likewise justify countries throughout the Middle East in engaging in anticipatory self-defense.[273] The DDoS attacks against Estonia's government websites would also qualify, though little tangible damage was done.

Even a more focused construction of the bounds of critical infrastructure is unable to save this approach. For example, it would label a mere reconnaissance scan of a portion of the electrical grid as force justifying self-defense, but would not consider a state-sponsored remote attack disabling the braking mechanisms on all automobiles of a certain make and model to be force.[274] Given its expansive breadth, as well as its limitations and contradictions, the target-based view falls short of providing the necessary analytical framework for assessing cyber attacks under *jus ad bellum*.

3. Effects-Based Approach

Recognizing that states are more concerned with the consequences of a cyber attack than the specific type of weapon or the precise nature of the target,

[271] *See* Demarest, *supra* note 10, at 347; Baker, *supra* note 11, at 1092.

[272] *See* PRESIDENTIAL POLICY DIRECTIVE 21, *supra* note 266.

[273] *See* Dave Lee, *Flame and Stuxnet Makers 'Co-operated' on Code*, BBC NEWS (June 11, 2012), http://www.bbc.co.uk/news/technology-18393985 (reporting that researchers have concluded that Stuxnet, Duqu, and Flame are connected and share some of the same source code); Perlroth, *supra* note 60 (reporting that the Flame and Duqu viruses were "designed to steal information from computers across the Middle East"); *cf.* Dave Lee, *Flame: UN Urges Co-operation to Prevent Global Cyberwar*, BBC NEWS (June 7, 2012), http://www.bbc.co.uk/news/technology-18351995 (describing an interview with Dr. Hamadoun Toure, head of the UN's International Telecommunications Union, in which Dr. Toure said that while Flame was clearly created by a nation state, he did not consider it to be an act of cyberwar).

[274] *See, e.g.*, Koscher et al., *supra* note 211, at 11 (describing experiments demonstrating that "without needing to unlock the [Electronic Brake Control Module, the researchers] were able to release the brakes and prevent them from being enabled, even with the car's wheels spinning at 40 MPH while on jack stands").

the effects-based approach structures its inquiry around repercussions and results. A cyber attack that produces physical destruction akin to that produced by a kinetic attack is more likely to qualify as the equivalent of force or armed attack, while an attack resulting in consequences similar to those resulting from political or economic coercion are less likely to so qualify. This approach is the most widely accepted view.[275]

For conventional military operations, gauging the force threshold against an attack's consequences may make sense. With kinetic attack, there is a strong correlation among intent, cause, and effect: the destruction of a nuclear facility is certainly the intended effect of an air strike directed against it. But these connections become much more attenuated in the cyber attack context. A cyber attack directed against a nuclear facility may cause the centrifuges within to malfunction and self-destruct; it may cause other centrifuges in the region with the same technology to self-destruct; or it may have little to no physical effect. Cyber attacks with a very narrow, focused objective may have wildly unpredictable results, leading to ripples of cascading destruction that cannot be slowed or halted.[276]

On the other hand, cyber attacks replete with malicious intent—targeting lives, property, and critical national assets—may never come to bear, even if repeatedly attempted. This disconnect among intent, cause, and effect renders effect a poor proxy for force, for it would tie the legality of a state's cyber operations to the vagaries of chance without accounting for the significance of intent. An effects-based approach would create a standard that essentially authorizes the unsuccessful cyber attack and fails to deter cyber attempts, while justifying a state's use of force in response to a cyber attack with unintended destructive results.

Michael Schmitt proposed the most prominent effects-based approach, which looks at six criteria distinguishing traditional (kinetic) armed force from political and economic coercion.[277] Schmitt argues that these six factors should affect the analysis of when a cyber attack constitutes a use of force: (1) severity—the degree of physical injury or property damage, (2) immediacy—how quickly the negative consequences manifest, (3) directness—the proximity of the act and its consequences, (4) invasiveness—the extent of territorial penetration, (5) measurability—to what extent the consequences can be quantified, and (6) presumptive legitimacy—whether the act is presumed valid

[275] *See* Hathaway et al., *supra* note 39, at 847 (noting that the effects-based approach "steer[s] a middle course between the instrument- and target-based views" and is the "most promising and most widely accepted approach"); Lin, *supra* note 58, at 73 ("As a number of analysts have noted, the relevant question is not so much whether a cyber attack constitutes a use of force but rather whether a cyber attack with a specified effect constitutes a use of force. That is, the effects of a given cyber attack are the appropriate point of departure for an analysis of this question rather than the specific mechanism used to achieve these effects.").

[276] *See* discussion *supra* Parts II.C.1 and II.C.2.

[277] Schmitt, *supra* note 27.

under domestic or international law (armed force is presumptively illegal, while other forms of coercion are presumptively legal).[278] Schmitt cites severity as "self-evidently the most significant factor in the analysis."[279]

These criteria are useful for parsing out many of the underlying characteristics that define an act as armed force. The greater the severity, immediacy, directness, invasiveness, and measurability, the more likely an action is armed force; if the act is presumptively legitimate, on the other hand, it is less likely to be armed force. But as some analysts have noted, "examination of the criteria suggests that virtually any [cyber attack] can be argued to fall on the armed force side of the line."[280]

Schmitt's own application of his framework to the 2007 DDoS attacks on Estonia is illustrative. Schmitt found that five of the six factors weigh in favor of use of force.[281] He argued that (1) the cyber attacks were severe because "[g]overnment functions and services were severely disrupted, the economy was thrown into turmoil, and daily life for the Estonian people was negatively affected"; (2) the disruption was immediate in effect; (3) the effects were a direct consequence of the denials of service; (4) the attacks were invasive because they affected some systems that had been designed to be secure; (5) the consequences were difficult to quantify because they involved disruption rather than destruction; and (6) the attacks were not necessarily presumptively legitimate because they involved intentional frustration of government and economic functions, rather than mere pressure.[282] On balance, he concluded, the incident "arguably reached the use-of-force threshold."[283]

Yet, the criteria are so malleable that one could easily frame the circumstances of the Estonia attacks to find against use of force: (1) the cyber attacks were not very severe because no one was physically injured, no property was damaged, and the DDoS attacks prevented users from accessing websites for generally no more than a few hours;[284] (2) consequences ranging from decreased confidence in government to lost business resulting from inaccessible websites were delayed; (3) these effects were indirect consequences of the DDoS attacks, compared to the direct effect of lost server availability; (4) the attacks were executed remotely and involved no physical, territorial penetration; (5) the consequences are difficult to quantify because no

[278] *Id.* at 914–15.

[279] Schmitt, *supra* note 32, at 576.

[280] Silver, *supra* note 37, at 89 (explaining why five of the six factors, excluding severity, would ordinarily result in a finding in favor of armed force when applied to computer network attacks); *cf.* Hathaway et al., *supra* note 39, at 847–48 ("These factors are illuminating, but they call for such a wide-ranging inquiry that they may not provide sufficient guidance to decision makers.").

[281] Schmitt, *supra* note 32, at 577.

[282] *Id.*

[283] *Id.*

[284] *See* Steven Lee Myers, *Cyber Attack on Estonia Stirs Fear of 'Virtual War,'* N.Y. TIMES (May 18, 2007), http://www.nytimes.com/2007/05/18/world/europe/18iht-estonia.4.5774234.html.

concrete injury or damage occurred; and (6) the attacks were presumptively legitimate because they merely interrupted communications systems, which, under the U.N. Charter, is not considered "force."[285]

These two contradictory interpretations of the same cyber attack demonstrate that Schmitt's six criteria can be too easily manipulated to create results supporting the geostrategic goals of the nation conducting the inquiry. And because cyber attacks often infect a computer system sight unseen and cause delayed and indirect harm, an attack's effects can be difficult to ascertain at the moment it occurs. Accordingly, an effects-based analysis may have limited utility for a state's leaders under pressure to determine the appropriate response to such an attack.

A further difficulty with the effects-based framework is that, for the same cyber attack, the use-of-force boundary will shift based on the characteristics of the target state. Nations vary widely in their respective abilities to detect cyber intrusions, repel cyber attacks, or mitigate their effects.[286] China, for example, is better equipped to prevent large-scale damage from a cyber attack because it has the capability to quickly and completely sever the nation's communications networks from the rest of cyberspace, a capability the U.S. government lacks because most of its networks are privately owned and operated.[287] Thus, in the event of a significant attack, China would be able to unilaterally take the entire nation's networks off the grid and prevent further damage. In the United States, the same process would be much slower, likely requiring congressional approval and the cooperation of several private entities. The effects of a cyber attack on a given state will also vary widely based on the state's technological dependence. For example, North Korea relies far less on networked computer systems than other nations do, which renders the country relatively impervious to cyber attacks.[288]

Thus, under the effects-based approach, the very same cyber attack can have widely divergent consequences depending on the target of the attack. But it makes little sense that a cyber attack on one nation would constitute illegal use of force, while the very same attack on another nation would be considered legal, simply because the former invested more resources into cyber security or was less dependent on computing technology than the latter nation. The legality of an attack must depend at least as much on the actions and intent of the attacker as on the defensive capabilities of the victim.

C. A New Approach: Force as Intentional Damage to Cyber-Physical Systems

The three leading approaches—instrument-based, target-based, and effects-based—each draws on useful analogies and insightful observations. But

[285] *See* U.N. Charter, art. 41.

[286] *See* CLARKE & KNAKE, *supra* note 29, at 148.

[287] *Id.*

[288] *Id.* at 149.

each suffers from significant theoretical and practical weaknesses. These approaches are overbroad, underinclusive, and expansive; some enunciate too rigid a rule and others permit too much flexibility in application. Overall, they fail to fully account for some of the nuances that distinguish cyber attacks from conventional military force.

If the *jus ad bellum* is to encompass the new threat that cyber attacks pose to international peace and security, it requires an analytical framework that is administrable across nation-states, forward-looking, and both consistent and sensible in its treatment of cyber attacks. At the same time, the framework should satisfy our basic intuitions about what constitutes an act of war. Intuitively and in terms of the threat to international peace and security that the U.N. Charter seeks to prevent,[289] operations intended to cause mere disruption of service or functionality, with reversible and non-permanent results, generally should not constitute illegal force. Such minor actions do little to endanger international peace and security,[290] and international law generally permits all acts that are not expressly prohibited.[291] On the other hand, acts that endanger life and property, instill fear, and threaten a nation-state's sovereignty generally should constitute illegal force. The Charter's prohibition on force refers specifically to "force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations," purposes which include maintaining international peace and security.[292] Thus, the framework must encompass cyber attacks that threaten a nation's sovereignty, peace, and security.

This Comment proposes that cyber attacks constitute armed attack when they are intended to cause irreversible disruption or physical damage to a cyber-physical system (CPS). As the ICJ noted in *Nicaragua*, not every instance of force constitutes armed attack,[293] so those cyber attacks intended to cause only trivial disruption or damage would not rise to the level of armed attack. Depending on the severity of the effects, these attacks may instead be considered an illegal use of force under Article 2(4). This would trigger international condemnation, but not responsive force by the target country. Conversely, a cyber attack aimed at a computer system without a physical control component could rise to the level of armed attack if it is intended to cause or may foreseeably cause irreversible disruption or damage, though this scenario would be exceptionally rare.

This approach accounts for the actor and the act, both of which are implicit in the terms "force" and "attack." Unlike the instrument-based

[289] *See* U.N. Charter, art. 1.

[290] *Id.* art. 2(3).

[291] *See* Schmitt, *supra* note 32, at 577.

[292] *See* U.N. Charter, art. 1, para. 1; art. 2, para. 4.

[293] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14 119 (June 27).

approach, and in keeping with the definition discussed in Part I, it acknowledges that a cyber attack is a weapon, the use of which can constitute force. The CPS-focused approach also recognizes that the target matters. The object of the attack must be a CPS because, by definition, the computing and physical components of these systems are tightly interwoven. Any disruption or damage to the computing component of a CPS will inevitably have a physical effect: computer code can shut down electrical grids, corrupt manufacturing processes, disable automobile brakes, and cause nuclear centrifuges to spin wildly out of control. It is these types of catastrophic, destabilizing harms, and the resulting disruption to peace and security, that are exactly what the *jus ad bellum* seeks to regulate.

This framework accounts for some of the major trajectories in technological development—cyber-physical convergence and increased network connectivity—as well as the challenges of unrestrained geographical scope, uncertain collateral damage, and unpredictable effects that plague the application of *jus ad bellum* to cyber attacks. Malware is a particularly potent and volatile weapon, one whose effects cannot easily be controlled.[294] For cyber attacks, unlike with kinetic attacks, intent does not necessarily correlate with outcome. A nation that directs such a cyber weapon at another nation's cyber-physical systems attacks not only computers, but also tangible matter. This dual attack risks unleashing far greater harm than intended, as it has high destructive potential that may be unstoppable once launched. These dangers animate the proposed standard, which recognizes that cyber attacks on cyber-physical systems are akin to physical attacks with an unpredictably broad strike zone. By labeling any cyber attack intended to cause irreversible disruption or damage to a CPS as armed force, the standard seeks to deter the most dangerous of cyber attacks.

The CPS-focused approach accounts for the unrestrained scope of cyber attacks involving self-replicating malware. Scope matters, but only to the extent that the cyber attack has the potential to produce significant, destabilizing harm to a nation's peace and security. For example, launching malware like the Conficker worm, which spread to over five million computer systems in over two hundred countries through rapid, indiscriminate propagation,[295] would become such a destabilizing attack if it carried a payload that had the actual ability to physically destroy, and would be considered an armed attack. In such cases, the danger of far-reaching effects is sufficiently real that it justifies labeling such an offensive operation as an "armed attack." It also justifies allowing a country to use responsive force to defend against such an attack.

The unpredictability of cyber attacks provides further support for drawing the *jus ad bellum* line at those attacks aimed at cyber-physical systems. As

[294] *See* discussion *supra* Part II.C and accompanying notes.

[295] *See* Markoff, *supra* note 137.

Part II.C describes, even the most narrowly targeted cyber attack can infect computers beyond its intended target, and the effects are practically uncontrollable. While this may matter little where an attack carries a payload that merely copies and transmits files for the purpose of espionage, it matters far more when the attack can affect the control of physical systems.

On the other hand, cyber attacks that do not threaten or result in physical effects should not constitute force under the *jus ad bellum*, because such attacks are largely reversible. At their core, cyber attacks are simply written instructions that are translated into the 0s and 1s of binary code, the language of machines. Cyber attacks transit computers, primarily affecting the data residing in or processed by those computers. If that data is critical, it is likely backed up elsewhere so that it can be reconstructed in the event of computer failure or malfunction. Such failure or malfunction occurs even in the absence of deliberate malicious activity; should a cyber attack be the source, it hardly seems tantamount to an act of war when the disruption is temporary or the damage is reversible. The CPS-focused approach thus accounts for the transitory nature of these types cyber attacks, permitting such minor incursions while prohibiting only those with the potential to produce irreversible damage.

Most denial-of-service attacks might be classified as inconveniences that interrupt normal routines, but have no direct physical impact equivalent to force. Even the Estonian attacks, one of the largest DDoS attacks to date,[296] involving over a million zombie computers controlled through multiple botnets,[297] are difficult to equate to historical notions of force when they resulted in no physical injury or property damage. No doubt, the DDoS attacks were a severe form of denial-of-service. They relentlessly flooded servers all over the country for several weeks, and affected the websites of government agencies, news organizations, schools, and banks.[298] But these attacks targeted only websites. There was no physical damage, and the only reported economic damage was one bank's operating loss of $1 million.[299] As such, even this massive a DDoS attack should not constitute armed force. Under the CPS-focused approach, it would not, because it meets neither the target nor intent criteria. First, the cyber attacks against Estonian websites were not aimed at

[296] Estonian officials asserted that the attack was the largest ever mounted against a country. *See* Steven Lee Myers, *'E-stonia' Accuses Russia of Computer Attacks*, N.Y. TIMES (May 18, 2007), http://www.nytimes.com/2007/05/18/world/europe/18cnd-russia.html.

[297] BRENNER, *supra* note 30, at 1–2.

[298] *See* Myers, *supra* note 284 ("[T]he attacks, coming in waves, began to strike newspapers and television stations, then schools and finally banks, raising fears that an initial nuisance could have economic consequences."); Ian Traynor, *Russia Accused of Unleashing Cyberwar to Disable Estonia*, THE GUARDIAN (May 16, 2007), http://www.guardian.co.uk/world/2007/may/17/topstories3.russia ("The main targets have been the websites of: the Estonian presidency and its parliament; almost all of the country's government ministries; political parties; three of the country's big news organisations; two of the biggest banks; and firms specializing in communications.").

[299] *See* Stephen Herzog, *Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses*, 4 J. STRATEGIC SECURITY 49, 51–52 (2011).

disrupting or damaging cyber-physical systems. Second, they did not evince an intent to cause harm greater than that which did result.

By focusing on cyber-physical systems, this approach encompasses more than those limited to critical national infrastructure. It recognizes that cyber attacks on targets other than critical infrastructure can, by manipulating the physical components of critical devices, cause widespread, large-scale destruction greater than many classic examples of conventional armed force. But at the same time, unlike strict liability, target-based approaches, it recognizes that not every cyber intrusion is force. It draws the line at attacks intended to cause irreversible disruption or physical damage to a CPS. This line excludes all cyber espionage and most forms of denial-of-service. Further, it brings cyber warfare beyond mere inconvenience and closer to our intuitions about the immediate, severe, and lasting types of harms traditionally classified as acts of war.

An additional benefit of the proposed CPS-focused approach is that it accounts for one of the shortcomings of effects-based approaches. Effects-based approaches ignore unsuccessful attempts at cyber attacks, permitting a state to launch repeated attacks without penalty. Such systems mete out punishment according to whether the victim state possessed an eggshell or titanium skull and turn a blind eye to assault that did not result in battery. But international law is not a tort system of compensation for harms; the U.N. Charter establishes aspirational standards for international relations. *Jus ad bellum* draws boundaries that are as much about deterrence and morality of conduct as about ex post judgments of harm actually inflicted. The proposed approach aims to address these principles by focusing on intent, to the extent it can be ascertained, rather than effect.[300]

Finally, the focus on CPS creates a clear and concrete standard that is relatively easy to apply. It suffers little in translation across national borders because it does not depend on malleable definitions and differing values. Rather, it employs an objective assessment of whether a state-sponsored cyber attack on a cyber-physical system carries a destructive payload. The instrument-based approach also benefits from this ease of administrability, an important characteristic in a world of widely divergent conceptions about what is permissible in pursuit of political and military goals, but it is obsolete. The multi-factor effects-based approach benefits from the flexibility of a standard that can evolve over time, but the standard can too easily be framed and manipulated to reach a desired conclusion. The CPS-focused approach

[300] As with attribution, determining a cyber attack's intended payload is a problematic evidentiary issue, but reverse engineering and other intelligence make such judgments more feasible than initial impressions may suggest. *See, e.g.*, Avi Pfeffer, et al., *Malware Analysis and Attribution Using Genetic Information*, 2012 7th International Conference on Malicious and Unwanted Software (MALWARE) (Oct. 16–18, 2012); Deguang Kong, et al., *Semantic Aware Attribution Analysis of Remote Exploits, in* SEC. AND COMMC'N NETWORKS (2012).

proposed here treads a middle ground, clarifying and adapting the UN Charter's guidelines to apply to modern warfare in today's cyber-connected world.

CONCLUSION

The age of cyber warfare is upon us, brought abruptly from theory to reality by Stuxnet, a piece of malware that demonstrated precisely how a state can use computer code as a weapon to cause dramatic physical destruction even in a supposedly secure system disconnected from the Internet. But Stuxnet also revealed the danger that even a sophisticated, narrowly tailored, and well-tested cyber attack can accidentally escape a closed system and undergo rapid, uncontrollable, worldwide proliferation. Although various forms of malware have been capable of infecting and damaging computer systems for decades, Stuxnet was the first to successfully target a critical cyber-physical system and cause real-world destruction beyond the computer system itself. Governments around the globe took notice, reassessing and augmenting their cyber operations strategies in light of a security threat that just became more real.

Stuxnet was no aberration or *deus ex machina*. Such an attack has long been predicted as the logical outgrowth of increasing cyber-physical convergence, network connectivity, and hacking ability. Along with warnings and predictions, commentators have offered various suggestions to address the applicability of *jus ad bellum* to cyber attacks. But this literature is relatively sparse and insufficient, with the commenters each attempting to resolve the challenge of drawing lines on a shifting, multi-dimensional landscape. This Comment revisits these debates in light of the mounting urgency of finding a consistent, principled standard by which to measure cyber attacks against international law's use-of-force boundary, offering an alternative analytical framework as a starting point for policy development.

Recognizing that physical harm remains the greatest threat to international peace and security, this Comment argues that cyber attacks should constitute armed force when they are intended to cause irreversible disruption or physical damage to a cyber-physical system. This standard addresses many of the gaps and limitations of previous approaches. It moves away from overly narrow, categorical definitions of instrument or target; it accounts for emerging trends in cyberspace and the distinctions between cyber attacks and kinetic attacks, including attempts and unsuccessful attacks as worthy of sanction; and it provides an objective standard facilitating consistent application. Treaty or state practice may ultimately determine the status of cyber attacks under international law, but this Comment hopes to provide another perspective as the policymaking unfolds.