Harvard Journal of Law & Technology
Volume 25, Number 2 Spring 2012

MITIGATIVE COUNTERSTRIKING: SELF-DEFENSE AND DETERRENCE IN CYBERSPACE[1]

Jay P. Kesan and Carol M. Hayes***

TABLE OF CONTENTS

---

1. An earlier version of this work received an Honorable Mention Award in the National Research Council's ("NRC") Competition on Research and Scholarship in Cyberdeterrence. Jay P. Kesan & Carol M. Hayes, *Thinking Through Active Defense in Cyberspace* (Ill. Pub. Law and Legal Theory Research Papers Series, Working Paper No. 10-11, 2010), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1691207.

* Professor, H. Ross & Helen Workman Research Scholar, and Director of the Program in Intellectual Property & Technology Law, University of Illinois College of Law.

** Research Fellow, University of Illinois College of Law. After receiving her J.D. from the University of Illinois, Carol Hayes served as a Christine Mirzayan Science and Technology Policy Graduate Fellow at the National Academy of Sciences in Fall 2010. The authors wish to thank Herb Lin, Jack Goldsmith, and the many NRC workshop participants, whose guidance and suggestions greatly contributed to the direction of this Article. We also thank Morell E. Mullins for his assistance with earlier drafts.

I. INTRODUCTION

> IF WE DO NOT WISH TO FIGHT, WE CAN PREVENT THE ENEMY FROM ENGAGING US EVEN THOUGH THE LINES OF OUR ENCAMPMENT BE MERELY TRACED OUT ON THE GROUND. ALL WE NEED DO IS TO THROW SOMETHING ODD AND UNACCOUNTABLE IN HIS WAY.[2]
>
> A STRANGE GAME. THE ONLY WINNING MOVE IS NOT TO PLAY.[3]

Ideas, computers, and intellectual property have become extremely important in the modern Information Age. The Internet has become so essential to modern life that several countries have declared Internet access to be a fundamental right.[4] But the importance of technology in the Information Age comes with a downside: the vulnerability of modern society and the global economy to minimally funded cyberattacks from remote corners of the world.

In the 1950s, American school children were taught to "duck and cover" in the event of an atomic bomb explosion.[5] A popular cautionary film from 1951 warns that a flash of light brighter than the sun accompanies such an explosion and that the flash could cause an inju-

---

2. SUN TZU, THE ART OF WAR 25 (Lionel Giles trans., El Paso Norte Press 2005) (1910).

3. WARGAMES (United Artists 1983). *WarGames* is a Cold War-era action film about a sentient computer operated by the U.S. Government and programmed to play through nuclear war scenarios to find an optimal outcome. The system is hacked by a teenage boy who unwittingly starts a simulation that brings the world to the brink of nuclear war. At the end of *WarGames*, the sentient computer controlling the U.S. nuclear arsenal finally learns one of the key tenets of deterrence during the Cold War: because of an opponent's capacity to counterstrike, sometimes foregoing aggressive actions is the only path to an optimal result. *See id.* Similar principles of deterrence underlie this Article, as we posit that a formalized active defense regime would be more effective at discouraging cyber aggressions than the currently available passive defense methods and legal options under criminal and civil law.

4. *See, e.g.*, COMM. ON OFFENSIVE INFO. WARFARE, NAT'L RESEARCH COUNCIL OF THE NAT'L ACADS., TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 38 (William A. Owens et al. eds., 2009) [hereinafter NRC REPORT] (noting Estonia's adoption of this position); *Internet Access Is 'a Fundamental Right,'* BBC NEWS (Mar. 8, 2010), http://news.bbc.co.uk/2/hi/8548190.stm (noting that Finland and Estonia take this view); Marshall Kirkpatrick, *Is Internet Access a Fundamental Human Right? France's High Court Says Yes*, READWRITEWEB (June 11, 2009, 9:29 AM), http://www.readwriteweb.com/archives/is_internet_access_a_fundamental_human_right_franc.php.

5. *See, e.g.*, DUCK AND COVER (Archer Productions 1951), *available at* http://www.archive.org/details/DuckandC1951.

ry more painful than a terrible sunburn.[6] The film, however, asserts that a child who "ducks and covers" will be more protected from the aftermath of nuclear detonation than otherwise.[7] Fortunately, no American city has ever experienced a nuclear attack, so no child has ever learned the hard way that a newspaper or a coat affords little protection against the heat from the detonation of an atomic bomb. The nuclear capabilities on both sides of the Cold War served as a deterrent against nuclear strikes and helped avoid an all-out nuclear conflict.[8] "Duck and cover," however, had no deterrent effect.

The Cold War ended about two decades ago, but new threats have emerged. The conflicts have shifted, the battlefields have morphed, and technologies that were not even dreamed of in 1951 now form the foundations for our everyday lives. The Internet, a technology partially developed to facilitate communication in the event of a nuclear attack,[9] changed the world forever. It is quite possible that future wars will be fought primarily in cyberspace, with the lines between civilian and military becoming increasingly blurred.[10] Instead of "duck and cover," computer users must now "scan, firewall, and patch."[11] However, like "duck and cover," purely passive defenses have questionable utility in the face of zero-day vulnerabilities[12] and sophisticated cyberweapons like the Stuxnet worm.[13] Likewise, law enforcement

---

6. *Id.*

7. *Id.*

8. *See* Louis René Beres, *Israel After Fifty: The Oslo Agreements, International Law and National Survival*, 14 CONN. J. INT'L L. 27, 54 (1999) (discussing the effectiveness of active defense in nuclear deterrence as turning on whether an opponent perceives that a possible target could retaliate in an "unacceptably destructive" manner).

9. *See* J.R. OKIN, THE INTERNET REVOLUTION: THE NOT-FOR-DUMMIES GUIDE TO THE HISTORY, TECHNOLOGY, AND USE OF THE INTERNET 130 (2005) (noting the military's need for a new, decentralized network architecture to withstand a nuclear attack).

10. *See* Pragati Verma, *Future Wars Will Be Fought in Cyberspace*, FIN. EXPRESS (Aug. 24, 2009), http://www.financialexpress.com/news/future-wars-will-be-fought-in-cyberspace/505992. Some sources indicate that China and North Korea already have units in their military that focus on cyberwarfare operations. *See* Sean M. Condron, *Getting It Right: Protecting American Critical Infrastructure in Cyberspace*, 20 HARV. J.L. & TECH. 403, 405 (2007) (noting China's capabilities); Arie J. Schaap, *Cyber Warfare Operations: Development and Use Under International Law*, 64 A.F. L. REV. 121, 133 (2009) (discussing North Korea's Unit 121).

11. *See* Mark Ward, *Tips to Help You Stay Safe Online*, BBC NEWS (Oct. 7, 2006), http://news.bbc.co.uk/2/hi/technology/5414992.stm (encouraging readers to regularly scan their systems for viruses and malware, maintain firewalls to prevent intrusions, and make sure that software and their operating system are updated and patched).

12. A zero-day exploit exists when there is a software vulnerability for which a malicious hacker creates an exploit prior to when the software vendor is made aware of the vulnerability. *See Top Cyber Security Risks — Zero-day Vulnerability Trends*, SANS INST. (Sept. 2009), http://www.sans.org/top-cyber-security-risks/zero-day.php.

13. *See* Dan Goodin, *Stuxnet Blitzed 5 Iranian Factories Over 10-Month Period*, REGISTER (Feb. 14, 2011, 6:53 PM), http://www.theregister.co.uk/2011/02/14/stuxnet_targeted_5_factories. The Stuxnet worm exploited four zero-day vulnerabilities — an unprecedented achievement according to the security company Symantec. *W32.Stuxnet*, SYMANTEC (Sept. 17, 2010, 8:53 AM), http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99.

and judicial action against malicious cyber intrusions currently do not present enough of a practical threat to deter potential attackers.[14]

The weaknesses of the current reliance on employing passive defense methods and seeking help from the authorities — who are both technologically and legally ill-equipped to seek justice for victims — present a difficult situation. Considering how modern society relies on the Internet and networked services, there is an urgent need for proactive policy to help insulate critical services from damage as well as mitigate harm from potential attacks. For a number of reasons explored below, we argue that, in some circumstances, permitting mitigative counterstrikes in response to cyberattacks would be more optimal. There is an urgent need for dialog on this topic as the development of technology has outpaced the law in this area.[15] While progress has been made in the form of executive orders addressing cybersecurity,[16] the proposed Cyber Intelligence Sharing and Protection Act ("CISPA"),[17] and cybersecurity provisions of the National Defense Authorization Act ("NDAA"),[18] these measures do not go far enough. New discussions and analyses are needed to ensure that responsive actions can be grounded in sound policy.

Because of the inadequacy in current means to address cyber threats, this Article examines other possible methods to deter cyberattacks, specifically the use of cyber counterstrikes as part of a model of active defense. Active defense involves (1) detecting an intrusion, (2) tracing the intruder, and (3) some form of cyber counterstrike.[19]

---

14. *See infra* Part II.B. For an explanation of our use of the term "cyber intrusion," refer to Part II.A.1.A.

15. *See* Rachael Fergusson, *Cyber Attacks Outpace Global Response, U.S. Warns*, ENGINEERING & TECH. MAG. (July 2, 2011), http://eandt.theiet.org/news/2011/jul/cyber-response.cfm.

16. *See, e.g.*, Exec. Order No. 13,010, 61 Fed. Reg. 37,347 (July 17, 1996).

17. Cyber Intelligence Sharing and Protection Act of 2011, H.R. 3523, 112th Cong. (2011). At the time of this writing, CISPA has passed through the House of Representatives, and its inclusion in the congressional dockets suggests that Congress is sensitive to the cyberspace issues that we raise in this Article.

18. National Defense Authorization Act for Fiscal Year 2012, Pub. L. No. 112-81, §§ 953–54, 125 Stat. 1298, 1550–51 (2011). Specifically, the NDAA contains provisions giving the President the authority to order the military to conduct cyberattacks, provided that the attacks comply with the rules that govern kinetic conflict and that the President complies with the requirements of the War Powers Resolution. *See infra* Part IV.A.3.C. Kinetic conflict refers to the use of conventional weapons intended to cause physical damage. *See* Timothy Noah, *Birth of a Washington Word*, SLATE (Nov. 20, 2002), http://www.slate.com/articles/news_and_politics/chatterbox/2002/11/birth_of_a_washington_word.html.

19. *See generally* Eric Talbot Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense*, 38 STAN. J. INT'L L. 207, 231 (2002) (noting active defense would likely include an in-kind response). For our purposes, we have designated three components to active responses. Detection, while not inherently active, is included because it is necessary for the subsequent components of active defense. We categorize tracing an intrusion as active because it necessitates going beyond the attacked system, and under current legal standards tracing itself may be viewed as an intrusion. *See* Bruce P. Smith, *Hacking, Poaching, and Counterattacking: Digital Counterstrikes*

Though intrusion detection and tracing are essential, counterstriking is key to enhancing the deterrent effects of active defense. At its core, cyber counterstriking is about two things: (1) deterring attackers and (2) ensuring that attacked parties are not deprived of the inherent right to defend themselves and their property. There are many views of deterrence, but deterrence is generally accomplished by the threat of some combination of the following elements: (1) punishing attackers by inflicting unacceptable costs, or (2) preventing attackers from succeeding in their attacks.[20] These two elements of deterrence have led us to apply the terms "retributive counterstriking" and "mitigative counterstriking," respectively, to the counterstriking component of active defense.

In the cyber context, a "counterstrike" can involve any number of actions. As discussed in Part III.B, a counterstrike can involve the target executing its own Denial of Service ("DoS") attack against the attacker (for example, by redirecting the attacker's packets back at the attacker to knock the attacker's systems offline),[21] infecting the attacker's system with a virus or worm to permit the victim to take control, or a number of other options. The technologies available to execute counterstrikes are generally the same ones used in initial attacks; as we examine in more detail below, some of these currently available technologies permit an attack to be traced back to its origin — with varying degrees of accuracy. Furthermore, there is now evidence that "cyber contractors" exist as part of what some have termed the new "military digital complex," whose work involves creating offensive cyber technologies that can have applications in the context of counterstriking.[22]

The goal of a counterstrike can vary, from punishing the attacker to simply mitigating the harm to the target. We call the former "retributive counterstriking"; this type should remain under the sole con-

---

and the Contours of Self-Help, 1 J.L. ECON. & POL'Y 171, 182 (2005) ("Given the broad and evolving contours of the CFAA, some commentators have suggested that even the relatively benign attempt to *trace* an originator of a computer-related attack through various intermediaries might run afoul of the statute."). The procedures of active defense then culminate in some form of counterstrike, which we argue may be retributive or mitigative.

20. *See* NRC REPORT, *supra* note 4, at 40. The United States Strategic Command defines deterrence as actions seeking to "convince adversaries not to take actions that threaten U.S. vital interests by means of decisive influence over their decisionmaking," where such decisive influence would be achieved through credible threats "to deny benefits and[/]or impose costs, while encouraging restraint by convincing the adversary that restraint will result in an acceptable outcome." U.S. ARMY TRAINING AND DOCTRINE COMMAND, U.S. DEP'T OF THE ARMY, THE UNITED STATES ARMY CONCEPT CAPABILITY PLAN FOR ARMY ELECTRONIC WARFARE OPERATIONS FOR THE FUTURE MODULAR FORCE 2015–2024 9, TRADOC PAMPHLET NO. 525-7-6, *available at* http://www.tradoc.army.mil/tpubs/pams/p525-7-6.doc (Aug. 16, 2007) (defining "Deterrence Operations").

21. *See infra* Part II.A.1.C.ii.

22. *See* Haroon Meer, *Lessons from Anonymous on Cyberwar*, AL JAZEERA (Mar. 10, 2011), http://www.aljazeera.com/indepth/opinion/2011/03/20113981026464808.html.

trol of the military, as a national security matter relating to sensitive domestic and international legal issues. We define "mitigative counterstriking" as taking active efforts to mitigate harm to a targeted system, in a manner strictly limited to the amount of force necessary to protect the victim from further damage. We recognize there may be overlap between retributive and mitigative counterstriking, as the latter could potentially result in damage to the attacker's system. However, the goal of mitigative counterstriking must be to *mitigate* damage from a *current and immediate* threat. We argue that whatever measures are deployed must be justifiable under a mitigation framework.

Cyber counterstrikes, however, are currently controversial, and it can be difficult under the current framework to differentiate between "hack back" vigilantism and legitimate exercises of a right to self-help.[23] Our proposal in this area is both modest and bold. Modest, because while we also discuss active defense as a broad topic, our primary focus is on mitigative counterstriking as a discrete subcategory of active defense activities. Bold, because we advocate for a significant shift from the prevailing approach to cyber intrusions. In recommending a new regime, we have chosen to focus on mitigative counterstriking as a starting point for two reasons. First, it is likely to be more effective than passive defense at accomplishing the goal of deterrence by denial. Second, a mitigative counterstriking regime would endow network administrators with the right to actively defend their property, thereby legitimizing the right to self-defense in the cyber realm. The current regime creates an unconscionable situation where parties are expected to give up the right to actively defend themselves against threats and instead rely on passive defense measures that may prove ineffective. Parties are left with no practical recourse through criminal enforcement or civil litigation for a number of reasons we discuss below.

Currently, the biggest barrier to defending against cyberattacks is the lack of a legal method to respond to cyberattacks that also has a credible deterrent effect on potential attackers. We posit that accurate and consistent use of mitigative counterstrikes could serve to deter cyberattacks against sensitive systems such as hospitals, government defense systems, and critical national infrastructure ("CNI"), and argue that implementing a regime to permit these sorts of counterattacks should be a priority. There is some evidence that the private sector has

23. *See, e.g.*, Smith, *supra* note 19, at 180 (using the term "hack back" to refer to digital counterstrikes); Deborah Radcliff, *Can You Hack Back?*, CNN.COM (June 1, 2000), http://archives.cnn.com/2000/TECH/computing/06/01/hack.back.idg (discussing retaliation against hostile cyber intrusions).

been tacitly utilizing this sort of technology to protect their systems,[24] effectively acting as cyber vigilantes under the current regime. Such behavior is at best legally ambiguous, and at worst illegal. Currently, the idea of mitigative counterstriking is treated like the proverbial elephant in the room, with legal commentators largely ignoring it.[25] After careful analysis, we conclude that this neglect is due to the lack of an analytical framework distinguishing between the perceived vigilantism of retributive counterstriking and the employment of self-help through mitigative counterstriking.

We thus propose a new policy and legal regime to address the threat of cyberattacks using active defense and mitigative counterstriking. There is a grave need to standardize approaches to mitigative counterstrikes,[26] and we must determine when the use of mitigative counterstrikes is appropriate, as well as who should be permitted to conduct mitigative counterstrikes. We recognize that counterstrikes of any variety can raise a number of legal and diplomatic concerns. While additional analysis and technological development may be desirable before implementing a broad self-defense regime, we argue that implementing mitigative counterstriking capabilities to protect CNI should be the first priority. Cyberattacks significantly affect private parties, including owners of CNI,[27] so it is important to legitimize active defense and mitigative counterstriking approaches in order to afford these private parties more protection against these threats.

In Part II, we examine the threat of cyber intrusions and possible responses, evaluating the methods and effects of cyberattacks and providing an overview of the current landscape of cyberattacks. We then turn to the available legal methods for addressing cyberattacks, arguing that each method has too many shortcomings to reliably address cyberattack issues and deter all categories of potential attackers. In Part III, we introduce active defense as the controversial fourth option for addressing cyberattacks, evaluating the different elements of active defense and arguing that when other methods of addressing cyberattacks are impractical or inadequate, permitting the use of mitigative counterstrikes is the socially optimal response to cyberattacks.

---

24. *See* Ruperto P. Majuca & Jay P. Kesan, *Hacking Back: Optimal Use of Self-Defense in Cyberspace* 5–6 (Ill. Pub. Law and Legal Theory Research Papers Series, Working Paper No. 08-20, 2009), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1363932.

25. *See, e.g.*, Katharine C. Hinkle, *Countermeasures in the Cyber Context: One More Thing to Worry About*, 37 YALE J. INTL. L. ONLINE 11, 12 (2011) (noting that little has been written on how the legal framework of countermeasures under international law would apply in the cyber context). This may be due in part to the controversial nature of active defense. *See* Matthew J. Sklerov, *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent*, 201 MIL. L. REV. 1, 83 (2009) ("Since active defenses represent a new frontier in cyberwarfare, their initial use will be controversial, no matter the situation.").

26. *See infra* Part VI.A.2 (discussing potential dangers of implementing a mitigative counterstriking regime in the private sector without a standardized approach).

27. *See infra* Part II.A.2.C.

In Part IV, we present a more detailed examination of the body of law relevant to cyberattacks, and in Part V, we focus on the aspects of the current legal regime that are particularly relevant to mitigative counterstriking as an act of self-defense. In Part VI, we set forth our recommendations for developing a viable active defense regime, taking into consideration the nuances and interactions of the cyber world and the various legal regimes examined in the Article.

II. THE THREAT: CYBER INTRUSIONS AND POSSIBLE RESPONSES

Networked computers, some say, are now "the nervous system of society."[28] Cyber intrusions have captured the public's imagination for the last several decades. Since the early 1980s, Hollywood's portrayal of hackers has ranged from a precocious teenager inadvertently hacking into computers located at "NORAD"[29] to a gang of cyberterrorists intent on taking over computer infrastructure in the United States.[30] While many of these portrayals employ significant artistic license to make movies more exciting, reality is starting to catch up with art. For example, consider Stuxnet, which the digital security company Kaspersky Lab calls "a working prototype of a cyberweapon that will lead to the creation of a new arms race in the world."[31] Understanding the problem of cyber intrusions requires a discussion of the technologies and threats, as well as an examination of the legal context. Cyber intrusions raise a myriad of issues that the

28. Sklerov, *supra* note 25, at 4. According to DOD's Dictionary of Military and Associated Terms, "cyberspace" is defined as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." DEP'T OF DEF., DICTIONARY OF MILITARY AND ASSOCIATED TERMS (2010), *available at* http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf. Graham Todd suggests that cyberspace's key feature is its nature as "a man-made domain designed to transfer data and information." Graham H. Todd, *Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition*, 64 A.F. L. REV. 65, 68 (2009). The National Military Strategy for Cyberspace Operations defines "cyberspace" as a "domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures." C. Todd Lopez, *Fighting in Cyberspace Means Cyber Domain Dominance*, AIR FORCE PRINT NEWS, Feb. 28, 2007, *available at* http://www.af.mil/news/story.asp?id=123042670.

29. *See* WARGAMES (United Artists 1983). "NORAD," the setting for much of the action in the film, is the abbreviation for the North American Aerospace Defense Command.

30. *See* LIVE FREE OR DIE HARD (20th Century Fox 2007); *see also* Walter Gary Sharp, Sr., *The Past, Present, and Future of Cybersecurity*, 4 J. NAT'L SECURITY L. & POL'Y 13, 13–14 (2010) (listing popular media depictions of cyber intrusions).

31. Press Release, Kaspersky Lab, Stuxnet Manifests the Beginning of the New Age of Cyber-Warfare, According to Kaspersky Lab (Sept. 24, 2010), http://usa.kaspersky.com/about-us/press-center/press-releases/stuxnet-manifests-beginning-new-age-cyber-warfare-according-kas.

current legal regimes fail to adequately address, underscoring the need for regulation and viable alternatives.

A. Attacks

Cyber intrusions can be devastating and can come from sources ranging from unsophisticated teenagers, to high-tech cyber criminals, to military officials.[32] It is almost impossible to accurately and consistently identify attackers,[33] which severely complicates any steps that might be taken to uncover those responsible and hold them accountable for their actions. Cyberattacks are not resource-intensive, which renders them even more dangerous because no practical requirement exists to limit the attackers to being members of organized and well-funded sources such as a nation's military.[34] One commentator has compared defense against cyberattacks to the Wild West because "the men in black hats can strike anywhere, while the men in white hats have to defend everywhere."[35]

Analyzing and responding to cyber threats have long been areas of interest for the U.S. Government. In Operation Eligible Receiver, a ninety-day cyberwarfare exercise the government conducted in 1997, thirty-five people acted as a rogue state.[36] Reports from the operation indicated that both government and commercial sites were susceptible to attacks using "off-the-shelf" technology.[37] In 2002, the U.S. Naval War College simulated a "digital Pearl Harbor" attack against CNI to gain insight into how such an attack would be carried out and what its effects would be.[38] Responding to such attacks is also time-sensitive — one expert estimates that an attack victim has only thirty-

32. *See Cyber Threat Source Descriptions*, U.S. COMPUTER EMERGENCY READINESS TEAM, http://www.us-cert.gov/control_systems/csthreats.html (last visited May 3, 2012).

33. Condron, *supra* note 10, at 417; *see also* NRC REPORT, *supra* note 4, at 37 (noting the technical difficulties of targeting a cyberattacker for responsive action).

34. *See* NRC REPORT, *supra* note 4, at 27; Steven R. Chabinsky, *Cybersecurity Strategy: A Primer for Policy Makers and Those on the Front Line*, 4 J. NAT'L SECURITY L. & POL'Y 27, 27 (2010); Sklerov, *supra* note 25, at 18. Some cyberattacks, like denial of service attacks, can be executed for as little as $50,000. *See, e.g.*, Press Release, M2 PressWIRE, Denial of Service Attacks Could Have Been Engineered by Anyone According to Imperva (July 13, 2009), http://www.m2.com/m2/web/story.php/20091759D17114ADDBC58025 75F2004A88CA (noting analysts' estimate of the cost of DoS attacks to attackers).

35. Neal Katyal, *Community Self-Help*, 1 J.L. ECON. & POL'Y 33, 60 (2005).

36. *See* Matthew Hoisington, *Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense*, 32 B.C. INT'L & COMP. L. REV. 439, 442 (2009).

37. *See id.* "Commercially available off-the-shelf item" is a term that is defined in the Federal Acquisition Regulation as referring to commercial items "sold in substantial quantities in the commercial marketplace." 41 U.S.C. § 104 (2006 & Supp. IV 2010), *amended by* Act of Jan. 4, 2011, Pub. L. No. 111-350, § 3, 124 Stat. 3679 (formerly codified at 41 U.S.C. § 431).

38. *See* Jason Krause, *Hack Attack*, 88 A.B.A. J. 51, 51 (2002). According to analysts at the time, an attack of sufficient strength to disable CNI would cost the attacker more than $200 million. *Id.*

six hours to identify the source of an attack before potential evidence is lost.[39] Michael Chertoff, the former Secretary of the Department of Homeland Security ("DHS") from 2005 to 2009, noted recently that cybersecurity is a top national security priority, especially in light of the potentially crippling effects of cyberattacks, as seen in the cases of Estonia and Georgia.[40]

A variety of cybersecurity issues have made headlines in recent years, from the penetration of campaign computers to reported vulnerabilities in the electrical grid and prolonged DoS attacks against computer networks.[41] To better explain the nature of these threats, we turn now to an examination of the technologies and actions involved.

1. What Is a Cyberattack?

One of the fundamental questions that arises when attempting to research and explain issues relating to cyberattacks is how to define a cyberattack. Because it is important to understand the conduct one seeks to regulate,[42] we provide more information about cyberattacks below.

A. Cyber-What? Attack or Exploitation?

The modern lexicon considers all types of online intrusions to be cyberattacks, even though many commentators would assert that such indiscriminate use of the term "cyberattack" is incorrect. The National Research Council's 2009 report about cyberattack capabilities ("NRC Report") defines "cyberattacks" 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."[43] The NRC Report distinguishes between cyberattacks,

---

39. *Id.* at 55.

40. Michael Chertoff, *Foreword to Cybersecurity Symposium: National Leadership, Individual Responsibility*, 4 J. NAT'L SECURITY L. & POL'Y 1, 1–2 (2010); *see also infra* Part II.A.2 (detailing the attacks on Estonia and Georgia). Chertoff's position is that there is a one-hundred percent probability of cyberattacks. Chertoff, *supra*. Chertoff has also spoken out against the sorts of rules and regulations that he thinks prevent intelligence agencies from investigating cybercrime domestically. *See* Jennifer Valentino-DeVries, *Chertoff: 'Rules and Regulations' Complicate Anti-Cybercrime Efforts*, WALL ST. J. (June 23, 2011, 9:40 AM), http://blogs.wsj.com/digits/2011/06/23/chertoff-rules-and-regulations-complicate-anti-cybercrime-efforts.

41. John Grant, *Will There Be Cybersecurity Legislation?*, 4 J. NAT'L SECURITY L. & POL'Y 103, 111 (2010).

42. *See* Sklerov, *supra* note 25, at 13.

43. NRC REPORT, *supra* note 4, at 80. Cyberattacks can also be viewed as actions that target the integrity, authenticity, and availability of components or devices on a network. *See* Herbert S. Lin, *Offensive Cyber Operations and the Use of Force*, 4 J. NAT'L SECURITY L. & POL'Y 63, 67 (2010).

which are destructive in nature, and "cyber exploitations," which are non-destructive actions that extract confidential information.[44] Crawlers are one form of cyber exploitation used to mine large quantities of data.[45] Though cyberattacks and cyber exploitations differ in their goals, it can be difficult to distinguish between the two because both use similar technology.[46]

The difficulty in distinguishing between cyberattacks and cyber exploitation occurs in many contexts, from informal discussions, to news articles, to academic commentary.[47] In this Article, we will primarily discuss cyberattacks as defined in the NRC Report. But because of the frequency with which the two terms are conflated, it is important to note that other authors may consider the term "cyberattack" to include cyber exploitation. In lieu of using the term "cyberattack" in a broad manner, we will use the term "cyber intrusion" when a broader concept is invoked; we will use "cyberattack" and "cyber exploitation" to denote the two specific subtypes of cyber intrusions.

Having defined what we consider to be a cyberattack, we should differentiate between the contexts in which cyberattacks may arise. The most effective approach in addressing a cyberattack depends on two variables: who conducts the cyberattack and how the cyberattack is conducted.

B. Categories of Attackers

There are three primary types of computer criminals: (1) unsophisticated "script kiddies" who conduct the majority of cyber intrusions, (2) more sophisticated hackers who tend to be curious rather than malicious, and (3) crackers who conduct cyberattacks for personal gain or malicious purposes.[48] There are also benign hackers who

---

44. NRC REPORT, *supra* note 4, at 10–11.

45. *See* Eric J. Feigin, Note, *Architecture of Consent: Internet Protocols and Their Legal Implications*, 56 STAN. L. REV. 901, 906 (2004) (defining a crawler as "an automated program that serially visits, or 'crawls,' websites and keeps a log of what it finds").

46. *See* NRC REPORT, *supra* note 4, at 81. For example, a cyberattacker's goal may be to destroy information, while the exploiter's goal is just to copy the information or observe network activity. *See id.* at 150. Duqu, a recent cyber exploit with some similarities to Stuxnet, demonstrates the overlap between the two concepts. Researchers posit that Duqu's purpose is to collect information for future attacks. *See W32.Duqu: The Precursor to the Next Stuxnet*, SYMANTEC (Oct. 24, 2011), http://www.symantec.com/connect/w32_duqu_precursor_next_stuxnet; Bob Gourley, *What You Need to Know About Duqu*, SYS-CON MEDIA (Dec. 15, 2011, 10:00 AM), http://www.sys-con.com/node/2103470.

47. *See, e.g.*, Siobhan Gorman, *China Hackers Hit U.S. Chamber*, WALL ST. J. (Dec. 21, 2011), http://online.wsj.com/article/SB10001424052970204058404577110541568535300.html (referring to cyber break-ins and information theft as "cyberattacks"); NRC REPORT, *supra* note 4, at 227; Chabinsky, *supra* note 34, at 30–31; Lin, *supra* note 43, at 82.

48. *See* Reid Skibell, *Cybercrimes & Misdemeanors: A Reevaluation of the Computer Fraud and Abuse Act*, 18 BERKELEY TECH. L.J. 909, 918–20 (2003); *see also* Krause, *supra* note 38, at 52, 54 (differentiating between hackers and crackers and quoting a source asserting that ninety-nine percent of attacks on the Internet come from script kiddies). A

use their skills to identify and suggest ways to improve systems and close exploitable holes,[49] though if they engage in this research without the authorization of the system's owner, they are potentially violating the law.[50]

Cyberattackers may be further categorized by group affiliation.[51] Cyberattackers with malicious intent may also be "patriotic hackers," engaging in cyber action to support possible military confrontations on behalf of their home countries.[52] Other cyberattackers may be "hacktivists," who differ from patriotic hackers insofar as hacktivists seek to make a statement about a political topic in a manner that may be contrary to the position of their home country.[53] A single cyberattack may involve multiple actors with a variety of intentions, and thus might not be attributable to a single category of attackers.[54]

"script kiddie" may be young as the label suggests, but this is not always the case. The major identifying feature of a script kiddie is a reliance on others for hacking tools, like scripts and code, with the script kiddies possessing little to no expertise themselves. *What Is a Script Kiddie?*, PC TOOLS, http://www.pctools.com/security-news/script-kiddie (last visited May 3, 2012).

49. *See* Skibell, *supra* note 48, at 938–39.

50. Such a violation may lead to a private cause of action like trespass to chattel. *See infra* Part IV.A.2. The Computer Fraud and Abuse Act also criminalizes the act of obtaining any information from a "protected computer" when the act is unauthorized or the actor exceeds granted authorization. 18 U.S.C. § 1030(a)(2) (2006). This statute defines "protected computer" so broadly that it would include any computer connected to the Internet. *See id.* § 1030(b) (defining a "protected computer" as a computer that "is used in interstate or foreign commerce or communication").

51. *See* MICHAEL A. VATIS, INST. FOR SEC. AND TECH. STUDIES AT DARTMOUTH COLL., CYBER ATTACKS DURING THE WAR ON TERRORISM: A PREDICTIVE ANALYSIS 1 (2001), *available at* http://www.ists.dartmouth.edu/docs/cyber_a1.pdf (citing four categories of cyber threats: terrorists, terrorist sympathizers, nation-states, and presumably non-affiliated thrill seekers).

52. *See* NRC REPORT, *supra* note 4, at 48. The NRC Report notes that patriotic hackers create diplomatic difficulties, and that the United States must take action to discourage patriotic hacking. *Id.*

53. *See Cyber Threat Source Descriptions*, U.S. COMPUTER EMERGENCY READINESS TEAM, http://www.us-cert.gov/control_systems/csthreats.html (last visited May 3, 2012) ("Hacktivists form a small, foreign population of politically active hackers that includes individuals and groups with anti-U.S. motives. They pose a medium-level threat of carrying out an isolated but damaging attack."). One example of a "hacktivist" group is Anonymous, which has become known in recent years for its attacks against the Church of Scientology, and more recently for claiming responsibility for DDoS attacks against opponents of WikiLeaks. David Kravets, *Guilty Plea in 'Anonymous' DDoS Scientology Attack*, WIRED THREAT LEVEL (Jan. 26, 2010, 5:01 PM), http://www.wired.com/threatlevel/2010/01/guilty-plea-in-scientology-ddos-attack; Paul Sims, *Anonymous, Wikileaks and the Age of Online Activism*, NEW HUMANIST (Dec. 9, 2010), http://blog.newhumanist.org.uk/2010/12/anonymous-wikileaks-and-age-of-online.html. In addition to DDoS attacks, another mark of an Anonymous attack is that hackers in the group will invade the target and acquire confidential files, as they did in their attacks on HBGary. Meer, *supra* note 22. A self-declared spokesman for Anonymous calls the DDoS and hacking acts of the group ethical acts of civil disobedience. Michael Isikoff, *Hacker Group Vows 'Cyberwar' on U.S. Government, Business*, MSNBC.COM (Mar. 8, 2011, 6:28 PM), http://www.msnbc.msn.com/id/41972190/ns/technology_and_science-security.

54. *See* Condron, *supra* note 10, at 412.

C. Categories of Attacks

There are three main categories of cyberattacks: distribution of malicious software (such as viruses, Trojan horses, and worms), unauthorized remote intrusions, and DoS attacks.[55] There is some overlap among these three categories of attacks, since Trojan horses may be used to enable unauthorized remote intrusions, and viruses may be used to create armies of zombie computers to execute Distributed Denial of Service ("DDoS") attacks.[56] In addition to these three types of attacks, an attacker who wishes to interrupt a service could also damage or steal the actual hardware.[57] Another type of attack, Domain Name System ("DNS") cache poisoning, attacks a protocol.[58] Cyberattacks can also be categorized based on the type of access used by the attacker: supply chain and vendor access, remote access, proximity access, or insider access.[59] This Part will focus on malicious software, DoS attacks, and the overlap between the two.

i. Malicious Software Attacks

Malicious software comes in a wide variety of forms, including Trojan horses, rootkits, exploits, and "zombies."[60] A Trojan horse is a piece of software that appears to be legitimate but has harmful effects that may include allowing malicious users to obtain "backdoor" access to the system.[61] For example, Trojan horses have been used to infiltrate computers at Microsoft headquarters.[62] Rootkits are "programs that use system hooking or modification to hide files, processes, registry keys, and other objects to hide programs and behaviors."[63] The Stuxnet worm is the first known rootkit that affects industrial

---

55. *See* Sklerov, *supra* note 25, at 13–14.

56. *See id.* at 16.

57. *See* Lilian Edwards, *Dawn of the Death of Distributed Denial of Service: How to Kill Zombies*, 24 CARDOZO ARTS & ENT. L.J. 23, 24 (2006).

58. *See* NRC REPORT, *supra* note 4, at 100. DNS cache poisoning involves corrupting a domain name system table through the use of malicious code, the effect of which is to cause visitors to think that they are visiting one domain, when they are actually visiting a different domain that likely hosts malware. *See Cache Poisoning (Domain Name System Poisoning or DNS Cache Poisoning)*, SEARCHSECURITY, http://searchsecurity.techtarget.com/definition/cache-poisoning (last updated May 2005).

59. *See* Chabinsky, *supra* note 34, at 32 (discussing the National Cyber Study Group's categorization of cyberattacks). In addition to the above categories of attacks, one could also distinguish attacks based on the underlying intent — similar to how mines can be used either defensively (to slow attacks) or offensively. *See* NRC REPORT, *supra* note 4, at 46.

60. *See* Sklerov, *supra* note 25, at 15.

61. *See What Is the Difference: Viruses, Worms, Trojans, and Bots?*, CISCO SYS., http://www.cisco.com/web/about/security/intelligence/virus-worm-diffs.html (last visited May 3, 2012).

62. *See* Jensen, *supra* note 19, at 209–10.

63. *Symantec Security Response: Windows Rootkit Overview*, SYMANTEC 4 (2005), http://www.symantec.com/avcenter/reference/windows.rootkit.overview.pdf.

control systems.[64] Zombifying software can be used to take control of an unprotected (or under-protected) computer, turning it into one zombie computer among thousands in a computer network known as a "zombie army" or "botnet."[65] The controller would then order the botnet to flood an organization's website with data and requests, in a DDoS attack.[66]

Viruses intended to zombify systems might rely on zero-day vulnerabilities to compromise a large number of systems in a short amount of time, illustrating the overlap between zero-day vulnerabilities, viruses, and DDoS attacks. Viruses and worms intended to zombify systems do not need to succeed against any particular machine, as some fraction of machines on the Internet will be vulnerable and thus will be infected if they encounter the zombifying software.[67]

Botnets are closely related to zombifying viruses in that the zombifying virus may include code that allows a botnet master to take control of the infected computer.[68] Botnets offer attackers many advantages, such as helping them to evade detection and enabling them to do more harm by controlling a large number of computers.[69] Botnets can be used to send spam, conduct DDoS attacks, or engage in a variety of other activities.[70] The botnet master does not necessarily need technical know-how to create the botnet, since control of botnets consisting of thousands of computers can be purchased for just a few hundred dollars.[71]

Because of the variety of threats botnets pose, countries must develop methods to cripple botnets. Japan has attempted to address the botnet problem by providing disinfection tools to the owners of infected computers, though the Japanese program does not have a very

64. *See* Nicholas Falliere, *Stuxnet Introduces the First Known Rootkit for Industrial Control Systems*, SYMANTEC, http://www.symantec.com/connect/blogs/stuxnet-introduces-first-known-rootkit-scada-devices (last updated Aug. 19, 2010); *infra* Part II.A.2.

65. *See Distributed Denial of Service Attack (DDoS)*, SEARCHSECURITY, http://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack (last updated June 2001) ("A computer under the control of an intruder is known as a zombie or bot. A group of co-opted computers is known as a botnet or a zombie army.").

66. *Id.*

67. *See* NRC REPORT, *supra* note 4, at 89.

68. *See id.* at 92. A botnet is "a network of computers, usually programmed for some repetitive task, under a single control mechanism." T. Luis de Guzman, *Unleashing a Cure for the Botnet Zombie Plague: Cybertorts, Counterstrikes, and Privileges*, 59 CATH. U. L. REV. 527, 528 (2010).

69. *See* de Guzman, *supra* note 68, at 529.

70. *See* NRC REPORT, *supra* note 4, at 96; *see also* Edwards, *supra* note 57, at 27–28. Edwards cites the Honeynet Project, which notes the use of zombie botnets for activities like sniffing network traffic, installing spyware, phishing, and click-fraud using Google's AdWords program. Edwards, *supra* note 57, at 28.

71. *See* Edwards, *supra* note 57, at 29.

high participation rate.[72] Researchers have also conducted "takedowns" of botnets by interrupting the controller's ability to issue commands to the infected computers.[73] However, these takedowns are generally only temporary measures because the zombie computers remain infected. It is theoretically possible, given enough information, to disseminate code to the botnet and thereby disinfect the zombie computers, but such actions would likely violate the Computer Fraud and Abuse Act ("CFAA") as well as international cybercrime statutes.[74]

ii. DoS and DDoS Attacks

Attackers execute DoS attacks by overwhelming the targeted computer system with data and requests that cause the system to cease functioning.[75] DoS attacks are examples of cyber operations that require multiple attacks over time because every time the attacks stop, the targeted system will recover.[76] CERT defines DoS attacks as attacks that are intended "to prevent legitimate users of a service from using that service."[77] According to a 2005 survey, seventeen percent of respondents, drawn from a range of companies with a bias towards those employing over one hundred workers, had experienced a DoS attack.[78] Because of the difficulty of distinguishing between a flood of legitimate requests and a DoS attack, some have noted that DoS attacks are difficult to criminalize (similar to the problem with criminalizing spam).[79]

Most systems today probably cannot be brought down by a single computer user executing a DoS attack.[80] But DDoS attacks, which are DoS attacks that the attacker launches simultaneously from multiple computers, pose a greater threat.[81] DDoS attacks are routinely perpe-

72. *See* Yasuhide Yamada, Atsuhiro Yamagishi & Ben T. Katsumi, *A Comparative Study of the Information Security Policies of Japan and the United States*, 4 J. NAT'L SECURITY L. & POL'Y 217, 226–28 (2010).

73. *See* Tillmann Werner, *The Inside Story of the Kelihos Botnet Takedown*, THREATPOST (Sept. 29, 2011, 11:10 AM), http://threatpost.com/en_us/blogs/botnet-shutdown-success-story-how-kaspersky-lab-disabled-hluxkelihos-botnet-092911.

74. *See* de Guzman, *supra* note 68, at 527–28. de Guzman discusses the Kraken botnet of 400,000 PCs that had been compromised to send spam. de Guzman, *supra* note 68, at 527–28. Although researchers learned how to direct the botnet to destroy itself, they chose not to because of uncertain legal consequences. *See id.*

75. *See* Schaap, *supra* note 10, at 134 (defining a DoS attack as "an assault on a network that floods it with so many additional requests that regular traffic is either slowed or completely interrupted"); Sklerov, *supra* note 25, at 16.

76. NRC REPORT, *supra* note 4, at 91.

77. *Denial of Service Attacks*, CERT, http://www.cert.org/tech_tips/denial_of_service.html (last updated June 4, 2001).

78. Edwards, *supra* note 57, at 31.

79. *See id.* at 24–25.

80. *See id.* at 25.

81. *See* Schaap, *supra* note 10, at 134; Sklerov, *supra* note 25, at 16.

trated using botnets[82] — there could be tens of thousands of infected machines in a network of zombie machines conducting a DDoS attack.[83] DDoS attacks are difficult to defend against and can also overwhelm passive defenses, thereby rendering the system more vulnerable to other attacks.[84] A 2004 survey indicated that over $26 million in losses were associated with DDoS attacks against respondents' networks in that year.[85] Data from 2011 indicates that DDoS attacks are still a very popular form of attack.[86] There are significant concerns that attackers might use DDoS attacks against CNI, such as hospitals or defense systems,[87] underscoring the importance of addressing DDoS attacks quickly and effectively.

D. Effects of Cyberattacks

The consequences of organized attacks generally fall into two broad categories: direct and indirect effects.[88] In the context of cyberattacks, direct effects impact the targeted computer system or network, whereas indirect effects impact systems that interact with the targeted system and people that rely on the targeted system.[89] Direct effects can include compromising the system's integrity, authenticity, or availability — but such direct effects are often reversible.[90]

Cyberattacks' indirect effects are generally larger than their direct effects because the attackers focus on causing disruption after the at-

---

82. *See* NRC REPORT, *supra* note 4, at 92. It should be noted, however, that DDoS attacks do not always rely on botnets. The hacktivist group Anonymous reportedly utilizes software called Low Orbit Ion Cannon ("LOIC") to enable thousands of users to execute simultaneous DoS attacks against a target, while other members of the group execute DDoS attacks using their own botnets. *See* Charles Arthur, *Thousands Download LOIC Software for Anonymous Attacks — But Are They Making a Difference?*, GUARDIAN TECH. BLOG (Dec. 10, 2010, 1:59 PM), http://www.guardian.co.uk/technology/blog/2010/dec/10/hackers-loic-anonymous-wikileaks. Another alternative to botnets for conducting DDoS attacks is a tool like d0z.me, which poses as a URL shortener. Bill Brenner, *LOIC and d0z.me: The Things Kids Teach Us*, CSO BLOGS (Dec. 22, 2010), http://blogs.csoonline.com/1310/loic_and_d0z_me_the_things_kids_teach_us (describing d0z.me as an exercise undertaken by a computer science major to illustrate some of the capabilities and dangers that lurk in seemingly benign services, like URL shorteners).

83. *See* Edwards, *supra* note 57, at 27.

84. *See* NRC REPORT, *supra* note 4, at 95; Sklerov, *supra* note 25, at 16–17.

85. Smith, *supra* note 19, at 172.

86. *Expect More DDoS Attacks Tomorrow*, KASPERSKY LAB (Aug. 29, 2011), http://www.kaspersky.com/about/news/virus/2011/Expect_More_DDoS_Attacks_Tomorrow.

87. *See* Edwards, *supra* note 57, at 35.

88. *See, e.g.*, Stephen Dycus, *Congress's Role in Cyber Warfare*, 4 J. NAT'L SECURITY L. & POL'Y 155, 163 (2010) (noting that both cyberattacks and nuclear attacks are marked by widespread and indiscriminate direct and indirect effects); Jill M. Sheldon, *Nuclear Weapons and the Laws of War: Does Customary International Law Prohibit the Use of Nuclear Weapons in All Circumstances?*, 20 FORDHAM INT'L L.J. 181, 188 (1996) (discussing direct and indirect health effects of nuclear weapons).

89. *See* NRC REPORT, *supra* note 4, at 30.

90. *See id.* at 111–12.

tacks rather than on affecting targeted systems themselves.[91] In some cases, a cyberattack's indirect effects can far outweigh its direct effects.[92] In addition to being more severe than direct effects, indirect effects are also generally not easily reversed.[93] The indirect effects of a cyberattack can include significant economic consequences. Repairing the system of a private company after an attack costs money, and the attack also has the potential to damage the company's reputation.[94] The fear of cyberattacks can also affect the behavior of Internet users, who might be deterred from using online resources to perform tasks such as filing tax returns online or even shopping online. If there is widespread avoidance of these online activities, cyberattacks could potentially cripple e-commerce.[95]

The outcome of a cyberattack is also inherently uncertain, and in some ways is more uncertain than an attack using traditional weapons.[96] Some commentators have noted that even a "minor" attack could eventually have destructive effects.[97] An indirect effect of particular relevance to the attacker is the danger of blowback, where the attacker experiences direct or indirect damage as a result of the initial attack.[98] Because the Internet is based on globally shared infrastructure, blowback effects also threaten entities in the United States if the U.S. Government conducts a cyberattack against a foreign enemy.[99]

2. Recent Cyberattack Threats

The potential danger of cyberattacks in the modern context has been discussed frequently over the last several years, especially fol-

---

91. *See id.* at 19.

92. *See id.* at 30.

93. *See id.* at 31 (comparing the difficulty of reversing the indirect effects of cyberattacks to the difficulty of reversing the direct effects of kinetic attacks). The NRC Report provides the example of a cyberattack that disrupts a computer controlling a generator, which has the indirect effect of destroying the generator. *Id.* at 113.

94. *See* Debra Wong Yang & Brian M. Hoffstadt, *Countering the Cyber-Crime Threat*, 43 AM. CRIM. L. REV. 201, 202 (2006). Some commentators suggest that companies underreport cyberattacks to authorities in part because of the potential damage to the companies' reputations. *See id.*

95. *See* Richard W. Downing, *Shoring Up the Weakest Link: What Lawmakers Around the World Need to Consider in Developing Comprehensive Laws to Combat Cybercrime*, 43 COLUM. J. TRANSNAT'L L. 705, 709 (2005). For example, the prevalence of fraud through cybercrime in Indonesia led some online retailers to block transactions to and from the country. *See id.*

96. *See* NRC REPORT, *supra* note 4, at 126. The NRC Report notes the unpredictability of cyberattacks in the context of the Sapphire/Slammer worm in early 2003, which was the fastest computer worm in history. The worm had a defective random number generator, and therefore did not spread as fast as it should have. *Id.* at 122. The presence of uncertainty, however, would not necessarily make military use of cyberattacks infeasible according to the findings of the National Research Council. *Id.* at 49.

97. *See, e.g.*, Todd, *supra* note 28, at 77.

98. *See* NRC REPORT, *supra* note 4, at 124.

99. *See id.* at 47.

lowing the attacks against Georgia and Estonia.[100] In April 2007, cyberattacks originating in Russia continued for weeks and crippled Estonian computer networks in the commercial and government sectors.[101] In June 2007, cyberattacks that originated in China disabled 1500 computers in the Pentagon.[102] Cyberattackers attacked Georgia shortly before the armed conflict between Russia and Georgia began in July 2008.[103] In 2009, DDoS attacks caused the shutdown of half of Kyrgyzstan's Internet Service Providers ("ISPs").[104] And in July 2009, a number of DDoS attacks were perpetrated against U.S. Government websites.[105]

The attacks on Estonia raised a number of questions under international law, including whether such attacks should be categorized as armed attacks. This is an issue that we examine in more detail in Part IV.B. The overlap of cyber and kinetic attacks against Georgia, however, suggests that cyberwarfare can be used aggressively and that our understanding of international law therefore must evolve to account for these new capabilities.

In addition to DDoS attacks against national communication systems, 2010 saw a number of interesting developments that illustrate the ways in which cyber intrusion capabilities can be used on a national level. For example, there is evidence that fifteen percent of worldwide Internet routes went through China for eighteen minutes in April 2010.[106] More destructive cyber intrusions occurred during that timeframe as well. In the summer of 2010, researchers discovered that

---

100. *See, e.g.*, John Markoff, *Before the Gunfire, Cyberattacks*, N.Y. TIMES, Aug. 13, 2008, at Al.

101. *See* Sklerov, *supra* note 25, at 4–5. Sklerov states that the attack on Estonia lasted three weeks, but other sources indicate that these attacks continued until mid-June. *See* Schaap, *supra* note 10, at 144. Ministry websites accustomed to receiving up to a thousand visits per day suddenly began receiving up to two thousand visits per second, which the websites were not equipped to handle. *See id.*

102. Sklerov, *supra* note 25, at 5; *see also* Hoisington, *supra* note 36, at 443.

103. *See* Sklerov, *supra* note 25, at 4–5. A second wave of attacks in August 2008 coincided with the advancement of Russian troops into South Ossetia and thus may represent the first time a country used a cyberattack in conjunction with a "ground war." Joshua E. Kastenberg, *Non-Intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law*, 64 A.F. L. REV. 43, 58 (2009) [hereinafter Kastenberg, *Neutrality*]. To enable government communications to stay online, Georgia moved some government websites to U.S. hosting companies. *Id.* at 46–47. These actions could have affected the status of the United States as a neutral party to this conflict even though the U.S. Government was not involved with the decision to provide these services to the Georgian government. *See id.* at 61.

104. *See* Patrick W. Franzese, *Sovereignty in Cyberspace: Can It Exist?*, 64 A.F. L. REV. 1, 4 (2009).

105. Ben Bain, *Cyberattacks Add Fuel to Cybersecurity Debate*, FED. COMPUTER WEEK, (July 10, 2009), http://fcw.com/articles/2009/07/10/cyberattacks-prompt-cybersecurity-debate.aspx; *see also* Sharp, *supra* note 30, at 24 (listing some issues of public concern raised by the DDoS attacks).

106. *See* Stew Magnuson, *Cyber Experts Have Proof that China Has Hijacked US-Based Internet Traffic*, NAT'L DEF. MAG. BLOG, (Nov. 12, 2010, 9:50 AM), http://www.nationaldefensemagazine.org/blog/Lists/Posts/Post.aspx?ID=249.

a worm called Stuxnet, which was apparently designed to interfere with industrial infrastructure, had infiltrated the nuclear program of Iran.[107] Some have suggested that the development of Stuxnet would have been too sophisticated and complicated to be undertaken by a private group, and thus assume that Stuxnet was developed with the support of a government.[108] One prominent researcher announced in December 2011 a new theory linking the Stuxnet worm, the infamous Conficker worm, and a more recent discovery named the Duqu worm.[109] Some suggest that Stuxnet originated in Israel, perhaps with the assistance of the United States.[110] Others hypothesize that the Chinese or Russian government developed Stuxnet.[111]

Apart from the prospect of international cyberconflict between states, there have also been a number of highly publicized cyberattacks involving members of the private sector as victims, perpetrators, or both. The "hacktivist" groups Anonymous and LulzSec have taken responsibility for a number of DDoS attacks over the last few years, including attacks by LulzSec on a variety of government and corporate targets over a span of fifty days in the summer of 2011,[112] and attacks by Anonymous on Paypal, Visa, and Mastercard in late 2010.[113] And it is still unknown who was behind the high-profile attacks on Sony's Playstation Network in the spring of 2011.[114] There have also been a number of recent reports in the media about massive data theft from private and public entities in the United States, much

107. *See* Robert McMillan, *Was Stuxnet Built to Attack Iran's Nuclear Program?*, PCWORLD (Sept. 21, 2010, 7:10 AM), http://www.pcworld.com/businesscenter/article/205827/was_stuxnet_built_to_attack_irans_nuclear_program.html. Iran has admitted that Stuxnet damaged its nuclear facilities. *See Iran Confirms Stuxnet Worm Halted Centrifuges*, CBSNEWS.COM (Nov. 29, 2010, 4:40 PM), http://www.cbsnews.com/stories/2010/11/29/world/main7100197.shtml.

108. *See, e.g.*, Josh Halliday, *Stuxnet Worm Is the 'Work of a National Government Agency'*, GUARDIAN (Sept. 24, 2010, 10:35 AM), http://www.guardian.co.uk/technology/2010/sep/24/stuxnet-worm-national-agency.

109. Jim Finkle, *Did "Worm" Help Sabotage Iran's Nuclear Program?*, REUTERS, Dec. 2, 2011, http://www.reuters.com/article/2011/12/02/us-cybersecurity-iran-newspro-idUSTRE7B112P20111202; *see also* Gourley, *supra* note 46 (explaining Duqu's similarities to Stuxnet).

110. *See, e.g.*, William J. Broad, John Markoff & David E. Sanger, *Israel Tests Called Crucial in Iran Nuclear Setback*, N.Y. TIMES, Jan. 15, 2011, at A1; Kim Zetter, *Did a U.S. Government Lab Help Israel Develop Stuxnet?*, WIRED THREAT LEVEL (Jan. 17, 2011, 10:13 PM), http://www.wired.com/threatlevel/2011/01/inl-and-stuxnet.

111. *See* Chris Demchak, *Stuxnet: Signs Could Point to Russia*, ATLANTIC COUNCIL (Nov. 26, 2010), http://www.acus.org/new_atlanticist/stuxnet-signs-could-point-russia.

112. *See* Andy Greenberg, *LulzSec Says Goodbye, Dumps NATO, AT&T, Gamer Data*, FORBES (June 25, 2011, 10:46 PM), http://www.forbes.com/sites/andygreenberg/2011/06/25/lulzsec-says-goodbye-dumping-nato-att-gamer-data.

113. *See* Kim Zetter, *FBI Arrests U.S. Suspect in LulzSec Sony Hack; Anonymous Also Targeted*, WIRED THREAT LEVEL (Sept. 22, 2011, 5:51 PM), http://www.wired.com/threatlevel/2011/09/sony-hack-arrest.

114. *See id.*

of which has been traced to a small number of hacker teams located in China.[115]

A. Frequency of Cyberattacks

Cyber intrusions occur with disturbing frequency, especially when computers are not protected. In 2004, the Honeynet Project began a study by connecting unprotected computers to the Internet and measuring how long it took for a hacker to compromise the computers.[116] As of 2004, while the study was still underway, it took three days for a Linux server to be successfully hacked, while a standard Windows computer with file sharing enabled was hacked five times within four days.[117] In July 2005, a British antivirus firm reported that unprotected home PCs had a fifty percent chance of becoming infected within twelve minutes of connecting to the Internet.[118] Another study found that computers running the then-latest Microsoft operating system (Vista) without any protection from cyberattacks had a "survival time" of around four minutes between being connected to the Internet and becoming compromised by malicious software.[119] Passive defense is thus critical, though we argue that passive protections alone are insufficient for the most sensitive targets.

Protected systems also come under frequent attack, though presumably the success rate lower than it is for unprotected systems. In 1999, the Department of Defense ("DOD") detected over 22,000 attacks against its system.[120] On a single day in 2008, the Pentagon computer systems received six million attempted intrusions from the outside.[121] Researchers in the summer of 2008 discovered an electron-

---

115. *See, e.g.*, *A Few Hacker Teams Do Most China-Based Data Theft*, CBSNEWS.COM (Dec. 12, 2011, 11:10 AM), http://www.cbsnews.com/8301-501366_162-57341365/a-few-hacker-teams-do-most-china-based-data-theft.

116. Edwards, *supra* note 57, at 30.

117. Bruce Schneier, *Foreword* to THE HONEYNET PROJECT, KNOW YOUR ENEMY: LEARNING ABOUT SECURITY THREATS xxvii–xxviii (2d ed. 2004), *available at* http://old.honeynet.org/book/Fore.pdf. The Honeynet Project ultimately estimated there were around a million infected zombie computers as of 2005. John Leyden, *Rise of the Botnets: Honeynet Project Lifts the Lid on Zombie Networks*, REGISTER (Mar. 15, 2005, 4:55 PM), http://www.theregister.co.uk/2005/03/15/honeypot_botnet_study/print.html.

118. *See* John Leyden, *Malware Authors Up the Ante*, CHANNEL REGISTER (July 1, 2005, 10:54 AM), http://www.channelregister.co.uk/2005/07/01/sophos_1h05_malware_report (citing the proliferation of viruses and worms as responsible for this increased threat of attacks on unprotected PCs).

119. *See* de Guzman, *supra* note 68, at 550. Another threat related to information security is identity theft, of which there were over ten million cases in the United States in 2009. Sharp, *supra* note 30, at 13.

120. *See* Jensen, *supra* note 19, at 210.

121. *See* Franzese, *supra* note 104, at 2. The use of social networking websites by the federal government, while helpful on some levels, may also increase vulnerability. *See* Sharp, *supra* note 30, at 19. Some of the risks may be due to the carelessness of federal employees — computers on the DOD network access the Internet mostly through the Non-Secure Internet Protocol Router Network ("NIPRNET"), and one study indicates that DOD

ic spying operation where malicious software was found on almost 1300 computers located in 103 countries.[122]

Private entities also experience a significant number of intrusions. In 2001, over thirteen percent of law firms reported that they had experienced attacks on their computer systems in the previous year.[123] In 2002, the Computer Security Institute of San Francisco compiled statistics with the FBI indicating that ninety percent of surveyed companies had their computer security breached in the previous year; eighty percent of those companies suffered financial losses, though only thirty-four percent notified law enforcement of the intrusions.[124] In 2004, a survey by the Computer Security Institute and the FBI concluded that only twenty percent of companies that experienced intrusions reported the intrusions to law enforcement.[125] CERT at Carnegie Mellon University received reports of 137,529 computer security incidents in 2003, and ceased tracking such incidents in 2004 because such incidents had become so common.[126] A survey published in 2005 noted that over half of the 693 responding U.S. businesses detected security breaches in their networks during the last twelve months.[127]

B. Potential Government Use of Cyberattacks and the Danger of Cyberwar

This Part discusses the actual and potential government use of cyberattacks, as well as cyberwar issues. Subsequent Parts explore international law issues in more detail, but such issues are introduced in this Part to underscore the gravity of the situation. Most discussion on government use of cyberattacks takes place in the context of the

---

computers access the Internet for non-official purposes over two-thirds of the time. Joshua E. Kastenberg, *Changing the Paradigm of Internet Access from Government Information Systems: A Solution to the Need for the DOD to Take Time-Sensitive Action on the NIPRNET*, 64 A.F. L. REV. 175, 183 (2009) (also noting that between the seven million DOD-owned computers, the Internet is accessed over a billion times every day) [hereinafter Kastenberg, *Paradigm*].

122. *See* Franzese, *supra* note 104, at 3. The software had the capability of putting a remote user in control of web cameras and audio recording devices. *Id.*

123. Krause, *supra* note 38, at 52.

124. *Id.*; *see also* Franzese, *supra* note 104, at 2 (discussing a New York-based financial house that was "attacked" one million times over the course of one day).

125. LAWRENCE A. GORDON ET AL., COMP. SECURITY INST., 2004 CSI/FBI COMPUTER CRIME AND SECURITY SURVEY 13 fig.20 (2004), *available at* http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2004.pdf.

126. *CERT Statistics (Historical)*, CERT, http://www.cert.org/stats (last updated Feb. 12, 2009). "An incident may involve one site or hundreds (or even thousands) of sites. Also, some incidents may involve ongoing activity for long periods of time . . . . The website does not further define the word 'incident,' but a discussion implies that it is some type of suspected attack on a computer system." Condron, *supra* note 10, at 404 n.7.

127. LAWRENCE A. GORDON ET AL., COMP. SECURITY INST., 2005 CSI/FBI COMPUTER CRIME AND SECURITY SURVEY 12 (2005), *available at* http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2005.pdf.

national government and national defense.[128] There are, however, indications that local law enforcement agencies have been involved with similar topics on a smaller scale, such as by using DoS attacks against wireless devices like garage door openers as well as jamming cellular phone traffic to help capture suspects.[129] However, there is no evidence that law enforcement authorities have ever launched cyber counterattacks, though it is possible that covert cyber counterstrikes occur.[130]

The NRC Report observes that cyberattacks raise issues similar to those raised by other instruments of war.[131] However, these issues are more complicated because of the importance of speed in using cyberweapons, the unpredictability of cyberweapons' effects, and the difficulty of noticing that cyberweapons are being used.[132] The NRC Report makes several recommendations for policymakers considering the use of cyber capabilities during conflict, including: (1) policymakers should judge the significance of launching a cyberattack based largely on the likely direct and indirect effects of such an attack, (2) policymakers should apply the principles of the law of armed conflict to cyberattacks, (3) the United States should possess cyberattack capabilities, and (4) there should be sufficient levels of trained personnel to handle cyberattack conflicts and concerns.[133]

The U.S. Government has systems in place for protecting government networks from the threats posed by cyberattacks. The U.S. Strategic Command ("STRATCOM") is the part of DOD that monitors attacks on DOD systems.[134] DOD is responsible for securing the .mil domain and recently established the U.S. Cyber Command for conducting defensive and offensive computer network operations.[135] Cyber Command, at present, does not defend commercial or civilian networks, but some argue this may be necessary in the near future.[136] DHS is responsible for securing the .gov domain,[137] and its protec-

128. *See* NRC REPORT, *supra* note 4, at 3 (focusing on the idea of a legal framework governing cyberattacks that turns on international law concepts).

129. *See* NRC REPORT, *supra* note 4, at 201. However, there is as yet no evidence that law enforcement engages in activities that involve altering data, in part because they want everything they obtain to be legally admissible evidence. *Id.* There has also been proposed legislation to permit prisons to jam cell phone signals. Matthew Harwood, *Bill Would Allow Prisons to Jam Cell Phone Signals*, SECURITY MGMT. (Jan. 16, 2009), http://www.securitymanagement.com/news/bill-would-allow-prisons-jam-cell-phone-signals-005082.

130. *See* NRC REPORT, *supra* note 4, at 203.

131. *Id.* at 55.

132. *Id.*

133. *Id.* at 67–70.

134. *Id.* at 35.

135. Chertoff, *supra* note 40, at 4.

136. *See, e.g.*, Mark D. Young, *National Cyber Doctrine: The Missing Link in the Application of American Cyber Power*, 4 J. NAT'L SECURITY L. & POL'Y 173, 174, 176 (2010).

137. *Id.* at 174.

tions include Einstein — also called the National Cyber Protection System — Einstein 2, and Einstein 3.[138] These three systems possess intrusion detection capabilities.[139] DHS also includes the U.S. Computer Emergency Readiness Team ("US-CERT"), which leads efforts in responding to threats and managing risks.[140] While the appropriateness of the government regulating its own systems is generally acknowledged, there is an argument that the government should not be charged with setting binding private security standards,[141] as this kind of governmental control could raise First Amendment issues.[142]

Beyond this sort of administrative question, however, there lies the foundational issue of how cyberwars might arise and be conducted. Steps taken to mitigate harm to a cyberattack victim must be carefully tailored to avoid characterization of these mitigative steps as acts of cyberwarfare. Understanding the threat of cyberwar will help underscore both the importance of implementing active defense regimes with an awareness of international law implications and the importance of placing the focus on mitigation rather than retribution.

i. Cyberwar and Warmaking Powers in the United States

Before we can properly analyze war and cyberwar, we must first provide definitions for these concepts. In the nineteenth century, the U.S. Supreme Court described war as "the exercise of force by bodies politic . . . against each other, for the purpose of coercion."[143] What is

138. Chertoff, *supra* note 40, at 4.

139. *Id.*; *see also* Gus P. Coldebella & Brian M. White, *Foundational Questions Regarding the Federal Role in Cybersecurity*, 4 J. NAT'L SECURITY L. & POL'Y 233, 239–40 (2010); Gregory T. Nojeim, *Cybersecurity and Freedom on the Internet*, 4 J. NAT'L SECURITY L. & POL'Y 119, 123 (2010). Much information concerning the Einstein system is still classified and thus unavailable for discussion in this Article. *See* Nojeim, *supra*, at 124–25. Some commentators have been critical of the low degree of openness in the national cybersecurity discussion. *See, e.g.*, *id.* at 135. If an IDS system like Einstein were implemented for civilian federal networks, policymakers would need to decide which agency would implement the IDS system, where it would be deployed, and what legal safeguards would be needed. *See* Coldebella & White, *supra*, at 234.

140. Chertoff, *supra* note 40, at 5.

141. *See* Nojeim, *supra* note 139, at 129–30 (suggesting that the private sector, rather than the federal government, should bear the responsibility for setting standards for the private sector). *But see* Coldebella & White, *supra* note 139, at 237, 242–43 (arguing that DHS has the traits to successfully overcome the systemic obstacles to implementing national cybersecurity policy).

142. *See* Chertoff, *supra* note 40, at 2. Chertoff suggests, however, that it may be possible to put trusted third parties in place as intermediaries between the government and the private sector to act as "cyber escrow agents" to provide "the benefit of government expertise" while avoiding direct control of the civilian domain by the government. *Id.* at 5.

143. The Prize Cases, 67 U.S. (2 Black) 635, 652 (1863); *see also* Susan W. Brenner with Leo L. Clarke, *Civilians in Cyberwarfare: Conscripts*, 43 VAND. J. TRANSNAT'L L. 1011, 1024 (2010). Brenner and Clarke note that regardless of the definition, war is always a purely collective undertaking that involves a struggle between two sovereigns. Brenner with Clarke, *supra*. If war activities are no longer monopolized by sovereigns, as may soon be the case with cyberwar, "traditional warfare may no longer be viable." *Id.* at 1025–26.

cyberwarfare or information warfare? Professor Stephen Dycus uses the term "cyberwarfare" to refer to conflicts utilizing cyberweapons offensively or defensively.[144] Major Arie Schaap of the U.S. Air Force proposes a definition for "cyberwarfare operations" as "the use of network-based capabilities of one state to disrupt, deny, degrade, manipulate, or destroy information resident in computers and computer networks, or the computers and networks themselves, of another state."[145] Cyberwarfare would likely fall within the category of "information operations," which DOD defines as including "electronic warfare, computer network operations, psychological operations, military deception and operations security."[146] Computer network operations include attack, defense, and exploitation.[147] More specific aspects of cyberwarfare may include operations that cause permanent damage to an enemy's system, such as deleting files or inserting malicious code.[148]

Cyberwarfare is likely to be especially attractive to military leaders because it conserves human and nonhuman resources, though the low costs may also remove disincentives against offensive operations.[149] However, there is no unified information operations doctrine for the whole military,[150] and creating such policies will require leaders to consider a number of highly technical issues that few leaders currently understand.[151] Thus, educating civilian and military leaders is an essential element to effectively addressing potential future international cyber crises.

Because cyberwar is an example of an information operation, it can be viewed as a subcategory of activities involved in physical war. Accordingly, discussions of cyberwar implicate fundamental issues of war, such as how war is initiated and the rules that govern it, includ-

---

144. Dycus, *supra* note 88, at 162. In the cyber context, however, it can be difficult to characterize cyberattacks as offensive or defensive. *See id.*

145. Schaap, *supra* note 10, at 127.

146. Cyberspace & Info. Operations Study Ctr., *What Are Information Operations?*, CYBERSPACE AND INFO. OPERATIONS STUDY CENTER, http://www.au.af.mil/info-ops/what.htm (last updated July 24, 2010).

147. *Id.*

148. *See* Schaap, *supra* note 10, at 159.

149. *See* Brenner with Clarke, *supra* note 143, at 1013–14. The availability of cyberattacks might lead to problems similar to those that have resulted from the use of tasers by law enforcement, as the option for non-lethal force might make hostile response more attractive. *See* NRC REPORT, *supra* note 4, at 39 (noting that the availability of cyberattacks in place of kinetic force may increase the likelihood that nations will intervene more than they would have when cyberattacks were not an option). This raises the question of whether the existence of non-lethal weapons creates legal or ethical obligations that these non-lethal weapons be used before resorting to lethal weapons. *Id.* at 301.

150. *See* Young, *supra* note 136, at 180. Some critics say that none of the branches of the military are currently qualified to control production or management of a cyber force. *See id.* at 185.

151. *See id.* at 193 ("The emerging discipline of network operations is a highly technical arena that few civilian or military leaders over the age of 30 adequately understand.").

ing the respective warmaking powers of the President and Congress. The Constitution explicitly vests in Congress the authority to declare war, but the President has some authority to take actions relating to war.[152] It is relatively uncontroversial to assert that the President has warmaking powers when acting in the nation's self-defense. However, when ordering military action without congressional authorization for reasons other than self-defense, the President must comply with the War Powers Resolution.[153] Congress passed the War Powers Resolution after the Vietnam War, requiring the President to notify Congress of the use of the military in hostile situations and placing a time limit on such actions unless Congress expressly approves of continued deployment.[154] In addition to his authority as the Commander-in-Chief, the President also has statutory authority to take control of telecommunications networks in times of war.[155] The potential overlap between this authority and cyberwar activities could prove very significant in the future, though a discussion of these implications is beyond the scope of this Article.

With as much conflict as currently exists between the executive and legislative branches with regard to warmaking powers, cyberwar will introduce even more strife.[156] The NRC Report indicates that Congress is likely not privy to regular or systematic information about cyberattacks in the United States.[157] Dycus asserts that congressional silence on cyberwar matters could potentially be viewed as giving full discretion to the President.[158] Dycus also proposes seventeen recommendations for creating a new policy on cyberwar, including an express prohibition on automating active defense.[159]

In addition to warmaking authority issues, there are also concerns about how the rules governing war should apply to cyberwar. Some might argue that cyberwar activities are substantially different from traditional war, and thus the requirements governing traditional war do not apply in the cyber context, but this is not necessarily the case. Michael Wynne, former U.S. Secretary of the Air Force, asserts "all

152. U.S. CONST. ART. I, § 8, cl. 11.

153. 50 U.S.C. §§ 1541–1548 (2006).

154. *See* Dycus, *supra* note 88, at 157–58. Dycus, however, argues that the War Powers Resolution notice requirements are too relaxed and unrealistic for cyberwar. *Id.* at 162. As part of the NDAA, Congress has authorized DOD to conduct offensive operations in cyberspace using the same rules that apply to kinetic conflict. National Defense Authorization Act for Fiscal Year 2012, Pub. L. No. 112-81, § 954, 125 Stat. 1298, 1551 (2011). Congress further stated in the NDAA that the President has the authority to direct DOD in these actions pursuant to the War Powers Resolution. *Id.*

155. 47 U.S.C. § 606 (2006).

156. *See* NRC REPORT, *supra* note 4, at 233.

157. *See id.* at 236.

158. Dycus, *supra* note 88, at 158. Dycus views congressional silence as dangerous because the national interest in electronic warfare is too great to leave electronic warfare decisions solely to the executive branch. *Id.*

159. *Id.* at 167–70.

aspects of air war will have some equivalent role in cyber war."[160] The NRC Report argues that we should apply the same rules and policies for both forms of conflict, stating "the only differences are operational."[161] In line with these arguments, the NDAA includes a provision directing the military to apply the laws of war to cyberwar.[162]

Some have argued, however, that additional military doctrines are necessary to specifically address cyberattacks.[163] This perceived need for policy guidance in the context of cyberattacks includes rules of engagement defining the appropriate use of force under specific circumstances.[164] Some have also noted the need for policies regarding cyberweapon use, arms control agreements, the delegation of authority, and transparency.[165] Transparency requirements — important for earning and maintaining the public's trust[166] — would bind agencies

160. Michael W. Wynne, *Senior Leader Perspective: Flying and Fighting in Cyberspace*, 21 AIR & SPACE POWER J. 5, 7–8 (2007), *available at* http://www.airpower.au.af.mil/airchronicles/apj/apj07/spr07/spr07.pdf.

161. NRC REPORT, *supra* note 4, at 164.

162. National Defense Authorization Act for Fiscal Year 2012, Pub. L. No. 112-81, § 954, 125 Stat. 1298, 1551 (2011).

163. *See* Young, *supra* note 136, at 178 (defining "military doctrine" as a codification of "how the government should be organized, what tasks it should be prepared to accomplish, and what resources it will need to fulfill its role"). Young argues that a national cyber doctrine is necessary, and that its design could be potentially based on the U.S. counterinsurgency doctrine — the development of which involved input from non-governmental organizations. *Id.* at 174–75. Young stresses the importance of having a cyber doctrine in place prior to a national crisis. *Id.* at 176. Young also suggests that a new cyber doctrine should include a chapter of definitions to ensure that everyone has common terms of reference. *Id.* at 191.

164. *See* Hoisington, *supra* note 36, 445–46, 451 (noting the need for rules of engagement and their possible use to govern acts like anticipatory self-defense). Rules of engagement might include guidelines such as the permissible scope and duration of cyberattacks and who should be notified when a cyberattack is conducted. *See* NRC REPORT, *supra* note 4, at 169. Developing rules of engagement is likely to be very difficult, and one of the big questions that needs to be addressed is under what circumstances and under what authority might active defense be appropriate to neutralize an immediate threat. The NRC Report examines a number of additional issues surrounding the developing rules of engagement for cyber counterstrikes. *Id.* at 51–53. World leaders have recently formally recognized the need for cyber rules of engagement, including cybersecurity in the agenda of the Munich Security Conference for the first time in 2011. *See* Susan Watts, *Proposal for Cyber War Rules of Engagement*, BBC NEWS, http://news.bbc.co.uk/2/hi/programmes/newsnight/9386445.stm (last updated Feb. 3, 2011). However, we urge that guidelines for cyberwar must be flexible because of the constantly shifting cyber environment.

165. *See* NRC REPORT, *supra* note 4, at 58–59, 62, 216–17, 229, 326; *see also* Young, *supra* note 136, at 189; Nojeim, *supra* note 139, at 120. Young also encourages cyber doctrine to be largely unclassified, though he notes that details about specific weapons and techniques should be classified. Young, *supra* note 136, at 188.

166. *See* John N. Greer, *Square Legal Pegs in Round Cyber Holes: The NSA, Lawfulness, and the Protection of Privacy Rights and Civil Liberties in Cyberspace*, 4 J. NAT'L SECURITY L. & POL'Y 139, 141 (2010) (discussing transparency, continued oversight, and the establishment of clear roles and missions for intelligence agencies as three ways to earn and maintain the public's trust); Nojeim, *supra* note 139, at 137 (arguing that a successful cybersecurity program will accomplish three objectives: ensuring transparency, promoting

to explain their actions "as openly and candidly as possible," although some aspects might be kept classified for national security.[167]

Discussions of cyberattack issues are often conducted in terms of analogies, such as a "cyber Pearl Harbor," or by comparing policy needs to those of the Cold War.[168] One issue with using the language of Cold War deterrence is that threatening retaliation in cyberwarfare is qualitatively different from threatening nuclear retaliation. Some argue that threats of executing cyberattacks would be less credible than nuclear threats, and thus the presence of cyber capabilities may have less of a deterrent effect.[169] We acknowledge that the idea of "credibility" with respect to a threat of retaliation is very different in the cyber and nuclear contexts. However, we disagree with the argument that cyberattack capabilities would not provide a deterrent effect. As we discussed above, a threat to punish or a denial of success may provide effective deterrence.[170] Nuclear deterrence worked because it was based on a threat of punishment. On the other hand, cyber deterrence — specifically, a model utilizing mitigative counterstriking — would be focused on deterrence by denial. Additionally, in the nuclear context, deterrence was aimed at large governmental bodies, whereas in the cyber context, there are a wide variety of potential attackers whose aggressive actions could be deterred to differing extents by different approaches. Thus it is important not to discount the potential deterrent effects of cyberattack capabilities at this stage.

ii. Cyberwar Preparations and the Private Sector

Many academics and political figures have weighed in on the potential for cyberwarfare. Nikolai Kuryanovich, a Russian politician, wrote in 2006 he expects that in the near future many conflicts will take place in cyberspace instead of traditional war environments.[171]

---

industry cooperation, and acknowledging the differences between the categories of infrastructure).

167. Greer, *supra* note 166, at 142; *see also* Coldebella & White, *supra* note 139, at 235 (asserting that DHS should be in charge of the federal government's cyber effort, but that there should be greater transparency for much of the information).

168. *See, e.g.*, Schaap, *supra* note 10, 172–73 (expressing the need to set out policies in advance of a "cyber Pearl Harbor-like attack").

169. *See* NRC REPORT, *supra* note 4, at 295. Rather than analogizing to the Cold War, Hunker suggests analogizing the development of doctrines addressing cyberwarfare to the development of the Chemical Weapons Convention. Jeffrey Hunker, *U.S. International Policy for Cybersecurity: Five Issues That Won't Go Away*, 4 J. NAT'L SECURITY L. & POL'Y 197, 214–15 (2010) (noting that the implementation of the Chemical Weapons Convention has taken a long time and is an ongoing process, requiring new infrastructure to monitor compliance).

170. *See supra* text accompanying note 20.

171. Brian Krebs, *Lithuania Weathers Cyber Attack, Braces for Round 2*, WASHINGTON POST SECURITY FIX BLOG (July 3, 2008, 12:10 PM), http://voices.washingtonpost.com/securityfix/2008/07/lithuania_weathers_cyber_attac_1.html. The Outer Space Treaty, for example, includes a Liability Convention that could make states liable if they conduct dam-

Some commentators have asserted that cyberspace provides potential asymmetric advantages, which may be utilized by less powerful nations to exploit the reliance of the United States on information infrastructure.[172] Specifically, China recognizes the value of cyberwarfare,[173] and its military includes "information warfare units."[174] Meanwhile, Russia has a cyberwarfare doctrine that views cyberattacks as force multipliers, and North Korea's Unit 121 focuses solely on cyberwarfare.[175] Many suspect that the Russian government conducted the cyberattacks against Estonia, Georgia, and Kyrgyzstan, though the Russian government's involvement has not been proven.[176] Estimates suggest there are currently 140 nations that either have or are developing cyberwarfare capabilities.[177]

It is fair to say that preparations are underway to make cyberwarfare a viable alternative to physical warfare, and that policymakers are recognizing the applicability of the laws of war to the cyber context.[178] The effects of these changes on the private sector cannot be ignored. The line between the government and the private sector on cyberwar matters is blurred. Dycus notes that the federal government has at times delegated to private companies the task of operating cyber technology for the purpose of collecting and analyzing intelligence.[179] Because of the degree to which the private sector is involved with cyber infrastructure, many commentators have observed that the private sector will likely be heavily implicated by future cyberwars.[180]

---

aging cyberwarfare operations against a satellite owned by another state. Schaap, *supra* note 10, at 164.

172. *See* Franzese, *supra* note 104, at 36–37 (arguing that China would be opposed to establishing state sovereignty in cyberspace in the interest of preserving certain asymmetric advantages). The United States may have a strong presence in cyberspace, but it is not realistic to expect the United States to have "enduring unilateral dominance" in that realm. NRC REPORT, *supra* note 4, at 39.

173. *See* Hunker, *supra* note 169, at 209 (noting that "China is developing cyber operations as a tool of warfare"); Schaap, *supra* note 10, at 132.

174. Condron, *supra* note 10, at 405. Condron also notes that China launched cyberattacks against Taiwan in August 1999, thereby initiating a "public hacking war." *Id.*; *see also* Matthew Robertson & Helena Zhu, *Slip-Up in Chinese Military TV Show Reveals More Than Intended*, EPOCH TIMES (Aug. 21, 2011), http://www.theepochtimes.com/n2/china-news/slip-up-in-chinese-military-tv-show-reveals-more-than-intended-60619.html (noting the possibly inadvertent disclosure in Chinese military propaganda that the Chinese military possesses and uses software to execute DDoS attacks against Falun Gong websites).

175. *See* Schaap, *supra* note 10, at 133.

176. *See* Hunker, *supra* note 169, at 209.

177. Brenner with Clarke, *supra* note 143, at 1012.

178. *See infra* Part IV.A.3.C (discussing the developments under the NDAA, which expanded the President's ability to conduct offensive cyber operations yet limited the exertion of such power to the restrictions that apply to the use of kinetic force).

179. Dycus, *supra* note 88, at 164–65. Dycus, however, would strongly oppose any delegation of cyberweapon operations to private contractors. *Id.* at 166.

180. *See* Brenner with Clarke, *supra* note 143, at 1029–30 (noting that cyberattackers are likely to target private companies operating national infrastructure).

This overlap between civilian and military roles may prove problematic. Some commentators express concerns that cyberwarfare may erode the distinction between combatants and noncombatants under international law, which currently protects noncombatants.[181] The degree to which conventional war doctrine applies to cyberwar is not yet clear. Some commentators argue that because of this uncertainty, aggressive countries may have carte blanche to launch cyberattacks against civilian targets in a manner that would be impermissible under the laws of kinetic war.[182] Given the importance of civilian targets in the cyberwar context, Brenner and Clarke suggest using a form of conscription to create a Cyberwar National Guard consisting of technologically savvy citizens to better protect CNI.[183] Indeed, one of the focuses of any national cybersecurity program should be on protecting CNI — the topic to which we now turn.

C. Danger to Critical National Infrastructure

CNI has frequently been discussed as a possible target of cyberattacks.[184] CNI is defined as the collection of systems that are essential to a state's well-being, including banking, communications, utilities, emergency services, and transportation.[185] Another definition of CNI can be found in the language of the USA PATRIOT Act of 2001, which defines "critical infrastructure" as "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."[186] In the United States, Supervisory Control and Data Acquisition ("SCADA") systems control much of the CNI.[187] SCADA, however, is vulnerable to cyberattacks,[188] so the importance of cybersecurity to CNI should not be

181. *See id.* at 1015. The segregation of war space and civilian space is effective in conventional warfare, but will likely not work in cyberwarfare, partially due to the federal government's reliance on civilian-owned infrastructure. *See id.* at 1026, 1035–36 (noting that ninety-five percent of DOD communications route through the Public Switched Network).

182. *See id.* at 1031–32. *But see* Todd, *supra* note 28, at 72 (asserting that *jus ad bellum* and *jus in bello* should both be considered in evaluating potential responses to attacks in cyberspace).

183. Brenner with Clarke, *supra* note 143, at 1064.

184. *See* Sklerov, *supra* note 25, at 2 (arguing that the law of war does not adequately address the modern ability for non-state actors to attack another state's CNI from the other side of the world).

185. *See id.* at 18.

186. USA PATRIOT Act of 2001 § 1016, 42 U.S.C. § 5195c(e) (2006).

187. *See* Sklerov, *supra* note 25, at 19.

188. *See id.* Some of this vulnerability may be due to the sorts of zero-day vulnerabilities that allowed Stuxnet to cause damage. *See W32.Stuxnet*, *supra* note 13. Part of the vulnerability of SCADA systems may also be due to insufficient controls being put in place. *See, e.g.*, Paul Roberts, *Hacker Says Texas Town Used Three Character Password to Secure Internet Facing SCADA System*, THREATPOST (Nov. 20, 2011, 3:42 PM),

underestimated. Some predict that cyberwarfare operations will be focused on CNI, not just on computer systems.[189] A successful cyberattack could disrupt hospitals, defense systems, financial systems, and a variety of other important services. Cyberattacks against the transportation sector could result in airplane crashes or train collisions, while cyberattacks against water services could cause floodgates to open or result in untreated sewage being dumped into the local environment.[190]

A very early form of cyberattack against CNI may have occurred in 1982. Some allege that the U.S. Government doctored software that was subsequently used in the U.S.S.R.'s natural gas pipeline control system, resulting in a large explosion.[191] As dangerous as some of these effects might be, some argue that the most worrisome potential form of cyberattack against CNI would be one directed at electronic emergency warning and response systems, with the goal of amplifying the total damage of a concurrent physical attack.[192] Because of the gravity of potential harm if attacks are conducted against CNI, some commentators urge permitting the use of cyber counterstrikes in response to such attacks[193] — an option that we examine in more detail below in Part III.B.1.C.

Over eighty percent of the nation's CNI is owned and operated by the private sector.[194] Although there is substantial governmental interest in protecting CNI, a survey of CNI and computer security executives indicated that forty-five percent did not believe that their government was very capable of preventing or deterring cyberattacks.[195] Some commentators suggest that private owners of CNI

---

http://threatpost.com/en_us/blogs/hacker-says-texas-town-used-three-digit-password-secure-internet-facing-scada-system-112011. DHS, the agency with the most direct responsibility for securing CNI, has acknowledged the weaknesses in SCADA systems. *See* Paul Roberts, *DHS Thinks Some SCADA Problems Are Too Big to Call "Bug,"* THREATPOST (Sept. 26, 2011, 3:30 PM), http://threatpost.com/en_us/blogs/dhs-thinks-some-scada-problems-are-too-big-call-bug-092611 (noting that DHS considered recategorizing some SCADA problems as design flaws rather than security holes).

189. *See, e.g.*, Brenner with Clarke, *supra* note 143, at 1028.

190. *See* Sklerov, *supra* note 25, at 20–21 (noting that 264,000 gallons of sewage were dumped in Maroochy Shire, Australia as the result of a cyberattack in 2000).

191. *See* NRC REPORT, *supra* note 4, at 195.

192. *See, e.g.*, Sklerov, *supra* note 25, at 20. A similar methodology was used by the invading Cylons in the 2003 pilot of Battlestar Galactica. *Battlestar Galactica: Miniseries*, *Part 1* (Syfy television broadcast Dec. 8, 2003).

193. *See* Condron, *supra* note 10, at 407–08, 416 (encouraging active responses to attacks on CNI immediately upon attack, and proposing that states be excused from liability if they engage in active defense in protection of CNI); Hoisington, *supra* note 36, at 453.

194. *See* Coldebella & White, *supra* note 139, at 240 (estimating that eighty-five percent of CNI is owned by the private sector).

195. STEWART BAKER ET AL., MCAFEE, IN THE CROSSFIRE: CRITICAL INFRASTRUCTURE IN THE AGE OF CYBER WAR 26 (2009), *available at* http://www.mcafee.com/au/resources/reports/rp-in-crossfire-critical-infrastructure-cyber-war.pdf. Given the involvement of the private sector in CNI ownership, private companies are likely to be pulled into the middle of cyberconflicts. Brenner with Clarke, *supra* note 143, at 1029–30.

should be encouraged to develop and adopt their own cyber-preparedness standards.[196] The urgency of protecting CNI and ensuring that potential harm can be effectively mitigated is one of the primary reasons why we propose the implementation of a legal regime permitting active defense and mitigative counterstriking. The lack of faith in the government's ability to protect privately-owned CNI also makes clear the importance of utilizing public-private partnerships to foster trust between the public and private sectors.

i. Federal Initiatives

Even though the U.S. Government has been discussing cybersecurity for fifteen years, there is still no effective and unified national cybersecurity program.[197] There are several pieces, but they are largely disconnected from one another. The National Strategy to Secure Cyberspace includes language encouraging cooperation between the private sector and federal agencies in the interest of protecting CNI.[198] The federal government also operates the Cyber Warning and Information Network and the National Cyber Alert System to provide an early warning in the event of cyberattacks.[199] The House of Representatives has also recently taken action on this topic by introducing CISPA, which would provide for cyber threat information sharing between the public and private sectors.[200]

DHS is entrusted with a variety of cybersecurity responsibilities, including developing a CNI protection plan.[201] DHS also has a National Cyber Security Division, and has the authority under the Critical Infrastructure Information Act of 2002 to provide assistance to private owners of CNI upon request by the private parties.[202] Because DHS already has this sort of legal authority, we propose that DHS

196. *See, e.g.*, Coldebella & White, *supra* note 139, at 241.

197. *See* Sharp, *supra* note 30, at 19.

198. WHITE HOUSE, THE NATIONAL STRATEGY TO SECURE CYBERSPACE ix (2003) [hereinafter WHITE HOUSE, NATIONAL STRATEGY], *available at* http://energy.gov/sites/prod/files/National%20Strategy%20to%20Secure%20Cyberspace.pdf ("Public-private engagement is a key component of our Strategy to secure cyberspace."); *see also* Grant, *supra* note 41, at 107 (noting that the Center for Strategic and International Studies has said there are serious shortcomings in the public-private partnership which DHS believes addresses cybersecurity questions).

199. CLAY WILSON, CONG. RESEARCH SERV., RL 32114, BOTNETS, CYBERCRIME, AND CYBERTERRORISM: VULNERABILITIES AND POLICY ISSUES FOR CONGRESS 31–32 (2007); *see also* Sklerov, *supra* note 25, at 25–26.

200. Cyber Intelligence Sharing and Protection Act of 2011, H.R. 3523, 112th Cong. (2011); *see also* Grant Gross, *Lawmaker Proposes Cyberthreat Sharing Organization*, PCWORLD (Dec. 6, 2011, 3:20 PM), http://www.pcworld.com/businesscenter/article/245580/lawmaker_proposes_cyberthreat_sharing_organization.html.

201. *See* Coldebella & White, *supra* note 139, at 240–41 (noting that DHS has established the Critical Infrastructure Protection Advisory Council, and also has Sector Coordinating Committees to address similar issues); Grant, *supra* note 41, at 106.

202. 6 U.S.C. § 143 (2006 and Supp. IV 2010).

would be a good candidate for a government entity that could be placed in control of mitigative counterstrikes.[203] However, the General Accounting Office ("GAO") has been critical of whether DHS has been satisfying its responsibilities in the cybersecurity area.[204] Some commentators urge DOD to play a bigger role in the protection of CNI, arguing that its protection is an important national security issue.[205] Congress, perhaps seeking to address the overlap between these two agencies on this topic, included provisions in the NDAA requiring DOD and DHS to collaborate with each other on cybersecurity matters.[206]

The three most recent presidential administrations have all taken positions that protecting CNI — including digital infrastructure — is a national security priority.[207] These positions have been expressed in a variety of executive orders and presidential directives. Broadly, executive orders are legally binding orders passed down from the President to administrative agencies under his authority.[208] Presidential directives, also called national security directives, are a specific category of executive orders relating to national security or defense.[209] The position of the Department of Justice ("DOJ") is that such directives have the same legal effect as an executive order.[210] While executive orders are generally published in the Federal Register, orders or

---

203. *See infra* Part V.A.

204. *See* Grant, *supra* note 41, at 106. Beyond whether DHS is effective, some commentators also argue against giving any area of the executive branch sweeping authority over cybersecurity issues. *See, e.g.*, David W. Opderbeck, *Cybersecurity and Executive Power* 37–38 (Seton Hall Pub. Law Working Paper No. 1788333, 2011), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1788333.

205. *See, e.g.*, Todd A. Brown, *Sovereignty in Cyberspace: Legal Propriety of Protecting Defense Industrial Base Information Infrastructure*, 64 A.F. L. REV. 211, 255 (2009) (suggesting that DOD could become involved with protecting CNI in a manner similar to how the Department of Energy regulates the energy sector); Condron, *supra* note 10, at 419. Condron also notes that DOD involvement may have implications under the Posse Comitatus Act, since the Act restricts the use of military assets for traditional law enforcement functions. Condron, *supra* note 10, at 419.

206. National Defense Authorization Act for Fiscal Year 2012, Pub. L. No. 112-81, § 1090, 125 Stat. 1298, 1603–04 (2011).

207. *See* Presidential Decision Directive NSC-63, Critical Infrastructure Protection (May 22, 1998) [hereinafter PDD-63], *available at* http://www.fas.org/irp/offdocs/pdd/pdd-63.htm; Homeland Security Presidential Directive 7, Critical Infrastructure Identification, Prioritization, and Protection, 39 Weekly Comp. Pres. Doc. 1816 (Dec. 17, 2003) [hereinafter HSPD-7], *available at* http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm; WHITE HOUSE, CYBERSPACE POLICY REVIEW (2009) [hereinafter WHITE HOUSE, CYBERSPACE POLICY], *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf; Chabinsky, *supra* note 34, at 28–29 (quoting President Obama's statements in May 2009 connected to the Cyberspace Policy Review).

208. *See generally What Is an Executive Order?*, THISNATION.COM, http://www.thisnation.com/question/040.html (last visited May 3, 2012).

209. *See id.*

210. Randolph D. Moss, *Legal Effectiveness of a Presidential Directive, As Compared to an Executive Order*, OFFICE OF LEGAL COUNSEL (Jan. 29, 2000), *available at* http://www.justice.gov/olc/predirective.htm.

directives that contain sensitive national security information may be kept classified.[211]

In July 1996, President Clinton issued Executive Order 13,010, which established the President's Commission on Critical Infrastructure Protection ("PCCIP").[212] President Clinton issued Presidential Decision Directive 63 ("PDD-63") in May 1998 in an attempt to effect the changes recommended in the PCCIP's report.[213] President Bush's actions on the topic include Executive Order 13,231,[214] Homeland Security Presidential Directive 7,[215] the National Strategy to Secure Cyberspace,[216] the National Infrastructure Protection Plan,[217] and several directives that are still classified, such as National Security Presidential Directive 16[218] and National Security Presidential Directive 54.[219] One of the most recent presidential actions on cybersecurity issues is President Obama's Cyberspace Policy Review.[220] The Cyberspace Policy Review recognizes the importance of establishing leadership within the federal government to improve cybersecurity issues, and describes cybersecurity as a global issue that also requires international cooperation.[221]

ii. Public-Private Partnerships

Some commentators argue that the private sector has more advanced cybersecurity technology than the federal government, claiming that the private sector generally has real-time intrusion detection

211. *See What Is an Executive Order?*, *supra* note 208.

212. Eric A. Greenwald, *History Repeats Itself: The 60-Day Cyberspace Policy Review in Context*, 4 J. NAT'L SECURITY L. & POL'Y 41, 44 (2010).

213. *See id.* at 45–46. PDD-63 also established the National Infrastructure Protection Center as a partnership between the public and private sectors to assess threats and work towards investigating and responding to threats against CNI. PDD-63, *supra* note 207.

214. Exec. Order No. 13,231, 3 C.F.R. 13231 (2001).

215. HSPD-7, *supra* note 207

216. WHITE HOUSE, NATIONAL STRATEGY, *supra* note 198.

217. DEP'T OF HOMELAND SEC., NATIONAL INFRASTRUCTURE PROTECTION PLAN: PARTNERING TO ENHANCE PROTECTION AND RESILIENCY (2009), *available at* http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

218. *See* NRC REPORT, *supra* note 4, at 10; CLAY WILSON, CONG. RESEARCH SERV., RL 31878, INFORMATION WARFARE AND CYBERWAR: CAPABILITIES AND RELATED POLICY ISSUES 10 (2004), *available at* http://digital.library.unt.edu/ark:/67531/metacrs6058.

219. *See* Brown, *supra* note 205, at 240–41; Chabinsky, *supra* note 34, at 29–30; Greenwald, *supra* note 212, at 53–54; Ellen Nakashima, *Bush Order Expands Network Monitoring*, WASH. POST, Jan. 26, 2008, at A03 (discussing a classified directive authorizing federal intelligence agencies to monitor federal agencies' computer networks).

220. WHITE HOUSE, CYBERSPACE POLICY, *supra* note 207. The Cyberspace Policy Review recommends establishing a cybersecurity coordinator who would coordinate cyberspace policy issues from the White House. *Id.* at 7. The cybersecurity policy official, however, would not have the authority to make policy. *Id.* at 8. The review also recommends identifying performance and security objectives for next-generation Internet infrastructure, and notes the importance of hiring and retaining federal employees with the necessary skills. *Id.* at 15, 31–33.

221. *Id.* at 7–9, 20–21.

systems and prevention procedures that it is reluctant to share with the federal government.[222] The private sector, however, still lacks the information that the federal government can access through intelligence and law enforcement activities.[223] Cybersecurity issues have the potential to affect citizens in their homes and workplaces. Approaching these issues with only a high-level national security perspective ignores their impact on private citizens. It is thus important to foster communication between the federal government and the private sector about information security threats.

Some suggest that malicious software is similar to fire damage, where the burden of preventing and reducing business loss should be allocated among many different actors.[224] Thus one option for addressing security concerns and facilitating information sharing is the creation of public-private partnerships. After issuing PDD-63, the Clinton administration published a report encouraging the protection of cyberspace through such public-private partnerships.[225] This report reinforced the position in PDD-63, wherein the administration proposed establishing Information Sharing and Analysis Centers ("ISACs"). Such ISACs were subsequently established, and continue to exist "to advance the physical and cyber security of the critical infrastructures of North America."[226] Several of these ISACs cover major sectors relating to CNI, including the Communications ISAC and the Information Technology ISAC ("IT-ISAC").[227]

Overall, ISACs are not viewed as being hugely successful,[228] perhaps in part due to the relatively low participation of the private sector. This low participation might be due to the inherent difficulties of fostering trust between the private and public sectors, as well as the resistance of some members of the private sector to fully cooperate and share information with their competitors. A full case study of the ISACs regime is outside the scope of this Article, but such a study would be helpful in understanding the advantages and pitfalls of developing public-private partnerships in the cyber context.

---

222. *See, e.g.*, Coldebella & White, *supra* note 139, at 240; Katyal, *supra* note 35, at 62 (noting that the private sector may have advantages with regard to responding to attacks in real-time). *But see* NRC REPORT, *supra* note 4, at 204 (arguing that the private sector's access to cyberattack expertise is likely far less than that of DOD).

223. *See* Coldebella & White, *supra* note 139, at 240.

224. *See, e.g.*, Yang & Hoffstadt, *supra* note 94, at 215.

225. WHITE HOUSE, DEFENDING AMERICA'S CYBERSPACE: NATIONAL PLAN FOR INFORMATION SYSTEMS PROTECTION (2000), *available at* http://www.fas.org/irp/offdocs/pdd/CIP-plan.pdf.

226. NAT'L COUNCIL OF ISACS, http://www.natlisacs.org (last visited May 3, 2012).

227. *Member ISACS*, NAT'L COUNCIL OF ISACS, http://isaccouncil.net/index.php?option=com_content&view=article&id=83&Itemid=195 (last visited May 3, 2012).

228. *See* Kathryn E. Picanso, *Protecting Information Security Under a Uniform Data Breach Notification Law*, 75 FORDHAM L. REV. 355, 361 (2006) ("Government attempts to promote information sharing and business collaboration have had mixed success, however, and currently most information sharing occurs through informal channels.").

Further steps are needed to ensure that CNI is adequately protected from the threats revealed by the discovery of the Stuxnet worm. Protecting CNI is so essential to national security that we urge implementation of mitigative counterstriking capabilities for CNI as soon as possible, even if current technology does not have a low enough margin of error to justify broad implementation. Good-faith attempts to protect CNI would likely be justified, even if there are risks of harming innocent third parties through a mitigative counterstrike.

B. Current Ways to Address Attacks

This Part will introduce the legally allowed options that are available to address cyberattacks as well as their shortcomings. Actions to respond to cyberattacks may include appealing to law enforcement for protection, seeking to impose civil liability on any involved party, and defending against attacks.[229] The two types of computer network defense methods that commentators generally discuss are active defense and passive defense.[230] Passive defense and its shortcomings are examined below. Active defense is examined in Part III.

Some advocate a risk-based approach to cybersecurity using the classic risk formula: Risk (R) = Threat (T) * Vulnerability (V) * Consequence (C).[231] Using the risk formula to reduce one's risk of contracting malaria might involve avoiding areas where malaria-carrying mosquitos live, thus reducing the threat; relying on mosquito repellant or mosquito nets, thus reducing your vulnerability to the carriers; or using calamine lotion to reduce the itching from malaria infection, thus reducing the consequence.[232] In the context of cybersecurity, vulnerabilities can be reduced by "hardening" the targets to reduce the effectiveness of attacks, and consequences can be reduced by either limiting the initial loss or by possessing the capabilities to quickly restore the attacked system.[233] Additionally, one can use this risk-based approach to reduce the risk of cyberattacks by: (1) increasing the effectiveness of criminal and civil law options to address such attacks, thereby reducing the threat through deterrence; (2) improving passive defense options, thereby reducing vulnerability; and (3) developing counterstrike capabilities with a deterrent effect. The last category could either reduce risk by reducing consequences or by

229. A related option is for the attack victim to utilize tracing technology and then provide that information to law enforcement to assist with investigations. *See* NRC REPORT, *supra* note 4, at 36.

230. *See* Jensen, *supra* note 19, at 230.

231. *See, e.g.*, Chertoff, *supra* note 40, at 3; Chabinsky, *supra* note 34, at 35 (suggesting that our goal in reducing risk should be either to reduce one of the variables to zero or to lower each of the three factors).

232. *See* Chabinsky, *supra* note 34, at 35–36 (listing examples where the risk formula can be applied to mitigate risk).

233. *See id.* at 37–38.

reducing the threat, since mitigative counterstriking deters with denial and retributive counterstriking deters with punishment.

Societies have long recognized that deterrence of socially harmful behavior is a primary policy objective.[234] Experts note that deterrence is based on two elements: (1) punishment (inflicting unacceptable costs on the attacker) and (2) denial (denying the attacker success).[235] Some argue that more stringent criminal laws and more vigorous enforcement of such criminal laws will deter cyberattacks.[236] However, such an approach generally requires specific knowledge of the adversary's identity, which is difficult in the context of cyberattacks.[237]

The primary criminal statute addressing cyberattacks in the United States is the CFAA.[238] Despite its legislative significance, the U.S. Sentencing Commission has stated that it is uncertain whether the CFAA is effective in deterring computer crime.[239] There are even some indications that higher penalties may exacerbate computer crime.[240]

While there is at least an arguable case for the deterrent effect of criminal law, it is unlikely that purely passive defenses have any deterrent effect at all, as passive defense involves neither punishing the attacker nor consistently denying the attacker success. Because there is no penalty to an adversary for failed attacks, the adversary can continue attacking until successful.[241] However, some commentators suggest that script kiddies, who are responsible for the majority of attacks on the Internet, can be deterred by purely passive defense.[242] Others

---

234. *See* Todd, *supra* note 28, at 79 (differentiating the deterrent effect of the criminal law approach from the effects-based approach of international law).

235. *See* NRC REPORT, *supra* note 4, at 40.

236. *See, e.g.*, Sklerov, *supra* note 25, at 71; Yamada, Yamagishi & Katsumi, *supra* note 72, at 227–28 (noting that the criminal approach of the United States has some deterrent effect against cybercrimes arising from bots, and that the Japanese approach of providing disinfection tools to users also provides deterrent effects).

237. *See* NRC REPORT, *supra* note 4, at 41. The NRC Report asserts that non-state actors may be too hard to identify for the purpose of punishment as deterrence, and that some hacker groups view counterattacks as a prospective challenge rather than as a deterrent. *Id.* at 42.

238. 18 U.S.C. § 1030 (2006 & Supp. IV 2010).

239. U.S. SENTENCING COMM'N, REPORT TO THE CONGRESS: ADEQUACY OF FEDERAL SENTENCING GUIDELINE PENALTIES FOR COMPUTER FRAUD AND VANDALISM OFFENSES 9 (1996), *available at* http://www.ussc.gov/Legislative_and_Public_Affairs/Congressional_Testimony_and_Reports/Computer_Crime/199606_RtC_Computer_Fraud_and_Vandalism_Offenses.pdf.

240. *See* Skibell, *supra* note 48, at 938. Even though some question the effectiveness of higher penalties, there has been more recent discussion to increase penalties for cybercrime. Some proponents urge amending the Racketeering Influenced and Corrupt Organizations Act ("RICO") to include CFAA offenses as predicate offenses for increased penalties. *See, e.g.*, Graeme McMillan, *Hackers Are the New Mob: White House Gets Serious on Cybercrime*, TIME: TECHLAND (Sept. 8, 2011), http://techland.time.com/2011/09/08/hackers-are-the-new-mob-white-house-gets-serious-on-cybercrime.

241. *See* NRC REPORT, *supra* note 4, at 13.

242. *See* Krause, *supra* note 38, at 54.

assert that to deter hostile attacks at all, cyber counterstrike capabilities must exist so that victims have a credible ability to respond with force.[243] We interpret this assertion as a reference to the effectiveness of deterrence by punishment, or retributive counterstriking. We argue, however, that the first step in an optimal active defense regime is to permit mitigative counterstriking, which would primarily focus on denying success to the attacker rather than on creating a threat of retaliation.

The military concept of deterrence came to the forefront during the Cold War. Given the frequent analogies drawn between nuclear and cyberattack capabilities, many view discussions of "cyber deterrence" in a similar light to its nuclear counterpart.[244] However, there are also many differences between the two. For instance, cyberattacks present an attribution issue that was largely absent during the Cold War, in part because cyberweapons are much more readily available than nuclear warheads.[245]

In a similar vein, one debate that occurred during the Cold War is reappearing in the cyber context — whether counterstrikes should be automated.[246] While automated counterstrikes arguably increase the deterrent effect, the potential damage from automation likely exceeds the benefit from removing the human element. While automating detection may be acceptable, we suggest that humans should execute counterstrikes instead of relying on an automated process, provided that a human also verifies the existence of a threat.

We acknowledge that the applicability of active defense may hinge on the effectiveness and practicability of the current legal options for addressing attacks, so we now turn to these options. More specific options under criminal and civil law will be examined in fur-

---

243. *See* Sklerov, *supra* note 25, at 10. The NRC Report, however, asserts that deterrence of cyberattacks by "the threat of in-kind response" would have limited applicability. NRC REPORT, *supra* note 4, at 5. The NRC Report does, however, note that there may be a deterrent effect under some circumstances. *Id.* at 16.

244. *See, e.g.*, Dycus, *supra* note 88, at 163 (comparing and contrasting the threats of nuclear and cyberattacks); Todd, *supra* note 28, at 97 (comparing the current cyber context with the age of mutually assured destruction ("MAD") of the Cold War, while also acknowledging that MAD does not have the same model of deterrence as present cyberspace operations, such as active defense and cyber counterstriking). There has even been limited discussion about the possibility of responding with nuclear weapons in the case of certain kinds of large-scale cyberattacks. *See* NRC REPORT, *supra* note 4, at 58 (citing JOINT CHIEFS OF STAFF, THE NATIONAL MILITARY STRATEGY OF THE UNITED STATES OF AMERICA (2004)).

245. *See* NRC REPORT, *supra* note 4, at 294–95.

246. *See* Young, *supra* note 136, 177–78 ("The risks in removing human judgment from the network operations decision cycle are significant. For example, in 1988, the automated Aegis computer system on board the *U.S.S. Vincennes* registered Iran Air flight 655 as a hostile Iranian F-14 fighter aircraft."); *see also* WARGAMES (United Artists 1983) (illustrating the danger of automating nuclear counterstrikes). Some of those principles can also be applied to this situation, including the importance of such final decisions being made by informed humans.

ther detail in Part IV, but we introduce the topics here to provide background for the discussion of active defense and mitigative counterstriking.

1. Criminal Law Shortcomings

Having a comprehensive legal structure to address cybercrime requires many elements, including laws specifying prohibited conduct and penalties for such conduct, law enforcement with sufficient authority to collect the necessary electronic evidence, and laws addressing complicated international jurisdictional issues.[247] Many view cyberattacks as a criminal matter that should be addressed by law enforcement,[248] even though law enforcement personnel may not have the resources necessary to investigate and track down cyber criminals.[249] Cybercrime issues are complicated by the nature of cyberspace, which allows criminals to perpetrate old crimes in new ways.[250] Jurisdictional issues also complicate matters, since national borders are at best amorphous in the cyber context. The European Convention on Cybercrime ("ECC") meets many of our suggested requirements for a legal approach to cybercrime, but the low participation rate in the ECC renders it less helpful than it might otherwise be.[251] Regardless of the uncertainty of a criminal law approach to cybercrime, some argue that this approach is less uncertain than one based on international law.[252]

---

247. *See* Downing, *supra* note 95, at 710. Downing suggests, however, that unlawful data interceptions should not be criminalized when there is a reduced expectation of privacy. *Id.* at 731.

248. Katyal has argued, however, that community self-help could also be a viable alternative in the context of cyberattacks. Katyal, *supra* note 35, at 33. Community self-help is most likely to provide benefits when the focus is on preventing crime rather than prosecution or retribution. *See id.* at 34. Purely individual self-help might be detrimental in cyberspace because it could fragment the Internet into a series of trusted networks that privilege user access. *See id.* at 41. A community self-help alternative might be to require software distributors to produce Crime Impact Statements about the vulnerabilities of their products. *Id.* at 53–54. Some reduction in the anonymity of the Internet might also result in a reduction in cybercrime, though that might scare users away from cyberspace. *See id.* at 56–57.

249. *See* Michael L. Rustad, *Private Enforcement of Cybercrime on the Electronic Frontier*, 11 S. CAL. INTERDISC. L.J. 63, 66 (2001) ("Law enforcement resources in cyberspace cannot keep pace with sophisticated cybercrime subcultures in anonymous offshore havens.").

250. *See* Downing, *supra* note 95, at 716 (citing Greg Miller, *Man Pleads Guilty to Using Net to Solicit Rape of Woman*, L.A. TIMES, Apr. 29, 1999, at C5 (describing a case of a cyber abuser who posted on an online bulletin pretending to be a specific woman and providing her address, telling readers that she had fantasies about being raped; the woman was subsequently approached by strangers at her home looking to fulfill her "fantasy")).

251. *See infra* Part IV.B.2 (describing the ECC's strengths and weaknesses).

252. *See* Sklerov, *supra* note 25, at 6–7. Sklerov, however, disagrees with this approach because he views criminal laws as providing insufficient deterrence due to the weak enforcement of cybercrime laws in various states. *Id.* Condron, however, argues that the cyberattacks should be viewed as threats to national security, rather than solely as criminal issues. Condron, *supra* note 10, at 408. Treating cyberattacks as a national security problem

In spite of the availability of cybercrime laws, victims have relied primarily on passive defense to protect their computer assets, in part because governments often cannot or will not pursue cyberattackers through the criminal process.[253] Another problem is the difficulty of attributing an attack to a specific party for the purpose of bringing criminal charges.[254] Information about attribution and scope of an attack is likely unavailable immediately after a cyber intrusion is detected.[255]

Even assuming that cybercrime laws can deter attackers, the deterrent effect is minimal if the laws are not sufficiently strong or effectively enforced.[256] For example, Russia has ignored requests for assistance in addressing specific attacks originating in its jurisdiction, while China has intentionally ignored the criminal acts of its hackers.[257] And for DoS attacks controlled from foreign jurisdictions, the prosecution of offenders located abroad is problematic at best.[258] Extraditing cyber criminals is difficult without treaties in place, unless a country wishes to resort to extralegal rendition.[259]

In cases where there is sufficient cooperation from foreign governments, there are still limitations due to jurisdictional issues. Currently, it is unclear whether jurisdiction should be determined based on the nationality of the victim, the location of the attack, or the location of the attacker.[260]

An additional obstacle to effective enforcement arises from the reluctance of many businesses to report intrusions.[261] Even when law enforcement undertakes an investigation, it still faces additional hin-

---

raises several issues, including: the need to clarify the distinction between homeland security and homeland defense, how to apply *jus ad bellum* to cyberattacks, and how to balance national security interests against civil liberties. *See id.* at 408. According to Condron, homeland security consists of efforts to prevent attacks within the borders of the United States and is handled by DHS, while homeland defense consists of protecting the United States from external threats and is handled by DOD. *Id.* The United States operates under the presumption that a cyberattack is a criminal act rather than a national security issue. *See id.* at 418. Condron argues that this presumption prevents law enforcement from acting immediately, robustly, and aggressively to prevent damage. *Id.*

253. *See* David E. Graham, *Cyber Threats and the Law of War*, 4 J. NAT'L SECURITY L. & POL'Y 87, 92 (2010). A related problem with the ECC is that some voice opposition to it based on a perception that the ECC is a threat to civil liberties. *See The Council of Europe's Convention on Cybercrime*, ELECTRONIC PRIVACY INFO. CENTER, http://epic.org/privacy/intl/ccc.html (last updated Dec. 16, 2005).

254. *See* Lin, *supra* note 43, at 77; Sklerov, *supra* note 25, at 7.

255. *See* Lin, *supra* note 43, at 83.

256. *See* Sklerov, *supra* note 25, at 8–9.

257. *See id.* at 10.

258. ALL PARTY PARLIAMENTARY INTERNET GRP., "REVISION OF THE COMPUTER MISUSE ACT": REPORT OF AN INQUIRY BY THE ALL PARTY INTERNET GROUP 4 (2004), *available at* http://www.apcomms.org.uk/apig/archive/activities-2004/computer-misuse-inquiry/CMAReportFinalVersion1.pdf.

259. *See* Hunker, *supra* note 169, at 204.

260. *See* NRC REPORT, *supra* note 4, at 36.

261. *See* Yang & Hoffstadt, *supra* note 94, at 212.

drances, including difficulties in collecting sufficient evidence, inadequate equipment for collecting the evidence, insufficient training, and ineffective national cybercrime laws.[262] Prosecuting cyberattackers is also difficult because these attackers generally conceal their identities with great ease.[263] Even a trace that is initially successful might "dead-end" at a cell phone that the criminal bought for one-time use.[264]

Another common criticism is that the criminal law has failed to keep pace with the development of technology, resulting in harmful activities on the Internet that are nonetheless technically legal.[265] For example, it is difficult to distinguish, for legal purposes, between actual DDoS attacks and innocent crashes that are caused by an overwhelming number of visits by users to popular websites.[266] Critics express concern that criminal laws specifically criminalizing DDoS attacks might also criminalize these innocent crashes because of the similarity in their effects.[267] The public's general knowledge about these issues also acts as a barrier because juries are drawn from a potentially uninformed public. Even if actions like DDoS attacks can be effectively addressed through the criminal process, the difficulty of explaining technical details to a jury of laypersons may be insurmountable.[268]

2. Civil Law Shortcomings

Because it is difficult to criminalize cyberattacks and to enforce existing criminal laws, some commentators have proposed using civil law instead.[269] Resorting to the civil legal system would enable victims to hold parties liable for behavior that leads to harm. Liability may be imposed on either the attacker or intermediary parties.[270] For instance, power company owners could be liable for a negligent failure to secure their computer system that results in harm to the victim. Owners of zombie computers could potentially be held liable for

262. *See* Downing, *supra* note 95, at 709–10.

263. *See id.* at 736; Krause, *supra* note 38, at 55.

264. *See* Katyal, *supra* note 35, at 50–51.

265. *See* Schaap, *supra* note 10, at 172; Todd, *supra* note 28, at 66.

266. *See* Edwards, *supra* note 57, at 41.

267. *See id.* at 41–42 (referring to such innocent crashes as "slashdots" after a popular online computer-culture journal).

268. *See id.* at 42–43 (discussing the United Kingdom case of *R v. Caffrey*, where the jury found reasonable doubt not to charge based on the defendant's excuse — similar to a sleepwalking defense in a murder case — that *he* did not hack into the computer system, and that instead his computer was infected by a self-deleting Trojan).

269. *See, e.g.*, *id.* at 43–44.

270. *See id.* at 44–45 (listing parties who might be viewed as complicit in DDoS attacks); Yang & Hoffstadt, *supra* note 94, at 212 (offering three options for addressing the burden of cybercrime: shifting upon (1) the victim, (2) the manufacturers of software or hardware, or (3) the government).

maintaining an insecure system that was hijacked into participating in a DDoS attack, or ISPs could be held liable for failing to monitor and secure the data being transmitted over their infrastructure.[271]

The victim's most obvious desire, though, will be to hold the attacker himself responsible. Suing the attacker directly requires that the victim be able to identify the attacker accurately, and this is not currently feasible as a general matter.[272] Even if technology were sufficient to accurately identify an attacker, the proper venue would be difficult to determine, since cyberattack activities are in no way limited by state or national boundaries. Also, a foreign defendant in a civil suit could move to have the case dismissed on *forum non conveniens* grounds.[273] Additionally, because executing cyberattacks does not require an attacker to have substantial financial resources, it is likely that many defendants are judgment-proof.[274]

Encouraging injured parties to sue the intermediaries who are arguably negligent in some manner also raises a slew of problems. For example, if liability were imposed on software manufacturers for the security holes in their software, the price of software would likely increase as manufacturers would pass on the costs of potential liability to their customers.[275] Imposing liability on the owners of zombie computers is problematic on several levels. Such liability may effectively function as "a tax on ignorance and technophobia," punishing those who do not know enough about protecting their personal computers.[276] Also, one of the largest potential hurdles for parties that look to recover under a theory of negligence against an intermediary is in the common law itself. Under the traditional doctrine of intervening and superseding causes, an intentional tort by a third party could be a superseding cause that severs the causal link between the defendant's action and plaintiff's injury, thereby preventing an otherwise

---

271. *See* de Guzman, *supra* note 68, at 528 (suggesting that it is unlikely that zombie computer owners could be held liable for maintaining an under-protected computer); Edwards, *supra* note 57, at 44–45 (listing ISPs among potential responsible parties in a DDoS attack).

272. *See* sources cited *supra* note 33.

273. *See* N. Light Tech., Inc. v. N. Lights Club, 97 F. Supp. 2d 96, 108 (D. Mass. 2000) (finding dismissal on *forum non conveniens* grounds inappropriate where defendant would bear the burden of bringing witnesses from Alberta, Canada to Massachusetts for litigation of cyber-squatting claim), *aff'd*, 236 F.3d 57 (1st Cir. 2001). It is currently unclear how a *forum non conveniens* motion would be received in the context of a civil suit alleging damage from an international cyberattack.

274. *Cf.* Randy G. Gerchick, Comment, *No Easy Way Out: Making the Summary Eviction Process a Fairer and More Efficient Alternative to Landlord Self-Help*, 41 UCLA L. REV. 759, 801–02 (1994) (asserting that tenants who cannot pay their rent are often judgment-proof, and that trying to recover damages from them is like trying to draw blood from a turnip).

275. *See* Edwards, *supra* note 57, at 53.

276. *Id.* at 47.

negligent defendant from being held liable for the harm caused to the victim.[277] These barriers are analyzed in more detail in Part IV.A.2.

3. Passive Defense Approaches

Finally, we turn to the passive defense approaches to cybersecurity. Passive computer security consists of four general categories: (1) controls over system access, (2) controls over data access, (3) security administration, and (4) secure system design.[278] A purely defensive approach to controlling access to servers and data includes measures such as encryption, firewalls, and automated detection.[279] The broader notion of passive defense also involves educating users and facilitating recovery from a potential attack.[280] Another passive defense option is to ensure greater software security by shifting to open source software, as the collaborative model of open source software permits more eyes to examine the source code and its potential vulnerabilities. If users identify vulnerabilities in open source software, anyone with the requisite skills can fix the problems rather than having to wait for an official patch from the only entity with access to the source code.

When an organization experiences a cyberattack, it will most likely utilize purely defensive responses, though it may also employ active defense,[281] which is addressed in more detail below. Many large organizations have security operations centers to handle cybersecurity issues, though currently these centers can legally focus only on passive defense, at least with respect to threats that are external to the perimeter of the organization it serves.[282] Organizations can also purchase "hacker insurance," though evidence suggests that participation in such programs is relatively low, with most businesses preferring to self-insure.[283]

Some defensive methods are a blend of active and passive. One such method is to create "honeypots" — decoy sites designed to at-

277. *See* discussion *infra* Part IV.A.2.

278. *See* Sklerov, *supra* note 25, at 21. System access controls keep people out, while data access controls keep data within a specific group. *See id.* at 22–23. Security administration manages the personnel side of computer security and requires administrators to properly maintain the system. *See id.* at 23. Sklerov also notes that it is possible to design a system to withstand DoS attacks. *Id.* at 24.

279. *See* Condron, *supra* note 10, at 410.

280. NRC REPORT, *supra* note 4, at 13. System access controls could also include controls to block certain IP addresses or countries of origin. *See, e.g.*, Downing, *supra* note 95, at 709 (discussing how the prevalence of fraud originating from Indonesia caused online retailers to block IP addresses associated with Indonesia).

281. *See* Brenner with Clarke, *supra* note 143, at 1032–33. Brenner and Clarke note that the distinction between offensive and defensive actions is that defensive actions are purely reactive, while offensive actions are aggressive. *Id.* at 1034.

282. *See* NRC REPORT, *supra* note 4, at 209.

283. *See* Yang & Hoffstadt, *supra* note 94, at 208–09.

tract hackers to discover their attack techniques, and potentially their identities.[284] Alternatively, a system or piece of software may include a "sandbox" where code execution may be isolated, limiting the possible harm that could be done to the whole system by malicious code.[285]

Active-passive approaches like honeypots and sandboxes are promising, but are not without their weaknesses. Honeypots, for example, cannot passively monitor a broad range of activities, and they only work when an attacker communicates directly with the honeypot.[286] On the other hand, sandbox features are vulnerable to being bypassed like other security features.[287] Furthermore, research indicates that a hacker could potentially use a web browser's sandbox feature to disable protections against "clickjacking."[288]

Some commentators suggest that passive methods to prevent hacking would effectively eliminate hacking crimes if they were more pervasive.[289] However, the reality remains that reliance on passive defense has many shortcomings. There is strong evidence that today's security environment provides few useful options for responding to severe cyberattacks.[290] Many commentators argue that purely passive defense is insufficient.[291] Military officials have also argued that purely passive defense is only marginally effective against sophisticated attackers.[292] For passive defense to be effective, the measures must succeed one hundred percent of the time, or attackers would have an

284. *See* Katyal, *supra* note 35, at 53. In this Article, we consider honeypots to be a passive defense technique rather than an active defense technique because they exist to collect information rather than to respond directly to attacks.

285. *See* Dan Goodin, *Chrome Is the Most Secured Browser — New Study*, REGISTER (Dec. 9, 2011, 1:45 PM), http://www.theregister.co.uk/2011/12/09/chrome_ie_firefox_security_bakeoff ("[S]andboxes are designed to lessen the damage attackers can do when they successfully exploit a vulnerability in the underlying code base.").

286. *See* Lance Spitzner, *Honeypot Farms*, SYMANTEC (Nov. 2, 2010), http://www.symantec.com/connect/articles/honeypot-farms (recognizing, however, the significant potential for honeypots to address cyberattacks).

287. *See* Robert Westervelt, *Researcher Breaks Adobe Flash Sandbox Security Feature*, SEARCHSECURITY (Jan. 6, 2011), http://searchsecurity.techtarget.com/news/1525813/Researcher-breaks-Adobe-Flash-sandbox-security-feature.

288. *See* Tom Espiner, *Enisa: W3C Web Standards Pose 51 Security Threats*, ZDNET UK (Aug. 1, 2011, 5:39 PM), http://www.zdnet.co.uk/news/security-threats/2011/08/01/enisa-w3c-web-standards-pose-51-security-threats-40093582/ (defining "clickjacking" as when "a user is fooled into clicking on a seemingly innocuous web object such as a button, which then reveals confidential information").

289. *See, e.g.*, Katyal, *supra* note 35, at 43. It is also important to evaluate the current norms of cyber behavior and to assess the need for cybersecurity-conscious behaviors to be integrated into such norms. *See* Hunker, *supra* note 169, at 202–03. Hunker suggests analogizing to public health norms — such as hand washing and vaccinating — as a model. *Id.*

290. *See* NRC REPORT, *supra* note 4, at 36.

291. *See, e.g.*, Graham, *supra* note 253, at 92–93; Sklerov, *supra* note 25, at 26 ("These vulnerabilities highlight the fact that passive defenses alone are not enough to protect states from cyberattacks.").

292. NRC REPORT, *supra* note 4, at 162.

incentive to continue trying to break through defenses.[293] Additionally, passive defense is inadequate protection against exploitations of zero-day vulnerabilities, which by definition are unknown to the software manufacturers and the creators of security patches and security software.[294] This deficiency becomes even more glaring when we consider the existence of cyber contractors that provide subscriptions to lists of zero-day vulnerabilities.[295] This evidence makes it clear that security experts who specialize in finding vulnerabilities stand to gain significantly more financially by selling the information than by reporting the vulnerabilities to software manufacturers.

Even if purely passive defense could be effective, however, some have observed that taking actions like raising security standards or requiring users to authenticate their identities for more purposes could potentially threaten privacy and innovation, as well as harm e-commerce.[296]

We argue that such heightened security standards might be difficult to enforce uniformly in the absence of government intervention, which raises additional problems. Downing notes a rule of thumb regarding privacy: "the more intrusive into individual privacy a particular authority is, the greater the need for safeguards to ensure that the authority is not abused."[297] Limits on the scope of searches are one way to address potentially intrusive authority.[298] In addition to potential privacy issues, if the government becomes too heavily involved in protecting cyberspace, new issues may arise involving intellectual property protection, network service availability, and additional risks of criminal and civil liability.[299]

A more detailed examination of the criminal and civil law approaches to cyberattacks is provided in Part IV. A cursory glance at the issue, though, should provide enough background knowledge to establish that none of the three options above are entirely adequate to

---

293. *See id.* at 13; *see also* Leo King, *NASDAQ Out of Date Software Helped Hackers — Report*, COMPUTERWORLD UK (Nov. 21, 2011, 6:30 PM), http://www.computerworlduk.com/news/security/3319825 (describing an FBI report stating that a cyberattack on NASDAQ was in part made possible by NASDAQ's failure to keep its network security measures up to date).

294. *See Top Cyber Security Risks — Zero-Vulnerability Trends*, *supra* note 12.

295. *See* Meer, *supra* note 22 (referencing a leaked document from Endgame Systems that advertises subscriptions to lists of zero-day exploits for $2.5 million per year); Michael Riley & Ashlee Vance, *Cyber Weapons: The New Arms Race*, BUSINESSWEEK (July 20, 2011, 11:45 PM), http://mobile.businessweek.com/magazine/cyber-weapons-the-new-arms-race-07212011.html.

296. *See, e.g.*, Nojeim, *supra* note 139, at 129. Nojeim notes, however, that privacy is arguably enhanced both by increased authentication requirements to protect users from identity theft and by lower traceability to preserve anonymity. *Id.* at 131.

297. Downing, *supra* note 95, at 745.

298. *See id.* at 746.

299. *See* Young, *supra* note 136, at 190.

address cyber threats. Thus we turn to the focus of this Article: active defense and mitigative counterstriking.

III. ACTIVE DEFENSE AND MITIGATIVE COUNTERSTRIKING

In Part II, we described the extent of the threat posed by modern cyberattack techniques and examined the currently available methods for addressing cyberattacks. Even if criminal and civil enforcement methods were consistently effective, using these methods is inherently *ex post facto*, addressing an injury after harm has already occurred. If a power grid is under siege from a cyberterrorist, the satisfaction of knowing that a future prosecution will be successful will not allay the immediate concerns of protecting public safety. There needs to be some method of addressing an attack that the operator of the system can control. Passive defense, including firewalls and antivirus software, is generally viewed as the primary method for a user to avoid being harmed by an attack attempt.

However, passive defense is all but useless against zero-day exploits. There are indications that it is more profitable to hoard lists of zero-day exploits for future offensive use than it is to report those exploits to the software manufacturers to fix the holes in their software code.[300] This makes it more difficult to close the holes that could lead to botnets being used in DDoS attacks. Similarly, passive options like dropping incoming packets are likely to be less effective with modern DDoS attacks than they would be with DoS attacks, where the repeated requests come from the same IP address.

In today's era of zero-day exploits and DDoS attacks, "scan, firewall, and patch" has become similar to "duck and cover." Cyberattack victims, particularly operators of CNI, should be empowered to repel as well as block attacks. This notion of actively repelling a cyberattack to mitigate harm to the victim system is what we have termed "mitigative counterstriking," which is at the core of the broad concept of active defense.

A. What Is Active Defense?

Given the weaknesses of passive methods to address cyberattacks, it is important to consider the use of cyber counterattacks in self-defense as a way to respond to and mitigate the harm from cyberattacks. There is a growing gap between passive defense capabilities and cyberattack capabilities,[301] so it is important to address these mat-

300. *See* Mathew J. Schwartz, *So You Want to Be a Zero Day Exploit Millionaire?*, INFORMATIONWEEK (Nov. 11, 2011, 8:00 AM), http://www.informationweek.com/news/security/vulnerabilities/231902813.

301. *See* NRC REPORT, *supra* note 4, at 41.

ters soon. It is unclear, however, when the right to self-defense may be invoked.[302]

Active defenses are a potential fourth category of response to cyberattacks and enable attacked parties to detect, trace, and then actively respond to a threat by, for example, interrupting an attack in progress to mitigate damage to the system.[303] Thus, we view "active defense" as beginning at the detection stage and assert that "active defense" includes three distinct types of technology: intrusion detection systems ("IDS"), technology to trace an attack to its source ("traceback"), and counterstrike capabilities — where counterstrikes involve some method of sending data back at the attacker to disrupt the attack.[304]

Interrupting attacks in such a way might be considered a form of active defense called "active threat neutralization."[305] Thus, active defense can also be characterized as offensive actions undertaken with the goal of neutralizing an immediate threat rather than retaliating.[306] The federal government currently authorizes STRATCOM to neutralize cyber threats that compromise the effectiveness of DOD missions.[307] In the event of a DDoS attack via a botnet, two potential neutralization responses may involve sending a DoS attack at the botnet controller or hacking the botnet controller and thereby taking control of the botnet.[308]

Even though counterstrikes are currently of questionable legality, counterstrikes have already been occurring on the Internet over the last decade, initiated by both government[309] and private actors.[310] Full

---

302. *See id.* at 37.

303. *See* NRC REPORT, *supra* note 4, at 13 (listing neutralizing attacks and imposing other costs on the attacker as alternatives to passive defense); Sklerov, *supra* note 25, at 21–22 (listing types of computer network defense). The NRC Report suggests cyber counterattacks as an example of a potential way to impose costs on the attacker. NRC REPORT, *supra* note 4, at 16.

304. *See infra* Part III.B.1.

305. NRC REPORT, *supra* note 4, at 54. The NRC Report suggests that the policy for active defense may require several hostile cyberattacks prior to taking a neutralization response. *Id.* at 146.

306. *See, e.g.*, *id.* at 142.

307. *Id.* at 63.

308. *See id.* at 64 n.26 (also noting that executing a DoS attack against the botnet controller would involve a greater risk of escalation). The recent takedown of the Rustock botnet involved the use of "legal and technical measures to sever the connection between the command and control structure of the botnet and the malware-infected computers operating under its control . . . ." Richard Boscovich, *Taking Down Botnets: Microsoft and the Rustock Botnet*, MICROSOFT ON THE ISSUES (Mar. 17, 2011, 6:36 PM), http://blogs.technet.com/b/microsoft_on_the_issues/archive/2011/03/18/taking-down-botnets-microsoft-and-the-rustock-botnet.aspx.

309. In late 1998, when the activist group Electronic Disturbance Theater attacked the Pentagon's website with a flood of requests, the Pentagon redirected the requests and sent graphics and messages back to the group's system to cause it to crash. Winn Schwartau, *Striking Back*, NETWORK WORLD (Jan. 11, 1999), http://www.networkworld.com/news/0111vigilante.html.

software packages designed for defense capabilities that are more active have also become commercially available.[311] It is thus apparent that cyber counterstriking is already an available practice within the IT industry, and the question then arises whether the active defense practice of cyber counterstriking should be regulated and standardized.

We argue that regulation and standardization are essential for active defense. Regulating and providing standards would serve to bring these activities into the light, and ensure that active defense is approached responsibly to minimize potentially destructive vigilantism. We suggest that the regulation and standardization should begin with a focus on mitigative counterstrikes because these counterstrikes derive their justification from the fundamental concept of self-defense. Because private retributive counterstriking may be viewed as vigilantism, it is important to set forth guidelines for the proper mitigative use of counterstriking technology.

Most cyber counterstriking capabilities are currently classified,[312] though some software is available to the public that can send destructive viruses to an attacker or packet-flood the machine of the intruder.[313] The NRC Report acknowledges that it is likely that the private sector will counterstrike to address threats when the costs of counterstriking are less than the benefits gained from neutralization of the incoming attack.[314] It is unknown, however, how frequently cyberattack victims resort to cyber counterstriking. Victims are generally unwilling to report such use openly due to legal uncertainty.[315]

A wide variety of possible active responses could be considered variations on mitigative counterstriking, including active counter-

310. In 2002, security software developer Mullen developed a technology for identifying and loading code on the attacking system to "neutralize" the attacking process and stop the propagation of the Code Red and Nimda worms. Thomas C. Greene, *Attacking Nimda-Infected Attackers*, REGISTER (Aug. 8, 2002, 4:58 PM), http://www.theregister.co.uk/2002/08/08/attacking_nimdainfected_attackers.

311. *See* Majuca & Kesan, *supra* note 24, at 5–6 (citing a survey indicating that a number of Fortune 500 companies had installed counterattack-capable software as of the late 1990s); *see also* Jensen, *supra* note 19, at 230 (referencing ForeScout's "ActiveResponse" technology that the company claims to be capable of "repelling" and blocking attackers); Press Release, Symbiot Security, Symbiot Security Announces World's First Solution to Strike Back Against Network-Based Attackers (Mar. 4, 2004), http://www.thefreelibrary.com/Symbiot+Security+Announces+World's+First+Solution+to+Strike+Back...-a0113905129 ("Symbiot provides the equivalent of an active missile defense system.").

312. *See* NRC REPORT, *supra* note 4, at 29; Kastenberg, *Paradigm*, *supra* note 121, at 178.

313. *See* Sklerov, *supra* note 25, at 25; *see also* de Guzman, *supra* note 68, at 530–31 (discussing software that purports to provide "graduated countermeasures" against cyberthreats); Edwards, *supra* note 57, at 33 (discussing Lycos Europe's short-lived "Make Love, Not Spam" screensaver from 2004, which was a free download that, when used, launched DDoS attacks against spam sites).

314. NRC REPORT, *supra* note 4, at 71.

315. *See id.* at 207.

strikes (e.g., sending a worm to the attacker's system), passive counterstrikes (e.g., as redirecting the attack back at the attacker), and preemptive defense.[316] News outlets have picked up stories about potential use of counterstrike technology to address worms like the Conficker worm,[317] the Nimda worm,[318] or the Code Red worm,[319] or botnets like Kraken, which was used for disseminating spam.[320] However, people have been hesitant to resort to these methods out of concern over potential legal liability.[321] Another potential active response is the use of "white hat" viruses, which could be effective at inoculating computers from the effects of other viruses, although "white hat" viruses may have unpredictable consequences.[322]

Mitigative counterstriking is not an immediate panacea. First, a number of international legal issues need to be considered. Because a mitigative counterstrike could potentially inflict harm on third parties across international borders, many discussions of cyber counterstriking address the law of war, international humanitarian law, and the United Nations Charter ("U.N. Charter").[323] However, permitting mitigative counterstriking would have a number of advantages, including avoiding drawn out prosecutions and complicated jurisdictional issues.[324] Eventually, there may be a sufficiently effective criminal law regime that can be used to accurately, consistently, and fairly pursue the perpetrators of cybercrime regardless of national boundaries. In the interim, however, we argue that mitigative counterstriking, as a specific subset of active defense, could provide an effective alternative to criminal prosecution. Nevertheless, there still remains the ques-

316. *See id.* at 148–49. The NRC Report also categorizes honeypots (also called honeynets) as an active response. *Id.* However, this Article treats honeypots as passive defense, since they purely gather intelligence based on infiltrations, rather than actively pursuing a target to infiltrate for information. *See supra* note 284 and accompanying text.

317. *See, e.g.*, John Markoff, *Worm Infects Millions of Computers Worldwide*, N.Y. TIMES, January 22, 2009 at A12 (quoting a researcher speaking about efforts to halt the progress of a worm through active methods as saying, "Yes, we are working on it, as are many others. Yes, it's illegal, but so was Rosa Parks sitting in the front of the bus.").

318. *See, e.g.*, Katyal, *supra* note 35, at 63–64 (discussing calls to allow an automated program to neutralize computers infected with Nimda by inserting a command into the infected computer's boot sequence).

319. *See, e.g.*, *id.* at 64 (describing the effects of the CodeGreen patch that was developed to respond to the Code Red worm).

320. *See, e.g.*, Ryan Naraine, *Kraken Botnet Infiltration Triggers Ethics Debate*, EWEEK.COM (May 1, 2008), http://www.eweek.com/c/a/Security/Kraken-Botnet-Infiltration-Triggers-Ethics-Debate.

321. *See id.*; *see also* de Guzman, *supra* note 68, at 527–28. However, executing mitigative counterstrikes to interrupt an ongoing DDoS attack would likely be effective only against DDoS attacks executed from a single botnet, and would be less effective in the case of coordinated attacks across several botnets or DDoS attacks that do not use botnets at all, such as LOIC and d0z.me.

322. *See* Katyal, *supra* note 35, at 62 ("Anyone who doubts [the unpredictable effects of beneficial viruses] should try running the Windows Service Pack 2 update.").

323. *See, e.g.*, Jensen, *supra* note 19, at 221–29; Sklerov, *supra* note 25, at 27–42.

324. *See* Katyal, *supra* note 35, at 60.

tion of who should be permitted to engage in active defense, for which there are two primary options: the government or cyberattack victims themselves.[325] These questions are examined in more detail in Part VI.

B. Different Parts of Active Defense

A fair amount of the academic commentary on the topic of active defense concerns military use of counterstrikes and discusses the topic on a national scale.[326] While this is important, we are primarily concerned with the effects of cyberattacks on private parties, especially private owners of CNI, and the need for active defense to protect them. When the topic turns to potential use of cyber counterstrikes to protect private parties, some commentators note the promise of permitting counterstrikes to address problems like DDoS attacks,[327] though most are wary of the possible harm that can be caused by counterstrikes.[328] Taken together, the current trend in academic opinion suggests that counterstrikes should be approached cautiously. We are also cautious about the subject matter, which is why we advocate a narrow view focused on mitigative counterstrikes as we begin to explore viable policy options to permit self-defense in cyberspace.

As noted above, there are many reasons why states or private parties may be dissatisfied with addressing cyberattacks through legal or purely passive means. If legal protection is inadequate, there is a risk that parties will use illegal and potentially harmful methods.[329] Thus it is important to ensure that this behavior is regulated and controlled so that there are sufficient legal means to address cyberattacks.

When deciding whether to permit parties to use cyber counterstrikes to mitigate harm, the discussion should involve an examination of issues relating to attributing and characterizing cyberattacks. Some have noted that there is a nontrivial danger that a counterstrike could harm intermediary systems through which the cyberattacker routed his signal.[330] They argue that for this reason self-defense should not be used unless the attack can be accurately attributed to the aggressor or

---

325. *See* NRC REPORT, *supra* note 4, at 207.

326. *See, e.g.*, NRC REPORT, *supra* note 4, at 16; Condron, *supra* note 10, at 410–11; Kastenberg, *Paradigm*, *supra* note 121, at 177–78; Sklerov, *supra* note 25, at 25.

327. *See, e.g.*, de Guzman, *supra* note 68, at 530–31.

328. *See* Jensen, *supra* note 19, at 237 (noting harm to potential third parties); Katyal, *supra* note 35, at 61 (arguing that counterstrikes may hit unintended targets or may cue more crimes); Smith, *supra* note 19, at 183 (analogizing the controversy over counterstrikes to the controversy over the use of spring guns in England in the 18th and 19th centuries).

329. *See* Sklerov, *supra* note 25, at 11; Katyal, *supra* note 35, at 40 (noting the prevalence of vigilantism in cyberspace).

330. *See* Jensen, *supra* note 19, at 237; Katyal, *supra* note 35, at 61; NRC REPORT, *supra* note 4, at 37. For example, hackers might route their traffic through a very specific target, like a hospital, in the hopes that a counterstrike would hurt the hospital's system. *See* Katyal, *supra* note 35, at 62–63.

aggressors.[331] Unfortunately, attribution is difficult in the context of cyberattacks.[332] Graham, however, suggests that nation-states could be held responsible for attacks made by private actors on a theory of imputed responsibility, even if completely accurate technical attribution were not possible.[333] Given the importance of accuracy, our proposal stresses the need for further technological improvements that permit attacks to be traced to their origin.

Aside from attribution, the other important requirement is that the party seeking to use defensive cyber counterstrikes must be able to characterize the attack as hostile — a determination that is more difficult to make in the cyber context than it is in the context of conventional kinetic weapons.[334] Under traditional conflict situations, tactical warning and attack assessment are processes by which an attack victim is alerted to an attack in progress and is made aware of the attack's "scale, scope, and nature;" with a cyberattack, however, it is difficult to even determine whether an attack is in progress.[335] Some propose that protection should be afforded to parties who use cyber counterstrikes to respond to attacks, especially attacks on CNI, in the event that attribution information and the characterization of the attack are incorrect.[336] In our proposal of mitigative counterstriking, we focus on the utility of such counterstriking as a response to DDoS attacks, whose hostile nature can be detected and distinguished from innocent requests.[337] Accordingly, accurate characterization is not as serious of a problem when mitigative counterstriking is used to respond to DDoS attacks, even if the attack is not on CNI.

Many have noted the potential danger of escalation following the use of mitigative counterstrikes, especially in international conflict, which suggests that counterstrike decisions should be made at very high organizational levels.[338] The NRC Report suggests that this does not mean that delegating counterstriking decisions is always improper, but rather that neutralization responses should perhaps be conducted "only when other methods for responding to a cyberattack have proven (or will prove) ineffective."[339] The NRC Report further suggests

---

331. *See, e.g.*, Graham, *supra* note 253, at 92–93.

332. *See* NRC REPORT, *supra* note 4, at 37; Condron, *supra* note 10, at 417.

333. Graham, *supra* note 253, at 93.

334. *See* NRC REPORT, *supra* note 4, at 135 (noting the importance of characterizing attacks); Jensen, *supra* note 19, at 235.

335. *See* NRC REPORT, *supra* note 4, at 135.

336. *See, e.g.*, Hoisington, *supra* note 36, at 453; Jensen, *supra* note 19, at 237 (asserting that active defense responses are legitimate without one hundred percent attribution or characterization).

337. *See, e.g.*, Y. Xiang, et al., *Detecting DDoS Attack Based on Network Self-Similarity*, 151 IEE PROC. COMM., 292, 292 (2004).

338. *See* NRC REPORT, *supra* note 4, at 63, 211; Graham, *supra* note 253, at 98.

339. NRC REPORT, *supra* note 4, at 64. Even if active defense responses can be delegated, it is doubtful that neutralization efforts should ever be automated because of the risks of inadvertent escalation. *See id.* If automated responses were to be permitted, the system

that a government-related institution should address cyber counterattack issues, thereby allowing cyberattack victims to seek prompt relief.[340] Our analysis similarly concludes that placing the government in charge of mitigative counterstrikes would minimize a number of potential conflicts. However, there are some concerns that if the U.S. Government executes cyber counterstrikes that result in harm to its citizens, this could potentially infringe certain civil liberties — including the right to privacy, protection from unreasonable searches, and due process.[341]

At least one commentator suggests the possibility of using letters of marque and reprisal to give private actors the authority to behave in a quasi-military way, such as to conduct cyber counterstrikes.[342] However, this might have a questionable effect on the private party's status as a noncombatant under the law of armed conflict.[343] There is also an active debate about whether the international law construct of anticipatory self-defense could apply in the cyber context.[344] Issues relating to the law of war and anticipatory self-defense are explored in more detail below in Part V.B.

Part of the underlying premise of this Article is that the optimal use of active defense and mitigative counterstriking is contingent upon the availability of accurate and effective technology. For that reason, this Part aims to give a cursory overview of the technology available for the first two stages of active defense: intrusion detection and traceback. The previous Parts in Part III.B discuss the importance of attributing an attack. Attribution, however, requires precision and accuracy.[345] Attribution is distinct from determining an access path back to the attacker;[346] thus it may be possible to counterstrike against a cyberattacker whose individual identity is unknown.

Tension exists between the policy need for responding rapidly to attacks and the technical reality that it takes time to detect and determine the origin of a cyberattack.[347] Cyberattacks occur very rapidly, so responses must be prompt to best mitigate harm to the targeted system. Detecting a cyber intrusion may require access attempts so that a

---

would still have to address the problems of attribution, characterization, and inviolability of neutral nations. *See* Jensen, *supra* note 19, at 231.

340. NRC REPORT, *supra* note 4, at 71.

341. *See* Condron, *supra* note 10, at 416.

342. NRC REPORT, *supra* note 4, at 208.

343. *See* Brenner with Clarke, *supra* note 143, at 1015 ("The right of the noncombatant population to protection . . . involves . . . a corresponding duty of abstaining from . . . hostilities . . . ." (omission in original)).

344. *See* Hoisington, *supra* note 36, at 451; Jensen, *supra* note 19, at 209.

345. *See* NRC REPORT, *supra* note 4, at 139, 146.

346. *See id.* at 141.

347. *See id.* at 23.

pattern may be detected.[348] Once an attack is detected, however, tracing it to its origin can take a matter of seconds.[349] Because of the intersection of policy and technology in this area, it is important that policymakers and agencies understand policy issues raised by cyberattack capabilities and the relationship between those policy issues and the basic technologies. In-depth analysis of the full and current state of the technical art is outside the scope of this Article, but it is important to note that the technology involved in active defense is reasonably well-developed, and is currently the subject of a significant amount of research aimed at improving its accuracy and efficiency.[350]

There are three essential elements to active defense technology: an intrusion detection system ("IDS"),[351] the ability to trace an attack back to its origin ("traceback"),[352] and then a method of response.

1. Intrusion Detection Systems

When engaging in active defense, the first essential technology is IDS, which has developed significantly over the past decade. IDS works partly by detecting patterns of intrusions by a particular intruder.[353] This means it may be harder for IDS to detect intrusions when

348. *See generally* Chenfeng Vincent Zhou, Christopher Leckie & Shanika Karunasekera, *A Survey of Coordinated Attacks and Collaborative Intrusion Detection*, 29 COMPUTERS & SECURITY 131 (2010).

349. *See* Ethan Katz-Bassett, et al., *Reverse Traceroute*, USENIX SYMP. ON NETWORKED SYS. DESIGN & IMPLEMENTATION, 12 (2010), *available at* http://www.cs.washington.edu/research/networking/astronomy/reverse-traceroute.html. Traceroute and traceback are not interchangeable terms. Traceroute is commonly used to evaluate Internet traffic to ensure that data is transmitted effectively. When adapted to identify an attack's source, this technology may be referred to as traceback. *See* Vamsi Paruchuri, Arjan Durresi & Leonard Barolli, *FAST: Fast Autonomous System Traceback*, 32 J. OF NETWORK & COMP. APPLICATIONS 448, 448–54 (2009) (using traceroute information to verify the accuracy of traceback); Alex C. Snoeren et al., *Single-Packet IP Traceback*, 10 IEEE/ACM TRANSACTIONS ON NETWORKING 721, 721–34 (2002) (defining traceback as "the ability to identify the source of a particular IP packet given a copy of the packet to be traced, its destination, and an approximate time of receipt").

350. *See, e.g.*, Francisco Maciá-Pérez, et al., *Network Intrusion Detection System Embedded on a Smart Sensor*, 58 IEEE TRANSACTIONS ON INDUS. ELECTRONICS 722, 722 (2011); Zhou, Leckie & Karunasekera, *supra* note 348, at 134, 136. For research about tracing, see Chao Gong & Kamil Sarac, *A More Practical Approach for Single-Packet IP Traceback Using Packet Logging and Marking*, 19 IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYS. 1310, 1311, 1312 (2008); Egon Hilgenstieler, et al., *Extensions to the Source Path Isolation Engine for Precise and Efficient Log-Based IP Traceback*, 29 COMPUTERS & SECURITY 383, 383 (2010); Katz-Bassett, *supra* note 349, at 9.

351. *See* Sklerov, *supra* note 25, at 73–74 (noting that intrusion detection includes detecting and classifying the attack). Because of limitations on attack detection, active defense would either need to happen very quickly or respond to a series of ongoing attacks. *Id.* at 75.

352. *See* Graham, *supra* note 253, at 99 (noting that the traceback capabilities of active defense permit direct targeting of the attacker and distinguishing attackers from noncombatants).

353. Karen Kent Frederick, *Network Intrusion Detection Signatures, Part One*, SYMANTEC, http://www.symantec.com/connect/articles/network-intrusion-detection-signatures-part-one (last updated Nov. 3, 2010).

the intrusion is a DDoS attack being executed remotely by one person attacking through thousands of compromised computers in a botnet.[354] One possible way of addressing collaborative attacks of this nature is to develop collaborative intrusion detection systems ("CIDS") — and a number of researchers have been examining various methods of doing so.[355] The three primary categories for approaches to CIDS are (1) centralized, (2) hierarchical, and (3) fully distributed.[356] Zhou et al. provide a helpful survey of the research concerning CIDS, and also set out the areas that should be the focus for further research, including expressiveness, scalability, and accuracy.[357]

2. Traceback

Once an attack has been detected, the next step in active defense is to identify the source of the attack. This identification is achieved through some form of traceroute, which is the most widely used diagnostic tool on the Internet.[358] Yong Guan's overview of network forensics provides a helpful look into the state of the art of traceback, giving summaries of the four primary IP traceback schemes: (1) active probing, (2) Internet Control Message Protocol ("ICMP") traceback, (3) packet marking, and (4) log-based traceback.[359] A recent study into reverse traceroute helpfully illustrates the improvements to the technology.[360] The researchers' reverse traceroute technique offered improvements in both the accuracy and coverage of traditional direct traceroute techniques.[361] The reverse traceroute study found that the median accuracy of reverse traceroute was eighty-seven percent, compared to seventy-five percent median accuracy for direct traceroute.[362]

Tracing is arguably the most important aspect of active defense because countermeasures cannot be implemented unless one can trace the attack to its source.[363] Tracing is often difficult because cyberattackers take many actions to hide their identities, and while trace programs can often find the actual source of an attack, they are not perfect and may incorrectly identify a source.[364] There are also tech-

354. *See* Zhou, Leckie, & Karunasekera, *supra* note 348, at 125.
355. *E.g.*, *id.* at 124.
356. *See id.* at 128–30.
357. *Id.* at 136.
358. *See* Katz-Bassett, *supra* note 349, at 1.
359. Yong Guan, *Network Forensics* (Chapter 20), *in* COMPUTER AND INFORMATION SECURITY HANDBOOK 339, 341–42 (John R. Vacca ed., 2009).
360. *See generally* Katz-Bassett, *supra* note 349.
361. *Id.* at 9–12.
362. *Id.* at 9.
363. *See* Katyal, *supra* note 35, at 62.
364. *See* Sklerov, *supra* note 25, at 77–78. It is also difficult for trace programs to pinpoint an attack after an attacker terminates the connection. *See id.* at 81.

nological limitations that currently limit the ability to make perfect surgical strikes with active defense.[365]

One additional concern about the technology used in active defense is that the attacker might be "spoofing" his IP address to evade detection.[366] Issues caused by IP spoofing (including harm to third parties) would be most acute in a situation where only traceback technology was used to determine an attack's origin. IDS provides additional information to the victim in the form of error messages that can indicate if the apparent origin identified by traceback may be inaccurate due to IP spoofing.[367] This knowledge can prevent the victim from counterstriking against an incorrect IP address and also potentially help locate the actual source of the attack.[368] However, these error messages would probably only appear in a limited number of cases, where a spoofed IP address does not correspond to a real IP address. Thus, it is questionable how much IDS adds to prevent counterstrikes against innocent parties.

3. Responding to an Attack

A response to cyberattacks could include more passive actions, such as turning over the attacker's identity to the government, or more active options, such as reflecting attacks back at the attacker or sending a new attack to interrupt the original attack.[369] Reflecting attacks back or initiating a new attack could, under the proper circumstances, both be considered mitigative counterattacks.

Though the government's cyber counterstrike capabilities are mostly classified, such counterstrikes might include a hack back feature that either inflicts damage on the attacker or that responds in some other way, perhaps automatically.[370] Publicly available layered security systems have included software such as ForeScout's "ActiveResponse" technology, which ForeScout claims is "capable of performing a perimeter defense and repelling would-be attackers

365. *See id.* at 80.

366. *See* Matthew Tanase, *IP Spoofing: An Introduction*, SYMANTEC, http://www.symantec.com/connect/articles/ip-spoofing-introduction (last updated Nov. 2, 2010) ("In IP spoofing, an attacker gains unauthorized access to a computer or a network by making it appear that a malicious message has come from a trusted machine by 'spoofing' the IP address of that machine.").

367. *See* Tom Chmielarski, *Intrusion Detection FAQ: Reconnaissance Techniques Using Spoofed IP Addresses*, SANS INST. (Apr. 4, 2001), http://www.sans.org/security-resources/idfaq/spoofed_ip.php ("One way to help determine which hosts did not send the packets (and therein which host did) is to search firewall and router logs for incoming error messages from the ten hosts that were spoofed, as those hosts react to the packets sent by the target in response to the stimulus from the attacker.").

368. *See id.*

369. *See* Radcliff, *supra* note 23 (providing an example of a hosting service redirecting packets from an attacker back to the attacker's web server).

370. *See* Jensen, *supra* note 19, at 231.

while tagging attackers and immediately blocking them if they try to return to the network."[371] In 2004, Symbiot Security announced a new product, iSIMS, that would enable firms to counterstrike when their network came under fire from malicious hackers.[372]

Before responding, however, a system administrator must map the system conducting the attack by assessing the system's functions and making an informed decision about the likely consequences of a counterstrike.[373] Such mapping is important in helping the system administrator avoid accidentally targeting innocent systems.[374] It is important to know the controller's specific hardware unit because a mitigative counterstrike needs to be able to neutralize the attack at its source, rather than at one of the intermediate nodes along the way.[375] Finally, although an attack can be neutralized without knowing the controller's physical location, that location is important from a legal standpoint because different laws may apply depending on the location of the hardware.[376]

C. A Need for More Advanced Technology

We acknowledge that the current state of technology may not be sufficiently advanced to serve as the basis of a mitigative counterstrike framework. Further research is needed to determine what level of confidence in a traceback should be necessary to permit mitigative counterstrikes against a particular target. For example, is an accuracy rating of eighty five percent sufficient, or should counterstrikes of all types remain illegal until traceback technology's standard error rate is five percent or less? Perhaps mitigative counterstrikes that involve sending malicious code at the attacker should require a higher standard of accuracy than a mitigative counterstrike that involves reflecting packets back at the attacker. We are flagging these suggestions as a potential area for further study, though our current focus is primarily on policy recommendations and the importance of setting forth standards and guidance in advance of a crisis.

The current posture of research into IDS and traceback technology provides strong evidence that the state of the art related to active defense is steadily improving. Because the state of the art suggests

---

371. *Id.* at 230. Discussions alleging various counterstrike capabilities have been ongoing for the past decade. DOROTHY E. DENNING, INFORMATION WARFARE AND SECURITY 393 (1999). One researcher claimed to have developed a "Blitzkrieg" server that could respond to cyberattacks by either sending viruses to the attacking machine or by instigating a DoS attack against the attacker. *Id.*

372. Press Release, Symbiot, Inc. *supra* note 311 ("Symbiot provides the equivalent of an active missile defense system.").

373. *See* Graham, *supra* note 253, at 100.

374. *See id.*

375. *See* NRC REPORT, *supra* note 4, at 144.

376. *See id.* at 145.

that we will eventually have the capability to address attribution problems, we provide a forward-looking analysis of the potential directions that policymakers might take concerning active defense and mitigative counterstriking once the technology is sufficiently advanced. We focus on an idea of active defense that utilizes IDS and traceback technology combined with mitigative counterstrikes in a detect-trace-counterstrike pattern. In this approach, an attack is detected via IDS, traced with traceback technology, and met with an active response. We argue that the first priority should be to develop a framework for mitigative counterstriking to protect CNI. Eventually, policymakers should develop a broader framework for active defense in order to deter attackers and to firm establish that the principles of self-defense and defense of property exist in cyberspace.

Because the availability of accurate technology is one of the key determinants of whether active defense is socially optimal,[377] we do not condone the vigilante behavior of those currently using less reliable active defense technologies. Instead, we support the continued prohibition of cyber counterstriking until such time as the technology is sufficiently advanced to enable victims to obtain reliable technical attribution data and execute counterstrikes in strict adherence to the principles of mitigation. Because our goal is to set forth a framework for preemptive policy, we next turn to a discussion of when active defense is the socially optimal approach to a cyberattack. While additional technological improvements would be beneficial, our current technological understanding is sufficiently advanced to allow us to evaluate the implementation of an active defense scheme, even if broad implementation must be delayed until the traceback technology is sufficiently accurate.

D. Socially Optimal Use of Active Defense

As noted above, a more enforceable criminal regime would likely deter cybercrime effectively. However, because no uniform enforcement of criminal cybercrime law currently exists, we urge that active defense and mitigative counterstriking could fill in the gaps by providing a framework grounded in deterrence. In addition to criminal enforcement, there are also other factors to consider when discussing active defense. In an earlier work, we used game theory to model the interaction between several measures: technological defenses (IDS and traceback), legal remedies (criminal law and tort-based litigation), and the economic incentives to engage in active defense.[378]

At its core, proportionate, mitigative counterstriking is self-defense. Self-defense is viewed as the use of reasonable force for self-

377. *See* Majuca & Kesan, *supra* note 24, at 11.
378. *See generally id.*

protection.[379] Our game theory model applies this idea of self-defense to cyber intrusions.[380] In an environment where it is possible to accurately identify the origin of cyber intrusions and to hold the hacker criminally liable across national borders, we suggest that criminal liability, rather than mitigative counterstriking, would provide a superior deterrent effect. Civil litigation and passive defense are also options, though these methods have significant weaknesses.[381]

Through analysis of the model, we have concluded that the socially optimal solution to the threat of cyber intrusions — in the absence of effective remedies through criminal law enforcement, civil litigation, or passive defense strategies — is to permit (but not require) parties to act in self-defense when reliable technology is available.[382] The model does not, however, address who should be permitted to engage in active defense. Our game theory model anticipates that mitigative counterstriking will be more appealing than civil litigation in situations where litigation would be impractical,[383] and that it will be a better option than relying purely on passive defense as long as passive defenses neither effectively deter attackers nor protect the target system.[384]

After considering the types of technology used in an attack and the possible methods of response, we conclude that our model of active defense and mitigative counterstriking is most applicable to DDoS attacks because it could help mitigate the harm from these repetitive attacks.[385] A sandbox solution, though capable of shortening the amount of time that it takes to recover from a DDoS attack, cannot mitigate ongoing harm.[386] Therefore, we assert that mitigative counterstriking appears to be a socially optimal solution to the threat of DDoS attacks for the protection of critical and sensitive systems, and may become socially optimal for other systems when sufficient technological standards are established and reached. The model further emphasizes the importance of the technology utilized: the victim should make reasonable efforts to employ IDS technology to detect intrusions and advanced traceback technology to ensure accurate targeting of the attacker.[387]

The model also anticipates holding counterstrikers liable for damage to innocent third parties, with the expectation that potential tort

379. *See* Jay P. Kesan & Ruperto Majuca, *Optimal Hackback*, 84 CHI.-KENT L. REV. 831, 833 (2010) [hereinafter Kesan & Majuca, *Optimal*].

380. *See id.* at 832.

381. *See supra* Part II.B.2–II.B.3.

382. Majuca & Kesan, *supra* note 24, at 24 ("The law should thus permit hackback as an option, but not force it as a requirement.").

383. Majuca & Kesan, *supra* note 24, at 39.

384. *Id.*

385. *See infra* Part VI.A.1.

386. *See supra* Part II.B.3.

387. Kesan & Majuca, *Optimal*, *supra* note 379, at 837; *infra* Part VI.A.1.

liability will give victims an incentive to avoid unnecessary force when executing mitigative counterstrikes.[388] This liability rule also incentivizes counterstrikers to use the most accurate technology so as to prevent collateral damage. The model posits that third-party damages are an important factor in attaining the socially optimal solution.[389] However, because some injured third parties may not have the knowledge or resources to litigate harm caused by a counterstrike, government regulation may be a way to protect these third parties from the unintended effects of mitigative counterstrikes.[390] The model also emphasizes that counterstrikers must only be permitted to use necessary and proportionate force and must refrain from "wantonly damag[ing] the hacker's digital systems out of retaliation,"[391] thus allowing such counterstrikers to engage only in *mitigative* counterstriking.

We argue that mitigative counterstrikes are justifiable as the best way to prevent social harm in response to an attack, but this idea is not revolutionary. The results of the model used to describe the social optimality of mitigative counterstriking resemble the "just war" doctrine for valid kinetic counterstrikes. This doctrine requires that (1) there is a threat of "grave damage" in the absence of a counterstrike, (2) the counterstrike has "a serious prospect of success," and (3) there are no practical or effective alternatives to counterstriking.[392] While retributive counterstriking may not meet the principles for a valid counterstrike under this doctrine, narrowing our focus to mitigative counterstriking places our proposal in clear consistency with the just war doctrine. There are many legitimate concerns about cyber counterstriking as a general matter, but we argue that the case for mitigative counterstriking is more compelling from a social welfare calculus than other types of responses to cyberattacks, and thus is the most readily justifiable approach to counterstriking in self-defense on the Internet.

We have established that applicable technology is headed in the right direction, that current legal methods for addressing cyberattacks are deficient in many respects, and that mitigative counterstrikes can — under the right circumstances — be the socially optimal response. We turn now to a thorough analysis of the legal regimes that must be considered before implementation of active defense can become a viable option. Further policy recommendations regarding the implementation of mitigative counterstriking are explored in Part VI.

---

388. *See* Kesan & Majuca, *Optimal*, *supra* note 379, at 838.

389. Majuca & Kesan, *supra* note 24, at 30.

390. *See* Kesan & Majuca, *Optimal*, *supra* note 379, at 838.

391. Kesan & Majuca, *Optimal*, *supra* note 379, at 838.

392. *Id.* at 838–39; *see also* Catechism of the Catholic Church ¶ 2309, *available at* http://old.usccb.org/catechism/text/pt3sect2chpt2art5.shtml.

IV. ANALYZING ATTACKS AND COUNTERSTRIKES UNDER CURRENT LEGAL REGIMES

While the previous discussion of legal options to address cyberattacks painted the issue with a broad brush, this Part will fill in the gaps and examine the different issues raised by cyberattacks, active defense, and mitigative counterstriking under criminal law, civil law, and international law. In Part II, we provided an overview of the weaknesses of current legal regimes in addressing cyberattacks. This Part further analyzes these legal regimes. We will first examine various facets of U.S. law, including statutes, common law, and presidential power — including whether presidential power could address cyber threats without a substantial shift in the legal regime. We will then analyze aspects of international law that could regulate cyber hostilities.

A. U.S. Law

Evaluating cyberattacks under U.S. law raises a wide variety of issues. One of the foundational questions in the domestic context is whether cyberattacks should be evaluated under a criminal law paradigm or a national security paradigm.[393] A third option is to require the private sector to address cyberattacks by resorting to civil litigation either against the attacker or against third parties who do not fulfill their duties to prevent cyberattacks.[394] Whether cybercrime is a national security issue, a criminal issue, or a civil issue, the United States currently has only a limited formal legal approach to addressing cybersecurity matters. Despite a number of executive orders, presidential statements, and administrative positions on cybersecurity, the government has not yet created a unified cybersecurity authority capable of issuing binding regulations.[395] In addition, there is currently

393. *See* Yang & Hoffstadt, *supra* note 94, at 210–11 (suggesting that the threat of cybercrime could be addressed by enforcing criminal laws like the CFAA). *But see* Condron, *supra* note 10, at 407–08 (urging that cybersecurity is a national security matter, not a criminal matter). Treating cyberattacks as national security matters raises several issues, including the need to clarify the distinction between "homeland security" and "homeland defense," the need to consider the application of *jus ad bellum* to cyberattacks, and the need to balance national security interests against civil liberties. Condron, *supra* note 10, at 408. According to Condron, homeland security consists of efforts to prevent attacks within the borders of the United States and is handled by the DHS, while homeland defense consists of protecting the United States from external threats, and is handled by the DOD. *Id.*

394. *See* Yang & Hoffstadt, *supra* note 94, at 207–08 (noting that the burden to prevent cybercrime could be placed on the victims — forcing the victims to protect themselves — or on software and hardware manufacturers).

395. *See* NRC REPORT, *supra* note 4, at 159 (noting that the "national policy with respect to cyberattack is fragmented and incomplete," with the need for secrecy preventing the development of coherent policy); Grant, *supra* note 41, at 115 (noting that it is unlikely that Congress will create a new cybersecurity agency due to cost constraints and that smaller

no effective mechanism for sharing cybersecurity information between different areas of the federal government.[396]

Many commentators have discussed potential congressional action on cybersecurity topics, with some calling for new legislation and others suggesting that Congress should clarify how the existing laws and authorities interact and apply to cybersecurity.[397] Some have noted that the executive branch may already have the authority to address cybersecurity issues, but that it might be better for Congress to legislate, ensuring that cybersecurity rules remain transparent and accountable to the public.[398] However, due to the lack of major cybersecurity crises, Congress is not currently under public pressure to prioritize cybersecurity legislation, and the technical nature of cybersecurity issues means that most members of Congress do not have a strong understanding of the issues and would likely not be comfortable fielding questions from the public.[399] Additionally, there is a lot of opposition to the idea of regulating the Internet, so it may be politically infeasible to pass strong cybersecurity legislation until there is a disaster.[400]

---

entities with limited authority may not be as effective as a new government agency); Sharp, *supra* note 30, at 20 (discussing that a national coordinator of cybersecurity does not exist, preventing the development of an "effective national cybersecurity program").

396. *See* Coldebella & White, *supra* note 139, at 237; *see also* Grant, *supra* note 41, at 108 (comparing cyber experts within the federal government to a "large fleet of well-meaning bumper cars" (quoting CTR. FOR STRATEGIC & INT'L STUDIES, SECURING CYBERSPACE FOR THE 44TH PRESIDENCY (2008), http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf)). One recent exception to this is the requirement that DOD and DHS must collaborate on cybersecurity matters. *See* National Defense Authorization Act for Fiscal Year 2012, Pub. L. No. 112-81, § 1090, 125 Stat. 1298 (2011).

397. *See* Grant, *supra* note 41, at 104; Edwards, *supra* note 57, at 36 (arguing for moving past "the inevitable knee-jerk call for new criminal offences" to address the problems of DoS attacks); Greer, *supra* note 166, at 140 (noting that policymakers and law enforcement must "interpret pre-cyberspace legal authorities and restrictions" in a manner that addresses cybersecurity concerns and also "protects privacy and civil liberties"). Grant argues that "if congressional action is needed" anywhere, it is needed to reorganize existing authorities. Grant, *supra* note 41, at 114.

398. *See, e.g.*, Grant, *supra* note 41, at 110; Dycus, *supra* note 88, at 166 ("Congress needs to act now to create authority and set boundaries within which the President may develop more refined protocols.").

399. *See* Grant, *supra* note 41, at 110–12.

400. *See id.* at 112; *see also* Fahmida Y. Rashid, *Forget SOPA. Is CISPA the Internet's New Enemy?*, PC MAGAZINE (Apr. 9, 2012, 12:01 PM), http://securitywatch.pcmag.com/security/296402-forget-sopa-is-cispa-the-internet-s-new-enemy (describing criticism of the Cyber Intelligence Sharing and Protection Act, H.R. 3523, 112th Cong. (2011)); Jonathan Weisman, *In Fight over Piracy Bills, New Economy Rises Against Old*, N.Y. TIMES (Jan. 19, 2012), http://www.nytimes.com/2012/01/19/technology/web-protests-piracy-bill-and-2-key-senators-change-course.html (describing Internet blackouts protesting the Stop Online Piracy Act, H.R. 3261, 112th Cong. (2011)). Regulatory efforts should be carefully tailored to preserve values like privacy, liberty, and innovation, as well as to protect the open nature of the Internet. Nojeim, *supra* note 139, at 119. Nojeim suggests that heavy-handed government regulation could put the open, decentralized nature of the Internet at risk. *Id.* at 119–20.

This Part will examine U.S. law applicable to cyberattacks to evaluate whether change is necessary. First, we will consider statutory schemes, with a focus on the CFAA. Next, we will turn to areas of the civil common law that could address cyberattacks. Finally, we will evaluate the executive branch's ability to unilaterally address cyber threats.

1. Statutes

Federal statutes regulating investigations and permitting certain activities by law enforcement may apply to cyberattacks. Responsibility for collecting information on cyberattack occurrence and attribution normally falls on the FBI or other domestic law enforcement agencies.[401] Agencies conducting computer monitoring must comply with the Fourth Amendment, the Electronic Communications Privacy Act ("ECPA") — which includes the Pen Register Act, the Federal Wiretap Act, and the Stored Communications Act ("SCA") — the Computer Security Act of 1987, and the CFAA.[402] The Foreign Intelligence Surveillance Act ("FISA") also has implications for the investigation of cyberattacks, since it requires law enforcement to obtain a warrant from the Foreign Intelligence Surveillance Court in order to collect foreign intelligence information.[403]

Under the ECPA, law enforcement has the legal authority to monitor electronic computer-based communications under certain circumstances, providing a statutory basis for the investigation of cyberattacks.[404] The SCA includes provisions setting out when Internet Service Providers can be compelled to disclose information about their customers, and when such providers are permitted to disclose information to the government absent a formal request.[405]

Another category of regulations requires certain security protections for federal systems[406] or provides for the establishment or en-

401. *See* NRC REPORT, *supra* note 4, at 291.

402. *See infra*; Greer, *supra* note 166, at 143–44; Nojeim, *supra* note 139, at 125–26.

403. 50 U.S.C. § 1805 (2006 & Supp. IV 2010) (setting forth procedures for obtaining an order for surveillance). There is at least one documented case of a FISA warrant authorizing a cyber exploitation of a MySpace account. *See* NRC REPORT, *supra* note 4, at 286–87. The warrant in that case was issued on June 12, 2007. *Id.*

404. 18 U.S.C. § 2510 (2006). Law enforcement officials may also obtain a warrant to search computers for documents relevant to a cyberattack investigation. NRC REPORT, *supra* note 4, at 200.

405. 18 U.S.C. §§ 2702, 2703 (2006 & Supp. IV 2010). The provisions for compelled disclosure to a government entity are found in § 2703. Depending on the information sought, the SCA may require a warrant, an administrative subpoena, or a § 2703(d) court order demonstrating "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." *Id.* § 2703.

406. The Federal Information Security Management Act ("FISMA") is aimed at protecting federal information and information systems, requiring agency-wide programs for in-

forcement of relevant standards.[407] There are also a number of sections in the U.S. Code that prohibit various activities or govern major segments of the U.S. Government.[408] The statute most applicable to our discussion, however, is the CFAA, which criminalizes a broad variety of behaviors relating to the misuse of computers. The CFAA also provides for civil relief when economic damage results from certain categories of cyberattack.[409] Because the CFAA is the most relevant federal statute on this topic, we turn now to a more detailed examination of its provisions.

A. Computer Fraud and Abuse Act

The CFAA criminalizes intentionally or recklessly causing damage to a computer that is under the exclusive control of a financial institution or the government, or that is used in interstate commerce.[410] Depending on the nature of the attack, such actions could be punished under either the felony or misdemeanor provisions of the CFAA. The felony provisions set out maximum sentences for violations of § 1030(a), which can range from five years to life in prison depending on the attack's intended results or actual consequences.[411] The CFAA currently has a $5000 minimum damage threshold for most types of felony violations of the Act,[412] though some have sug-

---

formation security. 44 U.S.C. § 3541 (2006). However, FISMA has been criticized for not being very effective. *See, e.g.*, Grant, *supra* note 41, at 105.

407. *See* Grant, *supra* note 41, at 107 (noting that another regulatory authority affecting cybersecurity issues is the Federal Energy Regulatory Commission, which has statutory authority to enforce standards under the Federal Power Act's electric reliability provision).

408. The commission of war crimes, defined as acts constituting breaches of the Geneva or Hague Conventions, is a federal offense. 18 U.S.C. § 2441 (2006). Other parts of the U.S. Code include various provisions relevant to government conduct, including Title 10, which contains provisions governing activities of DOD, and Title 50, which contains provisions governing activities of the intelligence community. NRC REPORT, *supra* note 4, at 282. One provision of Title 50 contains language distinguishing between "covert actions," "traditional counterintelligence activities," "traditional law enforcement activities," and "traditional diplomatic or military activities." 50 U.S.C. § 413(b) (2006 & Supp. IV 2010). The NRC Report suggests that it would be an intelligence collection activity instead of a covert activity if a party planted a Trojan horse key logger in another government's computers. NRC REPORT, *supra* note 4, at 285. The line between intelligence collection and covert action, however, is blurry. *See id.*

409. 18 U.S.C. § 1030 (2006 & Supp. IV 2010).

410. *Id.*

411. *Id.* § 1030(a). Life in prison is possible if the attacker attempts to cause a death or knowingly or recklessly causes a death. 18 U.S.C. § 1030(c)(4)(F) (2006 & Supp. IV 2010). The Obama administration has expressed interest in amending RICO to include computer fraud as a predicate offense, which would significantly increase the penalties for repeated violations. *Cybercrime: Updating the Computer Fraud and Abuse Act to Protect Cyber Space and Combat Emerging Threats: Hearing Before the S. Comm. on the Judiciary*, 112th Cong. 5 (2011) (statement of James A. Baker, Associate Deputy Att'y Gen., U.S. Department of Justice).

412. 18 U.S.C. § 1030(a) (2006 & Supp. IV 2010). The $5000 threshold can be met by including the cost of damage assessments, lost revenues, and other costs. 18 U.S.C.

gested eliminating any minimum damage requirement in the interest of increasing the deterrent effect of the CFAA.[413] The CFAA also creates a civil cause of action, permitting the attack victim to sue the attacker for compensatory damages or equitable relief in addition to any criminal sanctions for violating the Act's felony provisions.[414]

There is some evidence that when the CFAA was originally enacted in 1984, it was partially in response to the situations depicted in the action film WarGames.[415] When it was passed, the CFAA was criticized as being too vague and narrow, so Congress studied computer crime issues in more detail before passing a greatly revised version of the CFAA in 1986.[416] Between 1986 and 2008, Congress amended the CFAA nine times.[417]

The 1996 amendments to the CFAA replaced the term "federal interest computer" with "protected computer."[418] The CFAA now dis-

---

§ 1030(e)(11); EF Cultural Travel v. Explorica, Inc., 274 F.3d 577, 584–85 (1st Cir. 2001) (finding a CFAA violation when the plaintiff suffered no actual damage but spent $20,000 on diagnostics to determine if there was damage and $40,000 in "re-securing" costs); United States v. Middleton, 231 F.3d 1207, 1213 (9th Cir. 2000); *see also* Skibell, *supra* note 48, at 928–29 (stating that the inclusion of resecuring costs in damage awards is unusual). According to the 2002 CSI/FBI Computer Crime Survey, eighty percent of survey respondents had experienced financial losses stemming from cyberattacks, but only forty-four percent of respondents could quantify their losses. *See* Skibell, *supra* note 48, at 932. Some critics also allege that the FBI is encouraging inflation of damage assessments by informing companies in advance that damages must exceed $5000 to warrant prosecution. *See id.* at 933.

413. *See, e.g.*, Yang & Hoffstadt, *supra* note 94, at 213. However, some have argued that more severe penalties may actually exacerbate computer crime. *See, e.g.*, Skibell, *supra* note 48, at 938.

414. 18 U.S.C. § 1030(g).

415. Skibell, *supra* note 48, at 910 (arguing that "historically, there has been little connection between public policy and reality in this area of the law").

416. *See id.* at 912.

417. *See id.* (discussing the eight revisions between 1986 and 2003). The amendment in 2008 broadened § 1030(a)(2)(C), which criminalizes unauthorized access and obtaining of information from a protected computer, by removing the requirement that the unauthorized access involve interstate or foreign communications. Pub. L. No, 110-326, § 203, 122 Stat. 3560 (2008) (codified as amended at 18 U.S.C. § 1030(a)(2)(C) (2006 & Supp. IV 2010)).

418. National Information Infrastructure Protection Act of 1996, Pub. L. 104-294, § 201(4)(A)(i), 110 Stat. 3493 (codified as amended in 18 U.S.C.A. § 1030 (2006 & Supp. IV 2011)). The statute currently defines a "protected computer" as a computer:

> (A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or
>
> (B) which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States . . . .

18 U.S.C § 1030(e)(2). The deletion of the term "Federal interest," which greatly expanded liability under the Act, may have been accidental. Joint Chiefs of Staff, INFORMATION ASSURANCE: LEGAL, REGULATORY, POLICY, AND ORGANIZATIONAL CONSIDERATIONS C-14 (4th ed. 1999), *available at* http://www.au.af.mil/au/awc/awcgate/jcs/ia.pdf.

tinguishes between "computers" and "protected computers," where a "computer" becomes a "protected computer" by participating in interstate commerce or communication.[419] This means that the CFAA criminalizes intentionally or recklessly damaging virtually any computer connected to the Internet.[420] The Internet in 1996 may not have been sufficiently mainstream for the effects of such sweeping language to be appreciated.[421] But the definition of "protected computer" was amended again in 2008 to cover computers that were "used in *or affecting*" interstate or foreign commerce or communication,[422] and by then Congress would certainly have appreciated the reach of the statute's language.

The CFAA's language is very broad and can be read to prohibit the creation of botnets.[423] The CFAA "does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States," so it may be permissible under the law for the U.S. Government to create a botnet using private computers.[424] It should be noted, however, that the CFAA does not include an exemption for conduct by military agencies.[425]

The CFAA has been amended and expanded many times over the past few decades.[426] Courts have consistently interpreted the CFAA's language very broadly to prohibit a wide variety of acts,[427] in part be-

---

419. 18 U.S.C. § 1030(e). The term "protected computer" was not found in the original language of the CFAA and was instead added by Congress in 1996. Pub. L. 104-294, § 201(4)(A)(i), 110 Stat. 3488 (1996) (changing the language of the CFAA's definitions section from "Federal interest computer" to "protected computer").

420. *See* NRC REPORT, *supra* note 4, at 205.

421. *See* Steve Lohr, *Media Convergence*, N.Y. TIMES, June 29, 1998, at A1 (discussing data from 1995 that indicated that seven percent of the U.S. population was on the Internet).

422. Identity Theft Enforcement and Restitution Act of 2008, Pub. L. 110-326, § 207, 122 Stat. 3563 (codified as amended in 18 U.S.C. § 130(e)(2)(B)) (emphasis added to indicate language inserted by this amendment). Notably, § 207 was titled "Use of Full Interstate and Foreign Commerce Power for Criminal Penalties." *Id.*

423. *See* NRC REPORT, *supra* note 4, at 222; Ed Felten, *Botnet Briefing*, FREEDOM TO TINKER (Apr. 26, 2007, 5:41 AM), http://freedom-to-tinker.com/blog/felten/botnet-briefing (discussing applying the CFAA to botnets).

424. 18 U.S.C. § 1030(f).

425. *See* NRC REPORT, *supra* note 4, at 288 (noting, however, that the legislative history suggests that Congress may have intended to exempt overseas military operations from the CFAA).

426. *See, e.g.*, Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213 (codified as amended at 18 U.S.C. § 1030 (2006 & Supp. IV 2011)); "The Cyber Security Enhancement Act" of the Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2158 (codified as amended in scattered sections of 18 U.S.C.) (strengthening penalties for violations of the Act in section 18 U.S.C. 1030(c) (2006 & Sup. IV 2011)); *see also* Skibell, *supra* note 48, at 916 (referencing amendments contained in the USA PATRIOT Act that make it easier to charge cyberattackers with a felony by removing the monetary threshold when attacked computers "were used for national security or criminal justice"). Skibell notes that the first major reworking of the CFAA was in 1986, with a record reflecting careful deliberation and compromise, though later amendments (such as the 2002 amendments) seemed to undergo less scrutiny. *Id.* at 910.

427. *See, e.g.*, Pulte Homes v. Laborers' Int'l Union of N. Am., 648 F.3d 295, 301 (6th Cir. 2011) (interpreting the CFAA to cover voicemail as a "transmission" under the Act).

cause Congress has consistently enlarged the CFAA every time it was amended over the last twenty-five years.[428] We argue that the overly broad interpretations of the CFAA accepted by courts over the last several years weaken it as a statutory scheme for addressing cyberattack issues.[429]

The CFAA was read more narrowly, however, in the recent case of *United States v. Drew*.[430] In *Drew*, a federal judge entered a directed verdict to negate a jury's finding that defendant Lori Drew guilty under the CFAA's misdemeanor provisions by violating the terms of service of the MySpace website.[431] The *Drew* case provides evidence that there is a need for limits to the CFAA. The public outcry against Drew's involvement in harassing a young girl who then committed suicide led the U.S. Attorney in Los Angeles to prosecute Drew.[432] The theory of the case was that in violating the MySpace terms of service, Lori Drew had exceeded authorized access of the MySpace servers; the jury agreed that Drew's actions amounted to a violation of the misdemeanor provisions of the CFAA.[433] After the jury returned its guilty verdict, however, the judge overturned the conviction.[434] The *Drew* case, while arguably an extreme example of prosecutors pushing the boundaries of the CFAA, is an important one as it illustrates some judicial awareness of the need to rein in overly broad interpretations of this Act.

We also argue that the CFAA should be revised to address the distinction between the terms "computer" and "protected computer," and that the language should also be revised to address the concept of authorization. First, the CFAA clearly distinguishes between sections that apply broadly to "computers" and sections that apply only to

---

428. *See* Skibell, *supra* note 48, at 911.

429. Skibell criticizes the CFAA as profoundly oversimplifying "the cybercriminal archetype" and prohibiting behaviors that fall far short of malevolent intrusions and cyberterrorism, such as the cases of hackers breaking into a system and making a copy of a document only for trophy purposes. *Id.* at 918, 922. For example, the hacker Kevin Mitnick pled guilty under the CFAA to accessing Sun Microsystems' computer system and downloading the Solaris operating system source code. The court sentenced Mitnick based on the alleged $80 million value of the software, even though Sun never reported a loss and later made the stolen source code publicly available. *Id.* at 922–23.

430. 259 F.R.D. 449 (C.D. Cal. 2009).

431. *Id.* at 451, 467–68.

432. *See* Jennifer Steinhauer, *Woman Found Guilty in Web Fraud Tied to Suicide*, N.Y. TIMES, Nov. 27, 2008, at A25.

433. *Drew*, 259 F.R.D. at 451–53. Though rejected by a court, the DOJ continues to take the position that violating a website's Terms of Service should be considered a violation of the CFAA's prohibition on exceeding authorized access. *See* Declan McCullagh, *DOJ: Lying on Match.com Needs to Be a Crime*, CNET NEWS (Nov. 14, 2011, 11:58 PM), http://news.cnet.com/8301-31921_3-57324779-281/doj-lying-on-match.com-needs-to-be-a-crime/.

434. *Drew*, 259 F.R.D. at 468; *see also* Bobbie Johnson, *Judge Overturns Guilty Verdict in MySpace Suicide Case*, GUARDIAN TECH. BLOG (July 2, 2009), http://www.guardian.co.uk/technology/blog/2009/jul/02/lori-drew-myspace-acquitted.

"protected computers."[435] In practice, however, because the main distinction between a computer and protected computer is Internet access,[436] a large majority of household computers in the United States are protected computers.[437] This result makes the statutory distinction between "computers" and "protected computers" both vague and meaningless. Second, the language addressing access "without authorization" or that "exceeds authorized access"[438] to a "protected computer" is broad enough that the DOJ has argued that the CFAA criminalizes the violation of the Terms of Service of a private website.[439] A less culpable actor who inadvertently violates website terms that he did not read may thus face strict punishment under the "protected computer" penalties. We thus advocate for a reconceptualization of the terms "protected computer," "without authorization" and "exceeds authorized access" to preserve the vitality of the CFAA by ensuring that the Act does not apply to less culpable defendants. This reconceptualization could be accomplished if courts more narrowly interpret "protected computers" and what it means for access to be unauthorized, or if Congress amends the language to clarify these terms.

A provision of the CFAA that is potentially useful to victims of cyberattacks is the civil cause of action under § 1030(g). Nonviolent computer crimes that only cause economic harms might be better addressed through the civil liability provisions of the CFAA — or through tort law — than under the CFAA's criminal provisions.[440] The civil action provision of the CFAA, however, only provides that an attack victim may bring an action against "the violator" for compensatory damages or equitable relief.[441] Where an attacker is un-

---

435. *See, e.g.*, 18 U.S.C. § 1030(a)(2) (2006 & Supp. IV 2010) ("intentionally accesses a computer without authorization"); *id.* § 1030(a)(4) ("knowingly and with intent to defraud, accesses a protected computer without authorization"). The term "protected computer" originally applied only to "computers used by financial institutions or by the Federal Government when the perpetrator is an outsider." S. REP. No. 104-357, at 4 (1996). Congress intentionally expanded the term "protected computer" to cover civilian computers. *See id.* Section 1030(a)(2)(C) illustrates one of the more confusing instances of using these two terms simultaneously, since it refers to using a "computer" to obtain information from a "protected computer."

436. *See* 18 U.S.C. § 1030(e)(1) ("[T]he term 'computer' means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions . . . ."); *id.* § 1030(e)(2) (defining a "protected computer" as a computer exclusively used by or affecting a financial institution or the U.S. Government or "used in or affecting interstate or foreign commerce or communication").

437. *See* U.S. CENSUS BUREAU, STATISTICAL ABSTRACT OF THE UNITED STATES 724 tbl. 1156 (2012), *available at* http://www.census.gov/compendia/statab/2012/tables/12s1157.pdf.

438. *See, e.g.*, 18 U.S.C. § 1030(a)(1) ("Whoever — having knowingly accessed a computer without authorization or exceeding authorized access….").

439. *See Drew*, 259 F.R.D. at 452.

440. *But see* Skibell, *supra* note 48, at 941–42.

441. 18 U.S.C. § 1030(g).

known and difficult to identify, it will be difficult for an attack victim to bring a claim. This provision is thus arguably not very helpful as a practical matter given the current state of traceback technology. Since attackers may not have substantial resources, they may also be effectively judgment-proof, rendering the civil cause of action useless even in circumstances where an attacker can be personally identified.[442] Additionally, the CFAA's civil provisions are only available to the direct victim of an attack, thus failing to take into account harm to third parties who rely on the direct victim's systems.[443] The CFAA has the same weaknesses as other criminal law provisions addressing cyberattacks, including the difficulty of bringing an action against an unidentified attacker or providing a remedy for an indirect victim of a cyberattack.

2. Common Law

Another option under domestic law is to hold parties liable under theories of tort or contract,[444] leaving it to the free market to address the risk of cyberattacks. But which party or parties should be liable? And under what cause of action? There are three general causes of action available to civil litigants alleging tortious conduct: intentional torts, negligence, and strict liability. Strict liability generally applies when a party in control of an abnormally dangerous activity is held responsible for harm resulting from that activity regardless of fault.[445] Unless accessing the Internet using an unprotected system is considered to be an abnormally dangerous activity — a finding we think is very unlikely — a strict liability theory is not likely to provide a viable cause of action in the event of a cyberattack.

It is most likely that an action against an attacker would fall under some intentional tort theory. An intentional tort action against a third party, such as the owner of a zombie computer, is unlikely to succeed because the third party probably lacks the requisite intent.[446] This leaves negligence or contract law to address actions by these third parties. Contract actions would only be available when there is a contractual relationship between the plaintiff and a third party, and are

442. *See* Skibell, *supra* note 48, at 942.

443. *See supra* Part II.A.1.D.

444. *See* Edwards, *supra* note 57, at 51–52.

445. *See* AARON D. TWERSKI & JAMES A. HENDERSON, JR., TORTS: CASES AND MATERIALS 487 (2003).

446. "The word 'intent' is used . . . to denote that the actor desires to cause [the] consequences of his act, or that he believes that the consequences are substantially certain to result from it." RESTATEMENT (SECOND) OF TORTS § 8A (1965); *see also* Garratt v. Dailey, 279 P.2d 1091, 1094 (Wash. 1955) (requiring that the defendant know with substantial certainty that the harm would result).

likely to be less attractive than options under negligence because of remedy limitations.[447]

A. Intentional Tort

Assuming that an attacker can be individually identified, the most obvious way to pursue the attacker under common law is for committing an intentional tort — but which tort? de Guzman notes that the primary cause of action utilized against cyberattackers who execute DoS attacks is trespass to chattel, which has gained new life in the cyber context in spite of formerly being dismissed as "a little brother of conversion."[448] Several cyber intrusion cases have been decided on a trespass to chattel theory.[449] The tort of trespass to chattels requires an intermeddling with personal property,[450] which courts have consistently interpreted as encompassing a "denial of service" attack.[451] Other commentators have proposed using a nuisance cause of action to address spam and DoS attacks.[452]

The greatest difficulty with using a trespass to chattels or nuisance theory to hold an attacker liable is the same problem that has been noted many times before: the difficulty of identifying the indi-

---

447. *See* RESTATEMENT (SECOND) OF CONTRACTS § 344 (1981). In a negligence cause of action, the remedy may include a number of factors not related to the contract price, such as incidental damages and punitive damages. *Id.* § 355. However, a court will generally not grant punitive damages as a remedy when a party breaches a contract. *Id.*; *see also* Guevara v. Maritime Overseas Corp., 59 F.3d 1496, 1513 (5th Cir. 1995).

448. de Guzman, *supra* note 68, at 531 (citations and internal quotations omitted) (stating that trespass to chattels, once dismissed in PROSSER ON TORTS, is now the primary cause of action in response to a DoS attack).

449. *See, e.g.*, eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1071–72 (N.D. Cal. 2000) (granting a preliminary injunction and finding that eBay had made a strong showing that it was likely to prevail on the merits of its trespass to chattels claim when bots exceeded the scope of eBay's consent to access by downloading massive amounts of auction information); Compuserve Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1018, 1027 (S.D. Ohio 1997) (holding that the trespass to chattel cause of action applies to spam); Thrifty-Tel, Inc. v. Bezenek, 54 Cal. Rptr. 2d 468, 471–72 (Ct. App. 1996) (holding that use of a company's access code to gain free long-distance service was an unauthorized use of personal property sufficient to support a verdict on trespass to chattel theory); *see also* de Guzman, *supra* note 68, at 532–38 (discussing the previous cases). *But see* Intel Corp. v. Hamidi, 71 P.3d 296, 300 (Cal. 2003) (holding that trespass to chattels does not include "an electronic communication that neither damages the recipient computer system nor impairs its functioning"). The above cases would likely be categorized as cyber exploitations rather than cyberattacks, since the general goal of the defendants was to get information. However, one can infer from the holding in *Intel* that trespass to chattels would apply to cyberattacks. *See id.* at 300.

450. RESTATEMENT (SECOND) OF TORTS § 217 (1965).

451. de Guzman, *supra* note 68, at 545.

452. *See id.* at 546 & n.149 (examining commentary in favor of applying nuisance law in the cyber context); *see also* Dan L. Burk, *The Trouble with Trespass*, 4 J. SMALL & EMERGING BUS. L. 27, 53–54 (2000) (arguing that nuisance is better than trespass to chattels for addressing cyberspace issues); Adam Mossoff, *Spam — Oy, What a Nuisance!*, 19 BERKELEY TECH. L.J. 625, 641 (2004) (arguing that the court in *Hamidi* viewed spam as causing a nuisance injury).

vidual attacker. If an anonymous attacker cannot be identified, he cannot be sued. That said, if an IP address can be found, the ISP can be subpoenaed for the identity of the owner of the computer with that IP address, permitting civil action against a John Doe attacker.[453] Such an approach, however, may not be helpful if an attacker is located outside of the country, and it may lead to many dead ends or false accusations because of IP spoofing.[454] Because of the expenses associated with litigating, such an approach is also likely to be cost-prohibitive and impractical, especially for cyberattack victims with fewer assets.

B. Negligence

Another potential approach is to pursue negligence causes of action against intermediary parties other than the attacker. However, we still have the problem of determining which intermediary party should be held liable. Zombie computer owners, ISPs,[455] and software manufacturers are all possible parties. Under a negligence theory, even the victim of the attack could be held responsible for harm to collateral victims — for example, customers of a utility company who experience interruption of service because of an attack against the utility company — because the attack victim failed to secure his system.[456] Because ISPs do not initiate or profit from DDoS attacks, there is some opposition to formally holding ISPs legally responsible for such

---

453. Microsoft has used a similar approach by filing 117 lawsuits against unnamed individuals when seeking to identify perpetrators of phishing scams. Brian Krebs, *Microsoft Seeks to Identify Phishing Scam Authors*, WASH. POST (Mar. 31, 2005), http://www.washingtonpost.com/wp-dyn/articles/A16257-2005Mar31.html.

454. *See supra* Part III.B.2.

455. Some have suggested that ISPs could become more involved in cybersecurity issues. *E.g.*, Sharp, *supra* note 30, at 25 (suggesting that ISPs should require users to allow ISPs to clean up user machines to get rid of malicious software that permits the machines to be used as part of a botnet).

456. *See* Jennifer A. Chandler, *Security in Cyberspace: Combatting Distributed Denial of Service Attacks*, 1 U. OTTAWA L. & TECH. J. 231, 243–48 (2003–04) (discussing but not accepting view that third parties could be prosecuted for not securing computers); Edwards, *supra* note 57, at 44–45. de Guzman noted that using a negligence standard to hold zombie computer owners liable has the economic benefit of shifting a duty to take precautions onto the computer owner. de Guzman, *supra* note 68, at 553. Others, however, oppose holding zombie computer owners liable because imposing liability on the owners of unsecured systems amounts to "a tax on ignorance and technophobia." Edwards, *supra* note 57, at 47. Instead of holding individual computer owners liable, some commentators have argued that holding software writers liable might be more effective. *See, e.g.*, Chandler, *supra*, at 249. That said, Edwards notes that software prices might skyrocket if software writers were suddenly legally liable for buggy software. Edwards, *supra* note 57, at 52–53. He has also argued that imposing liability on software writers may be "an inequitable and impractical solution." *Id.* at 52. Software writers could potentially be sued under a negligence theory or a contract theory, but if they could show sufficient due diligence, they would likely not be held negligent, and current software writers are largely protected from contract liability by the terms of clickwrap licenses. *See id.* at 52–53.

attacks, though it is acknowledged that ISPs could be very helpful in addressing many of the issues raised by cyberattacks if they began acting as "Internet security guards."[457]

Under the common law, it would likely be difficult to hold any intermediary party liable in tort for harm caused by a DDoS attack. First, it is unclear whether any intermediary party owes a duty of care to the ultimate victim. The foundational case of *Palsgraf v. Long Island Railroad*[458] sets out two conflicting views of when negligence liability may attach. The majority characterizes negligence "as a term of relation" attaching to specific others to whom the defendant owes a duty of care,[459] while the dissent posits that liability for negligence could attach if the negligent actor engaged in an "act which unreasonably threatens the safety of others."[460] Under the majority rule, an intermediary party would not be held negligent for damage caused by a cyberattack, while under the minority rule, an intermediary party may be held responsible for "creat[ing] the hazard that made it possible for a third party to harm the plaintiff."[461] The modern rule is trending towards the minority position by looking at "the risks that an actor creates at the time of his allegedly negligent conduct."[462]

How does this apply to our potential non-attacker defendants? For zombie computer owners, the primary question concerning duty of care is whether the owner of a compromised system owes a duty to the ultimate victim.[463] There is currently no case law supporting the argument that zombie computer owners owe attack targets a duty of care to secure their systems.[464] As for software manufacturers, the most significant difficulty in showing a duty of care is likely to be the End User License Agreements, which often limit or completely disclaim all available warranties and potential liabilities against the com-

457. Edwards, *supra* note 57, at 59–60. ISPs, however, might need some sort of incentive to take on this sort of supervisory role, as some commentators have suggested that ISPs will not otherwise invest in Internet security if they are left to self-regulate. *See, e.g.*, *id.* at 61.

458. Palsgraf v. Long Island R.R., 162 N.E. 99 (N.Y. 1928).

459. *Id.* at 101 ("Affront to personality is still the keynote of the wrong [of negligence].").

460. *Id.* at 102 (Andrews, J., dissenting). That said, the distinction between the majority and dissent's views in *Palsgraf* is still a matter of some debate. *See* de Guzman, *supra* note 68, at 539–40 (2010).

461. de Guzman, *supra* note 68, at 541.

462. de Guzman, *supra* note 68, at 549.

463. If it is held that computer owners have a duty to prevent infection, this duty may also create a privilege to disrupt botnets with reasonable counterstrikes. *See* de Guzman, *supra* note 68, at 556. There are, however, many international law implications to permitting counterstrikes that must be taken into consideration before recommendations like this are adopted. *See supra* Part IV.B.

464. *See* Edwards, *supra* note 57, at 46. Edwards writes primarily from the perspective of the United Kingdom, but no case law directly on point exists in the United States to our knowledge, though analogies can be drawn.

pany.[465] Some critical service providers — such as electric companies — may also include contract language disclaiming liability for service interruptions that were beyond the provider's ability to avoid through reasonable diligence and care, such as interruptions caused by acts of God or war.[466] Under the current regime, it is therefore likely that software manufacturers and most other non-attacker defendants would be able to avoid liability for collateral damage by pointing to the terms of contracts accepted by the plaintiff.[467]

However, there may be a stronger argument for finding that a duty exists when there is a special relationship between the non-attacking intermediary and the injured plaintiff. For example, in *Bell v. Michigan Council 25*,[468] the court reasoned that a trade union with inadequate computer security could be held responsible for harm when its members' personal information was compromised.[469] The reasoning of *Bell*, though, is more immediately applicable in the context of identity theft. It is currently not clear under what circumstances a court will find a special relationship that imposes a duty on an intermediary.

The other major problem with holding non-attackers liable in tort is proving proximate cause. Traditionally, the wrongful act of a third party — here, the cyberattacker — would serve as a superseding cause that breaks the causal chain because the tortious behavior of a malicious third party is generally unforeseeable.[470] The traditional rule for superseding causes can be found in *Watson v. Kentucky & Indiana Bridge & Railroad*.[471] The case centered on whether the railroad was responsible for harm caused by a fire that started when a lit match fell onto a puddle of gasoline that a railroad employee had negligently spilled.[472] In *Watson*, the answer turned on whether the lit match was negligently dropped onto the puddle of gasoline — in which case the

---

465. *See, e.g.*, *End User License Agreement*, CISCO SYSTEMS, INC., http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html (last visited May 3, 2012) (setting the purchase price of the software as Cisco's maximum liability for any injury to a customer, regardless of the cause of action); David R. Collins, *Shrinkwrap, Clickwrap, and Other Software License Agreements: Litigating a Digital Pig in a Poke in West Virginia*, 111 W. VA. L. REV. 531, 548 (2009) (quoting language from the Mac OS X Software License Agreement as absolving Apple from liability for virtually all possible damages, even if the damages are caused by a known defect).

466. *See, e.g.*, SAN DIEGO GAS & ELEC. CO., RULE 14 (1983), *available at* http://www.sdge.com/tm2/pdf/ELEC_ELEC-RULES_ERULE14.pdf.

467. We note that these terms are generally part of contracts of adhesion. However, since such clickwrap agreements are typically upheld, we do not anticipate that the nature of these contracts would alter duties under negligence law.

468. Bell v. Michigan Council 25 of the Am. Fed'n of State, County, and Mun. Employees, AFL-CIO, Local 1023, No. 246684, 2005 WL 356306 (Mich. Ct. App. 2005).

469. *Id.* at *3 (noting that the organization, through its relationship to its members, had a responsibility to safeguard its members' private information).

470. Watson v. Ky. & Ind. Bridge & R.R., 126 S.W. 146, 150–51 (Ky. 1910).

471. *See id.*

472. *Id.* at 147.

railroad could be held liable for damages — or whether the lit match was intentionally thrown onto the puddle of gasoline by a third party intending to cause an explosion — in which case the railroad could not be held liable for damages due to the presence of a superseding cause.[473]

In the cyber context, an unsecured system or network or a vulnerable piece of software could be analogized to a negligently spilled puddle of gasoline, with a cyberattack that exploits these vulnerabilities analogized to a malicious third party who throws a lit match onto the gasoline. Under the traditional rule, therefore, it is unlikely that an intermediary could be held liable under a negligence theory, because the botnet master's intentional actions would be viewed as a superseding cause that severs the causal chain.[474] The modern rule in many American jurisdictions, though, allows for a finding of proximate cause despite the existence of an interceding intentional tort by another party, provided the circumstances are still foreseeable.[475] Because the connection between cybersecurity measures and cyberattacks is self-evident, and lax cybersecurity could foreseeably lead to negative consequences from cyberattacks,[476] a court following the modern rule would likely find that the causal relationship is preserved, and would thus be likely to conclude that proximate cause still exists.[477]

Thus civil liability for third party intermediaries may be largely ineffective as a means of recourse for cyberattack victims. In order for a claim of negligence to be viable, a court that follows the modern

---

473. *Id.* at 150–51.

474. *See* de Guzman, *supra* note 68, at 538. de Guzman suggests recharacterizing duties of care to hold zombie computer owners liable for negligence. *Id.* at 548–50. Whether a zombie computer owner can be held liable has been compared with "parked car" cases in negligence law, where the plaintiff was injured by being struck by a stolen car, and the defendant is the owner of the stolen car who had left the keys in the ignition. de Guzman, *supra* note 68, at 540–41 (noting the majority view is that the defendant car owner is not liable). de Guzman points out, however, that parked cars are dissimilar from unsecured computers because zombie computers are never completely out of the owner's control. *Id.* at 554–55.

475. Kentucky, for example, no longer follows the rule its own court set down in *Watson*. *See* Britton v. Wooten, 817 S.W.2d 443, 451–52 (Ky. 1991) (holding that the source of a spark that ignited a fire on a negligently collected pile of trash was not a superseding cause sufficient to excuse defendant of negligence liability); Morales v. City of New York, 521 N.E.2d 425, 426 (N.Y. 1988) (selling gasoline in milk cartons to a customer who later committed arson did not permit plaintiffs to recover from the gas station because it was not foreseeable that a technical violation concerning gasoline containers would lead to the harm that occurred). *But see* Edwards, *supra* note 57, at 48–49 (arguing that it would not be reasonably foreseeable that one computer owner's failure to secure her system would cause harm to another party).

476. Data regarding the "survival time" of unprotected computers strongly supports this point. de Guzman, *supra* note 68, at 550 (citing a four minute survival time for unprotected computers running Windows Vista).

477. *See* RESTATEMENT (SECOND) OF TORTS § 448 (1965) (stating that an intentional tort is a superseding cause "unless the actor at the time of his negligent conduct realized or should have realized the likelihood that such a situation might be created, and that a third person might avail himself of the opportunity to commit such a tort or crime").

rule for proximate cause would also have to follow the *Palsgraf* minority view concerning the duty of care for third-party intermediaries. And even in the unlikely event that a court finds both a duty and proximate cause, the defendant still has several potential defenses that reduce the overall likelihood of success for a given claim for negligence.

C. Defenses to Negligence Claims

When responding to allegations of negligence, a defendant has several options, including negating an element of the prima facie case for negligence,[478] arguing that the plaintiff assumed the risk, and claiming that the plaintiff's own negligence contributed to his injury.[479]

An assumption of risk argument may be an unattractive theory in the cyberattack context. Our view is that some courts might view it as unconscionable to assert that a party assumed the risk of a cyberattack by using modern conveniences — many of which are essential elements of everyday life.

But a non-attacker defendant might be able to successfully argue that the injured party's own negligence contributed to his injury. Even if the court agrees that the plaintiff's injuries were in part due to his own negligence, the effect of that determination on the outcome of the case will depend on the jurisdiction. In a contributory negligence jurisdiction, any negligence on the plaintiff's part acts as a complete bar to recovery.[480] However, pure contributory negligence jurisdictions are rare.[481] In contrast, in most comparative negligence jurisdictions the plaintiff's negligence is not a complete bar to recovery. Instead, its effect will depend on the relative fault of the parties.[482]

3. Presidential Authority

Another avenue to address cyberattacks is to interpret the President's authority as including the power to order action — either to execute cyberattacks or to defend against them. In the absence of an effective legal regime, does the President possess the power to take action concerning cyberattacks?

---

478. *See* Part IV.A.2.B.

479. TWERSKI & HENDERSON, *supra* note 445, at 405.

480. *See, e.g.*, Baltimore & Potomac R.R. v. Jones, 95 U.S. 439, 442 (1877).

481. Carol A. Mutter, *Moving to Comparative Negligence in an Era of Tort Reform: Decisions for Tennessee*, 57 TENN. L. REV. 199, 230 (1990) (noting that only six states at that time still followed a pure contributory negligence rule where any negligence on the part of the plaintiff precluded recovery).

482. TWERSKI & HENDERSON, *supra* note 445, at 412 (noting that thirty-three states, representing a strong majority, have modified forms of comparative fault where if a plaintiff's degree of fault reaches fifty or fifty-one percent, the plaintiff is barred from recovery).

Article II of the Constitution discusses the executive powers of the President.[483] Congress has explicitly set out the authority of the President over certain sectors during times of crisis, such as in section 606 of the Communications Act. Section 606(a) provides for presidential authority to prioritize communications that are viewed as essential to national defense and security.[484] Section 606(d) provides the President with authority to suspend rules applicable to wire communications, to shut down wire communication facilities, or to place the government in control of communications facilities and equipment — provided just compensation is provided to the facility owners — when there "exists a state or threat of war."[485] Sections 1701 and 1702 of Title 50 of the U.S. Code also set forth presidential authority to take control of activities involving transactions with foreign countries when a national emergency has been declared to address an "unusual and extraordinary threat" that in substantial part arises from outside the United States.[486] Commentators have discussed giving the President the authority to shut down networks in cases of emergency, but some have noted that this would be risky and would not necessarily address a demonstrable need.[487] Under certain circumstances, the President can also utilize his authority as Commander-in-Chief to order limited military action without advance congressional approval under the War Powers Resolution of 1973.[488] Short of formal administrative action, martial law or military action, does the President have binding authority to order private parties to take specific action? We assert that presidential authority would likely be limited to the national security context and could likely not be used to impose standards on software manufacturers or individual computer owners. However,

---

483. U.S. CONST. art. II.

484. *See* 47 U.S.C. § 606(a) (2006).

485. *Id.* § 606(d); *see also* Brenner with Clarke, *supra* note 143, at 1044–46 (noting that it is unclear whether section 606's use of the term "war" in the early twentieth century could be extended to the concept of cyberwarfare in the early twenty-first century). Because of the cultural importance of the Internet, however, Opderbeck strongly argues against giving the President broad authority to shut down the Internet in the event of an emergency. Opderbeck, *supra* note 204, at 39–40. Brenner and Clarke evaluated the possibility of nationalizing telecommunications networks to address potential cyberwar issues. Brenner with Clarke, *supra* note 143, at 1046–48. Black's Law Dictionary defines nationalization as the "act of bringing an industry under governmental control or ownership." BLACK'S LAW DICTIONARY 1129 (9th ed. 2009). When the government nationalizes an industry, the industry still executes all of its traditional activities, but may do so more efficiently or effectively. *See* Brenner with Clarke, *supra* note 143, at 1047.

486. 50 U.S.C. §§ 1701–02 (2006 & Supp. IV 2011), *amended by* Continuing Appropriations Act, Pub. L. 112-33, 125 Stat 363 (2011), Continuing Appropriations Act, Pub. L. 112-36, 125 Stat 386 (2011) and Consolidated Appropriations Act, Pub. L. 112-74, 125 Stat 786 (2011).

487. Nojeim, *supra* note 139, at 133–34. Nojeim is also critical of the idea of making the NSA responsible for securing civilian systems because of public distrust of the NSA. *See id.* at 136.

488. *See* 50 U.S.C. §§ 1541–48 (2006).

due to the importance of CNI to the public, there could potentially be some authority to require providers of CNI to better secure their technology.

Some have argued that the President possesses inherent authority to take certain actions as Commander-in-Chief. In *Youngstown Sheet & Tube Co. v. Sawyer*,[489] the Supreme Court evaluated whether President Truman could seize steel mills to prevent a strike from interrupting manufacturing during a time of conflict absent a formal declaration of war.[490] While a majority of Justices agreed that such a seizure went beyond the scope of the executive power under the Constitution,[491] the Justices viewed the case in many different ways, resulting in five solo concurrences.[492] The majority opinion viewed the seizure as analogous to legislating, which is the exclusive providence of Congress and not the President.[493] Justice Black, a strict textualist, did not read the Constitution as allowing any inherent presidential powers.[494] Justice Frankfurter, on the other hand, suggested that the President may have limited inherent powers,[495] while Justice Jackson's concurring opinion provided a more helpful test for evaluating whether a President has authority to act.[496] Under Justice Jackson's test, there are three different situations in which the President may exercise his powers. The President has the most authority when Congress approves the President's action, the least authority when his acts go against the express or implied will of Congress, and intermediate authority when Congress has said nothing for or against the President's actions.[497]

A. Applying Justice Jackson's Test from Youngstown

If we assume that the President's authority as the Commander-in-Chief and as the head of the Executive Branch includes inherent powers, we can apply Justice Jackson's test in *Youngstown* to evaluate whether the President has the authority to require private actors, especially owners of CNI, to implement stronger cybersecurity measures.

---

489. 343 U.S. 579 (1952).

490. *Id.* at 582–85.

491. *Id.* at 587.

492. *See* Edward T. Swaine, *The Political Economy of* Youngstown, 83 S. CAL. L. REV. 263, 264–65 (2010) (noting that it was somewhat unexpected for Jackson's concurrence to become the most famous part of *Youngstown*, since it was one of five solo concurrences in a case with a six-person majority).

493. *Youngstown*, 343 U.S. at 588.

494. *Id.* at 587 ("The Constitution limits [the President's] functions in the lawmaking process to the recommending of laws he thinks wise and the vetoing of laws he thinks bad.").

495. *See id.* at 610–11 (Frankfurter, J., concurring).

496. *See id.* at 635–38 (Jackson, J., concurring).

497. *Id.*; Swaine, *supra* note 492, at 266.

Is cybersecurity an area where Congress has expressly supported the use of presidential authority? Under § 606(d) of the Communications Act, the President may have the authority to take control of communications providers and require additional security if there is a "threat of war" — a phrase that is not defined[498] — but does not appear to have explicit correlating authority over other CNI such as power and water companies. The wording of § 606(d), however, is potentially broad enough to permit the President to exercise substantial control over the cybersecurity of CNI providers, since it authorizes government control over wire communications facilities and equipment when a state or threat of war exists.[499]

There may be an argument that in enacting § 606(d), Congress intended for the President to have control over critical communications infrastructure in times of crisis, and that this intent would extend to control over the elements of non-communications CNI that are not severable from critical communications infrastructure. Insofar as power companies utilize the Internet to render services, § 606(d) might permit the President to exert some level of control over the methods through which these power companies are connected by wired communications technology to the outside world. Therefore there does not appear to be explicit statutory authorization for Presidential authority over CNI other than communications during a state of war or a threat of war. There may, however, be implied authorization, though further analysis of the legislative history would be beneficial in evaluating whether such implied authorization exists.

The more important question in determining the scope of any such power is whether the exercise of presidential authority would be counter to the express or implied will of Congress. Looking at the context of various statutes, we can begin to infer the conditions under which Congress may approve the use of presidential authority to unilaterally impose requirements on private operators of CNI. Under § 143 of Title 6, DHS may provide cybersecurity assistance to private operators of CNI "upon request."[500] This focus on voluntary election suggests that Congress would not approve of the Executive Branch interfering with the private entities controlling CNI as a matter of everyday affairs. However, § 606(d) of the Communications Act suggests that Congress would approve of this exercise of presidential authority when the country was under a state or threat of war.[501] Additionally, §§ 1701 and 1702 of Title 50 suggest that Congress would approve of the exercise of presidential authority over transactions with foreign nations when the exercise relates to a present declared national emer-

498. 47 U.S.C. § 606(d) (2006).
499. *See id.*
500. 6 U.S.C. § 143 (2006 & Supp. IV 2011).
501. 47 U.S.C. § 606(d).

gency.[502] It is also not clear whether Congress's use of the term "war" should be interpreted as including cyberconflicts or only kinetic war, though the NDAA's reference to applying the laws of war to cyberconflicts suggests that perhaps the term "war" should cover cyberconflicts.[503]

After looking at other statutes, we conclude from our analysis that while there is not explicit support for the exercise of presidential authority in this context, it would not necessarily be counter to Congressional will. However, presidential authority to impose cybersecurity requirements on private entities may be limited to cases of armed conflict or declared national emergency.

Further analysis would be beneficial to evaluate whether Congress intended to give the President authority over measures taken to secure wired communications equipment in areas of CNI. Even if that intent is unclear, it would not be in opposition to congressional will for the President to exercise authority in situations of conflict or declared national emergency. Thus, under Justice Jackson's framework, as long as Congress continues to remain neutral on the topic, the President can exercise authority in the interest of protecting national security.

To summarize, the authority of the President to compel action by private citizens to address cybersecurity concerns is likely limited to situations where a crisis has already arisen. This is not ideal, which is why we advocate for the creation of policy to address these issues prospectively instead of retrospectively. However, if an effective regime is not in place at the time that a cybersecurity crisis arises, the President's authority to intervene could be used to ensure that the crisis is handled promptly.

B. Voluntary Cooperation

An alternative model of presidential authority focuses on the voluntary cooperation of private citizens. For this we look at the wiretapping controversy that began under President Bush. In evaluating the actions of the National Security Agency ("NSA"), the DOJ found that the wiretapping was consistent with the authority of the President under the Constitution.[504] The DOJ concluded that the President has the authority to conduct activities that are critical to national security.[505]

---

502. 50 U.S.C. §§ 1701–02 (2006 & Supp. IV 2011), *amended by* Continuing Appropriations Act, Pub. L. 112-33, 125 Stat 363 (2011), Continuing Appropriations Act, Pub. L. 112-36, 125 Stat 386 (2011) and Consolidated Appropriations Act, Pub. L. 112-74, 125 Stat 786 (2011).

503. *See infra* Part IV.A.3.C.

504. U.S. DEP'T OF JUSTICE, LEGAL AUTHORITIES SUPPORTING THE ACTIVITIES OF THE NATIONAL SECURITY AGENCY DESCRIBED BY THE PRESIDENT 1 (2006), *available at* http://www.justice.gov/opa/whitepaperonnsalegalauthorities.pdf ("The President has the

It should be noted, however, that the telecommunications companies that cooperated with the NSA's wiretapping efforts did so voluntarily, not under legal compulsion.[506] In contrast to the above discussion, where we concluded that the President may have the authority to compel action in times of crisis, a model based on the wiretapping analogy would depend on voluntary cooperation.[507]

In this situation, the important question is what incentives might encourage voluntary participation. Regardless of one's position on whether the wiretapping violated FISA, the presence of voluntary compliance on the part of major telecommunications players like AT&T suggests that incentives can be effective.[508] Some companies include in their terms of service a reference to their intention to cooperate with authorities in the interest of public welfare.[509] Even though the wiretapping controversy arguably does not provide a formal model for voluntary participation, it establishes that securing voluntary industry cooperation in a controversial area is not without precedent.

In the wiretapping controversy, telecommunications companies had to balance a sense of patriotic obligation against the potential for liability. If they acted at the behest of government organizations, they became state actors and were complicit in any violations of the Fourth Amendment from the government's use of private data.[510] People opposed to the wiretaps praised Qwest for its refusal to cooperate with

---

chief responsibility under the Constitution to protect America from attack, and the Constitution gives the President the authority necessary to fulfill that solemn responsibility.").

505. *Id.* at 5.

506. This is not to say the government did not pressure providers to comply with its requests. Qwest, a major telecommunications provider that refused the NSA's requests, was reportedly pressured by suggestions that Qwest might lose out on future classified contracts or that its failure to cooperate could endanger national security. *See* Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls*, USA TODAY (May 11, 2006), http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm.

507. This Article does not take a position on the wiretapping controversy. We are invoking the wiretapping controversy only as an illustration of an administrative agency obtaining voluntary compliance from the private sector in the interest of taking actions viewed by the agency as being in the interest of national security.

508. After the wiretapping controversy became big news, AT&T revised its privacy policy to make explicit AT&T's intent to use confidential user information "to protect its legitimate business interests, safeguard others, or respond to legal process." David Lazarus, *AT&T Rewrites Rules: Your Data Isn't Yours*, S.F. CHRON. (June 21, 2006), http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2006/06/21/BUG9VJHB9C1.DTL&ao=all (citations and internal quotation marks omitted).

509. *See, e.g.*, *id.*; *Privacy Statement*, MID CENTURY TELECOM, http://www.midcentury.com/html/privacy_statement.html (last revised Dec. 9, 2010) ("[W]e have an obligation to assist law enforcement and other government agencies responsible for protecting the public welfare, whether it be an individual or the security interests of the entire nation."); *Terms of Use*, PINGMOBILE, http://www.pingmobile.com/terms_of_use (last visited May 3, 2012).

510. The issue of company liability for wiretapping was largely resolved by Congress in 2008 when companies were granted statutory immunity for complying with NSA requests. *See* Eric Lichtblau, *Senate Approves Bill to Broaden Wiretap Powers*, N.Y. TIMES, July 10, 2008, at A1.

NSA wiretapping requests, and other companies denied that they had participated — even though other sources indicated that they had.[511] Private companies have a greater incentive to cooperate with passive cybersecurity requests than with wiretapping requests, because cybersecurity requests are not likely to impact customer privacy and thus would generate less pushback from customers. Comparing cybersecurity standards with FISA surveillance is like comparing a store that installs stronger locks with a store that hires a security guard to follow customers and record their conversations.

Companies often include language in their privacy policies stating that they may disclose confidential information to the government when the government makes requests in accordance with the law.[512] While companies would not have cooperated with wiretapping requests that they viewed as contrary to FISA, these privacy policies suggest that many companies would be quick to cooperate with legal government requests to enhance cybersecurity measures. As long as the government only requests companies to implement passive defense standards, it is doubtful that these companies would oppose such requests. However, if the President requested CNI providers to implement active defense mechanisms — such as installing software to enable mitigative counterstrikes — these mechanisms would require more careful oversight. Potential liability issues could arise if a mitigative counterstrike harms an innocent party. If a mitigative counterstrike hit targets located in foreign countries, a company could be drawn into complicated international law conflicts.

We thus conclude that the executive branch could request voluntary compliance with passive cybersecurity standards. However, the risk of zero-day vulnerabilities means that this type of voluntary compliance may not be effective in the absence of mitigative counterstriking. Private owners of CNI are much less likely to voluntarily implement capabilities to actively mitigate harm in the absence of a legal regime that minimizes their liability. A CNI provider that accepts a role as a state actor for the purpose of conducting mitigative counterstrikes would also run the risk of becoming a combatant — and thus a legitimate target for military strikes — under international law.[513] It is important to have a reliable legal framework to permit mitigative counterstrikes in order to protect CNI; this is one of the most important reasons that we argue in favor of implementing a new legal regime to regulate active defense.

---

511. *See* Jim Zarroli, *Phone Companies Distance Themselves from NSA*, NPR (May 16, 2006), http://www.npr.org/templates/story/story.php?storyId=5409137.

512. For example, Twitter includes a provision in its privacy policy stating that it may disclose its users' information "to comply with a law, regulation or legal request." *Twitter Privacy Policy*, TWITTER (effective June 23, 2011), http://twitter.com/privacy.

513. *See* Graham, *supra* note 253, at 97 (discussing whether parties who initiate active defense measures must be viewed as lawful combatants according to the law of war).

C. National Defense Authorization Act

In late 2011, the NDAA[514] emerged from Congress amid considerable controversy stemming from what many in the media termed the "indefinite detention" provision.[515] However, the NDAA also contained provisions addressing cybersecurity and the President's authority, which largely went unnoticed by the public. Section 953 addresses strategies to acquire more advanced detection capabilities, and provides in part:

> The Secretary of Defense shall develop and implement a plan to augment the cybersecurity strategy of the Department of Defense through the acquisition of advanced capabilities to discover and isolate penetrations and attacks that were previously unknown and for which signatures have not been developed for incorporation into computer intrusion detection and prevention systems and anti-virus software systems.[516]

Section 953 indicates that Congress has recognized the need to actively pursue improvements in passive defense and in some of the core technologies discussed in our active defense model.

Additionally, Congress used § 954 to clear up several questions about the President's authority, rules governing cyberattacks, and the role of the DOD. In a very short section, Congress stated that the President has the authority to direct the DOD to "conduct offensive operations in cyberspace to defend our Nation, Allies and interests," while applying the same rules that govern kinetic capabilities, and subject to the limitations placed on the President by the War Powers Resolution.[517] In § 954, Congress recognized the importance of cyberspace to future international conflicts and the need to codify rules in advance. The question of Congress's position on the President's authority to direct formal cyberwarfare activities is thus partly answered by § 954 of the NDAA. Given § 954's reference to offensive cyber operations undertaken in defense, it is likely that Congress would approve

514. National Defense Authorization Act for Fiscal Year 2012, Pub. L. No. 112-81, § 1021, 125 Stat. 1298 (2011).

515. *See, e.g.*, *Montanans Launch Recall of State's Congressional Delegation Over Votes on NDAA, Indefinite Detention*, HUFFINGTON POST (Dec. 27, 2011), http://www.huffingtonpost.com/2011/12/27/montana-recall-ndaa-indefinite-detention_n_1171044.html; Hans Nichols & Roger Runningen, *Obama Signs Defense Spending Law, with Interpretations*, BLOOMBERG (Jan. 2, 2012, 4:44 PM), http://www.bloomberg.com/news/2011-12-31/obama-signs-defense-authorization-law-with-own-interpretations-on-custody.html.

516. National Defense Authorization Act for Fiscal Year 2012 § 953(a).

517. *Id.* § 954.

military use of active defense as described in this Article. However, these provisions address only the President's authority to order the DOD to use cyber capabilities in a formal military context, leaving unanswered the issue of possible federal involvement in protecting privately held CNI.

Congress has now explicitly spoken on the President's authority to direct military cyber activities, but has not yet addressed the President's authority to exercise control over cybersecurity matters in the private sector outside of the context of national emergencies and wartime. Therefore, under Justice Jackson's test in *Youngstown*, the President may have intermediate authority on matters involving cybersecurity and the private sector, though we argue that setting out guidelines in advance of a crisis would be preferable to ad hoc presidential management of individual issues as they arise.

B. International Law

This Part will examine the implications of international law for cybersecurity issues. This Article generally does not discuss how foreign nations address their domestic cybersecurity issues, though we do note that there are many different approaches.[518] We are instead focused on the current difficulties of addressing cyberattacks within our borders. However, addressing cyberattacks where the victims are within the United States may nonetheless implicate international law. This Part will provide background on the complicated issues associated with cyberattacks under international law in order to underscore the importance of a unified international framework. Because there is significant uncertainty over how to address cyberattacks under international law, potential attackers are unlikely to be deterred by the threat of criminal charges in other countries or by war crimes charges. Thus an alternative regime to permit mitigative counterstriking is necessary.

The issue of whether a cyberattack violates U.S. law is of questionable relevance when the attacker is located outside the jurisdiction of U.S. criminal courts. If authorities can specifically identify an attacker, one option is to extradite the offender to the United States to try him for his crimes; another option is to alert the host nation and rely on that nation to pursue criminal sanctions against the attacker.[519]

Both options require authorities to attribute the attack to a specific party. Attribution of cyberattacks is important in the international law

518. "Japanese law, for example, does not criminalize unauthorized access to a computer unless the intruder has circumvented a security measure." Downing, *supra* note 95, at 722. Some have argued that the United Kingdom's Computer Misuse Act of 1990 could be interpreted as criminalizing DDoS attacks. *See, e.g.*, Edwards, *supra* note 57, at 36.

519. *But see* Sklerov, *supra* note 25, at 7 (noting that several major nation-states refuse to extradite or prosecute cyber criminals within their borders).

context in part because different laws will govern if a state actor conducted the attack.[520] In the cases of the attacks on Estonia, Georgia, and the United States, members of the attacked governments suspected that foreign governments had sponsored the attacks but no responsibility could be established.[521] If the attack is attributed to a non-state actor and the host nation agrees to pursue criminal sanctions, some nations may punish the attacker differently depending on the identity of the victim, perhaps by increasing sanctions for attacking a more sensitive system.[522] Some areas of international law also address the investigative abilities of law enforcement, such as the Schengen Agreement of the European Union, which permits law enforcement officials to pursue suspects into another state, provided they cease their pursuit upon the other state's request.[523]

If a cyberattack is attributed to a state actor, this could lead to cyberwarfare, either as a substitute for or precursor to kinetic warfare.[524] It is not completely clear what international framework should apply to cyberwarfare, but there are many potential authorities to guide behavior in the cyber context. Two sources of international obligations are treaties — such as the U.N. Charter, the Hague Convention, and the Geneva Convention — and customary international law ("CIL").[525] Additionally, the International Telecommunication Convention prohibits parties from harmfully interfering with telecommunications,[526] and the Agreement on the Prevention of Dangerous Military Activities prohibits harmful interference with the command and control systems of military opponents.[527] Many commentators argue that cyberattacks should be judged according to the law of armed conflict ("LOAC") and the U.N. Charter.[528]

---

520. *See* Condron, *supra* note 10, at 414–15.

521. *See* Sklerov, *supra* note 25, at 8.

522. *See* Downing, *supra* note 95, at 741.

523. Convention Implementing the Schengen Agreement art. 41, June 14, 1985, 2000 O.J. (L 239) 19, 30.

524. Schaap, *supra* note 10, at 172. Schaap refers to the danger of cyberwarfare operations escalating "into a full blown armed conflict." *Id.* However, the term "armed conflict" has a low threshold under international law, and we disagree with Schaap's implication that cyberwarfare operations automatically fall short of "armed conflict" simply because they are not kinetic attacks. *See supra* Part IV.B.1.

525. *See* NRC REPORT, *supra* note 4, at 241. The U.N. Charter limits the ability of a nation to resort to war. *See* U.N. Charter art. 2, para. 4 (prohibiting use of force or threat of force); Jensen, *supra* note 19, at 215.

526. International Telecommunication Convention, art. 35, Oct. 25, 1973, 28 U.S.T. 2495, 1209 U.N.T.S. 255; Hoisington, *supra* note 36, at 445; Schaap, *supra* note 10, at 164–65. Schaap notes that cyberwarfare operations that involve transmitting deceptive identification signals would be unlawful under Article 37 of the International Telecommunication Convention. *Id.* at 165.

527. Union of Soviet Socialist Republics-United States: Agreement on the Prevention of Dangerous Military Activities, U.S.-U.S.S.R., June 12, 1989, 28 I.L.M. 877; Hoisington, *supra* note 36, at 445.

528. *See* NRC REPORT, *supra* note 4, at 21–22; Condron, *supra* note 10, at 413; Lin, *supra* note 43, at 73. *But see* NRC REPORT, *supra* note 4, at 358; *id.* at 32 (noting LOAC and

Even if the national government is not directing a cyberattack, the government may be held responsible for the acts of a third party within its borders.[529] In *Corfu Channel*, the International Court of Justice ("ICJ") held that a state has an "obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States"[530]; this holding was later reaffirmed in *Tehran*.[531] Under international law, a state will be held responsible by the ICJ for the acts of a third party — such as a terrorist organization — if it has at least "indirect responsibility" over the actor and if the state refuses to stop sheltering the actor after another state asks it do so.[532]

Duties owed by a nation under CIL may include passing stringent laws criminalizing certain conduct, investigating crimes vigorously, prosecuting the attackers, and cooperating with the victim state during the investigation.[533] There are also international law cases supporting the existence of an affirmative duty on the part of states to prevent attacks on other states.[534] Whether these cases apply to cyberattacks as well as kinetic attacks, however, is an open question.

1. The Law of War and the U.N. Charter

There are two parts to the law of war: *jus ad bellum*, which is the law of conflict management, and *jus in bello*, which is the law of armed conflict.[535] *Jus ad bellum* is the body of law that applies prior

---

the U.N. Charter "fail to account for non-state actors and for the technical characteristics of some cyberattacks"); Brenner with Clarke, *supra* note 143, at 1031 (arguing that the U.N. Charter and LOAC "probably do not apply" to cyberattacks).

529. *See* NRC REPORT, *supra* note 4, at 273; Todd, *supra* note 28, at 89 ("The unique attributes of cyberspace, such as its speed and lack of physical borders, are key reasons why host states must be responsible for actions within their territory when they do not take reasonable measures to stop the attack and warn the victim state.").

530. Corfu Channel (U.K v. Alb.), 1949 I.C.J. 4, 22 (Apr. 9) (finding Albanian government responsible for minefields located in Albanian territory because it must have had knowledge of the minefields even though it did not place them in the Corfu Channel).

531. United States Diplomatic and Consular Staff in Tehran (U.S. v. Iran), 1980 I.C.J. 3, 32–33, 44 (May 24) (holding that Iran did not take necessary steps to protect the U.S. Embassy from non-state actors).

532. Sklerov, *supra* note 25, at 44–46; *see* S.C. Res. 1373, ¶ 2(a), U.N. SCOR, 4385th mtg., U.N. Doc. S/RES/1373, at 2 (Sept. 28, 2001) (prohibiting states from providing active or passive support to terrorists); *see also* Vincent-Joël Proulx, *Babysitting Terrorists: Should States Be Strictly Liable for Failing to Prevent Transborder Attacks?*, 23 BERKELEY J. INT'L L. 615, 638 (2005).

533. *See* Sklerov, *supra* note 25, at 62. Sklerov asserts that the concept of CIL is actually made up of three different categories: "international conventions, international custom, and the general principles of law common to civilized nations." *Id.* at 63.

534. *See*, *e.g.*, *Corfu Channel*, 1949 I.C.J. at 22; *see also* Sklerov, *supra* note 25, at 70.

535. *See* Sean Kanuck, *Sovereign Discourse on Cyber Conflict Under International Law*, 88 TEX. L. REV. 1571, 1585 (2010); *see also* Schaap, *supra* note 10, at 149 (noting the general principles of the law of war); Sklerov, *supra* note 25, at 27. Some commentators, however, use the term "law of armed conflict" as a replacement for the term "law of war" and consider *jus ad bellum* and *jus in bello* to be aspects of the "law of armed conflict." *See, e.g.*, NRC REPORT, *supra* note 4, at 242. Since some argue that the formal declaration of war

to a conflict (such as Article 2(4) of the U.N. Charter, which prohibits uses of force),[536] while *jus in bello* governs behavior during a conflict (primarily governed by the Hague and Geneva Conventions and CIL).[537]

Some commentators have expressed concern that *jus ad bellum* does not provide adequate safeguards to address cyberattacks, in part due to the difficulties of attributing and characterizing cyberattacks.[538] Articles 2(4), 39, and 51 of the U.N. Charter are frequently cited in discussions of international law and cyberattacks.[539] Article 2(4) prohibits "the threat or use of force" against states in a "manner inconsistent with the Purposes of the United Nations."[540] There are only two exceptions to this absolute prohibition on the use of force: acts authorized by the Security Council and acts undertaken in self-defense.[541] Article 39 gives the U.N. Security Council the authority to (1) determine when there is a threat to or breach of the peace, or an act of aggression, and to (2) make recommendations to preserve international peace and security.[542] Under Article 51, members of the U.N. have the right to use self-defense in response to an "armed attack" against them, though the party utilizing self-defense must immediately notify the Security Council.[543] Article 42 permits the Security Council to use military force in order to restore peace when the conditions in Articles 39, 41, and 42 are met.[544]

Jus in bello is focused on the use of weapons. However, since there is currently no accepted definition for "weapon" under interna-

---

is an obsolete concept, with the focus now on armed conflict instead of on the declaration of war, referring to the body of law as the "law of armed conflict" may be more accurate. *See* Condron, *supra* note 10, at 417–18.

536. U.N. Charter art. 2, para. 4 ("All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."); *see also* NRC REPORT, *supra* note 4, at 242; Brenner with Clarke, *supra* note 143, at 1017; Sklerov, *supra* note 25, at 27.

537. *See* NRC REPORT, *supra* note 4, at 246; Brenner with Clarke, *supra* note 143, at 1017 (noting that *jus in bello* is especially concerned with protecting civilian populations); Sklerov, *supra* note 25, at 27.

538. *See, e.g.*, Condron, *supra* note 10, at 415 (suggesting that there should be a safe harbor for states that respond in good faith to a cyberattack without sufficient information to attribute or characterize the attack).

539. *See infra* Part IV.B.1.A (examining the importance of the U.N. Charter for understanding the concepts of use of force and armed attacks); *see also* Graham, *supra* note 253, at 88; Lin, *supra* note 43, at 71.

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

541. *See* Brenner with Clarke, *supra* note 143, at 1030; Graham, *supra* note 253, at 88; Sklerov, *supra* note 25, at 28–29.

542. U.N. Charter art. 39.

543. *Id.* art. 51; *see also* Hoisington, *supra* note 36, at 449.

544. U.N. Charter art. 39 (empowering the Security Council to determine the existence of a threat to the peace); *id.* art. 41 (listing non-military measures to restore peace and security); *id.* art. 42 (creating an obligation to attempt methods in Article 41 before using military force); *see also* Sklerov, *supra* note 25, at 29–30 (listing Article 42 as one of two exceptions to the prohibition against uses of force).

tional law, it is unclear whether the principle would apply to cyberweapons.[545] *Jus in bello* includes restrictions on targets, limiting targets to entities that directly contribute to the enemy's war effort and that would produce a military advantage if damaged or destroyed.[546] *Jus in bello* allows for direct attacks on combatants, but noncombatant civilians cannot be targeted unless they directly participate in the hostilities.[547] *Jus in bello* also requires that the attacks be proportionate to the military advantage gained,[548] and that actors adhere to the principle of military necessity and make reasonable efforts to distinguish between military and civilian assets and personnel in executing attacks.[549] It also prohibits acts of perfidy.[550] Another important aspect to *jus in bello* is the immunity from attacks enjoyed by neutral nations so long as they remain neutral, but neutrality may be complicated by

545. *See* Todd, *supra* note 28, at 79–80. Each branch of the U.S. military has its own definition of "weapon." *See id.* at 80. The U.S. Air Force defines "weapon" to specifically exclude "electronic warfare devices" and devices that "disable" property. *Id.* The U.S. Army and Navy both define "weapon" to include devices that disable property. *Id.* Todd proposes that "cyberspace weapon" should be defined as "any capabilities, device, or combination of capabilities and techniques which, if used for its intended purpose, is likely to impair the integrity or availability of data, a program, or information located on a computer or information processing system." *Id.* at 83.

546. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) art. 52(2), June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Geneva Protocol I]; *see also* NRC REPORT, *supra* note 4, at 246; Schaap, *supra* note 10, at 156. The NRC Report notes that under LOAC, there is a category of universally protected facilities that includes hospitals and religious institutions. NRC REPORT, *supra* note 4, at 246.

547. *See* Brenner with Clarke, *supra* note 143, at 1021; Schaap, *supra* note 10, at 155. Combatants are defined under Article 43(2) of the Geneva Convention as "[m]embers of the armed forces of a Party to a conflict" that "have the right to participate directly in hostilities." Geneva Protocol I, *supra* note 546, art. 43(2). The United States currently takes the position that there are three categories of people in a war: lawful combatants, unlawful combatants, and civilians. *See* Brenner with Clarke, *supra* note 143, at 1022.

548. *See* NRC REPORT, *supra* note 4, at 246–47; Schaap, *supra* note 10, at 150–51. Proportionality does not require that a counterstrike be proportional to the damage done to the original victim, just that the damage caused be proportional to the military advantage gained through the attack. *See* NRC REPORT, *supra* note 4, at 247. However, significant intelligence would be needed to predict possible collateral damage from a cyberattack, and it would be difficult to refute false claims of collateral damage from states asserting that a cyberattack was disproportionate and thus violated LOAC. *See id.* at 262–64.

549. *See* Schaap, *supra* note 10, at 149–50. Parties are encouraged to use weapons that discriminate between military and civilian assets, though there is no overt ban on the use of indiscriminate weapons. *See* NRC REPORT, *supra* note 4, at 249–50. It is unclear how the principle of distinction should apply in the context of cyberattacks against civilian-owned national infrastructure. *See id.* at 265.

550. *See* NRC REPORT, *supra* note 4, at 247 (defining perfidy as including some — but not all — categories of deception in wartime); Schaap, *supra* note 10, at 151. The rule against perfidy means that a combatant cannot use his enemy's adherence to LOAC against him. *See id.* at 152.

obscure national borders or threatened by private actors in neutral nations taking steps to help combatants.[551]

Many commentators assume that military doctrine on cyberattacks will adhere to the principles of *jus in bello*.[552] The U.S. military itself applies the standard principles of *jus in bello* to cyberattacks, taking the position that cyberattacks should meet the *jus in bello* requirements of military necessity, proportionality, and distinction.[553] However, applying the current international law regime to cyberattacks is difficult, because the language of the U.N. Charter traditionally has been applied to kinetic attacks.[554] Commentators disagree over whether and to what extent the phrases "uses of force" under Article 2(4) and "armed attacks" under Article 51 include cyberattacks.[555] No consensus has been reached, and so our analysis now turns to this issue.

A. What Is a Use of Force? What Is an Armed Attack?

The U.N. Charter contains two different terms referring to attacks: "use of force" under Article 2(4)[556] and "armed attack" under Article 51.[557] Some scholars have noted that it is unclear what a "use of force" is under Article 2(4).[558] Conventional weapon attacks definitely fall within the category of "use of force" in Article 2(4), and

---

551. *See* Schaap, *supra* note 10, at 153; *see also* Kastenberg, *Neutrality*, *supra* note 103, at 47 (examining the issue of U.S. neutrality in the Georgian conflict, during which U.S. information technology companies assisted the Georgian government).

552. *See, e.g.*, NRC REPORT, *supra* note 4, at 7 ("U.S. policy makers should apply the moral and ethical principles underlying the law of armed conflict to cyberattack even in situations that fall short of actual armed conflict."); Young, *supra* note 136, at 195.

553. *See* NRC REPORT, *supra* note 4, at 34.

554. *Compare* Brenner with Clarke, *supra* note 143, at 1031 (asserting that the U.N. Charter would not apply to cyberattacks), *with* NRC REPORT, *supra* note 4, at 251 (concluding that *jus ad bellum* and *jus in bello* would still apply to cyberattacks, especially when the effects are similar to those of a kinetic attack), *and* Lin, *supra* note 43, at 73 (arguing that a cyberattack that causes property damage should be treated as a use of force).

555. *See, e.g.*, Brenner with Clarke, *supra* note 143, at 1031 (doubting the applicability of the U.N. Charter to cyberattacks); Franzese, *supra* note 104, at 5 (discussing questions that arise regarding whether a cyberattack is a use of force in different scenarios); Lin, *supra* note 43, at 73 (describing when a cyberattack may be a use of force under the U.N. Charter).

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

557. U.N. Charter art. 51. We argue that the use of this language indicates that a "use of force" describes something less than an "armed attack." Thus, it is possible for a state to be the victim of an attack that constitutes a "use of force" in violation of Article 2(4), even though the attack is not severe enough to be an "armed attack" to which the victim can respond in self-defense under Article 51.

558. *See, e.g.*, Hoisington, *supra* note 36, at 440; Lin, *supra* note 43, at 71–72 (noting precedent that espionage, economic sanctions, and political coercion are not considered uses of force). Lin notes that although espionage is not a use of force, and cyber exploitations are sometimes compared with espionage, some cyber exploitations may be viewed as sufficiently hostile to violate the U.N. Charter. *Id.* at 84. Lin also notes the distinction between the treatment of economic sanctions, which are not considered uses of force, and economic blockages, which are. *Id.* at 80.

many commentators argue that cyberattacks that are intended to cause physical damage or injury can be categorized as uses of force.[559] For the most part, however, the international community is conflicted on whether cyberattacks are weapons, uses of force, or acts of armed conflict.[560]

Though the articles of the U.N. Charter do not contain clear definitions of "armed attack" and "use of force," there are additional documents that provide guidance on how these terms should be understood. As discussed below, our analysis leads us to conclude that "use of force" is better understood as a broad category that encompasses a range of aggressive actions, from less destructive to more destructive, with "armed attacks" being a stronger or more destructive subcategory of "use of force." The use of related terms, including "armed conflict" and "acts of aggression," in other areas of international law supports this conclusion.

According to the official commentary accompanying Common Article 2 of the Geneva Conventions, "de facto hostilities" are sufficient to find an "armed conflict," which makes clear that the Conventions intended the term "armed conflict" to have a low threshold.[561] The U.N. General Assembly's "Definition of Aggression" provides examples of state actions that qualify as acts of aggression.[562] That resolution also defines aggression as the "use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations . . . ."[563]

Graham points to the Definition of Aggression as providing guidance on defining an "armed attack" under international law, though the Definition of Aggression primarily refers to "armed forces" and aggression.[564] Helpfully, though, the Definition of Aggression refers to "acts of aggression *and other uses of force* contrary to the Charter of the United Nations,"[565] indicating that not all uses of force are acts of aggression, but that all acts of aggression are uses of force. Additionally, Article 39 of the U.N. Charter refers to the Security Coun-

559. *See, e.g.*, Hoisington, *supra* note 36, at 447.

560. *See* Schaap, *supra* note 10, at 124. Whether cyberweapons are considered weapons under international law, however, may be largely irrelevant, as the International Court of Justice has ruled that Articles 2(4) and 51 of the U.N. Charter apply to all uses of force, regardless of the weapons utilized. *See* Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, 244 (July 8).

561. Commentary for Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea (Second Geneva Convention) art. 2, para. 1, Aug. 12, 1949, 6 U.S.T. 3217, 75 U.N.T.S. 85 ("The occurrence of de facto hostilities is sufficient."); *see also* Todd, *supra* note 28, at 73.

562. Definition of Aggression, G.A. Res. 3314 (XXIX), Annex, U.N. Doc. A/3314 (Dec. 14, 1974); Graham, *supra* note 253, at 90; Todd, *supra* note 28, at 75–76.

563. G.A. Res. 3314, *supra* note 562; Todd, *supra* note 28, at 75–76.

564. Graham, *supra* note 253, at 90.

565. G.A. Res. 3314, *supra* note 562 (emphasis added).

cil's authority to determine the existence of an "act of aggression" and respond accordingly.[566]

Taken together, these provisions suggest that (1) "use of force" under the U.N. Charter is akin to "armed conflict" under the Geneva Conventions, and (2) "armed attack" under Article 51 of the U.N. Charter should be read as akin to an "act of aggression" under the Definition of Aggression resolution, with "armed attacks" viewed as aggravated "uses of force." The lowest threshold would thus be "uses of force," with "armed attacks" requiring a higher showing. The analysis then turns to when a "use of force" is severe enough to be an "armed attack."

When evaluating whether an attack that is a "use of force" rises to the level of an "armed attack," one method is to use Pictet's test, which considers the scope, duration, and intensity of the attack.[567] There are three recent models applying Pictet's test in the cybercrime context. Instrument-based models look at whether the damage caused was of the kind that previously would have required a kinetic attack, such as shutting down a power grid.[568] Effects-based models focus on the overall effect on the victim state, such as whether an information attack on financial institutions causes significant damage to the state's economic well-being.[569] Finally, a strict liability model would consider any cyberattack directed at CNI an armed attack.[570] One of the most well-received effects-based models is Schmitt's, which considers six elements to determine whether a cyberattack is a use of force under international law: severity, immediacy, directness, invasiveness, measurability, and presumptive legitimacy.[571] Another option for determining whether an action is a "use of force" or an "armed attack" considers (1) whether the cyberweapon was used "against the property or persons of a state" and (2) "whether a foreign state knowingly al-

566. U.N. Charter art. 39.

567. *See* Graham, *supra* note 253, at 90; Sklerov, *supra* note 25, at 51–52. Jean Pictet was a Swiss jurist and the General Editor for the official commentary on the Geneva Conventions of 12 August 1949. *The Geneva Conventions of 12 August 1949: Commentary*, THE LIBRARY OF CONGRESS (July 16, 2010), http://www.loc.gov/rr/frd/Military_Law/Geneva_conventions-1949.html.

568. *See* Graham, *supra* note 253, at 91; Sklerov, *supra* note 25, at 54 & n.343.

569. *See* Graham, *supra* note 253, at 91; Sklerov, *supra* note 25, at 54–55; *see also* NRC REPORT, *supra* note 4, at 21, 252 (noting that the effects-based model focuses on "whether a cyberattack *with a specified effect* constitutes a 'use of force'").

570. *See* Graham, *supra* note 253, at 91; Sklerov, *supra* note 25, at 55. Strict liability, however, may not be a good approach due to the danger of escalation. *See* Sklerov, *supra* note 25, at 58.

571. 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); *see also* Sklerov, *supra* note 25, at 56–58 ("Of all the scholars who advocate effects-based models, Michael N. Schmitt has advanced the most useful analytical framework for evaluating cyberattacks.").

low[ed] an entity under its legal control to use the cyber[]weapon against the victim."[572]

One of the first concerns raised about the terms "use of force" and "armed attack" is that an attack on a computer or network instead of a traditional target may or may not meet the threshold for either term.[573] Some have also argued that even if a cyberattack could be an "armed attack," it may be difficult to argue that a cyberattack undertaken in anticipation of another cyberattack is self-defense.[574] The effects-based model for cyberattacks would appear to require an attack to be conducted before the effects can be evaluated to determine whether the cyberattack violates the U.N. Charter. We view this potential reliance on an ad hoc determination after harm has already occurred as a major weakness for current approaches to cyberattacks under international law.

Another difficulty of trying to regulate cyberattacks is that cyberattack capabilities could potentially become widely available to non-state actors, such as terrorist organizations that have no intention to adhere to any agreements between nations. This might in turn reduce the willingness of states to adhere to the U.N. Charter.[575] Graham suggests that responsibility for cyberterrorist attacks might be imputed to their host state when a cyberattack rises to the level of an "armed attack."[576] However, this is not a guaranteed solution either, since imputing responsibility for cyberattacks is often impossible. With these considerations in mind, we now turn to an examination of the only formal criminal model to address international cyberattacks: the European Convention on Cybercrime ("ECC").[577]

2. European Convention on Cybercrime

The ECC is currently the only international treaty that addresses cybercrime concerns,[578] and it stresses the need to address cyberat-

572. Todd, *supra* note 28, at 93–94.

573. *See* NRC REPORT, *supra* note 4, at 251. The NRC Report asserts that cyberattacks do not automatically fall short of being "armed attacks" or "uses of force" and that *jus ad bellum* and *jus in bello* apply to cyberattacks. *Id.* Davis Brown has proposed extending LOAC to explicitly take into account the use of information systems. Davis Brown, *A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict*, 47 HARV. INT'L L.J. 179, 183 (2006) ("The emergence of cyberspace as a theater of operations has far-reaching repercussions for the law of armed conflict.").

574. *See, e.g.*, Jensen, *supra* note 19, at 223; Sklerov, *supra* note 25, at 76–77.

575. *See* NRC REPORT, *supra* note 4, at 325; Jason Barkham, *Information Warfare and International Law on the Use of Force*, 34 N.Y.U. J. INT'L L. & POL. 57, 104 (2001).

576. Graham, *supra* note 253, at 93 (noting that acts of non-state actors, such as terrorists, can rise to the level of armed attacks).

577. Convention on Cybercrime, *opened for signature* Nov. 23, 2001, E.T.S. No. 185, *available at* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm [hereinafter ECC].

578. *See* NRC REPORT, *supra* note 4, at 62; Sklerov, *supra* note 25, at 63–64. Sklerov suggests that the presence of other international treaties that criminalize terrorism provides indirect support for a duty to prevent cyberattacks. Sklerov, *supra* note 25, at 64.

tacks through law enforcement and state cooperation.[579] It directs signatories to adopt criminal laws against unauthorized access and interference with data and computer systems.[580] The ECC also contains provisions recommending procedures and safeguards for signatories to adopt in their domestic law, and several articles mandating international cooperation between signatories.[581]

The ECC aims to create consistency in criminal laws that relate to activities on the Internet,[582] but it does not explicitly define "cyberweapons," instead identifying *activities* that should be criminalized.[583] It also creates a framework for cooperation between nations conducting investigations.[584] The ECC establishes minimum standards that signatories should adopt and apply as cybercrime statutes, calling on signatories to prohibit illegal access, illegal interception of non-public transmissions, data interference, system interference, and misuse of devices.[585] It separately addresses two types of damage: (1) damage to data and (2) damage to computer functioning.[586] The ECC requires criminalization of computer offenses committed within the nation's jurisdiction and requires signatory nations to have the necessary jurisdiction to prosecute an offender if the nation refuses to extradite.[587] In addition to criminalizing cyberattacks, the ECC affirms that states have a duty to prevent non-state actors from using the state's territories to conduct cyberattacks against other states.[588]

The ECC negotiations lasted approximately four years, with the agreement becoming effective on July 1, 2004.[589] By December 21, 2007, forty-three nations had signed the ECC and twenty-one had ratified it, including the United States.[590] However, there are fairly broad grounds on which signatories may decline to cooperate with the ECC,

---

579. *See* ECC, *supra* note 577, pmbl.; NRC REPORT, *supra* note 4, at 62.

580. ECC, *supra* note 577, arts. 1–6.

581. *See* ECC, *supra* note 577, art. 15 (safeguards), art. 23 (international cooperation), art. 24 (extradition).

582. ECC, *supra* note 577, pmbl.

583. *See* ECC, *supra* note 577, art. 2 (illegal access), art. 3 (illegal interception), art. 4 (data interference), art. 5 (system interference), art. 6 (misuse of devices); *see also* Edwards, *supra* note 57, at 35 (noting that the ECC criminalizes "the serious hindering without right of the functioning of a computer system by inputting . . . data").

584. *See* ECC, *supra* note 577, ch. III (international cooperation).

585. Id. arts. 1–6.

586. *Id.* art. 4 (data interference), art. 5 (system interference).

587. *Id.* art. 22.

588. *Id.* art. 22.

589. Downing, *supra* note 95, at 711.

590. NRC REPORT, *supra* note 4, at 280. However, the United States is the only nation outside the Council of Europe to have ratified the ECC. Hunker, *supra* note 169, at 205. Two notable non-signatories are Russia and China. *Id.* Russia's official position with the United Nations is that there should be a prohibition on developing and using cyberattack tools. *See* NRC REPORT, *supra* note 4, at 329, 332 (noting, however, that "it is widely believed that Russia is fully engaged in, or at least developing, the capability for launching cyberattacks, regardless of its U.N. stance"). China, on the other hand, acknowledges the potential value in acquiring cyberattack capabilities. *See id.* at 332–33.

and the ECC lacks an effective enforcement mechanism.[591] Some have noted that the ECC is helpful with regard to criminal matters, but that there still exists a gray area between LOAC and criminal law for certain kinds of cyberattack.[592] We argue that the ECC could potentially provide a framework to address international cybercrime issues. However, the relatively low participation in the ECC and the difficulty of enforcing the ECC's provisions prevent it from being an acceptable solution to the problem of cyberattacks across international borders. Thus, the existence of the ECC does not change our conclusion that mitigative counterstriking is a socially optimal solution.

V. LAW RELEVANT TO THE USE OF SELF-DEFENSE

We propose a characterization of counterstrikes as either retributive or mitigative, with mitigative counterstriking firmly grounded in the principles of self-defense. Because we argue in favor of the viability of a mitigative counterstriking regime to ensure that self-defense becomes accepted in the cyber realm as well as the physical realm, this Part will examine aspects of the current legal regime that can support or hinder implementation of mitigative counterstriking capabilities. While there are some elements of existing law that appear to oppose any form of counterstriking on the Internet, we argue that the importance of self-defense in virtually all other areas of law suggests that current laws should be read to permit actions in self-defense, provided such actions adhere to the principles of mitigation.

There are some bodies of law that could conceivably permit mitigative counterstriking. However, a major barrier to implementing even an optimal active defense regime is that other bodies of law do not differentiate between a malicious first strike against an important system such as CNI and an optimal use of a mitigative counterstrike that is in the best interest of society. This Part examines relevant domestic and international law and provides suggestions for creating a policy that permits active defense and mitigative counterstriking without running counter to these laws.

A. U.S. Law

One of the first questions when recommending an active defense regime is who should be permitted to engage in mitigative counterstriking. The two primary options are to permit the target to counterstrike against the attacker or to allow only the government to conduct mitigative counterstrikes. If the latter option is adopted, private parties

591. *See* NRC REPORT, *supra* note 4, at 280.
592. *See id.* at 34.

should be supplied with a mechanism to request government intervention when they find themselves under a sustained cyberattack.

If individuals are permitted to engage in active defense, this raises many potential liability issues. Some have noted that the simple act of determining an attack's source through traceback may violate the CFAA and the ECPA, and that using mitigative counterstrikes to interrupt an attack and mitigate damage would most likely violate the CFAA.[593] However, the common law has long recognized that individuals may be privileged to defend themselves and their property to prevent a crime from being committed,[594] as well as to use self-help to abate a nuisance.[595] Deadly force generally cannot be used in response to a non-lethal threat[596] or in defense of property.[597] But it is unlikely that mitigative counterstrikes would be considered "lethal."

Under the common law, an individual who wishes to use force in defense of property must first ask the aggressor to stop (unless such a request would be futile or counterproductive), must hold a reasonable belief that force is necessary, and must use only reasonable force.[598] It is possible, therefore, that a party who is prosecuted or sued for taking actions pursuant to a mitigative counterstrike could claim that it was defending itself and its property, though it does not appear that this defense has ever been invoked.[599] If actions in defense of property are misdirected and result in harm to an innocent third party, then there may still be a plausible defense to a criminal prosecution if the counterstriker had made "reasonable efforts" to trace the attack to the actual attacker — even if these efforts resulted in erroneous information.[600] Erroneous use of mitigative counterstrikes could lead to civil liability for the counterstriker who injures a third party, though the liability may be reduced if the injured third party was, for example, the owner of a zombie computer who negligently permitted his computer to be compromised.[601]

We argue in Part VI that permitting private individuals to engage in mitigative counterstriking directly would be undesirable because

---

593. *See, e.g.*, *id.* at 36–37.

594. *See id.* at 204. It should be noted, though, that self-defense under U.S. common law is very different from self-defense under international law. *See id.* at 204–05. Under U.S. law, while persons may be privileged to defend property, they are not entitled to retaliate in response to crime. *Id.*

595. Katyal, *supra* note 35, at 61.

596. *See, e.g.*, 18 PA. CONS. STAT. § 505(b)(2) (2011) ("The use of deadly force [in self-protection] is not justifiable under this section unless the actor believes that such force is necessary to protect himself against death, serious bodily injury, kidnapping or sexual intercourse compelled by force or threat . . . .").

597. *See, e.g.*, *id.* § 507 (limiting the use of force in defense of property to narrow exceptions relating to personal dwellings).

598. Katyal, *supra* note 35, at 61.

599. *See* NRC REPORT, *supra* note 4, at 37.

600. *Id.* at 210.

601. *See id.*

such a position would permit case-by-case decisions about counterstriking, leading to the application of inconsistent standards. As we examine in Part V.B, consistent standards are essential because permitting individuals to engage in mitigative counterstriking could also have implications for international law. This need for consistency suggests that the government should control mitigative counterstriking. Even if individuals were permitted to engage in mitigative counterstriking, the government should still be involved in situations where cyberattacks against government computers warrant mitigative counterstrikes as an appropriate response.

The government is likely in a good position to take action in defense of private parties to mitigate harm to systems as a result of cyberattacks. However, there are a number of potential restrictions on the federal government that would hinder federal implementation of a full active defense regime. Monitoring private networks for cybersecurity issues could potentially cause the government to run into problems with the ECPA, the CFAA, the Computer Security Act of 1987, and the Fourth Amendment.[602] For this reason, we suggest that the initial stage of active defense — the use of IDS — be the responsibility of the private parties whose systems are eligible for federal protection through mitigative counterstrikes.

The next matter of concern is which branch of the U.S. Government should be authorized to conduct mitigative counterstriking. Congress has explicit warmaking powers under the Constitution,[603] while the President is given the authority as Commander-in-Chief and has some limited ability to order the military to take action prior to Congress giving explicit authorization.[604] Acting in self-defense is often regarded as the least controversial basis for the President's authority to order the armed forces to undertake hostile actions.[605] The nation's armed forces could likely launch mitigative — or even retributive — counterstrikes under the order of the President without the explicit authorization of Congress.[606] To authorize active defense and cyber counterstriking, the Office of General Counsel of the DOD would require evidence of provocation attributable to an agent of the nation where the attack originated, or a showing that the originating state is a sanctuary nation that has failed to stop the attacker after being notified of the activities and given a chance to address it.[607]

Some provisions of U.S. law, however, may restrict the ability of the government to implement a system permitting counterstriking in

602. *See* Greer, *supra* note 166, at 143–44; Nojeim, *supra* note 139, at 125–26.

603. U.S. CONST. art. I, § 8, cl. 11.

604. *Id.* art. II, § 2, cl. 1; 50 U.S.C. § 1541 (2006).

605. *See, e.g.*, NRC REPORT, *supra* note 4, at 232.

606. *See id.* at 55. Under the Constitution, the DOD cannot use force to defend the United States unless authorized by the President. *See* Sharp, *supra* note 30, at 24.

607. Jensen, *supra* note 19, at 239.

this manner. The Posse Comitatus Act prohibits the armed forces from taking actions to execute domestic law unless explicitly authorized by statute or under the Constitution.[608] This suggests that DOD would be prohibited from conducting cyber operations to support domestic law enforcement.[609] However, there are two constitutional exceptions to the Posse Comitatus Act: (1) to address emergencies when local law enforcement authorities cannot control the situation, and (2) to protect federal property or functions when the local authorities cannot or will not provide adequate protection.[610] Condron states that responses to cyberattacks on CNI would fall within one of these constitutional exceptions, so the Posse Comitatus Act does not act as a complete bar on DOD domestic involvement in cyber defense.[611]

Another option would be to entrust active defense and mitigative counterstrikes to a separate agency, such as DHS or a new sub-agency that could be created to address cyberattack issues. Protecting CNI has been an increasingly important priority over the last decade, and the statute creating DHS assigned to the agency a number of responsibilities and authorities to oversee issues regarding information security and protecting CNI.[612] The statute includes a provision indicating that private owners of CNI could contact DHS for assistance with protecting CNI.[613] CNI providers thus have the option of requesting government assistance in cybersecurity matters, though these providers may hesitate to request government assistance out of concerns about sharing confidential customer data. To this end, under the ECPA there are broad self-defense provisions that can permit the private sector to share communications information with the government in the interest of responding to an attack.[614]

Some critics express concern that there may be a due process problem if the government responds to a cyberattack using a mitigative counterstrike, because the target does not receive a fair trial.[615]

---

608. Posse Comitatus Act, 18 U.S.C. § 1385 (2006). In spite of some recent public debate to the contrary, the Posse Comitatus Act is probably still good law. *See Indefinite Detention, Endless Worldwide War and the 2012 National Defense Authorization Act*, ACLU (Feb. 22, 2012), http://www.aclu.org/indefinite-detention-endless-worldwide-war-and-2012-national-defense-authorization-act (noting a public debate about whether the NDAA effectively repealed the Posse Comitatus Act). We do not view the NDAA as being inconsistent with the Posse Comitatus Act, due to the Posse Comitatus Act's exception for circumstances "expressly authorized by . . . [an] Act of Congress." 18 U.S.C. § 1385.

609. *See* NRC REPORT, *supra* note 4, at 288.

610. *See* Condron, *supra* note 10, at 420.

611. *Id.*

612. *See* 6 U.S.C. § 133 (2006); *see also* Grant, *supra* note 41, at 106; Sharp, *supra* note 30, at 16. The Government Accountability Office, however, has been critical of DHS's performance in this area. *See* Grant, *supra* note 41, at 106.

613. 6 U.S.C. § 143 (2006 & Supp. IV 2010).

614. 18 U.S.C. §§ 2510–2522 (2006 & Sup. IV 2010).

615. *See, e.g.*, Katyal, *supra* note 35, at 61 (noting the argument but countering that the same would be true of any use of self-defense). The Fifth Amendment guarantees that no

However, we argue that mitigative counterstriking must be a proportionate response aimed at mitigating harm to a target, and therefore properly executed mitigative counterstrikes do not constitute punishment so as to raise due process concerns.[616] If a counterstrike does not meet the requirements to be considered mitigative, in some situations, post-deprivation hearings may be sufficient to satisfy due process.[617]

Another potentially relevant clause in the Fifth Amendment is the Takings Clause, which prohibits the government from taking private property for public use without just compensation.[618] However, the Constitution requires the takings to be for a "public use," and under Supreme Court takings jurisprudence, there must be some sort of prolonged interference.[619] If the government created botnets using private computers and used these botnets for purposes benefiting the public, this might amount to a taking that requires compensation, but it is unlikely that lesser government cybersecurity activities would rise to the level of a taking.

B. International Law

There are a number of international law provisions that address issues of self-defense. Self-defense under U.N. Charter Article 51,[620] anticipatory self-defense under CIL, and reprisals are all possible frameworks under which active defense and mitigative counterstriking can be analyzed. Oppenheim's treatise on international law asserts that a use of armed force can be self-defense when it is in response to an armed attack or, in the case of anticipatory self-defense, when (1) an armed attack is immediately threatened, (2) an urgent necessity exists for defensive action, (3) there is no practicable alternative but to act in self-defense, and (4) the action taken in self-defense is limited to the needs of defense.[621]

---

person shall be "deprived of life, liberty, or property, without due process of law." U.S. CONST. amend. V.

616. A due process problem might arise if a government counterstrike harms the property of an attacker within the United States. However, we view this due process argument as more applicable to retributive counterstrikes. In that case, an attacker may claim that he is being punished without a fair trial or that the government deprived him of the use of his property without adhering to proper procedures. Mitigative counterstriking, on the other hand, would be less problematic because of the limitations of a strict mitigation framework.

617. *See, e.g.*, Potts v. Pope, No. 95-60702, 1998 WL 792661, at *1 (5th Cir. Oct. 29, 1998) ("[T]he availability of post-deprivation remedies satisfies due process when exigent circumstances exist that allow a property seizure without a predeprivation hearing.").

618. U.S. CONST. amend. V.

619. *See* Loretto v. Teleprompter Manhattan CATV Corp., 458 U.S. 419, 426 (1982) (finding a per se taking where the government required property owners to install cable wires on their property).

620. U.N. Charter art. 51.

621. 1 OPPENHEIM'S INTERNATIONAL LAW 422 (Robert Jennings & Arthur Watts eds., 9th ed. 1992). Some have noted that espionage is also related to a state's right to use self-

Under international law, states have a "duty to prevent non-state actors within their borders from committing cross-border attacks."[622] Sklerov suggests that because of this duty, victim states have the legal authority to use cyber counterstrikes if the attacker's host state has insufficient criminal laws or declines to enforce them against the attacker.[623] The presence of a right of self-defense may increase the deterrent effect of international law,[624] which supports our argument that permitting mitigative counterstrikes is likely to improve the deterrent effect of a legal regime addressing cyberattacks.

1. Self-Defense Under Article 51 of the U.N. Charter

As discussed above in Part IV.B, whether a state is privileged to act in self-defense is governed by Article 51 of the U.N. Charter. The existence of privilege turns on whether the initial cyberattack is an "armed attack."[625] Because of the complicated nature of gaining Security Council approval for a use of force, some argue that it is more likely that a state would use self-defense to respond to a cyberattack in lieu of seeking Security Council approval.[626] The language of Article 51 refers to "the inherent right of individual or collective self-defence" in the event that an armed attack occurs against a U.N. member.[627] Analysis and commentary about Article 51 often concludes that the right to self-defense under Article 51 is triggered even when the armed attack against a state is by a non-state actor.[628] Since the language of the U.N. Charter seems to permit it — and the reality of cyberwarfare may even require it — we argue that the U.N. Charter should be interpreted to apply to cyber "armed attacks" by non-state actors. But who should determine whether a cyberattack is severe enough to justify self-defense under Article 51? Some suggest that system administrators will need authority to characterize an intrusion and decide if mitigative counterstriking is appropriate.[629] This raises a

---

defense. *See, e.g.*, Schaap, *supra* note 10, at 140 (noting the right of nations to engage in espionage during peacetime).

622. Sklerov, *supra* note 25, at 12.

623. *Id.* at 12–13. Sklerov posits that if the duty of prevention is reinterpreted to require enforcement, this will help remedy the difficulties raised by attribution issues. *Id.* at 13.

624. *See* Todd, *supra* note 28, at 71.

625. NRC REPORT, *supra* note 4, at 34; *see* Jensen, *supra* note 19, at 208 (questioning whether a cyberattack triggers the right to self-defense in the absence of a more traditional military attack).

626. *See, e.g.*, Graham, *supra* note 253, at 89.

627. U.N. Charter art. 51.

628. Jordan J. Paust, *Self-Defense Targetings of Non-State Actors and Permissibility of U.S. Use of Drones in Pakistan*, 19 J. TRANSNAT'L L. & POL'Y 237, 238 (2010) ("The vast majority of writers agree that an armed attack by a non-state actor on a state, its embassies, its military, or other nationals abroad can trigger the right of self defense . . . .").

629. *See, e.g.*, Sklerov, *supra* note 25, at 59, 73. Lin suggests that senior policymakers would ideally be responsible for choosing between offensive use of cyber exploitations and cyberattacks but notes that given the detachment of policymakers from the operational de-

number of concerns, and we emphasize that a mitigative counterstriking regime should ensure that high-level government leaders are involved in setting the standards to determine whether mitigative counterstriking is appropriate.

Article 51 preserves an inherent right of self-defense in response to armed attack,[630] but the use of self-defense is limited by requirements of necessity and proportionality.[631] An analysis of necessity examines "whether effective peaceful means of resolution exist[,] the nature of the aggression, each party's objectives, and the likelihood of effective intervention by the international community."[632] Proportionality requires a target to limit its response to the amount of force reasonably necessary to interrupt an ongoing attack or to deter future attacks,[633] but does not require the target to limit its response to the amount or type of force initially used by the attacker.[634] Thus, a kinetic attack could potentially be used in response to a cyberattack. However, some argue that responding to a cyberattack in kind — rather than through a kinetic attack — is more likely to comply with the similar *jus in bello* principles of distinction, humanity, necessity, and proportionality.[635] In addition to necessity and proportionality, self-defense under *jus ad bellum* also requires immediacy, though the principle of immediacy is very broad under international law and would permit a response to occur days or weeks after the initial attack.[636]

These three principles prohibit retaliatory or punitive cyber counterstrikes.[637] As a matter of international law, therefore, it is essential that parties undertaking a mitigative counterstrike strictly adhere to the principles of mitigation and avoid retributive counterstriking. The principles also echo the traditional requirements for valid counterstrikes under the "just war" doctrine, as discussed above in Part III.C.

---

tails of a mission, such choices are likely to be placed on field operators who might not be as sensitive to the important diplomatic difference between cyber exploitations and cyberattacks. Lin, *supra* note 43, at 82–83.

630. U.N. Charter art. 51 ("Nothing in the present Charter shall impair the inherent right of individual or collective self-defence . . . ."); *see also* Sklerov, *supra* note 25, at 30–31 (asserting that the right of self-defense is an inherent right "derived from the fundamental right of states to survive").

631. *See* Graham, *supra* note 253, at 89; Jensen, *supra* note 19, at 218; Sklerov, *supra* note 25, at 32–33; Todd, *supra* note 28, at 98.

632. Todd, *supra* note 28, at 98.

633. Graham, *supra* note 253, at 89.

634. Schaap, *supra* note 10, at 148. The use of kinetic weapons to respond to cyberattacks might be disproportionate and less effective than responding to a cyberattack in kind. *See* Graham, *supra* note 253, at 99.

635. Graham, *supra* note 253, at 98–99; *see also* Sklerov, *supra* note 25, at 79–80.

636. *See* Condron, *supra* note 10, at 413–14. Necessity, proportionality, and immediacy are requirements of both *jus in bello* and *jus ad bellum*. *Id.*

637. *See id.* at 415.

We argue that optimal use of mitigative counterstrikes should follow the principles of necessity and proportionality.

Above, we analyzed the circumstances under which a cyberattack is an "armed attack."[638] If a cyberattack is an "armed attack," it is unclear whether a response in self-defense would be permitted if the attack is not attributable to a state actor.[639] If a nation is indirectly responsible for a cyberattack by a non-state actor, however, a cyberattack victim may be permitted to employ self-defense against the attacker.[640] In such a scenario, "the victim-state must limit its targets to the non-state actors, unless the host-state uses force to oppose the lawful cross-border operations."[641]

Even when the victim can identify the attacking source, "the victim-state's system administrator must map out the attacking computer system to distinguish its functions and the likely consequences that will result from shutting it down."[642] Mapping the attacking computer would thus help ensure that the use of mitigative counterstriking complies with the principles of distinction and proportionality.[643] Because of current technical limitations, it would likely be impossible to make a surgical strike against a specific attacker, and so the resulting harm to innocent systems could violate the law of war's principles of distinction and proportionality.[644] The danger of running afoul of international law is another reason why use of the most accurate technology in detecting, tracing, and counterstriking is of paramount importance. We thus argue that active defense should not be broadly implemented until the technology is sufficiently advanced to protect against such collateral damage, though limited implementation to protect CNI may be desirable.

2. Anticipatory Self-Defense

Under the *Caroline* doctrine, states may engage in anticipatory self-defense when the need for self-defense is instant and overwhelming, there is no other way to respond, and there is no time for delibera-

638. *See supra* Part IV.B.1.A.

639. *See* Graham, *supra* note 253, at 92. In these situations, the victim cannot intervene in the other state's domestic affairs and must rely on the other state to address the attack through its criminal law system. *See* Sklerov, *supra* note 25, at 38. However, in extreme situations, a state may have a right to respond to non-state actors in self-defense, such as in the case of the September 11, 2001 al-Qaeda attacks on the United States, where the U.N. Security Council reaffirmed that the United States had the right to engage in self-defense under Article 51. *Id.* at 40–41.

640. *See* Graham, *supra* note 253, at 93; Sklerov, *supra* note 25, at 38. States have the duty to prevent persons within their borders from perpetrating crimes against other states. *See supra* text accompanying note 532.

641. Sklerov, *supra* note 25, at 49.

642. *Id.* at 81.

643. *Id.* at 81–82.

644. *See* Graham, *supra* note 253, at 99–100.

tion.[645] The immediacy requirement has evolved to permit anticipatory self-defense where (1) the aggressor is committed to an armed attack and (2) the victim's ability to defend itself is hindered by a delaying its response.[646] If there is evidence of an ongoing campaign against a state, anticipatory self-defense may be authorized because future attacks are imminent.[647]

Scholars disagree about whether Article 51 should be interpreted to permit anticipatory self-defense. Some say that self-defense is strictly limited to responding to an "armed attack."[648] Others argue that Article 51 merely codifies an inherent right of self-defense, and that anticipatory self-defense under the *Caroline* standard is still available.[649] Still others have argued, however, that the requirement to demonstrate immediacy under the *Caroline* standard makes it unlikely that anticipatory self-defense would apply to cyber counterstrikes.[650]

If self-defense is strictly limited to responding to an "armed attack," then complications arise from the fact that cyberattacks are currently unlikely to be viewed as per se "armed attacks."[651] To characterize cyberattacks as armed attacks, scholars often look to the traits, consequences or effects of a specific cyberattack.[652] If a cyberattack is not declared to be an "armed attack" until it has already occurred and the traits, consequences, or effects can clearly be seen, it is difficult under such a fundamentally backward-looking model to ever justify actions taken in self-defense before the harm occurs.

Schmitt argues that anticipatory self-defense can be used to address cyberattacks if three factors are present: (1) the attack is "part of an overall operation culminating in an armed attack," (2) the attack is an "irrevocable step" towards an "imminent (near-term) and probably unavoidable attack," and (3) the anticipatory response to the attack is undertaken at the last possible moment to counter the attack.[653] These requirements create a high bar, however, and anticipatory self-defense

---

645. The *Caroline* standard arose out of "the invasion of U.S. territory across the Niagara River by British forces to prevent aid to Canadian revolutionaries from the *Caroline*" in 1837. Jensen, *supra* note 19, at 218–19 (quotations and internal citations omitted); *see also* Hoisington, *supra* note 36, at 450; Sklerov, *supra* note 25, at 34, 48; *cf.* NRC REPORT, *supra* note 4, at 243 (discussing a related conception of anticipatory self-defense).

646. Sklerov, *supra* note 25, at 35.

647. *Id.* at 36.

648. *See* Condron, *supra* note 10, at 412–13.

649. *See, e.g.*, NRC REPORT, *supra* note 4, at 243; Condron, *supra* note 10, at 412–13; Sklerov, *supra* note 25, at 31–32.

650. *See, e.g.*, Graham, *supra* note 253, at 90.

651. *See supra* Part IV.B.1.A.

652. *See* Jensen, *supra* note 19, at 224–25 (citing Michael N. Schmitt, *supra* note 571, at 886); *see also supra* Part IV.B.1.A. Jensen states that Schmitt's backward-looking view of when a cyberattack is a "use of force" or "armed attack" is currently the most accurate view of cyberattacks under international law, but also acknowledges that in the future there will likely be a need for a more permissive construction of these terms as they apply to cyberattacks. Jensen, *supra* note 19, at 228.

653. Schmitt, *supra* note 571, at 932–33.

would be largely unavailable as a justification for counterstriking if Schmitt's proposed standard is adopted.

Our analysis leads us to conclude that using mitigative counterstriking to respond to an ongoing attack, such as a DDoS attack, is consistent with international law. Additionally, relevant literature notes that anticipatory self-defense may be authorized in response to an ongoing campaign against a state.[654] Therefore, it is possible that mitigative counterstriking can be used against a party that previously completed a cyber "armed attack" if there is evidence that the prior attack was part of an ongoing campaign and that future cyber "armed attacks" are thus "imminent."

3. Reprisals

In addition to the traditional concept of self-defense, states are also entitled to use reprisals, or proportionate countermeasures, to respond to a use of force.[655] Reprisals themselves, though, may not involve a "use of force," and they must meet three additional requirements: (1) the countermeasure is used in a state-versus-state context, (2) the victim state told the aggressor state to stop its attack, and (3) the countermeasure's effects are commensurate with the harm suffered.[656] Reprisals, therefore, are not an option if a state wishes to respond to an attack by a non-state actor. Additionally, reprisals would be unavailable if cyberattacks are considered a "use of force" under international law. However, if the international community declares that cyberattacks are not a "use of force," such that a cyberattack would not violate Article 2(4) of the U.N. Charter, then utilizing cyber counterstrikes in a manner consistent with the definition of reprisal would be a valid way for states to protect their interests in the event of a kinetic "use of force" by a foreign state.[657]

Now that we have examined the currently available paradigms for addressing cyberattacks and self-defense in cyberspace, we turn to our main proposal: recommending a new regime to govern the issues raised by active defense and mitigative counterstrikes and how such a regime can be implemented.

---

654. *See* Sklerov, *supra* note 25, at 36.

655. *See* Jensen, *supra* note 19, at 220.

656. *See* Sklerov, *supra* note 25, at 36–37.

657. A cyber counterstrike to a kinetic "use of force" that does not rise to the level of an "armed attack" potentially would be a way for a state to protect its interests without resorting to the U.N. Security Council.

VI. POLICY CONCERNS RELATING TO MITIGATIVE COUNTERSTRIKING

In this Part, we examine various policy issues raised by the potential implementation of an active defense regime emphasizing mitigative counterstriking. We evaluate the specific circumstances in which mitigative counterstriking would be an optimal response, the potential for governments to take responsibility for mitigative counterstriking, and the potential role of public-private partnerships. We also provide suggestions for mitigative counterstriking procedures and on how to protect third parties harmed as a result of a counterstrike.

A. The When and Who of Active Defense and Mitigative Counterstriking

Under an active defense regime, two of the most important questions are which types of intrusions warrant mitigative counterstrikes and who may engage in these counterstrikes. These are fundamental issues that underlie our goal of implementing a broad active defense regime in a socially optimal and consistent manner. Answering these questions requires consideration of a broad range of issues, including technological capabilities, domestic law, international law, and the viability of alternatives to active defense.

1. Relevant Types of Intrusions

The first important consideration is which types of intrusions our model of active defense could counteract. For this threshold question, the key point in the active defense process is the detection stage, including whether multiple intrusions are detected. For mitigative counterstriking to be a valid response, there has to be an ongoing threat, the harm from which can be mitigated by a counterstrike that interrupts the operations of the attacker. Mitigative counterstriking would likely not be an appropriate recourse in circumstances where the intrusion is a single event, since there would not be a continuing threat to mitigate. For this reason, there are two types of intrusions that we argue pass this threshold: DDoS attacks and spiders.[658]

DDoS attacks are cyberattacks. One way to undertake a DDoS attack is by compromising a large number of computers to create a horde of zombie systems that flood a target with data in order to knock it offline.[659] When an attacker undertakes a DDoS attack of this type, he must first identify a vulnerability to exploit and then dissemi-

658. *See generally supra* Part II.A.1 (discussing types of cyberattacks and cyber exploitations).

659. *See supra* Part II.A.1.C.ii (discussing DDoS attacks).

nate malicious code — like a virus or a worm — to take advantage of that vulnerability in a large number of systems — perhaps hundreds of thousands. Once the attacker has control of this zombie horde, he has at his disposal an army of computers that he can order to attack repeatedly until the target is taken out. The repetitive nature of a DDoS attack makes it well-suited to the detect-trace-counterstrike method of active defense.

The use of spiders to mine data is cyber exploitation, rather than cyberattack, because the goal is to obtain data, not to cause immediate harm.[660] Because the intruder accesses the target system repeatedly, there would likely be sufficient activity for a firm's IDS to detect a pattern,[661] making the use of spiders another kind of intrusion that can be interrupted by a mitigative counterstrike — here, to reduce the amount of information obtained by the intruder. Whether mitigative counterstrikes should be used to respond to the threat of spiders, however, is a question related to the severity of the intrusion. A policymaker deciding whether an intrusion is sufficiently severe might apply tests that have been used by other researchers in analyzing cyberattacks under international law. These options are examined in further detail in Part IV.B.

One option we have considered is that mitigative counterstrikes might be an appropriate response to repetitive attacks that would be considered an "armed attack" under the U.N. Charter.[662] We propose using an effects-based approach that evaluates whether the effects of a cyberattack would justify the use of self-defense under Article 51 of the U.N. Charter. If the principle of mitigation is adopted, counterstriking might be appropriate at a lower threshold of harm to the victim.[663] Mitigative counterstriking might also be permissible when an attack is a "use of force."[664] Because spiders are exploitations and not attacks, however, international law likely would not permit the use of mitigative counterstriking to interrupt these spiders. In addition, passive defense methods, such as blocking the IP address associated with the spider, would likely provide sufficient protection against cyber intrusions, since these intrusions are not targeting the victim system with the goal of harming its functionality.

Having established that mitigative counterstrikes would be the most appropriate response in the event of an ongoing DDoS attack,

---

660. *See* Feigin, *supra* note 45, at 906 (defining a spider as "an automated program that serially visits, or 'crawls,' websites and keeps a log of what it finds").

661. *See generally supra* Part III.B.1.

662. *See supra* Part IV.B.1.

663. Previously, we set forth a definition of mitigative counterstriking as an active effort to mitigate harm to a victim system in a manner strictly limited to the amount of force necessary to protect the victim from further damage, where the goal is limited to mitigating damage from a current and immediate threat. *See supra* Part I.

664. *See supra* Part IV.B.1.A.

we now turn to the question of who should be responsible for executing mitigative counterstrikes. The three options we consider are private industry, government actors, or a hybrid of both.

2. Options for Control over Active Defense

A. Private Sector Participation

In a socially optimal situation where accurate technology is used and no other means of recourse are practicable, there are advantages to permitting private sector victims to counterstrike directly. Private parties could engage in counterstrikes more quickly than government actors. However, there are also many concerns about permitting this type of counterstrike. Technology often outpaces legal developments, so private sector actors would likely have access to technology that potentially has significant negative effects on third parties, without the adversely affected third parties enjoying adequate protections under a relevant regulatory framework. This could lead to hundreds of companies competing to provide IDS, traceback, and counterstrike technologies to thousands of private firms without regulatory oversight to protect third parties. A lack of technological uniformity could also result in harm to third parties. Significant competition among software providers may lead some developers to cut costs, resulting in low quality software that is potentially harmful to third parties due to inconsistent or incompatible technologies.

Beyond the issues of consistency in implementation and product quality, there is a more significant downside to entrusting mitigative counterstriking to private firms. We observed in a previous work that there are threshold points where permitting counterstrikes would be the socially optimal solution.[665] However, our model does not define these thresholds, and determining what they are requires the establishment of standards. It would be unwise to allow individual companies to make these decisions on a case-by-case basis. We posit that some companies would be more risk averse, while some may be more inclined to behave like cyber vigilantes. It is unclear how a firm's risk profile would affect its vulnerability to a cyberattack. If a firm is more risk-averse and less willing to use active defense, an attacker might view it as a more attractive target. Similarly, if a firm is more risk seeking, a cyberattacker might view it as a challenge to overcome. A uniform approach could counteract the effect of firm behavior on their attractiveness as targets, and contribute to the deterrent effect of mitigative counterstriking.

665. *See* Majuca & Kesan, *supra* note 24, at 21–22.

Another potentially severe effect of private parties engaging in cyber counterstriking under international law concerns the idea of "lawful combatants" and noncombatants.[666] If a private party conducts a mitigative counterstrike against a foreign attacker and causes harm to other citizens of the state, the private party could lose its status as a protected noncombatant.[667] This distinction between lawful combatants and noncombatants supports our argument that the government should be responsible for some aspects of active defense, especially mitigative counterstriking. Such a regime would not only serve to provide consistency, but it would also protect private parties from being treated as combatants and thus valid targets for military strikes under the law of war.

In order to ensure that only socially optimal, mitigation-focused counterstriking occurs, implementation of an active defense program requires standardization. One possible way to achieve this sort of standardization is to utilize a central government entity for the purpose of deciding when mitigative counterstriking would be appropriate. We suggest that DHS might be the appropriate agency to set these standards, given its involvement in the cybersecurity arena.

Due to the significant downsides of permitting private firms to counterstrike directly, it may be advisable to implement a mitigative counterstriking regime in a different way. As an alternative to entrusting mitigative counterstrikes to private firms, the government (or a government contractor) may also be placed in charge of counterstriking.[668] This option is considered in the following Part.

B. Government Involvement

The next option we examine is whether the government should be placed in charge of conducting mitigative counterstrikes. The legal implications of this sort of approach are examined in Part V. This proposal has several advantages, though there are also potential pitfalls that must be carefully monitored. This Part proceeds primarily on the theory that government control of counterstrikes has fewer downsides than private control. However, the part of active defense that involves monitoring private systems for intrusions would likely be best left to the private sector, who would then communicate with the

---

666. *See* Graham, *supra* note 253, at 97.

667. *See generally* Brenner & Clarke, *supra* note 143, at 1015 ("The right of the noncombatant population to protection . . . involves . . . a corresponding duty of abstaining from . . . hostilities . . . ." (quoting Henry Droop, *On the Relations Between an Invading Army and the Inhabitants, and the Conditions Under Which Irregular Troops Are Entitled to the Same Treatment as Regular Soldiers*, *in* TRANSACTIONS OF THE GROTIUS SOCIETY 713 (1871))).

668. *See* NRC REPORT, *supra* note 4, at 7 (suggesting building a government institution to provide private sector entities immediate relief when they are victimized by cyberattacks).

designated counterstrike authority after detecting an intrusion. This would avoid the legal issues that the government would encounter as a result of monitoring private networks, including restrictions arising from ECPA, the CFAA, the Computer Security Act of 1987, and the Fourth Amendment.[669]

If the government were placed in charge of mitigative counterstrikes, this would ensure technological uniformity in software utilized for counterstriking. Placing the responsibility for mitigative counterstriking on government entities would also create uniformity in personnel training and policies, which could help ensure that employees responsible for mitigative counterstriking would be informed of the processes and dangers. In addition to the advantage of uniformity, allowing only the government to undertake mitigative counterstriking would ensure that parties could request protection based on need and urgency rather than their ability to pay to protect their systems.[670]

We recognize, however, that any advantage that the government has in putting the best technology in place is almost exclusively an advantage on the front end only, as once that technology is in place, there may be insufficient incentives to ensure that the technology is consistently kept up to date.[671] Additionally, the nature of government action requires that all actions be undertaken slowly and carefully. While this serves to protect third parties from the hasty responses of others, this is a concern for attack victims because it increases response time to cyberattacks.

In the interests of uniformity and limiting the burden on private parties, we recommend that the government either subsidize or supply IDS technology to the private parties that are responsible for monitoring their own networks. The government could exercise control over the type of traceback technology implemented in order to ensure technological accuracy. IDS and traceback technologies are developing rapidly, and government assistance in obtaining this technology could help companies better prepare for future threats. However, whether

---

669. *See* Greer, *supra* note 166, at 143–44; Nojeim, *supra* note 139, at 125–26; *supra* Part IV.A.1.

670. Government involvement in mitigative counterstriking is analogous to community law enforcement, which subsidizes legal protections for the poor, who otherwise would not be able to afford the same security measures as those with more resources. *See* Katyal, *supra* note 35, at 36 (describing the problems associated with self-help policing). While we acknowledge that broad use of mitigative counterstriking, including by private parties, may be desirable in the future, at this time the use of such counterstrikes should be undertaken only by the government.

671. The bureaucratic process occasionally causes problems for the acquisition of and updates to technology. In the past, the procurement procedures for the Federal Aviation Administration (FAA) have been so cumbersome that newly purchased equipment was out-of-date by the time the contract went through. *See* Janie Lynn Treanor, *Privatization v. Corporatization of the Federal Aviation Administration: Revamping Air Traffic Control,* 63 J. AIR L. & COM. 633, 641 (1998).

executing traceback should be entrusted to the private parties or the government is not yet fully clear.

As to which party or parties should control each aspect of active defense, we have argued that private parties should control IDS, perhaps with government subsidization of IDS technology, but that the government should have more control over mitigative counterstriking. Which party should have primary control over the third aspect of active defense, traceback, is not as clear. The act of tracing an intrusion might implicate the Fourth Amendment rights of the intruder if the traceback is either conducted by the government or by a private party acting with the government's permission. However, there are a number of exceptions to the Fourth Amendment's warrant requirement, such as the exceptions for hot pursuit and other exigent circumstances,[672] which may justify the government's use of traceback without a warrant. These constitutional issues give us pause, but do not persuade us that purely private use of traceback would be more appropriate.

There are potentially severe diplomatic implications of government involvement in mitigative counterstriking, including international political conflicts resulting from a government action that has negative effects on another nation's government or population. If individual actors in one country execute mitigative counterstrikes against aggressors in another country and inadvertently harm innocent individuals, the state in which the aggressors are located likely would not be held responsible if it did not encourage the harmful acts. If government-sanctioned mitigative counterstrikes caused harm to innocents in the other country, however, this state would be held responsible. This sort of accountability can also be an advantage, but only if all governments uniformly accept responsibility for regulating active defense and mitigative counterstrikes within their borders. Accountability would help ensure that cyberattacks are addressed consistently across different countries.

C. Public-Private Partnerships: An Alternative to Pure Government Control

As noted above, there are both advantages and disadvantages to putting either the government or the private sector in exclusive control of active defense and mitigative counterstriking. We argue that a core competency of the private sector is its potentially superior technologi-

672. *See* Dale Joseph Gilsinger, Annotation, *When Is Warrantless Entry of House or Other Building Justified Under "Hot Pursuit" Doctrine*, 17 A.L.R. 6th 327 (2006). There is insufficient case law to determine whether an exception to the Fourth Amendment would support the warrantless use of traceback. The hot pursuit exception is a potential option, though a thorough examination is outside the scope of this Article.

cal expertise and access to cutting-edge technology.[673] The corresponding core competencies of the public sector include access to enforcement mechanisms, the ability to develop uniform procedures, and access to highly relevant, non-public information.[674] The balance appears to weigh in favor of careful government oversight of cyber counterstriking. The importance of the private sector to the future of handling cyberconflicts cannot be overemphasized, however, since the private sector arguably has an interest in addressing vulnerabilities that is equal or greater than that of the government.

In part because of the drawbacks of either government or private parties acting alone to address cyberattacks, we advocate for the establishment of a public-private partnership to regulate active defense and permit mitigative counterstriking. Such a public-private partnership could combine the respective active defense capabilities of the government and the private sector. Though its current effectiveness is disputed, the IT-ISAC[675] compiles alerts and provides members of the public with a method to submit suspicious computer files to the organization's attention.[676] An analogous arrangement in the context of active defense could consist of frequent updates concerning IDS and traceback research, reports concerning potential cyber intrusion trends, and alerts about newly discovered vulnerabilities.

Some members of Congress also appear to see the benefits of public-private partnerships in the cyber context. In November 2011, CISPA was introduced in the House of Representatives, and on April 26, 2012, the House approved the bill.[677] CISPA includes provisions that would permit and encourage the sharing of cyber threat information between the private and public sectors, which we view as an important part of forming a solid defense against cyber threats.[678]

We urge that public-private partnerships could address the current shortcomings of regulating cybersecurity and defense issues and help establish a formal right of self-defense in cyberspace. As is evident from the example of IT-ISAC, however, public-private partnerships

673. *See generally* Michael W. Mutek, *Implementation of Public-Private Partnering*, 30 PUB. CONT. L.J. 557 (2001).

674. *See* Exec. Order No. 12,968, 3 C.F.R. 391 (1995), *reprinted as amended in* 50 U.S.C. § 435 (2006), *available at* http://www.fas.org/sgp/clinton/eo12968.html (describing the importance of classified information to the functioning of the government); Mark B. Baker, *Promises and Platitudes: Toward a New 21st Century Paradigm for Corporate Codes of Conduct?*, 23 CONN. J. INT'L L. 123, 163 (2007) (listing enforceability and uniformity as two advantages of government regulation of private conduct).

675. *See supra* note 226.

676. *See Reported Alerts*, IT-ISAC, https://www.it-isac.org/reported_alerts_n.php (last visited May 3, 2012).

677. Cyber Intelligence Sharing and Protection Act of 2011, H.R. 3523, 112th Cong. (2011).

678. *Id.* CISPA raises privacy concerns, however, since it would permit covered entities to share information about their customers with the government for "cybersecurity purposes." *Id.* § 2.

can be difficult to implement. The private and government sectors are dominated by different cultures, and convincing the two groups to work together can be problematic. For instance, a lack of trust could result in resistance on both sides against fully sharing with the other, leading to informational asymmetry where one party knows more than the other with respect to some matters. To reduce these informational asymmetries, the public and private parties need to be encouraged to trust each other and share their expertise so that they can work together in a coordinated fashion that creates synergies. If a public-private partnership is to succeed, building trust will be critically important.

B. Potential Procedures for Mitigative Counterstriking

Having evaluated the possible advantages and pitfalls of various approaches to active defense, the next important consideration is the procedures that should be followed when engaging in mitigative counterstriking. Because of the need for quick action when engaging in mitigative counterstrikes, the first important point is that these procedures should contain elements conducive to expedited review.

One possible approach is to establish procedures that resemble how wiretapping approvals are obtained. Currently, wiretaps are available through procedures in the Wiretap Act[679] and FISA, which provides a process for requesting surveillance of a foreign power or an agent of a foreign power through the FISA court.[680] An analogous process for mitigative counterstrikes would allow an independent body staffed by persons skilled in Internet-related legal issues, and who are also specialists in complicated computer networks and cyber intrusions, to make decisions concerning potential mitigative counterstrikes. Such a body could be responsible for evaluating when mitigative counterstriking is appropriate and could also serve to verify the precision of the technology used.

This independent body responsible for evaluating mitigative counterstriking issues could be located within an existing administrative agency, such as the DOD or DHS. DHS may be the most logical candidate, since it is currently the agency most involved with national cybersecurity issues.[681] The agency responsible for mitigative counterstriking must also establish the threshold requirements necessary to justify counterstrikes. When experiencing a cyber intrusion, the entity requiring assistance could be permitted to petition the agency for a counterstrike response by providing specific information about the

679. 18 U.S.C. § 2518 (2006).

680. 50 U.S.C. § 1805 (2006 & Supp. IV 2010).

681. *See* Grant, *supra* note 41, at 106 (noting DHS's responsibilities in the cybersecurity area).

intrusion and any harm currently inflicted or anticipated if the harm is not mitigated.

The agency in charge of mitigative counterstriking might decide to utilize higher threshold requirements for counterstrikes when the victim is a private organization rather than a government entity or an operator of CNI. Government entities or operators of CNI might be authorized to act immediately and submit information on the mitigative counterstrike for ex post facto approval. Such disparate treatment may be justified given the national security importance of prompt termination of cyber intrusions on sensitive government systems and CNI.

C. Addressing the Effect of Mitigative Counterstriking on Third Parties

When selecting a policy approach to address cybercrime, there are several important considerations, such as the policy's effectiveness, its political feasibility, and the burden it will place on society.[682] If mitigative counterstrikes were adopted as a matter of policy, attackers could potentially route their attacks with the specific goal of not only harming the initial target, but also prompting the target to counterstrike in a way that will harm third-party intermediaries. That would create a new danger of "catalytic cyberconflict," where a conflict is instigated between two parties because of the actions of a third party.[683] To help blunt the potential for catalytic cyberconflict, a legal regime addressing cyberattacks must provide reasonable protection to intermediaries, reducing the incentive to resort to self-help against counterstrikers. The potential effect on third parties is the issue to which we now turn. Part IV.A.2 evaluates the possibility of holding zombie computer owners liable for harm to attack victims; this Part considers the reverse: holding mitigative counterstrikers liable for harm to zombie computer owners.

Cyberattackers who engage in cyber intrusions generally seek to avoid getting caught. One method that they use to evade detection is to route their messages through other computers on the Internet in order to obscure the origin of their signal.[684] In addition to using other

682. *See* NRC REPORT, *supra* note 4, at 147 (noting questions including whether active defense should be a last resort, a first resort, or something in between; whether counterstrikes are likely to be effective; and how to prioritize the protection of different targets); Yang & Hoffstadt, *supra* note 94, at 213–14. Other issues include whether active defense should be automated, whether adopting active defense is a sound diplomatic policy, and whether the benefits of active defense are worth the risk of collateral damage. *See* Sklerov, *supra* note 25, at 82–83.

683. NRC REPORT, *supra* note 4, at 312.

684. *See Spoofing*, INTERNET SECURITY SYSTEMS, http://www.iss.net/security_center/advice/Underground/Hacking/Methods/Technical/Spoofing/default.htm (last visited May 3, 2012).

computers to evade detection, an attacker who compromises a large number of systems could use those computers as a botnet to attack the ultimate victim with a DDoS attack.[685] A firm that is monitoring for such attacks could then execute a mitigative counterstrike. But what if the counterstrike causes harm to the zombie computers, whose owners were not involved with — or aware of — the attacker's malicious intentions?

One persuasive argument is that these third parties, who we will refer to as "oblivious intermediaries," should be protected from damage caused by a mitigative counterstrike. However, if ignorance of the law is no excuse, why should ignorance of technology — or at least the basic protections provided by easily available support software — be acceptable? Additionally, in some circumstances the oblivious intermediaries may be unaware not only of the intrusions by the initial attacker, but also of the harm caused by mitigative counterstrikes. If these oblivious intermediaries are unaware that their system has been harmed, has their system truly been harmed? And if the oblivious intermediary firms unwittingly become tools of the attacker because of the negligent maintenance of their systems, why should they be afforded extra protection? One possible solution, then, is to afford no protection for injured third parties, because additional protection creates a moral hazard by permitting firms to avoid the consequences of their negligence. Policymakers could point to the risk of damage resulting from mitigative counterstrikes as another incentive for computer operators to consistently protect their systems via security updates, firewalls, antivirus products, and anti-malware products.

As a policy matter, however, such a harsh approach may be inappropriate. A company with a thousand responsible corporate employees should not necessarily be punished for the careless actions of a single employee on the network. While firms are routinely held responsible for the actions of their employees, denying a legal remedy against cyberattackers based on a single negligent employee's conduct would be too harsh, creating a per se rule that does not consider the totality of the circumstances. Therefore, an oblivious intermediary should be permitted to sue the original target of the attack if the oblivious intermediary's system suffered harm as a result of a negligent or reckless mitigative counterstrike.

However, we are still left with the problem of avoiding the moral hazard posed by rewarding computer users who willingly remain ill equipped to handle avoidable modern cyber threats. The first step that should be taken is education. In order to minimize potential zombie botnets, the government should disseminate educational materials underscoring the importance of timely security updates and the use of

685. *See* John Markoff, *Attack of the Zombie Computers Is Growing Threat*, N.Y. TIMES (Jan. 7, 2007), http://www.nytimes.com/2007/01/07/technology/07net.html.

software packages that prevent infiltration and detect if the system has been compromised. Using education to reduce the number of potential third parties that might be harmed by cyber counterstrikes could ease the implementation of a liability rule as part of a regime designed to permit defensive actions under the appropriate circumstances. Another option would be to adopt the Japanese model, where the owners of infected computers are provided with assistance in disinfecting their machines.[686]

If we do not wish to make oblivious intermediaries ineligible to pursue causes of action against counterstrikers, we suggest allowing courts to decrease the damages owed to oblivious intermediaries based on their negligence in managing their IT infrastructure. Because states take a variety of approaches to negligence, and specifically to the defense of contributory or comparative negligence,[687] federal statutory intervention may be necessary, potentially in the form of a federal cybertort statute. Such a statute should make available a comparative negligence defense to reduce damages owed by a mitigative counterstriker to an oblivious intermediary. For example, a firm with one careless employee who inadvertently renders the firm's entire network vulnerable would likely be entitled to a larger damage award than a firm that lacks any systematic network security. A vulnerability that was the result of a zero-day exploit, in contrast, should not decrease damages, since it would be almost impossible for a user to prevent his computer from being compromised by an unknown vulnerability.

A final problem is the issue of protection for oblivious intermediaries in other countries. If the government controls mitigative counterstrikes, the Federal Tort Claims Act ("FTCA")[688] may permit suits by foreign citizens against the United States. The government could resolve the dispute between the injured foreign third party and the counterstriking party, recovering damages from the counterstriking party to ensure that the counterstriking party remains accountable for harm. The most significant problem with using the FTCA in this manner, however, is that the FTCA contains an exception for claims that arise in a foreign country.[689] The Internet age makes it difficult to determine where a claim arises, potentially raising the same issues as jurisdiction analysis: does the claim arise where the attack originates,

686. *See* Yasuhide Yamada, Atsuhiro Yamagishi & Ben T. Katsumi, *supra* note 72, at 226–28.

687. *See Contributory Negligence vs. Comparative Negligence*, THE PERSONAL INJURY LAWYER DIRECTORY, http://www.the-injury-lawyer-directory.com/negligence.html (last visited May 3, 2012).

688. 28 U.S.C. § 1346(b) (2006 & Supp. IV 2010).

689. *See* HENRY COHEN & VANESSA K. BURROWS, CONG. RESEARCH SERV., 95-717, FEDERAL TORT CLAIMS ACT 2 (2007), *available at* http://www.fas.org/sgp/crs/misc/95-717.pdf.

where oblivious intermediaries are located, or where the targeted victim is located? One possible solution could be to treat the harm as arising in the jurisdiction where the counterstrike's effects were first felt and require the dispute to be governed by the negligence law of that jurisdiction.

VII. CONCLUSION

The threats of cybercrime, cyberterrorism, and cyberwarfare loom over modern society. Specific examples of threats range from DDoS attacks against government systems that coincide with kinetic warfare, such as in the case of Georgia, to standalone attacks using sophisticated cyberweapons, such as in the case of the Stuxnet worm and the damage it caused to Iranian nuclear infrastructure. It is no overstatement to assert that cyber defense technology and infrastructure are essential to any modern approach to conflict.

However, private parties, including private owners of CNI, have no legal options that are consistently effective against the variety of threats that they face. Criminal enforcement is complicated by the lack of a consistently enforced international paradigm, complex jurisdictional issues, and the difficulty of identifying an attacker in a manner specific enough to support criminal prosecution. Civil litigation is similarly of questionable utility for two reasons: (1) the difficulty of identifying the attacker and (2) the low likelihood of successfully holding third parties liable in tort. Passive defense is unlikely to be sufficiently effective in part because of the inconsistency with which passive defenses are implemented, and in part because passive defense alone will often prove inadequate in the face of zero-day exploitations.

Mitigative counterstrikes would be the socially optimal solution if there was sufficiently accurate active defense technology in an environment where other methods of addressing attacks would be ineffective. We urge that even if the technology still needs further development, the lack of reliable alternatives necessitates a dialog to set forth a regime permitting active defense, especially mitigative counterstrikes to protect CNI.

Self-defense, we have argued, is accepted in virtually all other legal contexts, and should be preserved in the cyber realm. For this reason, we urge the creation of a legal regime that permits mitigative counterstrikes. The use of self-defense, however, is not without complications. There are questions about how to address harm to oblivious intermediaries. In the international context, if a mitigative counterstrike harmed innocent parties in a foreign country, it could lead to a diplomatic crisis.

In analyzing the existing framework, we note that current law could potentially support implementation of an active defense regime that permits counterstrikes grounded in the principles of mitigation. Areas of the law that are consistent with mitigative counterstriking include the recognition of self-defense exceptions under U.S. common law and statutes, and provisions of the U.N. Charter that preserve a right of self-defense in international conflicts. However, it is unclear how to apply the U.N. Charter to cyber conflict, and the CFAA is another potential barrier to implementing active defense due to its broad prohibitions.

Even with these potential barriers, mitigative counterstriking is the most readily justifiable type of counterstrike in an active defense regime. We further argue that implementing mitigative counterstriking capabilities for CNI should become a national security priority to protect CNI against potential hostilities.

Having examined the intersection of elements of active defense with the current legal regime, we also provide recommendations for designing a potential procedure for utilizing mitigative counterstrikes. We suggest that a government-affiliated agency, preferably a public-private partnership, be primarily responsible for the active defense regime. Such an agency would implement guidelines, provide resources for private parties to detect and trace intrusions, share information, and oversee counterstrikes to ensure that they adhere to the principles of mitigation. Finally, we argue that a system to promote active defense and permit mitigative counterstriking should also include a liability rule to protect third party intermediaries whose systems are compromised by attackers.

The hesitation that many commentators and scholars express with regard to using active defense can be attributed in part to the tendency of modern commentary to treat active defense as a singular concept. We argue, however, that active defense consists of three distinct elements: detecting intrusions, tracing the attack back to the attacker, and executing a counterstrike. Further, there are two different types of counterstrikes: retributive counterstrikes, with a goal of punishing the attacker, and mitigative counterstrikes, which strictly adhere to the principles of mitigation. Mitigative counterstrikes can potentially deter future attacks in addition to preserving the right of self-defense in cyberspace.

With this Article, we introduce a new approach to analyzing active defense, as well as provide some suggestions for how to create a system for mitigative counterstrikes. The first priority is to use mitigative counterstriking to protect privately owned CNI. If an active defense system that emphasizes mitigative counterstriking is later broadly implemented to protect other private parties, we suggest that the private parties be in control of detecting intrusions, given the stat-

utory and constitutional concerns raised by directing the government to monitor private networks. The government should carefully oversee mitigative counterstriking measures to ensure consistent application. It is vital that formal policy be set forth while there is still time for thoughtful deliberation and analysis of all of the potential implications of mitigative counterstriking before we are faced with the fallout from a crippling cyberattack.