Illinois Public Law and Legal Theory Research Papers Series No. 11-16

Illinois Program in Law, Behavior and Social Science Research Paper No. LBSS12-08

Self Defense in Cyberspace: Law and Policy

Jay P. Kesan*

Carol M. Hayes**

*Professor and H. Ross & Helen Research Scholar, University of Illinois College of Law

**University of Illinois, College of Law

Abstract

In the last year, public discussion of cybercrime has a few major buzz words, including Stuxnet, zero-day vulnerabilities, Anonymous, HBGary, RSA, and Lockheed Martin. The Stuxnet worm exploited four zero-day vulnerabilities in the summer of 2010 and damaged Iranian nuclear infrastructure. In February 2011, security firm and government contractor HBGary Federal announced that they intended to go after individuals involved in the loose knit group of hackers that call themselves Anonymous, and Anonymous responded by hacking into HBGary Federal's systems and publishing confidential company emails on the web that revealed some of HBGary Federal's questionable activities. Security firm RSA, which produces SecurID two-factor authentication technology, revealed in March 2011 that information relating to this technology was obtained by advanced hacking techniques. The effects of the RSA breach started to become more apparent in May 2011 when government contractor Lockheed Martin experienced cyber intrusions using counterfeit SecurID security keys. In August 2011, another term was added when McAfee's research division announced the results of an investigation: Five years. McAfee asserts that for the last five years, major cyber intrusions have been occurring, likely by the same actor or group, giving the intruders access to national secrets, SCADA configurations, source code, design schematics, and much more. The source of these intrusions is not known, though many suspect state actors, and Republican presidential primary candidate Jon Huntsman stated during the Republican presidential debates that he considers such cyber attacks to be acts of war.

With the significant technological development occurring in this area, the legal framework is still lacking. There is arguably not currently an effective way of addressing cybercrime under criminal law, and private remedies through lawsuits are likely to be inadequate. Congress has been making progress towards addressing cybersecurity issues, but between a Congressional Cybersecurity Caucus, a Cybersecurity Task Force, and several different congressional committees that assert jurisdiction over cybersecurity issues, clear congressional consensus on the topic is likely to be a long time coming. The urgency of the topic and the current lack of guidance leaves potential targets with the need to defend their own systems. Our research began with a broad focus: analyzing the legal framework surrounding cybersecurity issues and making recommendations for implementing a framework that would permit the use of active self-defense in cyberspace ('active defense'), as opposed to requiring network administrators to always rely solely on the passive defense options of firewalls, patches, and antivirus software. Active defense includes technologies that detect attacks, trace the attacks to their source, and enable counterstrikes to halt the attacks.

Self Defense in Cyberspace: Law and Policy

Jay Kesan, *University of Illinois*, and Carol M. Hayes, *University of Illinois*

I. Introduction

In the last year, public discussion of cybercrime has a few major buzz words, including Stuxnet, zero-day vulnerabilities, Anonymous, HBGary, RSA, and Lockheed Martin. The Stuxnet worm exploited four zero-day vulnerabilities in the summer of 2010 and damaged Iranian nuclear infrastructure.[1] In February 2011, security firm and government contractor HBGary Federal announced that they intended to go after individuals involved in the loose knit group of hackers that call themselves Anonymous, and Anonymous responded by hacking into HBGary Federal's systems and publishing confidential company emails on the web that revealed some of HBGary Federal's questionable activities.[2] Security firm RSA, which produces SecurID two-factor authentication technology, revealed in March 2011 that information relating to this technology was obtained by advanced hacking techniques.[3] The effects of the RSA breach started to become more apparent in May 2011 when government contractor Lockheed Martin experienced cyber intrusions using counterfeit SecurID security keys.[4] In August 2011, another term was added when McAfee's research division announced the results of an investigation: Five years. McAfee asserts that for the last five years, major cyber intrusions have been occurring, likely by the same actor or group, giving the intruders access to national secrets, SCADA

[1] William J. Broad, John Markoff, and David E. Sanger, Israeli Test on Worm Called Crucial in Iran Nuclear Delay, NY Times (Jan. 15, 2011), available at http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html.

[2] Tim Greene, Anonymous Forces HBGary Federal CEO to Step Down, Network World (Feb. 28, 2011), http://www.networkworld.com/news/2011/022811-hbgary-anonymous-ceo-resigns.html.

[3] Arthur W. Coviello, Jr., Open Letter to RSA Customers, http://www.rsa.com/node.aspx?id=3872; Tony Bradley, RSA SecurID Hack Shows Danger of APTs, PCWorld (Mar. 18, 2011), http://www.pcworld.com/businesscenter/article/222555/rsa_securid_hack_shows_danger_of_apts.html.

[4] Tony Bradley, Lockheed Martin Attack Signals New Era of Cyber Espionage, PCWorld (May 28, 2011), http://www.pcworld.com/businesscenter/article/228927/lockheedmartin_attack_signals_new_era_of_cyber_espionage.html.

configurations, source code, design schematics, and much more.[5] The source of these intrusions is not known, though many suspect state actors, and Republican presidential primary candidate Jon Huntsman stated during the Republican presidential debates that he considers such cyber attacks to be acts of war.[6]

With the significant technological development occurring in this area, the legal framework is still lacking.[7] There is arguably not currently an effective way of addressing cybercrime under criminal law, and private remedies through lawsuits are likely to be inadequate. Congress has been making progress towards addressing cybersecurity issues, but between a Congressional Cybersecurity Caucus, a Cybersecurity Task Force, and several different congressional committees that assert jurisdiction over cybersecurity issues, clear congressional consensus on the topic is likely to be a long time coming.[8]

The urgency of the topic and the current lack of guidance leaves potential targets with the need to defend their own systems. Our research began with a broad focus: analyzing the legal framework surrounding cybersecurity issues and making recommendations for implementing a framework that would permit the use of active self-defense in cyberspace ("active defense"), as opposed to requiring network administrators to always rely solely on the passive defense options of firewalls, patches, and antivirus software. Active defense includes technologies that detect attacks, trace the attacks to their source, and enable counterstrikes to halt the attacks. Along the

[5] Posting by Dmitri Alperovitch, Revealed: Operation Shady RAT, to McAfee Labs Blog Central, Aug. 2, 2011, http://blogs.mcafee.com/mcafee-labs/revealed-operation-shady-rat.

[6] China Cyberwar Topic Raised in Republican Presidential Debate, National Cyber Security (Aug. 12, 2011), http://nationalcybersecurity.com/2011/08/china-cyberwar-topic-raised-in-republican-presidential-debate/.

[7] This piece is derived from a larger piece the authors have written and which is forthcoming in the Spring 2012 issue of the Harvard Journal of Law and Technology. Jay Kesan and Carol Hayes, Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace (Apr. 2011 Working Paper, Illinois Public Law Research Paper No. 10-35), Harvard Journal of Law and Technology, Forthcoming.

[8] Ben Pershing, On Cybersecurity, Congress Can't Agree on Turf, Wash. Post (Jul. 18, 2011), available at http://www.washingtonpost.com/politics/on-cybersecurity-congress-cant-agree-on-turf/2011/07/18/gIQACGCWMI_story.html.

way, we noted substantial uncertainty in the scholarly literature towards the idea of permitting "hack back," the street term for the counterstriking portion of active defense.[9] This uncertainty is what we will first attempt to resolve.

At its core, cyber counterstriking is about two things: deterring attackers, and ensuring that 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 through the existence of one or both of the following elements: punishing the attacker through the infliction of unacceptable costs, or denying the attacker success.[10] It is these two elements of deterrence that have led us to apply the terms "retributive counterstriking" and "mitigative counterstriking" to the counterstriking portion of active defense.

In the cyber context, a "counterstrike" can involve a number of actions. It can involve the target redirecting the attacker's packets back at the attacker, executing its own Denial of Service (DoS) attack at the attacker to knock the attacker's systems off-line, infecting the attacker's system with a virus or worm to permit the victim to take control, and a number of other options or combinations of options. Additionally, there is now evidence that "cyber contractors" exist as part of what some have termed the new "military digital complex," whose work involves the creation of offensive cyber technologies that could have application in the context of counterstriking.[11]

The goal of a counterstrike can also vary between punishing the attacker or simply

---

[9] *E.g.*, Bruce P. Smith, *Hacking, Poaching, and Counterattacking: Digital Counterstrikes and the Contours of Self-Help*, 1 J.L. ECON. & POL'Y 171, 180 (2005) (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/ (referring to the act of retaliating against hostile cyber intrusions).

[10] NAT'L RESEARCH - COUNCIL OF THE NAT'L ACADS., TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 40 (William A. Owens et al. eds., 2009) [hereinafter "NRC REPORT"].

[11] Haroon Meer, *Lessons from Anonymous on Cyberwar*, AL JAZEERA, Mar. 10, 2011, http://english.aljazeera.net/indepth/opinion/2011/03/20113981026464808.html.

mitigating the harm to the target. The former can be termed "retributive counterstriking," which we argue should remain under the sole control of the military as a national security matter at this stage because of the sensitivity of constitutional issues and international law issues. "Mitigative counterstriking," on the other hand, can be defined as active efforts to mitigate harm to a victim system in a manner that is strictly limited to the amount of force necessary to prevent the victim from being further damaged. We recognize that there may be some overlap between retributive and mitigative counterstriking, since an incidental consequence of mitigative counterstriking (harm to the attacker's system) may be a primary goal of retributive counterstriking. However, the goal of mitigative counterstriking must be to *mitigate* damage from a *current and immediate* threat, and we urge that whatever measures are deployed must be justifiable under this mitigation framework.

Active defense currently exists in legal limbo, primarily due to the current view of cyber counterstrikes. Our proposal in this area is both modest and bold. It is 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, and we acknowledge that it does not apply to all cyberattack situations. It is at the same time bold because we are advocating a significant shift from the prevailing approach to cybercrime. In recommending a new regime, we have chosen to focus on mitigative counterstriking as a starting point for two reasons. First, because it is likely to be more effective than passive defense at accomplishing the goal of deterrence by denial, and second because mitigative counterstriking is an essential concept in endowing network administrators with the right to actively defend their property, and ensuring that the right to defend oneself and one's property becomes recognized in the cyber realm in a manner similar to the physical realm. The current regime creates an unconscionable situation where parties are

expected to give up a right to actively defend themselves against threats, limited instead to installing passive defense measures and crossing their fingers that it will be enough, with little to no practical recourse available through criminal enforcement or civil litigation.

Currently, the biggest problem is that there is no legal method of responding 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 certain types of cyberattacks against sensitive systems such as hospitals, government defense systems, and critical national infrastructure (CNI), and urge that implementing a regime to permit these sorts of counterstrikes should be a priority. There is some evidence that the private sector has been utilizing this sort of technology to protect their systems without reporting it publicly,[12] effectively acting as cyber vigilantes in the current regime where such behaviors are, at best, a gray area, and at worst, illegal. Currently, the premise of mitigative counterstriking is treated like the proverbial elephant in the cyber room, with most legal commentators largely ignoring it. We argue that this lack of treatment is due to the lack of an analytical framework distinguishing between the perceived vigilantism of retributive counterstriking and the necessity of the availability of self-help through mitigative counterstriking.

II. We thus propose a new policy and legal regime to address the threat of cyberattacks through the use of "active defense" and "mitigative counterstriking." There is a grave need for standardization in an approach to mitigative counterstrikes, 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 the premise of counterstrikes of any variety can potentially raise a number of legal and

[12] Ruperto P. Majuca & Jay P. Kesan, Hacking Back: Optimal Use of Self-Defense in Cyberspace 5-6 (Mar. 2009 Working Paper, Illinois Public Law Research Paper No. 08-20), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1363932.

diplomatic concerns. While additional analysis and technological development may be beneficial before implementing a broad self-defense regime, we urge that the first priority should be implementing mitigative counterstriking capabilities to protect CNI.

LAW RELEVANT TO THE USE OF SELF-DEFENSE

This section will examine the possible application of current law to the notion of cyber self-defense. Because our thesis argues in favor of the viability of a mitigative counterstriking regime to ensure that self-defense becomes recognized in the cyber realm as well as the physical realm, this section 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 would lead to a reading of the current laws as permitting actions in self-defense, provided such actions adhere to the principles of mitigation. In our view, one of the main barriers to an optimal active defense regime focused on mitigative counterstriking is that current 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 in the best interest of society. This section will examine relevant laws as well as barriers in the domestic and international law context and provide some suggestions about how to create a policy that permits active defense and mitigative counterstriking without running counter to the law.

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, and the potential legal barriers differ based on the answer. The two primary options are to permit the target to counterstrike against the attacker,

or to require mitigative counterstrikes to be conducted solely by the government. If the latter option is adopted, counterstrikes would be state action giving rise to potential constitutional violation claims. If the former option is adopted, there are a number of potential legal implications that private parties must consider.

If individuals are permitted to engage in active defense, this could lead to many potential legal liability issues. Some have noted that the simple act of determining an attack's source through traceback may violate the Computer Fraud and Abuse Act (CFAA) and the Electronic Communications Protection Act (ECPA), and that using mitigative counterstrikes to interrupt an attack and mitigate damage would most likely violate the CFAA.[13] However, the common law has long recognized that individuals may be privileged to defend themselves and to defend property to prevent a crime from being committed,[14] as well as to use self-help to abate a nuisance.[15] Self-defense utilizing lethal actions generally must not be used except as a last resort, but it is unlikely that mitigative counterstrikes would be considered "lethal." Non-lethal actions in self defense or defense of property would likely not be required to be used as a last resort.[16]

Under the common law, if an individual wishes to use force in defense of property, they must first generally ask the criminal to stop (unless such a request would be futile or counterproductive), there must be a reasonable belief that force is necessary, and the amount of force used must be reasonable.[17] It's possible that a party who is prosecuted or sued because of taking actions pursuant to a mitigative counterstrike could claim that they were defending themselves and their property, but evidence does not suggest that this defense has yet been

[13] NRC REPORT, *supra* note 10, at 37.
[14] *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, and that while persons may be privileged to defend property, they are not entitled to retaliate in response to the crime. *Id.* at 205.
[15] Neal Katyal, *Community Self-Help*, 1 J.L. ECON. & POL'Y 33, 61 (2005).
[16] NRC REPORT, *supra* note 10, at 209-10.
[17] Katyal, *supra* note 15, at 61.

invoked.[18] But what if an innocent third party is harmed during a counterstrike? If actions in defense of property are misdirected and result in harm to an innocent third party, 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 efforts resulted in erroneous information.[19] Erroneous use of mitigative counterstrikes could potentially lead to civil liability, though the liability might be reduced based on contributory negligence of the injured party.[20]

However, we argue in Section III that permitting private individuals to engage in mitigative counterstriking directly would be undesirable because such a position would permit individuals to make case-by-case decisions about counterstriking while applying standards that are not consistent from one individual to the next. Additionally, mitigative counterstriking could also potentially have international law implications even if committed by private actors, so consistent standards are essential. This need for consistency suggests that the government should be placed in control of mitigative counterstriking. Even if individuals were permitted to engage in mitigative counterstriking, there still may be cyberattacks against government computers for which mitigative counterstrikes are an appropriate response. This raises another issue related to self-defense: government actors taking action in defense of the country.

If the government conducts mitigative counterstriking, either to defend its own systems or on behalf of private actors, the next question is which part of the United States government could respond using mitigative counterstriking. Could, or should, cyber counterstrikes be a solely military matter? Congress has explicit warmaking powers under the Constitution,[21] while the President is given the authority as Commander-in-Chief and has some limited ability to order the

[18] NRC REPORT, *supra* note 10, at 37.
[19] *Id.* at 210.
[20] *Id.*
[21] U.S. CONST. art. 1, s. 8, para. 11.

military to take action prior to Congress giving explicit authorization.[22] Acting in self-defense is often regarded as the least controversial basis for the President ordering the armed forces to undertake hostile actions.[23] Mitigative *or* retributive counterstrikes thus could likely be launched by the nation's armed forces without the explicit authorization of Congress under the order of the President.[24] The position of the Office of General Counsel of the DOD regarding active defense and cyber counterstriking is that there must be a provocation that's attributable to an agent of the nation where the attack originated, or the originating state must be a sanctuary nation that has failed to put a stop to the attacker upon being notified of the activities and given a chance to address it.[25]

Some provisions of U.S. law, however, may restrict the ability of the government to implement a system permitting counterstriking in this manner. The Posse Comitatus Act prohibits the armed forces from taking actions to execute domestic law unless explicitly authorized.[26] This suggests that the DOD would be prohibited from conducting cyber operations to support domestic law enforcement.[27] There are two constitutional exceptions to the Posse Comitatus Act, however: (1) When there is an emergency and 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.[28] Condron suggests that responses to cyberattacks on CNI would fall within one of these constitutional exceptions, so the Posse

[22] U.S. CONST. art. 2 s. 2 para. 1; 50 U.S.C. § 1541 (2008) (setting forth the purpose and policy of the War Powers Resolution, codified in Chapter 33 of Title 50).

[23] NRC REPORT, *supra* note 10, at 232.

[24] *Id.* at 55. Under the Constitution, the DOD cannot use force to defend the United States unless authorized by the President. Walter Gary Sharp, Sr., *The Past, Present, and Future of Cybersecurity*, 4 J. NAT'L SECURITY L. & POL'Y 13, 24 (2010) (noting, however, that the U.S. National Guard is given the authority "to perform duties under the laws of the states.. or under their federal service.").

[25] 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, 239 (2002).

[26] NRC REPORT, *supra* note 10, at 288; Sean M. Condron, *Getting It Right: Protecting American Critical Infrastructure in Cyberspace*, 20 HARV. J.L. & TECH. 403, 419 (2007).

[27] NRC REPORT, *supra* note 10, at 288.

[28] Condron, *supra* note 26, at 419-20.

Comitatus Act might not act as a complete bar on DOD domestic involvement in cyber defense.[29]

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 critical infrastructure.[30] The statute includes a provision indicating that private owners of critical infrastructure could contact DHS for assistance with protecting CNI.[31] However, we stress that this is a voluntary provision. Similar provisions of the U.S. Code restrict the government to intervening in private citizens' cybersecurity matters only upon voluntary election of the citizens, even operators of CNI, putting the fate of private sector cybersecurity in their own hands. These providers may hesitate to request government assistance, however, out of concerns about sharing their customers' confidential data. To this end, under the Federal Wiretap Act and 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.[32]

The government, it seems, is in a good position to take actions in defense of private parties to mitigate harm to systems as a result of cyberattacks. However, commentators point out a number of potential restrictions on the federal government that would hinder federal

[29] *Id.*

[30] John Grant, *Will There Be Cybersecurity Legislation?*, 4 J. NAT'L SECURITY L. & POL'Y 103, 106 (2010); Sharp, *supra* note 24, at 16. The GAO, however, has been critical of DHS's performance in this area. Grant, *supra* note 30, at 106; *see also* 6 U.S.C. § 131 (defining terms relevant to the Critical Infrastructure Information Act of 2002).

[31] 6 U.S.C. § 143 (2008). No public record currently exists suggesting that DHS has been authorized to utilize active defense on behalf of any member of the private sector, including owners of critical infrastructure. NRC REPORT, *supra* note 10, at 203.

[32] Gregory T. Nojeim, *Cybersecurity and Freedom on the Internet*, 4 J. NAT'L SECURITY L. & POL'Y 119, 126 (2010).

implementation of a full active defense regime. Monitoring private networks for cybersecurity issues could potentially cause the government to run into issues with the ECPA, the CFAA, the Computer Security Act of 1987, the Federal Wiretap Act, and the Fourth Amendment.[33] For this reason, we suggest that the initial stage of active defense, the use of intrusion detection systems (IDS), should be the responsibility of the private parties whose systems are eligible for federal protection.

If the government responds using a mitigative counterstrike pursuant to a model of active defense, some critics express concern that there may be a Due Process problem because the target does not receive a fair trial.[34] However, our position is that mitigative counterstriking must be a proportionate response aimed at mitigating harm to a target, and therefore properly executed mitigative counterstrikes are not punishment that would raise Due Process concerns. 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.

B. International Law

There are a number of international law provisions that address issues of self-defense and that are relevant to the current topic. Self-defense under U.N. Charter Article 51, anticipatory self-defense under customary international law (CIL), and reprisals are all possible means under which active defense and mitigative counterstriking can be analyzed. Oppenheim's treatise on

[33] John N. Greer, *Square Legal Pegs in Round Cyber Holes: The NSA, Lawfulmess, and the Protection of Privacy Rights and Civil Liberties in Cyberspace*, 4 J. NAT'L SECURITY L. & POL'Y 139, 143-44 (2010); Nojeim, *supra* note 32, at 125-26.

[34] Katyal, *supra* note 15, at 61 (noting the argument but countering that the same would be true of any use of self defense). The Fifth Amendment guarantees adequate procedures to ensure against improper deprivation of life, liberty, or property. U.S. CONST. amend. V. Another potentially relevant clause in the 5th amendment is the Takings Clause, which prohibits the government from taking private property for public use. If state actions cause damage to someone's computer due to cyber counterstriking, this could potentially be a taking under the 5th amendment. It is unclear, however, how Supreme Court Takings jurisprudence would apply in the cyber context. Beyond the threshold question of whether a taking occurred, a takings argument would likely fail unless it is shown that the interference with computer property was related to a "public use," which is unlikely unless the situation involves a government-run botnet.

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.[35] The presence of a right of self-defense has been argued to increase the deterrent effect of international law,[36] which supports our argument that permitting mitigative counterstrikes is likely to improve the deterrent effect of a legal regime addressing cyberattacks.

Whether a state is privileged to act in self-defense is governed by Article 51 of the U.N. Charter. This turns on whether the act being responded to is an "armed attack."[37] Because of the complicated nature of getting Security Council approval for a use of force, some argue that it is more likely that a state would use self-defense in responding to cyberattacks in lieu of seeking Security Council approval.[38] The language of Article 51 refers to "the inherent right of individual or collective self-defense" in the event that an armed attack occurs against a U.N. Member.[39] This suggests that individual actions may be covered by the U.N. Charter, just like state actions. Since the language seems to permit it and the reality of cyber warfare may even require it, it's possible that considerations relating to articles of the U.N. Charter should be interpreted as potentially applying to private actors in the context of cyberspace where national boundaries are at best amorphous. But who should determine whether a cyberattack is severe enough to justify

[35] NRC REPORT, *supra* note 10, at 243 (citing 1 OPPENHEIM'S INTERNATIONAL LAW 412 (9th ed. 1992)). Some have noted that espionage is also related to a state's right to use self-defense. Arie J. Schaap, *Cyber Warfare Operations: Development and Use Under International Law*, 64 A.F. L. REV. 121, 140 (2009) (noting commentary about the right of nations to engage in espionage during peacetime).

[36] Graham H. Todd, *Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition*, 64 A.F. L. REV. 65, 71 (2009).

[37] NRC REPORT, *supra* note 10, at 34*; see* Jensen, *supra* note 25, at 208 (questioning whether a cyberattack triggers the right to self defense or whether a nation cannot use self defense in the absence of a more traditional military attack).

[38] David E. Graham, *Cyber Threats and the Law of War*, 4 J. NAT'L SECURITY L. & POL'Y 87, 89 (2010).

[39] U.N. Charter art. 51.

self-defense under Article 51? Some suggest that system administrators will need to be entrusted with characterizing an intrusion and deciding if mitigative counterstriking is appropriate.[40] This raises a number of concerns, and we emphasize that a mitigative counterstriking regime should include a number of provisions to ensure that high level government leaders are involved with the setting of standards to determine whether mitigative counterstriking is appropriate.

Article 51 preserves an inherent right of self-defense in response to armed attack,[41] but the use of self-defense is limited by requirements for necessity and proportionality.[42] Evaluating whether the necessity requirement is met involves determining whether a more peaceful resolution would be possible, evaluating the nature of the aggression and each party's objectives, and estimating the likelihood that intervention would be effective.[43] Proportionality requires the response to be limited to the amount of force that is reasonably necessary to interrupt an ongoing attack or to deter future attacks,[44] but does not require the response to be limited to the amount or type of force initially used by the attacker.[45] In addition to necessity and proportionality, self-defense under *jus ad bellum* also requires immediacy, but the principle of immediacy is very broad under international law and would permit a response to occur days or weeks after the initial attack.[46] Cyber counterstrikes would be limited by these three principles, and could not

[40] 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, 59, 73 (2009). Lin suggests that senior policymakers would ideally be responsible for distinguishing between cyber exploitations and cyberattacks, but notes that given the detachment of policymakers from the operational details of a mission, such characterization is likely to be placed on field operators who might not be as sensitive to the important diplomatic difference between cyber exploitations and cyber attacks. Herbert S. Lin, *Offensive Cyber Operations and the Use of Force*, 4 J. NAT'L SECURITY L. & POL'Y 63, 82-83 (2010).

[41] Sklerov, *supra* note 40, at 30-31 (asserting that the right of self defense is an inherent right "derived from the fundamental right of states to survive.").

[42] Graham, *supra* note 38, at 89; Jensen, *supra* note 25, at 217-18; Sklerov, *supra* note 40, at 32-33; Todd, *supra* note 36, at 98.

[43] Graham, *supra* note 38, at 89; Todd, *supra* note 36, at 98.

[44] Graham, *supra* note 38, at 89; Todd, *supra* note 36, at 98.

[45] Schaap, *supra* note 35, at 148. However, the use of kinetic weapons to respond to cyberattacks might be disproportionate and less effective than responding in kind. Graham, *supra* note 38, at 99.

[46] Condron, *supra* note 26, at 414-15.

amount to retaliatory or punitive actions.[47] As a matter of international law, therefore, it is essential that execution of mitigative counterstrikes strictly adhere to the principles of mitigation and not take on the goals of retributive counterstriking.

Accepting that in some situations, a cyberattack can be an "armed attack," some argue that a state still cannot legitimately respond in self-defense unless the state establishes that another state is responsible for the cyberattack.[48] If another state cannot be held responsible, the Law of War might not be effective at addressing a situation where non-state actors targeted another state, even if they were targeting the other state's CNI.[49] Because of the attribution problem, states that are the victim of an international cyberattack are forced into a "response crisis": even if they could attribute the attack to a specific non-state actor, they couldn't intervene in the domestic affairs of the other state, so they generally have to rely on the other state to address it through their domestic criminal law system.[50] Some commentators suggest that the right of self-defense could be preserved by permitting responsibility to be imputed to the state in the event of an attack by a third party located within the state's borders.[51] Currently, international law permits a state to be held responsible if they have "indirect responsibility" for the actions of third parties within their borders, which means that the state had neglected its duty to prevent persons within its borders from perpetrating crimes against other states.[52] However, the victim state's targets must be limited to the non-state actor attacker unless their lawful cross-border

[47] *Id.* at 415.

[48] Graham, *supra* note 38, at 92.

[49] Jensen, *supra* note 25, at 234 (noting the difficulty of responding to cyberattacks from non-state actors); Sklerov, *supra* note 40, at 2. Sklerov notes, however, that most legal scholars believe that the Law of War can be applied to address attacks by non-state actors. Sklerov, *supra* note 40, at 39.

[50] Sklerov, *supra* note 40, at 38. However, in extreme situations, it may be recognized that a state has a right to respond to non-state actors in self-defense, such as in the case of al Qaeda attacks on the United States on 9/11, when the United Nations Security Council reaffirmed that the United States has the right to engage in self-defense under Article 51. *Id.* at 40-41.

[51] Graham, *supra* note 38, at 93; Sklerov, *supra* note 40, at 38.

[52] Graham, *supra* note 38, at 96; *see also* Sklerov, *supra* note 40, at 12, 48 (noting scholars who have posited that it is unnecessary to conclusively attribute attacks because of states' ability to respond to non-state actors' attacks with force under international law).

operations are opposed with force by the host state.[53]

Even when the attack's source can be identified, however, the system administrator for the victim state's system must also map the attacking computer system in order to determine the system's functions and what consequences are likely to result from shutting the system down.[54] This would help ensure that the use of mitigative counterstriking complies with the principles of distinction and proportionality.[55] Because of current technical limitations, it would likely be impossible to make a "surgical strike" against a specific attacker, and harm to innocent systems could potentially be viewed as violations of the Law of War's principles of distinction and proportionality.[56] 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.

Another debated issue is whether mitigative counterstriking can only be undertaken by persons who would be considered "lawful combatants" under the Law of War.[57] If a private party conducts a mitigative counterstrike against a foreign attacker and causes harm to other citizens of that state, the private party could potentially lose their status as a protected noncombatant. This distinction between lawful combatants and noncombatants supports our argument that the government should be responsible for many aspects of active defense, especially mitigative counterstriking. Such a regime would serve to not only provide consistency; it would also protect private parties from being treated as combatants and thus valid targets for military strikes under the Law of War.

---

[53] Sklerov, *supra* note 40, at 49.
[54] *Id.* at 81-82.
[55] *Id.*
[56] Graham, *supra* note 38, at 99-100.
[57] *Id.* at 97.

Under international law, states have a duty to prevent their territories from being used by non-state actors to commit crossborder attacks.[58] Sklerov suggests that because of this duty, states also have a legal authority to use cyber counterstrikes if the attacker's host state has insufficient criminal laws or declines to enforce them against the attacker.[59] The current international law paradigm limits the response options that are available, so it is difficult to respond to an attack without potentially violating international law.[60] However, some argue that responding to a cyberattack with a cyberattack is more likely to comply with the *jus in bello* principles of distinction, humanity, necessity, and proportionality than would the use of kinetic attacks in response to cyberattacks.[61]

International law also includes the concept of anticipatory self-defense, which is permitted when the need for self-defense is instant and overwhelming, there is no other way to respond, and there is no time for deliberation.[62] The immediacy requirement of anticipatory self-defense is relative to the strength of the state, and requires that the aggressor has committed to an armed attack and that the defender's ability to defend itself would be hindered if it waited to respond.[63] If there is evidence of an ongoing campaign against a state, anticipatory self-defense may be authorized because future armed attacks are considered imminent.[64]

There is disagreement among scholars about how Article 51 should be interpreted with regard to whether it permits anticipatory self-defense. Some say that self-defense is strictly

[58] Sklerov, *supra* note 40, at 12.

[59] *Id.* 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.

[60] 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, 452 (2009).

[61] Sklerov, *supra* note 40, at 79.

[62] This is the *Caroline* standard of anticipatory self-defense that arose concerning an attack on a ship in 1837. NRC REPORT, *supra* note 10, at 243; Hoisington, *supra* note 60, at 450; Jensen, *supra* note 25, at 218-19; Sklerov, *supra* note 40, at 34, 48.

[63] Sklerov, *supra* note 40, at 35.

[64] *Id.* at 36.

limited to responding to an "armed attack."[65] 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 as a response.[66] Some have argued, however, that the requirements of the *Caroline* standard that the necessity for response be "instant, overwhelming, and leaving no choice of means, and no moment for deliberation" make it unlikely that anticipatory self-defense could apply in a cyberattack context.[67]

If self-defense is strictly limited to responding to an "armed attack," a lot of complications then arise due to the nature of cyberattacks, especially the fact that cyberattacks are very unlikely to be viewed as *per se* "armed attacks." Arguments about characterizing cyberattacks as armed attacks often look to the traits, consequences or effects of a cyberattack to characterize it as an armed attack.[68] It would be very difficult to argue that a nation is on the verge of an armed attack when the definition of "armed attack" in the cyberattack context is primarily backward-looking.[69]

Schmitt argues that anticipatory self-defense can be used to address cyberattacks if three factors are present: First, the attack is part of an overall operation that culminates in an armed attack; Second, the attack is irrevocable as a step towards an imminent and unavoidable attack; Third, the anticipatory response to the attack is undertaken at the last possible moment to counter the attack.[70] This creates a high bar, however, so we suggest that anticipatory self-defense would be largely unavailable as a justification for counterstriking.

---

[65] Condron, *supra* note 26, at 412-13

[66] NRC REPORT, *supra* note 10, at 243; Condron, *supra* note 26, at 412-13; Sklerov, *supra* note 40, at 31-32.

[67] Graham, *supra* note 38, at 90.

[68] *See* Jensen, *supra* note 25, at 224-25.

[69] *See id.* at 221 (concluding that there would be no anticipatory self-defense for computer network attacks if such attacks are always viewed as falling below the armed attack threshold). Jensen provides an analysis of the contrasting views of Schmitt and Sharp and concludes that while Schmitt's view of international law is more accurate, Sharp's is more forward looking. *Id.* at 228.

[70] *Id.* at 225.

Our analysis leads us to conclude that using mitigative counterstriking to respond to an ongoing attack, such as a DDoS attack, would likely be consistent with international law. Additionally, the literature notes that anticipatory self-defense may be authorized when evidence suggests an ongoing campaign against a state.[71] Therefore, it is possible that mitigative counterstriking could be used against a party that previously completed a cyber "armed attack" against the state if there is evidence that the prior attack was part of an ongoing campaign and thus future cyber "armed attacks" of the type just experienced are "imminent."

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.[72] Reprisals themselves, though, may not involve a "use of force," and they must meet three additional requirements to be considered reprisals: (1) the countermeasure must be in a state versus state context; (2) the defending state told the aggressor state to stop; and (3) the countermeasure's effects are commensurate with the harm suffered.[73] Reprisals, therefore, would likely not be an option if a state is looking to respond to an attack by a non-state actor. Additionally, reprisals would be unavailable as an option 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," and that a cyberattack thus does not violate Article 2(4) of the U.N. Charter, 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 "use of force" by a foreign state.[74]

---

[71] Sklerov, *supra* note 40, at 36.
[72] Jensen, *supra* note 25, at 220.
[73] Sklerov, *supra* note 40, at 36-37.
[74] As noted, however, reprisals are potential responses to a "use of force" that cannot rise to the level of "use of force" themselves. If cyberattacks are not uses of force, a mitigative counterstrike would not be a reprisal. However, a cyber counterstrike to a non-cyberattack "use of force" that doesn't rise to the level of an "armed attack" would potentially be a way for a state to protect its interests without resorting to the U.N. Security Council.

III. Policy Concerns Relating to Mitigative Counterstriking

In the previous section, we established that mitigative counterstriking can be justified under current law governing self-defense, and described various issues that might arise in the context of both domestic and international law. In this section, we examine various new policy issues that may be raised coinciding with the 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 government to take responsibility for mitigative counterstriking, and the potential role of public-private partnerships. We also provide suggestions for possible procedures for mitigative counterstriking and how to protect third parties who might be harmed as a result of a counterstrike.

A. The When and Who of Active Defense and Mitigative Counterstriking

When making suggestions relating to active defense and mitigative counterstriking, two of the most important questions are: when an active defense regime could be implemented, and by whom. These are fundamental issues that underlie our goal of implementing a broad active defense regime in a socially optimal and consistent manner.

1. Relevant types of intrusions

The first important consideration is the type of intrusions that could be appropriately addressed using mitigative counterstriking. For our purposes, the key point in the active defense process is the detection stage. Because of the nature of IDS as requiring multiple attempts at accessing the target, mitigative counterstriking would likely not be applicable in circumstances where the intrusion is a single event, since there would not be a continuing threat to mitigate. There are two types of intrusion that we anticipate as being appropriate to address by mitigative counterstriking: DDoS attacks and spiders.

One way that a DDoS attack can be undertaken is for the attacker to compromise a large number of computers to create a hoard of zombie systems in order to flood a target with data to knock it off line. When an attacker undertakes a DDoS attack of this type, he must first identify a vulnerability to target and then disseminate malicious code to take advantage of that vulnerability (like a virus or a worm) in a large number of systems (perhaps hundreds of thousands). Once the attacker has control of this zombie hoard, he has at his disposal an army of computers that can be ordered to attack repeatedly until the target is taken out. The repetitive nature of a DDoS attack makes it well-suited for the detect-trace-counterstrike pattern of active defense.

The use of spiders to mine data would be categorized as cyber exploitation, rather than cyberattack, because the goal is to obtain data, not to cause immediate harm.[75] Because the intruder accesses the target system repeatedly, there would likely be sufficient activity for a firm's IDS to detect a pattern, making the use of spiders another kind of intrusion that *can* be interrupted by a mitigative counterstrike 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.

In terms of severity, it is important to develop a standard to determine whether an intrusion is sufficiently severe to justify a mitigative counterstrike. This could potentially be done by applying tests that have been used by other researchers in analyzing whether international law would apply to prohibit either cyberattacks or mitigative counterstrikes. One option we've considered is that mitigative counterstrikes might be an appropriate response to repetitive attacks that would be considered an "armed attack." We propose using Schmitt's

[75] *See* Lahle Wolfe, What are Robots, Spiders, WebAnts, and Worms?, http://womeninbusiness.about.com/od/internetmarketingandseo/a/what-r-robots.htm (last visited Apr. 1, 2011) (defining robots, spiders, and web crawlers as programs that are designed to collect large amounts of data).

effects-based approach that evaluates whether the effects of a cyberattack are the type of effects that would be interpreted as justifying a counterstrike under Article 51 of the U.N. Charter. If a sufficient framework can be provided to ensure adherence to principles of mitigation, however, a lower threshold might be appropriate. Mitigative counterstriking might thus also be permissible when an attack would be considered a "use of force." Because spiders are exploitations and not attacks, however, spiders would likely not be uses of force, and therefore it is unlikely that it would be justifiable to use mitigative counterstriking to interrupt the use of spiders.

Having established that mitigative counterstrikes would be the most appropriate response in the event of an ongoing DDoS attack, we now turn to who should be responsible for executing mitigative counterstrikes. The three primary options are private industry, government actors, or some hybrid of the two.

2. Private sector participation

When accurate technology is used and no other means of recourse would be practicable, there are potential advantages to permitting the attacked firms to counterstrike directly, including the increased speed with which counterstrikes could be undertaken. However, there are many concerns about permitting this as well. Technology often outpaces legal developments, so private sectors would likely have access to technology that potentially has significant negative effects on third parties, but that essentially exists outside the law. This could lead to hundreds of companies competing to provide IDS, traceback, and counterstrike technologies to thousands of private firms in the absence of any kind of oversight to ensure quality and protect third parties. The lack of technological uniformity could also raise issues. If there is a significant amount of variation and competition among software providers, developers may have incentive to cut costs in order to compete, leading to some software being cheaper but lower quality than others.

Beyond the issues of consistency of implementation and product quality, there is a more significant downside of entrusting mitigative counterstriking to private firms. We assert that there are threshold points where permitting counterstrikes would be the socially optimal solution. However, determining these thresholds requires some sort of standardization. It would be unwise to allow individual companies to make these decisions on a case by case basis. Some companies would be more risk averse, while some may be more inclined to behave like cyber vigilantes. Because it is essential to have a solid framework to ensure adherence to principles of mitigation, it is thus important to not place this significant discretion in the hands of private firms, because that would result in a wide array of differing results. In order to ensure that only socially optimal, mitigation-focused usage of counterstriking occurs, implementation of an active defense program emphasizing mitigative counterstrikes must be standardized. 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 a good agency to set these standards, given their activities in the cybersecurity arena.

If private firms were permitted to directly engage in mitigative counterstriking, one possible restriction that the government could impose would be a requirement that a counterstriking firm have a certain percentage of its capital invested in IT infrastructure. This could potentially help ensure that mitigative counterstriking was only engaged in by firms that had the most to lose from an attack that cripples its IT system. If this sort of restriction is adopted, it should not apply to firms that control essential services such as hospitals and power grids. However, given the significant downsides of permitting private firms to counterstrike directly, an alternative implementation may be advisable. As an alternative to entrusting mitigative counterstrikes to the private firms who are injured by the initial cyber intrusions, the

government (or a government contractor) may also be placed in charge of any counterstrike deemed necessary.[76] This option is considered in the following section.

3. Government involvement

The next option we examine is whether the government should be placed in charge of conducting mitigative counterstrikes. This proposal has several advantages, though there are also some potential pitfalls that must be carefully monitored. This section proceeds primarily on the theory that there would be fewer downsides to government control of counterstrikes than if private parties were permitted to execute mitigative counterstrikes. 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 designated counterstrike authority when an intrusion is detected. This would more effectively avoid the legal issues that government would encounter as a result of monitoring private networks, including restrictions arising from the ECPA, the CFAA, the Computer Security Act of 1987, the Federal Wiretap Act, and the Fourth Amendment.[77]

If the government were placed in charge of any necessary mitigative counterstrike, this would simplify matters by ensuring technological uniformity in the software utilized for counterstriking. Another advantage of placing the responsibility for mitigative counterstriking on government entities is that there will be uniformity of personnel, and the uniformity can help ensure that all employees responsible for mitigative counterstriking will be adequately informed of the processes and dangers. In addition to uniformity of technology and personnel, requiring mitigative counterstriking to be undertaken by the government would ensure that protection was provided to parties based on need and urgency, rather than based on how much money the parties

[76] *See* NRC REPORT, *supra* note 10, at 7 (suggesting potentially building a government institution to provide private sector entities immediate relief when they are victimized by cyberattacks).

[77] Greer, *supra* note 33, at 143-44; Nojeim, *supra* note 32, at 125-26.

could afford to pay to protect their systems.[78]

In the interests of uniformity and limiting the extra burden on private parties, if the government is placed in full control of this sort of regime, we also recommend that the government obtain IDS technology and supply it to the private parties who will be responsible for monitoring their own networks. The government in that circumstance should also exercise control over the choice of traceback technology that is implemented in order to ensure technological accuracy. However, whether executing traceback should be entrusted to the private parties or the government is not yet fully clear. IDS and traceback technologies are developing rapidly, and having one actor responsible for acquiring the technology will ensure that the best technology is put into place for the benefit of society.

Our analysis also leads us to conclude that a liability rule is important to preserve the optimality of mitigative counterstriking. Targeted firms, under such a liability rule, would be responsible for harm a counterstrike causes to innocent third parties. We also suggest retaining this liability rule if government is responsible for coordinating mitigative counterstrikes. If firms are still held responsible for harm caused to innocent third parties, on the theory that the government, in counterstriking, was acting as an agent of the firm, that would ensure that firms will not capriciously submit a request to the relevant government agency for counterstrike assistance. A potential liability rule is discussed in more detail below.

Another advantage of placing mitigative counterstriking under government control is that such a system would help to control for the dangers of rapid escalation. The future battlefields of cyber wars will likely be found in the private sector. As discussed above, some members of the

[78] This argument is similar to the argument that community law enforcement subsidizes legal protections for the poor, who would not be able to afford the same protections as those with more resources if self-help were the only option to address crime. Katyal, *supra* note 15, at 36 (describing the problem of the atomization of self-help). While we acknowledge that eventually, broad use of mitigative counterstrike may be desirable, at this time the use of such counterstrikes should be prioritized for the most sensitive targets.

private sector are already resorting to self-help to defend themselves against cyberattacks. This could lead to a dangerous pattern of attack-counterstrike-countercounterstrike that will escalate rapidly and cause significant damage. Placing control of mitigative counterstriking with the government could help to control this and prevent potentially dangerous rapid escalation of cyberattacks by strictly limiting counterstrikes to the principles of mitigation.

On the other hand, there are some potential downsides of permitting the government to control all aspects of active defense. As we have previously noted, if the government handled the detecting element of active defense, that could raise a number of issues relating to the monitoring of private networks. We also recommend that the government be responsible for putting active defense technologies in place, including by supplying detection technology to private parties. However, we recognize 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 incentive to ensure that the technology is consistently kept up to date. Additionally, the nature of government action requires that all actions are undertaken slowly and carefully. While this serves to protect third parties from the hasty responses of others, it may cause issues for those who are the actual victims of attacks due to the increase in response time before a mitigative counterstrike can be executed.

There are also potentially severe diplomatic implications. Government involvement could lead to international political conflicts if a government action has negative effects on another nation's government or population. If individual actors in one country executed mitigative counterstrikes against aggressors in another country and inadvertently harmed innocent individuals, the government would likely not be held responsible if it did not somehow encourage the harmful acts. The same government, however, would be the party held responsible

if government-sanctioned mitigative counterstrikes caused harm to innocents in the other country. This sort of accountability could also be an advantage of government involvement, but it would likely only be optimal if world governments uniformly accepted responsibility for regulating active defense and mitigative counterstrikes within their borders. This could ensure that the behavior was addressed consistently between all potentially affected countries.

a. An alternative to pure government control

Even though there are several advantages to permitting the government to have control over counterstriking, it is important to acknowledge the weaknesses of a pure, state-run regime. As noted above, while there is a benefit to having uniformity in software due to a single state entity having control, that benefit exists primarily on the front end, and the benefit would degrade over time if the contractor who supplies the software is not given incentive to continue to improve its product. A purely private regime, on the other hand, would be undesirable because an entirely privatized active defense regime would be unpredictable and difficult to standardize.

The importance of the private sector to the future of handling cyber conflicts cannot be under emphasized, however, since the private sector arguably has an interest in addressing vulnerabilities that is at least equal to that of the government. The private sector also may have access to more advanced technologies and more experts than are readily available to the government, since considerable development is undertaken as part of for-profit ventures. One core competency of the private sector, then, is its potentially superior technological expertise and access to cutting edge technology. The corresponding core competencies of the public sector include access to highly relevant, non-public information, the ability to develop uniform procedures, and access to enforcement mechanisms.

One potential way to address these disparities in strengths is to establish a public-private

partnership to address active defense issues. If the private sector and government routinely coordinated on matters of active defense, this would provide the uniformity and legal benefits of government-coordinated active defense, while taking advantage of the private sector's access to top technologies and experts. However, public-private partnerships can be difficult to implement because of the vast differences between the cultures of private industry and government actors. We urge that finding common ground between private industry and government could be very beneficial in this context. In part because of the weaknesses of either government or private parties acting alone on this topic, we argue that establishing a public-private partnership to design a system to regulate active defense and permit mitigative counterstriking would be the most beneficial approach to this contentious issue.

B. Potential Process for Mitigative Counterstriking

Having evaluated the possible advantages and pitfalls of various approaches to active defense and mitigative counterstriking, the next important consideration is the process that should be followed. Because of the necessity for quick action when engaging in mitigative counterstrikes, the first important point is that the process should contain elements conducive to expedited review.

One possible approach might be to establish a process that in some ways resembles the manner in which wiretapping approvals are obtained. Currently, wiretaps are available through the Foreign Intelligence Surveillance Act (FISA), which provides a process for requesting surveillance of a foreign power or an agent of a foreign power through the FISA court.[79] An analogous process could be developed whereby decisions concerning potential mitigative counterstrikes are made by an independent body staffed by persons skilled in Internet-related legal issues and who are also specialists in matters concerning complicated computer network

[79] 50 U.S.C. § 1805 (2008).

and cyber intrusion issues. Such a body could be responsible for evaluating whether mitigative counterstrike was 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 Department of Defense or the Department of Homeland Security. DHS may be the most logical candidate, since it is currently the agency that is the most involved with national cybersecurity issues.[80] The agency responsible for mitigative counterstriking must also establish criteria to clearly set forth the threshold requirements necessary to justify counterstrikes. When experiencing a cyber intrusion, the entity requiring assistance should be permitted to petition the agency for such assistance, providing specific information about the intrusion and any harm currently inflicted or anticipated to be inflicted if the harm is not mitigated.

The agency in charge of mitigative counterstriking might decide that it would be appropriate to have higher threshold requirements in situations where the victim organization is a private entity versus when the victim organization is a government entity or an operator of CNI, who 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, the burden it will place on society, and

[80] *See* Grant, *supra* note 30, at 106 (noting the involvement of DHS in cybersecurity issues relating to CNI).

whether the policy is politically feasible.[81] If mitigative counterstrikes were adopted as a matter of policy, attackers could also 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 the intermediaries. That would create a new danger of catalytic cyber conflict, whereby a conflict is instigated between two parties because of the actions of a third party.[82] To help blunt the potential for catalytic cyber conflict, the intermediaries must be provided with reasonable protections under the new legal regime to reduce their own incentives to resort to self-help against counterstrikers. The potential effect on third parties is the issue to which we now turn: whether and how to hold mitigative counterstrikers liable for harm to zombie computer owners.

Cyber criminals who engage in cyber intrusions generally seek to avoid getting caught. One method that they use to evade detection is to route their message through other computers on the Internet in order to obscure the origin of their original signal. In addition to using other 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.[83] A firm that is monitoring for such attacks could then initiate the process to execute a mitigative counterstrike, but what if the mitigative counterstrike causes harm to the zombie computers, whose owners were not involved with or aware of the attacker's malicious intentions?

One very persuasive argument is that these third parties, who we will refer to as "oblivious intermediaries," should be protected from damage caused by a mitigative

[81] NRC REPORT, *supra* note 10, at 147 (noting questions including whether active defense should be a last resort, a first resort, or something in between; likely effectiveness of a counterstrike; and which targets should be protected); Debra Wong Yang & Brian M. Hoffstadt, *Countering the Cyber-Crime Threat*, 43 AM. CRIM. L. REV. 201, 213-14 (2006). Other issues to be considered include whether active defense should be automated, whether adopting active defense is a sound diplomatic policy, and the risks of collateral damage from counterstrikes. Sklerov, *supra* note 40, at 82-83.

[82] NRC REPORT, *supra* note 10, at 23, 312.

[83] How Zombie Computers Work, http://computer.howstuffworks.com/zombie-computer3.htm (last visited Apr. 1, 2011).

counterstrike – but if ignorance of the law is no excuse, why should ignorance of the 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 harm caused by mitigative counterstrikes. Thus, enforcement of the rights of the oblivious intermediaries would be difficult, and if the harms are learned of at the same time, it would likely be difficult to differentiate between the harm caused by the attack and the harm caused by the counterattack.

Another important concern is the duty that oblivious intermediary firms owe to themselves. If the oblivious intermediary firms unwittingly became tools of the attacker because of their negligence in maintaining their own 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 consequence of their own negligence. Policymakers could point to the risk of damage due to mitigative counterstrikes as another incentive for computer operators to consistently protect their systems via security updates, firewalls, anti-virus products, and anti-malware products.

As a policy matter, however, such a harsh approach may be inappropriate. A company with a thousand responsible computer-using corporate employees should not necessarily be punished (via the denial of a remedy) for the careless actions of a single employee on the network. It is standard practice to hold a firm responsible for the negligence of its employees, but ineligibility for remedy would be too harsh, since it would be a *per se* rule that does not easily lend itself to flexibility when considering the circumstances of the situation. Therefore, the firm that finds itself as an oblivious intermediary should be afforded remedy by being 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 armies, educational materials should be disseminated to underscore the importance of timely security updates and use of software packages that prevent infiltration and that detect if the system has been compromised. Using education to reduce the number of potential third parties that can be harmed could potentially 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.[84]

Second, if we do not wish to make oblivious intermediaries ineligible for causes of action, what other options would we have at the litigation stage? We suggest allowing the neglect of the oblivious intermediaries to decrease the damages owed. This may be an appropriate compromise to ensure that all firms are provided with the incentive to exercise due care in managing their IT infrastructure. Because of variations in tort law between the states, federal statutory intervention may be necessary, potentially in the form of some type of federal cyber tort statute. Such a statute should include provisions stating that contributory negligence is not a defense available to a mitigative counterstriker in a lawsuit brought by the oblivious intermediary. The statute should, however, make available a comparative negligence option for reducing damages owed. 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

[84] Yasuhide Yamada, Atsuhiri Yamagishi, and 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, 227-28 (2010).

than a firm that lacks any systematic controls of network content and quality. A vulnerability that was the result of a zero-day exploit, in contrast, should not decrease damages owed at all, since it would be almost impossible for a user to prevent his computer from being compromised via an unknown vulnerability.

If the government is placed in control of conducting mitigative counterstrikes, civil liability may be extended by permitting suits by foreign citizens against the United States under the Federal Tort Claims Act (FTCA).[85] The government could resolve the dispute, and then begin a new process to recover the damages from the party that required government assistance. 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.[86] The nature of the Internet age leads to many complications when the question becomes where a cyber harm "arises." One possible solution could be to treat the harm as arising in the state where the counterstrike's effects were first felt and require the dispute to be governed by the tort law for negligence of that state.

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 as in the case of Georgia, to the harm caused to Iranian nuclear infrastructure by the Stuxnet worm. One would not be overstating the matter 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. For this reason, we urge policy makers to be

[85] *See* 28 U.S.C. 1346(b) (2008).

[86] HENRY COHEN AND VANESSA K. BURROWS, CRS REPORT FOR CONGRESS, FEDERAL TORT CLAIMS ACT 5 (Dec. 11, 2007), *available at* http://www.fas.org/sgp/crs/misc/95-717.pdf.

open to discussions of active defense to address these issues. Self-defense, we have argued, is accepted as an essential element of protection 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 to permit mitigative counterstrikes.

The hesitation that many commentators express with regard to active defense can be attributed in part to the tendency of modern commentary about active defense to treat it like a singular entity. We argue, however, that active defense consists of three distinct elements: detecting intrusions, tracing the attack back to the attacker, and executing a counterstrike. The counterstrike, in turn, can be characterized in two primary ways: 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.

The use of self-defense, however, is not without complications. There are questions about how to address harm to oblivious intermediaries, as well as many the difficulties that would arise in the international context if a mitigative counterstrike harmed innocent parties in a foreign country and led to a diplomatic crisis.

In analyzing the existing framework, we observe that parts of the existing framework could potentially support implementation of an active defense regime that permits counterstrikes grounded in the principles of mitigation. There are also potential barriers, such as the language of the CFAA and unclear wording of international treaties like the U.N. Charter, but even with these potential barriers, mitigative counterstriking is the most readily justifiable type of counterstrike that could be involved 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 a potential process for a broader implementation of an active defense regime utilizing mitigative counterstrikes. We suggest that a government-affiliated agency, desirably a public-private partnership, be primarily responsible for the different elements of an active defense regime. This includes implementing guidelines, providing resources for private parties to detect and trace intrusions, and executing counterstrikes to ensure that counterstrikes adhere to the principles of mitigation. Additionally, 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.

With this article, therefore, we introduce a new approach to analyzing active defense, as well as provide some suggestions for how the details of a system for mitigative counterstrikes could be laid out. The first priority is to enable mitigative counterstriking to be used to protect private owners of 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 statutory and constitutional concerns that would be raised by directing the government to monitor private networks, but that mitigative counterstriking measures should be carefully overseen by the government to ensure consistent application. It is vital that formal policy be set forth at this stage, while there is still time for thoughtful deliberation and analysis of all of the potential implications, before we are faced with the fallout from a crippling cyberattack.

* * *