Active Defense: An Overview of the Debate and a Way Forward

Anthony D. Glosson

August 2015

MERCATUS WORKING PAPER

MERCATUS CENTER
George Mason University
3434 Washington Blvd., 4th Floor, Arlington, Virginia 22201
www.mercatus.org

Anthony D. Glosson. "Active Defense: An Overview of the Debate and a Way Forward." Mercatus Working Paper, Mercatus Center at George Mason University, Arlington, VA, August 2015.

Abstract

As the information economy expands, network security threats proliferate. Large-scale data breaches have become something of a fixture in today's news cycle: Target, Sony, Home Depot, JPMorgan Chase—the list goes on. Some estimates place the global costs of cyber insecurity at more than $400 billion. The United States is at something of a crossroads on one particularly crucial security issue: active defense. Sometimes called *hacking back* or *counterhacking*, the practice of confusing, identifying, and even incapacitating an attacker is increasingly catching the attention of security professionals and policymakers. This paper seeks to synthesize the available legal resources on active defense. It confronts the intertwined definitional, legal, and policy questions implicated in the active defense debate. The paper then proposes a legal framework to authorize active defenses subject to liability for third-party damages, an approach grounded in the technical and economic realities of the network security market.

JEL codes: K290

Keywords: cybersecurity, security, privacy, technology, CFAA, Computer Fraud and Abuse Act, hacking, hacking back, active defense, counterhacking, networking, systems administration

Author Affiliation and Contact Information

Anthony D. Glosson
The George Washington University Law School, '15
anthony@anthonyglosson.com

All studies in the Mercatus Working Paper series have followed a rigorous process of academic evaluation, including (except where otherwise noted) at least one double-blind peer review. Working Papers present an author's provisional findings, which, upon further consideration and revision, are likely to be republished in an academic journal. The opinions expressed in Mercatus Working Papers are the authors' and do not represent official positions of the Mercatus Center or George Mason University.

Active Defense

An Overview of the Debate and a Way Forward

Anthony D. Glosson

I. Introduction

Late in 2014, hackers calling themselves the Guardians of Peace (#GOP) released a cache of files stolen from Sony Pictures' systems—including several unreleased titles and employee social security numbers—while issuing ominous threats to Sony employees via Sony's internal network.[1] Sony is hardly alone in its security quandaries; in 2014, Home Depot, Anthem, JPMorgan Chase, Neiman Marcus, Jimmy John's, Staples, and many other household names all suffered major security lapses.[2]

Sony, however, is alone in its reported response to the breach. According to the news website Re/code, Sony launched a counteroffensive that sought to impede the hackers' distribution of its data.[3] Engaging the help of Asia-based Amazon Cloud service infrastructure, Sony allegedly flooded the servers hosting sensitive stolen information.[4] Sony has not confirmed the tactic, and it is unclear whether the company succeeded in delaying or disabling access to the stolen data.[5] Nevertheless, these reports raise an important question: Should firms be permitted to undertake such aggressive responses to breaches? This paper submits that the answer is a qualified yes, and it concludes that now more than ever policymakers should avoid hamstringing security professionals in pursuit of a safer Internet.

[1] Matt Donnelly, *Sony Hackers Flash Disturbing New Warning on Staffers' Computers (Exclusive)*, THE WRAP (Dec. 11, 2014), http://www.thewrap.com/sony-hackers-flash-disturbing-new-warning-on-staffers-computers-exclusive/.

[2] Bill Hardekopf, *The Big Data Breaches of 2014*, FORBES (Jan. 13, 2015), http://www.forbes.com/sites/moneybuilder/2015/01/13/the-big-data-breaches-of-2014/.

[3] Dawn Chmielewski & Arik Hesseldahl, *Sony Pictures Tries to Disrupt Downloads of Its Stolen Files*, RE/CODE (Dec. 10, 2014), https://recode.net/2014/12/10/sony-pictures-tries-to-disrupt-downloads-of-its-stolen-files/.

[4] Pierluigi Paganini, *Sony Pictures Entertainment Is Fighting Back*, SECURITY AFF. (Dec. 16, 2014), http://securityaffairs.co/wordpress/31154/cyber-crime/sony-pictures-fighting-back.html.

[5] *Id*.

Part II of this paper attempts to disambiguate active defense by surveying a sample of actions within its ambit and sorting them into descriptive categories. Part III addresses the current state of domestic law governing active defenses. Part IV turns to the policy considerations at play in the active defense debate. Finally, Part V proposes a legal framework to authorize active defenses subject to liability for third-party damages.

II. Types of Active Defenses

Active defense tactics vary significantly, with some countermeasures going so far as to cause damage to computer systems suspected of waging an attack. A legal framework is needed to guide firms attempting to cope with cyberattacks.

Terminology and Active Defense Tactics

Active defenses are, roughly, countermeasures that entail more than merely hardening one's own network against threats and instead seek to unmask one's attacker or disable the attacker's system.[6] These countermeasures come in a variety of forms, and analysts disagree about which tactics are properly categorized as active defense measures.[7] As David Dittrich of Washington University Law School has observed, it is perhaps helpful to think of active defense as a broad continuum of increasingly aggressive measures.[8] A few examples of tactics that have been

[6] Piotr Duszynski, *Fun with "Active Defense,"* SPIDERLABS BLOG (Aug. 9, 2013), http://blog.spiderlabs.com/2013/08/having-fun-with-active-defense-in-practice.html.

[7] Ellen Nakashima, *When Is a Cyberattack a Matter of Defense?*, WASH. POST (Feb. 27, 2012), http://www.washingtonpost.com/blogs/checkpoint-washington/post/active-defense-at-center-of-debate-on-cyberattacks/2012/02/27/gIQACFoKeR_blog.html (discussing the definitional ambiguity in the context of government active defense applications).

[8] DAVID DITTRICH, *Defining the Terms of the Debate*, THE ACTIVE RESPONSE CONTINUUM: ETHICAL AND LEGAL ISSUES OF AGGRESSIVE COMPUTER NETWORK DEFENSE § 1.1 (May 27, 2013), https://staff.washington.edu/dittrich/arc/book/definitions.html.

characterized as active defense measures are honeypots, tar pits, beacon files, tracebacks, traffic deflection, and more sophisticated forensic techniques.[9]

Honeypots are bogus system resources designed to divert an attacker's attention from more sensitive information.[10] They serve both to distract and to confuse, as well as to track and report.[11] By reviewing information documented in a honeypot's log files, security teams can often assess the capabilities and motivation of an adversary.[12] Perhaps more importantly, honeypots can serve as early warning mechanisms that alert administrators when their networks have been compromised.[13] Similarly, *tar pits* are phony directories or functions that are deliberately designed to react slowly, stalling the attacker's progress to buy time for defenders to react.[14] Both honeypots and tar pits generally operate exclusively within a firm's network.[15]

Beacon files, in contrast, are essentially bait files planted in hopes that attackers will download them to their own systems.[16] After an attacker downloads and opens a beacon file—say, a Word or Excel document—the file "phones home," pinging a system on the firm's

[9] *Cf. id.*; Chris Hoff, *Six Degrees of Desperation: When Defense Becomes Offense . . .*, RATIONAL SURVIVABILITY (July 15, 2012), http://www.rationalsurvivability.com/blog/2012/07/six-degrees-of-desperation/.

[10] Laurent Oudot & Thorsten Holz, *Defeating Honeypots: Network Issues, Part 1*, SYMANTEC COMMUNITY (Jan. 7, 2015), http://www.symantec.com/connect/articles/defeating-honeypots-network-issues-part-1.

[11] *Id*. *See also* Gaurav Kaushik & Rashmi Tyagi, *Honeypot: Decoy Server or System Setup Together Information Regarding an Attack*, 2 VSRD INT'L J. COMP. SCI. & INFO. TECH. 155 (2012), *available at* https://web.archive.org /web/20140110215558/http://www.vsrdjournals.com/CSIT/Issue/2012_02_Feb/Web/10_Gaurav_Kaushik_586 _Research_Communication_Feb_2012.pdf.

[12] Cory Janssen, *Honeypot*, TECHOPEDIA (last visited Apr. 24, 2015), http://www.techopedia.com/definition/10278 /honeypot.

[13] Roger A. Grimes, *No Honeypot? Don't Bother Calling Yourself a Security Pro*, INFOWORLD (Apr. 9, 2013), http://www.infoworld.com/article/2614083/security/no-honeypot--don-t-bother-calling-yourself-a-security-pro.html.

[14] *See* Joe Stewart, *HTTP DDoS Attack Mitigation Using Tarpitting*, DELL SECUREWORKS (June 25, 2007), http://www.secureworks.com/cyber-threat-intelligence/threats/ddos/. For an SMTP application of tarpitting, *see SMTP Tar Pit Feature for Microsoft Windows Server 2003*, MICROSOFT SUPPORT (Dec. 3, 2007), https://support .microsoft.com/kb/842851.

[15] Josh Johnson, *Implementing Active Defense Systems on Private Networks*, SANS INSTITUTE (2013) at 4.

[16] Mark Rasch, *Active Defense and Self Help: A Legal Quagmire*, SECURITYCURRENT (Nov. 5, 2014), http://www .securitycurrent.com/en/writers/mark-rasch/active-defense-and-self-help-a-legal-quagmire.

network.[17] This interaction unmasks the attacker's system and potentially enables a security team to identify the attacker.[18] Similarly, *traceroutes* are methods of tracking traffic across a series of nodes.[19] The most common traceroute utilities track outgoing traffic for troubleshooting purposes, but similar methods (*tracebacks*) are designed to determine the source of incoming traffic.[20]

Traffic deflection involves isolating and filtering out an attacker's traffic.[21] A common way to implement traffic deflection is through iptables rules, which direct a router to take a specific predefined action with respect to traffic that fits a particular pattern or originates from a given location. The traffic can be simply rejected,[22] quarantined to a safe location for further observation,[23] or in some cases, directed back toward the attacker's own system.[24] This tactic can help to counteract some denial of service (DoS) attacks.[25]

In addition to these tactics, large firms often have the capabilities to pursue more advanced strategies by employing security professionals to identify and, if necessary, disable an attacker's system (see part IV). In certain cases, these professionals might be able to make use of tools commonly associated with black hat hackers. A few examples of these mechanisms include

[17] Brian M. Bowen et al., *Baiting Inside Attackers Using Decoy Documents in* SECURITY AND PRIVACY IN COMMUNICATION NETWORKS 51, 56 (Yan Chen et al. eds., 2009), *available at* http://www.cs.columbia.edu/~bmbowen/papers/DecoyDocumentsCameraReadySECCOM09.pdf.

[18] *Id.* at 64.

[19] *E.g.*, Linux main page, *Traceroute(8)*, DIE.NET (last accessed Dec. 2, 2014), http://linux.die.net/man/8/traceroute.

[20] JAMES JOSHI ET AL., NETWORK SECURITY: KNOW IT ALL 95–99 (2008), *available at* http://cdn.ttgtmedia.com/searchSecurityChannel/downloads/NetSecKIACH04-P374463.pdf.

[21] Ho-Seok Kang et al., *Traffic Deflection Method for DOS Attack Defense Using a Location-Based Routing Protocol in the Sensor Network*, 10 COMP. SCI. & INFO. SYSTEMS 685 (2013), *available at* http://www.doiserbia.nb.rs/img/doi/1820-0214/2013/1820-02141300029K.pdf.

[22] Bahaa Qasim M. Al-Musawi, *Mitigating DoS/DDoS Attacks Using Iptables*, 12 INT'L J. ENG'RING & TECH. 101 (2012), *available at* http://www.ijens.org/vol_12_i_03/1210803-7474-ijet-ijens.pdf.

[23] CISCO, *A Cisco Guide to Defending against Distributed Denial of Service Attacks* (last visited Apr. 24, 2015), http://www.cisco.com/web/about/security/intelligence/guide_ddos_defense.html#_Toc374453072.

[24] Deborah Radcliff, *Can You Hack Back?*, CNN (June 1, 2000), http://www-cgi.cnn.com/2000/TECH/computing/06/01/hack.back.idg/.

[25] Raghu, *Linux Iptables to Block Different Attacks*, LINOXIDE (May 10, 2011), http://linoxide.com/firewall/block-common-attacks-iptables/.

remote access tools (RATs) and other sophisticated exploits, which can enable an outsider to monitor or control functions surreptitiously on a target system,[26] and logic bombs, which can deliver a destructive payload when a predefined set of parameters are met, such as an attacker's attempt to copy stolen data or upload the data to a hosting site.

Line-Drawing: A Difficult But Necessary Exercise

Those examples, which are only a small fraction of the tools available to security professionals, should serve to illustrate the broad range of tactics that can come under the label of active defense.[27] As a result, it is imprudent to design policy around any particular tactic or set of tactics. Instead, the law should use adaptable terminology that is based on a tactic's effects on its target rather than on its technical features. Paul Rosenzweig's active defense typology (table 1) supplies one such adaptable framework, which contrasts in-network actions with out-of-network ones.[28] In both of those categories, Rosenzweig proposes subcategories of "observation," "access," "disruption," and "destruction."[29] This framework reflects the diverse nature of active defense tactics. For example, it seems intuitive that in-network observation should generate fewer legal problems than out-of-network destruction.[30] This effects-based descriptive framework makes Rosenzweig's typology a particularly helpful way to approach active defense policy.

[26] Steve Lynch, *Remote Access Tool*, INFOSEC INST. (Apr. 24, 2014), http://resources.infosecinstitute.com/remote-access-tool/.

[27] *E.g.*, Tim Wilson, *Network Security Technology Evolving Rapidly, Forrester Says*, DARKREADING (May 15, 2012), http://www.darkreading.com/attacks-breaches/network-security-technology-evolving-rapidly-forrester-says/d/d-id/1137701?.

[28] Paul Rosenzweig, *International Law and Private Actor Active Cyber Defensive Measures*, 50 STAN. J. INT'L L. 103, 106 (2014).

[29] *Id.*

[30] *See id.* at 105–6.

Table 1. Rosenzweig Active Defense Typology

	Observation	Access	Disruption	Destruction
In-network	***Tools*** • Honeypots • Tar pits ***Actions*** • Obtaining early warning of breach • Delaying or frustrating attacker • Deducing attacker’s motive • Ascertaining attack vectors	N/A—one is generally already authorized and able to access, disrupt, or destroy resources on one’s own network.	N/A—one is generally already authorized and able to access, disrupt, or destroy resources on one’s own network.	N/A—one is generally already authorized and able to access, disrupt, or destroy resources on one’s own network.
Out-of-network	***Tools*** • Beacon files • Tracebacks ***Actions*** • Identifying the attacker • Deducing attacker’s motive	***Tools*** • RATs • Exploits (zero day and wild) • Social engineering ***Actions*** • Viewing files • Mapping resources • Gathering evidence	***Tools*** • All of the previous • Iptables rules • Logic bombs ***Actions*** • Deflecting traffic Toward adversary • Crashing system	***Tools*** • All of the previous • Other advanced tactics ***Actions*** • Deleting files • Changing passwords • Breaking things

Source: Paul Rosenzweig, *International Law and Private Actor Active Cyber Defensive Measures*, 50 STAN. J. INT’L L. 103 (2014).

Note: This table attempts to fill in Rosenzweig’s typology with examples of tools and actions that would fall under each category. Notice that active defense actions begin having perceptible adverse effects on target systems to the right of the darkened line. N/A = not applicable.

This paper deals primarily with out-of-network actions. To be sure, legal questions arise concerning certain in-network actions, and at times the definitional line between in-network and out-of-network actions is not clear.[31] Nonetheless, in-network actions tend to be considered legal because administrators are generally authorized to modify their own networks.[32] For purposes of space and simplicity, this paper draws an analytical line between *access* and *disruption*, collapsing *observation* into the former and *destruction* into the latter. The less precise categorization is suitable for the purposes of this analysis because the economic and technical considerations that this paper advances apply roughly evenly within each of the condensed categories.

III. Current State of Domestic Law Governing Active Defense

The law and public policy have not kept up with the capabilities of attackers and firms developing countermeasures. As a result, firms are unsure how far they can go when they respond to attacks.

The $64,000 Question: What Is "Authorization"?

The law governing active defense is currently unsettled. The statute that addresses hacking is the Computer Fraud and Abuse Act (CFAA).[33] In short, the statute prohibits accessing a computer without "authorization" to do so.[34] The critical question is whether the statute applies to

[31] *See* Paul Rosenzweig, *A Typology for Evaluating Active Cyber Defenses*, LAWFARE (Apr. 15, 2013), http://www.lawfareblog.com/typology-evaluating-active-cyber-defenses/.

[32] *See infra* part III; *see also* James Morris, *The Legality of "Hack-Backs*,*"* NAT'L SECURITY L. BRIEF (Oct. 24, 2012), http://www.nationalsecuritylawbrief.com/the-legality-of-quothack-backs-quot/ (noting the theory that "under the CFAA, a corporation has the authorization to modify any part of its own network").

[33] Computer Fraud and Abuse Act, 18 U.S.C. § 1030.

[34] *Id.* at § 1030(a)(1).

counterattacks equally and in the same way as it does to attacks.[35] The weight of authority seems to suggest that it does,[36] but there are prominent technology law scholars who disagree. The most enlightening debate on the topic played out on the *Volokh Conspiracy* blog.[37] Orin Kerr, a leading legal expert on computer crimes, maintained that the CFAA does not allow victims to use active defense techniques.[38] In contrast, Stewart Baker of Steptoe & Johnson's technology law practice argued that the CFAA may reasonably be construed to permit active defense as authorized access.[39] Baker and Kerr focused specifically on an aggressive method of active defense called *data retrieval*—a destructive method that entails deleting files from an adversary's system. It is worth noting that the focus on a destructive tactic likely shaped the contours of Baker and Kerr's debate in a way that probably impedes the legal case for active defense, at least relative to tactics that seek only to identify an attacker.

In an early post on the topic, Baker argued that the CFAA is unclear about whether active defense constitutes accessing a computer without authorization, so the rule of lenity should create a presumption of legality.[40] Kerr countered this argument by contending that the term *authorization* is actually not ambiguous at all.[41] He characterized the CFAA as a computer trespass statute,[42] a view he has recently expounded in detail.[43] Kerr drew an analogy between

[35] Jody Westby, *Caution: Active Response to Cyber Attacks Has High Risk*, FORBES (Nov. 29, 2012), http://www.forbes.com/sites/jodywestby/2012/11/29/caution-active-response-to-cyber-attacks-has-high-risk/.
[36] *E.g.*, Todd Taylor, *Defending against Cyber-Attacks: Can Companies "Hack Back" against Their Attackers?*, INSIDECOUNSEL (Dec. 14, 2012), http://www.insidecounsel.com/2012/12/14/defending-against-cyber-attacks.
[37] *See* Steptoe & Johnson LLP, *The Hackback Debate*, STEPTOE CYBERBLOG (Nov. 2, 2012), http://www.steptoecyberblog.com/2012/11/02/the-hackback-debate/.
[38] *Id.*
[39] *Id.*
[40] Stewart Baker, *RATs and Poison II—The Legal Case for Counterhacking*, VOLOKH CONSPIRACY (Oct. 14, 2012), http://volokh.com/2012/10/14/rats-and-poison-ii-the-legal-case-for-counterhacking/.
[41] Orin Kerr, *The Legal Case Against Hack-Back: A Response to Stewart Baker*, VOLOKH CONSPIRACY (Oct. 15, 2012), http://volokh.com/2012/10/15/the-legal-case-against-hack-back-a-response-to-stewart-baker/.
[42] *Id.*
[43] *See* Orin Kerr, *Norms of Computer Trespass*, (GWU Law School Public Law Research Paper No. 2015-17, May 2015).

stolen data and common-law trespass to chattel: one generally is not authorized to trespass on another person's property to retrieve stolen goods.[44] Similarly, Kerr argued, data owners are not authorized to trespass on a network to retrieve stolen data.[45]

Baker, however, noted that the statute itself defines *authorization* in terms of entitlement, and he suggested that courts could find that some interests are strong enough to entitle a victim to engage in active defense, whereas others are not.[46] Thus, copyright holders would not be authorized to compromise a computer merely because it stored infringing information, but victims of security breaches could be authorized to pursue the attackers and potentially disable their system.[47]

Months later, the two scholars revived this debate in a Federalist Society teleforum.[48] During that discussion, Kerr and Baker agreed that a firm experiencing a prolonged attack could reach out to law enforcement and obtain proxy authorization under section 1030(f) of the CFAA.[49] Subsection (f) provides that the CFAA's unauthorized access ban "does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States."[50] Under such a scheme, the Federal Bureau of Investigation or any local law enforcement agency could effectively deputize private firms to act under their authority in pursuing attackers, thereby providing subsection (f)'s immunity for the firm. Kerr and Baker still dispute the legality of going it alone, however.

[44] Kerr, *Legal Case against Hack-Back*, *supra* note 41.

[45] *Id.*

[46] Stewart Baker, *The Legality of Counterhacking: Baker Replies to Kerr*, VOLOKH CONSPIRACY (Oct. 16, 2012), http://volokh.com/2012/10/16/the-legality-of-counterhacking-baker-replies-to-kerr/ (*quoting* 18 U.S.C. § 1030(e)(6)).

[47] *Id.*

[48] Stewart Baker, *The Hackback Debate Revisited*, STEPTOE CYBERBLOG (Mar. 4, 2013), http://www.steptoecyberblog.com/2013/03/04/the-hackback-debate-revisited/.

[49] *Id.*

[50] 18 U.S.C. § 1030(f).

Both scholars offered strong arguments in support of their respective views. At this point, Kerr's argument seems more likely to persuade a court because it invokes a well-established body of law to resolve nebulous CFAA issues.[51] Although Baker's argument is also quite plausible, he ultimately admits that his theory is the more complex one.[52] That complexity seems likely to weigh against his theory in court given that most courts do not regularly deal with computer crimes and are unlikely to be familiar with the specifics of the CFAA. In that environment, having the simpler interpretive framework pays dividends.

The Common Law and Affirmative Defenses: More Murky Legal Questions

Other commentators have offered helpful insights into the legal status of active defense under the CFAA. For example, Eugene Volokh, a professor at the University of California, Los Angeles, School of Law, has introduced a third perspective.[53] Although Baker had mostly eschewed direct application of common-law self-defense theories to the CFAA, Volokh embraced direct application of those defenses.[54] He contended that the CFAA's lack of explicit self-defense provisions does not preclude the application of the common-law defense-of-property defense.[55] Volokh pointed out that every American jurisdiction has recognized a defense-of-property defense by default. Noting that "the federal law of criminal defenses is common law," Volokh observed that the Model Penal Code (MPC) and the Restatement (Second) of Torts recognize

[51] *See* ORIN KERR, COMPUTER CRIME LAW (3d ed. 2012).

[52] *See* Stewart Baker, *The Legality of Counterhacking: Baker Replies to Kerr*, VOLOKH CONSPIRACY (Oct. 16, 2012), http://volokh.com/2012/10/16/the-legality-of-counterhacking-baker-replies-to-kerr/.

[53] Eugene Volokh, *The Rhetoric of Opposition to Self-Help*, VOLOKH CONSPIRACY (Apr. 11, 2007), http://www.volokh.com/posts/1176319370.shtml.

[54] *Id.*

[55] *Id.*

some form of defense-of-property defenses.[56] The latter, in fact, explicitly allows for nonlethal force against persons to defend property.[57] Volokh acknowledged that neither the MPC nor the Restatement contemplates computer crimes, but he contended that the common law regularly requires reasoning by analogy, so the defense-of-property defense could apply to active defense measures.[58]

Likewise, University of Illinois law professor and common-law scholar Bruce Smith has argued that one of the comments to section 218 of the Restatement "makes clear that the possessors of chattels retain the 'privilege to use reasonable force' to protect their possessions—even against those 'harmless' interferences for which a formal legal action would be unavailing."[59] Interestingly, Smith also notes that the Restatement contemplates self-help through the use of "'mechanical devices not threatening death or serious bodily harm' to protect land or chattels 'from intrusion.'"[60] According to Smith, the language of these passages seems well suited for analogizing to active defense. Other scholars have discussed using the common law to justify active defense as well.[61]

In sum, though Kerr is probably correct that courts will interpret the CFAA to apply to active defenses, Volokh seems persuasive on the applicability of common-law defenses to the

[56] *Id.* (*citing* Model Penal Code § 3.06); Eugene Volokh, *Response to Orin Kerr*, VOLOKH CONSPIRACY (Apr. 14, 2007), http://www.volokh.com/posts/1176499503.html (*citing* Restatement (Second) of Torts § 79) (*n.b.*, Volokh likely intended to cite § 77 of the Restatement, *Defense of Possessions by Force Not Threatening Death or Serious Bodily Harm*).

[57] Restatement (Second) of Torts § 77.

[58] Volokh, *Response*, *supra* note 56.

[59] Bruce P. Smith, *Hacking, Poaching, and Counterattacking: Digital Counterstrikes and the Contours of Self-Help*, 1 J.L. ECON. & POL'Y 171, 190 (2005) (*citing* Restatement (Second) Torts, § 218, comment e).

[60] *Id.* (*citing* Restatement (Second) of Torts § 84).

[61] *E.g.*, Shane McGee et. al., *Adequate Attribution: A Framework for Developing A National Policy for Private Sector Use of Active Defense*, 8 J. BUS. & TECH. L. 1 (2013). Alternatively, Kesan and Hayes have noted that the common law permits victims to resort to self-help to abate a nuisance. Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 HARV. J.L. & TECH. 429, 430 (2012). The authors make the case that hacking could be considered a nuisance, and firms would be privileged to use active defense to abate it.

CFAA. Combined with Smith's common-law argument in favor of "mechanical" means of self-help, it appears that common-law defenses to CFAA violations stand a reasonable chance of being accepted in court. As Baker noted earlier, though, the unpredictability of affirmative defenses renders them largely unhelpful for firms that consider engaging in active defense.[62] For practical purposes, then, the risk-reward analysis under current law will likely end with Kerr's determination that the CFAA does, indeed, facially apply to active defenses. All things considered, the most promising route for firms seeking to pursue active defense tactics under current law seems to be the Baker-Kerr point of agreement on the prospect of "borrowing" authority from law enforcement entities under subsection (f).

IV. Policy Considerations Surrounding the Use of Active Defense

As policymakers debate what limits should be placed on active defense, they should take note of the considerations addressed in this section.

Active Defense Realigns Firm Incentives in a Socially Beneficial Manner

A number of policy factors weigh in favor of legalized active defense. For example, individualized active defense measures tend to be more efficient than does a process that relies solely on a centralized response model. Firms employ network security professionals, who, of necessity, are more familiar with firm networks and can spot anomalies more easily than outside investigators.[63] Moreover, firms are frequently far better positioned to engage an adversary than the government is to track it down because many firms have the talent and technical capacity to

[62] *See* Stewart Baker, *The Legality of Counterhacking: Baker's Last Post*, VOLOKH CONSPIRACY (Oct. 16, 2012), http://volokh.com/2012/10/16/the-legality-of-counterhacking-bakers-last-post/.

[63] *See* Kevin Townsend, *Security: Should It Be In-House or Outsourced?*, ITSECURITY (Feb. 10, 2013), http://kevtownsend.wordpress.com/2013/02/10/security-in-house-or-outsourced/.

respond to adversaries while they are still online.[64] This advantage is particularly helpful as identifying adversaries becomes more difficult, or even impossible, after they have completed their attack and terminated their connection. Finally, most observers agree that law enforcement simply does not have the resources at present to follow up effectively on "the cyber equivalent of stolen-bicycle paperwork."[65] Placing the burden of identifying and deterring attackers entirely on law enforcement, therefore, "inefficiently stretch[es] government resources."[66] US Department of Defense veteran Chris Rouland has noted that the government's inability to keep up with security threats means that "[t]here is no concept of deterrence today in cyber. It's a global free-fire zone."[67] Consequently, as another commentator noted, "we might favor hackbacks because there currently is no better method to enforce cyberspace violations."[68]

Additionally, the current regime creates perverse incentives for compromised firms to remain silent, thereby making the Internet less secure. First, firms may not want to report security breaches to the government out of concern that the news could, if leaked, deplete consumer and investor confidence in their network security.[69] Second, firms are doubtless taking note that the Federal Trade Commission has adopted a strategy of aggressively

[64] *See* Ericka Chickowski, *Getting the Most out of a Security Red Team*, DARKREADING (Aug. 27, 2013), http://www.darkreading.com/vulnerabilities---threats/getting-the-most-out-of-a-security-red-team/d/d-id/1140356?; Mark Yanalitis, RED TEAMING APPROACH, RATIONALE, AND ENGAGEMENT RISKS (2014), *available at* http://www.researchgate.net/profile/Mark_Yanalitis/publication/; Bank Governance Leadership Network, *Addressing Cybersecurity as a Human Problem*, VIEWPOINTS 4 (Dec. 13, 2013), *available at* http://www.ey.com/Publication/vwLUAssets/EY_-_Addressing_cyber_security_as_a_human_problem/$FILE/EY-BGLN-ViewPoints-Addressing-cybersecurity-as-a-human-problem-Dec2013.pdf (describing red team applications in the financial sector). Red team skill sets substantially overlap those required to implement active defense tactics.

[65] Stewart Baker, *RATs and Poison: Can Cyberespionage Victims Counterhack?*, SKATING ON STILTS (Oct. 13, 2013), http://www.skatingonstilts.com/skating-on-stilts/2012/10/us-law-keeps-victims-from-counterhacking-intruders.html.

[66] Shane Huang, *Proposing A Self-Help Privilege for Victims of Cyber Attacks*, 82 GEO. WASH. L. REV. 1229, 1256 (2014).

[67] Shane Harris, *The Mercenaries*, SLATE (Nov. 12, 2014), http://www.slate.com/articles/technology/future_tense/2014/11/how_corporations_are_adopting_cyber_defense_and_around_legal_barriers_the.html.

[68] Jan E. Messerschmidt, *Hackback: Permitting Retaliatory Hacking by Non-State Actors as Proportionate Countermeasures to Transboundary Cyberharm*, 52 COLUM. J. TRANSNAT'L L. 275, 294 (2013).

[69] Melanie J. Teplinsky, *Fiddling on the Roof: Recent Developments in Cybersecurity*, 2 AM. U. BUS. L. REV. 225, 256 (2013).

prosecuting the victims of security breaches[70] and has provided precious little guidance for firms to guard against liability in the event of a breach.[71] Thus, firms are well advised to avoid involving the government in network security incidents unless legally required to do so. Third, the legal ambiguity surrounding active defense probably discourages firms that have previously engaged in active defense from sharing their findings with law enforcement and industry groups.

Active Defense Is Proven to Work

One of the most remarkable features of the active defense debate is that, for all the controversy, there are good examples of the benefits of active defense and none of the socially harmful effects that opponents fear. Most prominently, in 2009, a group of Chinese hackers attempted to appropriate Google's account login technology.[72] The attack was part of an advanced persistent threat (APT) against Google and other tech giants. APTs consist of coordinated, long-term campaigns targeting a specific entity or network.[73] This particular APT was dubbed "Operation Aurora."[74] Although the details are incomplete, many researchers

[70] *E.g.*, Federal Trade Commission v. Wyndham Worldwide Corp., No. CIV.A. 13-1887 ES, 2014 WL 1349019 (D.N.J. Apr. 7, 2014), motion to certify appeal granted (June 23, 2014); LabMD v. Federal Trade Commission, No. 13-15267-F (11th Cir. Nov. 15, 2013).

[71] *E.g.*, Grant Gross, *Critics Question FTC's Authority to Bring Data Security Complaints*, PCWORLD (Sept. 12, 2013), http://www.pcworld.com/article/2048653/critics-question-ftcs-authority-to-bring-data-security-complaints.html; Marianne McGee, *FTC Must Reveal Security Standards*, GOVINFOSECURITY (May 6, 2014), http://www.govinfosecurity.com/ftc-must-reveal-security-standards-a-6814.

[72] Kim Zetter, *Google Hack Attack Was Ultra Sophisticated, New Details Show*, WIRED (Jan. 14, 2010), http://www.wired.com/2010/01/operation-aurora/.

[73] Damballa, *Advanced Persistent Threats: A Brief Description* (2010), https://www.damballa.com/advanced-persistent-threats-a-brief-description/.

[74] Matthew J. Schwartz, *Google Aurora Hack Was Chinese Counterespionage Operation*, DARKREADING (May 21, 2013), http://www.darkreading.com/attacks-and-breaches/google-aurora-hack-was-chinese-counterespionage-operation/d/d-id/1110060?.

agree that Operation Aurora contained ties to the Chinese government, along with the Chinese search giant and Google rival Baidu.[75]

In response, Google mounted an active defense campaign.[76] Google security teams compromised a server used by the hackers that contained evidence of the hack, in addition to evidence of attacks on other US tech firms.[77] Google shared the information with law enforcement and intelligence agencies.[78] That information sharing led to a public-private partnership in an effort to develop better attribution and response capabilities to combat Operation Aurora.[79] As some recent legislative proposals have illustrated, public-private information sharing can go too far and endanger consumer privacy,[80] but enabling law enforcement to share information with firms in the interest of a more secure Internet is likely to benefit consumers.

Google is not alone in its application of active defense. In 2011, the "Koobface" gang compromised Facebook servers and used its access to propagate malware to consumers, amassing a botnet of surreptitiously infected computers.[81] Facebook used active defense tactics to take control of the "Mothership," the Koobface gang's primary command-and-control server.[82] After exfiltrating the available evidence from the server, Facebook

[75] *Id.*; *see also* MANDIANT, APT1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS (Feb. 18, 2013), *available at* http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.
[76] David E. Sanger & John Markoff, *After Google's Stand on China, U.S. Treads Lightly*, N.Y. TIMES (Jan. 14, 2010), http://www.nytimes.com/2010/01/15/world/asia/15diplo.html.
[77] Shane Harris, *Google's Secret NSA Alliance: The Terrifying Deals between Silicon Valley and the Security State*, SALON (Nov. 16, 2014), http://www.salon.com/2014/11/16/googles_secret_nsa_alliance_the_terrifying_deals_between_silicon_valley_and_the_security_state/.
[78] *Id.*
[79] *Id.*
[80] Andrea Castillo, *The White House Wants to Create a Cyber Police State*, PLAIN TEXT (Jan. 20, 2015), https://medium.com/plain-text/the-white-house-cybersecurity-proposal-would-arm-a-cyber-police-state-ed1d657db0dd; Andrea Castillo, *What You Should Know about CISA*, PLAIN TEXT (Mar. 23, 2015), https://medium.com/plain-text/what-you-should-know-about-cisa-950c395dddf6.
[81] Facebook Security Team, *Facebook's Continued Fight Against Koobface*, FACEBOOK (Jan. 17, 2012), https://www.facebook.com/notes/facebook-security/facebooks-continued-fight-against-koobface/10150474399670766.
[82] *Id.*

technicians disabled the Mothership.[83] Facebook subsequently shared information gleaned from its active defense campaign with the network security community to assist in securing other consumer services.[84]

As a final example, the World Trade Organization's web hosting service has applied an active defense strategy to repel a denial-of-service attack by an angry horde of "electrohippies."[85] The hosting service isolated the offending traffic and redirected it toward the originating server.[86] While DoS tactics have become more sophisticated through increasing use of botnets rather than centralized systems, DoS attacks are still generally directed by command-and-control servers that theoretically provide a central point of vulnerability.[87]

Notably, the government has not prosecuted any of the firms that have undertaken active defense measures.[88] This decision may be an implicit recognition that active defense measures have at least some social value.[89] Despite the lack of prosecutions, though, examples indicate that the legal uncertainty surrounding the issue is preventing socially desirable outcomes. In 2008, for example, researchers exploring the "Kraken" botnet discovered an exploit that could have been used to direct the malware to remove itself from many of its 400,000 zombie

[83] Tom Brewster, *Koobface Crooks Unmasked?*, ITPRO (Jan. 17, 2012), http://www.itpro.co.uk/638350/koobface-crooks-unmasked.

[84] *Id.*

[85] Radcliff, *Can You Hack Back?*, *supra* note 24. The author disclaims all responsibility for this term; the electrohippies self-identified as such.

[86] *Id.*

[87] *E.g.*, Spamhaus Project, *Spamhaus Botnet Controller List*, SPAMHAUS.ORG (last visited Apr. 24, 2015), http://www.spamhaus.org/bcl/.

[88] *Cf.* Huang, *Self-Help Privilege*, *supra* note 66 at 1249–51.

[89] *Id.* Indeed, some government entities have issued reports tentatively embracing the exploration of active defense proposals. *See* 9/11 COMMISSION, REFLECTIONS ON THE TENTH ANNIVERSARY OF *THE 9/11 COMMISSION REPORT* 39 (July 2014), *available at* http://bipartisanpolicy.org/wp-content/uploads/sites/default/files/files/%20BPC%209-11%20Commission.pdf ("Congress should also consider granting private companies legal authority to take direct action in response to attacks on their networks."); IP COMMISSION, THE REPORT OF THE COMMISSION ON THE THEFT OF AMERICAN INTELLECTUAL PROPERTY 82 (May 2013), *available at* http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf ("Informed deliberations over whether corporations and individuals should be legally able to conduct threat-based deterrence operations against network intrusion, without doing undue harm to an attacker or to innocent third parties, ought to be undertaken").

computers.[90] Instead of sending the command to do so, however, researchers felt constrained to leave the malware in place because of the legal ambiguity of taking corrective action.[91] Active defensive continues to raise concerns among many commentators.

Objections to Active Defense Are Surmountable

Orin Kerr and Georgetown University law professor Neal Katyal both have raised important misattribution concerns in objecting to active defense regimes. Katyal argues that "tracing is tough, even in realtime, and the risk of identifying the wrong party is high."[92] Likewise, Kerr contends that "it is very easy to disguise the source of an Internet attack. . . . As a result, the chance that a victim of a cyber attack can quickly and accurately identify where the attack originates is quite small."[93] Undeniably, these concerns constitute a strong challenge for individuals advocating the legalization of active defenses. The underlying architecture of the Internet facilitates anonymity and thereby increases the dangers of misattribution.[94] In this sense, an active defense regime could generate costs (the risk of damage to nonaggressing systems) that firms availing themselves of active defense may ignore.

However, a carefully crafted active defense regime could mitigate misattribution problems by forcing firms to internalize those costs. That is, Kerr and Katyal's concerns could be addressed by requiring firms to compensate the owners of systems compromised by mistake

[90] T. Luis de Guzman, *Unleashing A Cure for the Botnet Zombie Plague: Cybertorts, Counterstrikes, and Privileges*, 59 CATH. U. L. REV. 527 (2010).

[91] *Id.* at 528.

[92] Neal Katyal, *Community Self-Help*, 1 J.L. ECON. & POL'Y 33, 62 (2005).

[93] Orin S. Kerr, *Virtual Crime, Virtual Deterrence: A Skeptical View of Self-Help, Architecture, and Civil Liability*, 1 J.L. ECON. & POL'Y 197, 205 (2005).

[94] *See, e.g.*, Matthew Tanase*, IP Spoofing: An Introduction*, SYMANTEC (Nov. 2, 2010), http://www.symantec.com/connect/articles/ip-spoofing-introduction; Patrick Lambert, *The Basics of Using a Proxy Server for Privacy and Security*, TECHREPUBLIC (Dec. 4, 2012), http://www.techrepublic.com/blog/it-security/the-basics-of-using-a-proxy-server-for-privacy-and-security/.

during an active defense campaign. In fact, the same anonymity problem that generates misattribution concerns also counsels in favor of applying a liability rule to network security. As Judge Guido Calabresi and Stanford University law professor A. Douglas Melamed have observed, society can protect entitlements (such as rights or property ownership) through liability rules or property rules.[95] A property rule bans any nonvoluntary encroachment on the entitlement by a third party, and a liability rule permits the encroachment but requires that the third party compensate the holder of the entitlement.[96] A classic example of the enforcement of a property rule is a court-issued injunction against a particular party's course of conduct, and a typical means of enforcing a liability rule is the imposition of damages on the encroaching party.[97]

As Calabresi and Melamed explain, liability rules are better suited than are property rules for transactions in which there is little possibility for bargaining.[98] As an illustration of a liability rule, Calabresi and Melamed invoked the law's approach to car accidents.[99] An at-fault driver cannot ex ante bargain with another driver harmed by a collision because such accidents occur largely between strangers and are unanticipated.[100] Consequently, the law imposes a liability rule—damages—on at-fault drivers after the fact.[101] Misdirected active defense efforts, like car accidents, similarly occur between strangers and are unanticipated. (That is, although security professionals, of course, understand that they are undertaking an active defense effort, they do not anticipate failing to identify the target accurately in a given operation.) Just as it is infeasible for the at-fault driver to ex ante bargain with other drivers for the "right" to swap paint in an

[95] Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089 (1972).
[96] *See generally id.*
[97] *See generally id.*
[98] *Id.* at 1091, 1126–27.
[99] *Id.*
[100] *Id.* at 1127.
[101] *Id.*

accident, it is also infeasible for firms to bargain with operators of wrongfully targeted networks for the "right" ("authorization" in CFAA verbiage) to mistakenly access those networks during an active defense campaign. Thus, the optimal solution in both scenarios is to apply a liability rule. And just as the law assigns the applicable entitlement to the injured driver, it should assign the entitlement to the operator of the wrongfully targeted network.[102] An *ex post* compensation requirement would fulfill that goal in the active defense context, just as it does in the car collision context.

More recently, some commentators also have suggested that active defense should remain illegal because of the risk that it might provoke attackers to become more aggressive than they would be if firms left them alone. Advocating a continued ban on active defense, Rick Howard of Palo Alto Networks advanced this argument:

> Do you think the bad guy will just go away simply because you took a swing at him? Do you think he will say, "Wow, these guys are tough. I guess I will hang up my hacking spurs forever?" More likely than not, you would have succeeded in poking the beehive and you may have unleashed a world of hurt on your organization that it did not need.[103]

Jeffrey Carr of the consulting firm Taia Global concurred, warning that "[w]hat may start as simple [intellectual property] theft could, after a 'hacking back' attempt, result in the utter destruction of the entire network."[104]

[102] *Id.* at 1106–10. Here, it does not make sense to assign the entitlement to the firm engaging in misdirected active defense. That arrangement would force a network administrator concerned about a firm mistakenly targeting his or her network to pay damages to the firm, which would then be enjoined from engaging in active defense that is misdirected at the administrator's network. (Calabresi & Melamed Rule 4). However, an injunction against making a mistake is unlikely to prove particularly effective—even setting aside the practical problems of correctly guessing which firms an administrator should seek to enjoin. Thus, although Rule 4 is a perfectly plausible means of dealing with polluters or noxious livestock feedlots, *cf.* Spur Industries v. Del E. Webb Development Co., 108 Ariz. 178, 494 P.2d 700 (Ariz. 1972), it does not always work well for unanticipated transactions.

[103] Sara Sorcher, *Influencers: Companies Should Not Be Allowed to Hack Back*, CHRISTIAN SCI. MONITOR (Apr. 1, 2015), http://www.csmonitor.com/World/Passcode/Passcode-Influencers/2015/0401/Influencers-Companies-should-not-be-allowed-to-hack-back.

[104] *Id.*

The trouble with these criticisms, however, is that they represent precisely the type of considerations that would likely inform a firm's active defense policies as a matter of economic efficiency. It seems quite remarkable to suggest that a one-size-fits-all blanket ban better accounts for the particular circumstances and capabilities of every large and small firm in the country than would a case-by-case evaluation by the actual operators of the victim networks.

Indeed, the well-funded hackers that Howard and Carr feature in their warnings are frequently interested in achieving economic objectives, such as obtaining proprietary software and other trade secrets.[105] Attackers that regard hacking as a business (or are state sponsored in an effort to obtain trade secrets for domestic industry) may well conclude that attacking a firm with strong response capabilities is an inefficient use of resources.[106]

Thus, despite the objections raised by active defense critics, this paper submits that the real-world experience with active defense confirms its net social benefit. Policymakers should adopt a first-do-no-harm posture toward active defense and allow those who are best positioned to respond to breaches to deploy their full comparative advantage in securing their networks. The precautionary principle is especially inadvisable in the dynamic realm of tech policy, and until the ostensible harms of active defense materialize, the law should facilitate maximum innovation in the network security field.[107]

[105] *E.g.*, Ellen Nakashima, *U.S. Launches Effort to Stem Trade-Secret Theft*, WASH. POST (Feb. 20, 2013), http://www.washingtonpost.com/world/national-security/us-launches-effort-to-stem-trade-secret-theft/2013/02/20/26b6fbce-7ba8-11e2-a044-676856536b40_story.html.

[106] *See* Messerschmidt, *Hackback*, *supra* note 68, at 292 ("Active defense measures, by contrast, can respond rapidly and may significantly drive up the costs that hackers incur, deterring future conduct"), *citing* RICHARD POSNER, ECONOMIC ANALYSIS OF LAW 242 (5th ed. 1998).

[107] Although firms currently may, in theory, work with law enforcement to obtain active defense authorization under 18 U.S.C. § 1030(f), this arrangement is unsatisfactory for two reasons. First, it would unfairly advantage large firms, which are likely to be repeat players in the active defense field, over smaller competitors, which may find the bureaucratic burden of obtaining authorization impractical. Second, threats occur in real time, but government permitting programs tend to process applications at something less than that rate. Consequently, although permitting could conceivably work in response to advanced persistent threats, it would provide little help in counteracting one-off attacks.

V. Designing an Active Defense Framework That Captures Social Benefits and Minimizes Costs

A policy that supports the rights to active defense would work best within a framework that permits firms to defend themselves but provides for damages to deter careless actors.

A Strict-Liability Framework That Balances Self-Defense Rights and Misattribution Risks

The previously mentioned policy considerations suggest that active defense has the potential to confer real benefits on society but that it also carries risks of substantial harms. An active defense framework should seek to capture those benefits while carefully reducing the societal risks to the greatest extent possible. Furthermore, the framework should recognize that different active defense tactics implicate different risks. To achieve these objectives, the framework should account for the distinction between observation/access on the one hand, and disruption/destruction on the other. Additionally, the framework should confront the technical reality of the attribution problem.

Congress can accommodate all these considerations by adding a qualified active defense right to the CFAA.[108] The right would balance the active defense privilege with misattribution concerns by imposing strict liability for harm caused during misdirected active defense efforts, forcing those who invoke the right to internalize the costs of misattribution. Furthermore, it would recognize the technical distinctions between active defense tactics by limiting firms to only observation/access tactics against intermediary networks through which an attacker is routing traffic while privileging the full range of observation/access and disruption/destruction

[108] *Cf.* Huang, *Proposing a Self-Help Privilege*, *supra* note 66. Huang offers a thoughtful active defense proposal, but he does not distinguish among active defense tactics. Huang also places strict limitations on the extent of acceptable damage to the attacker's assets, a feature rejected in this proposal for deterrence reasons discussed *infra*.

tactics against the attacker's own network.[109] Active defense measures against intermediary networks, though sometimes necessary to track an adversary back over a series of nodes,[110] would be privileged *only* when the adversary had very recently routed traffic through the intermediary, and only when it was infeasible to obtain the intermediary network operator's cooperation.

The strict liability framework amendment would temper excessive retribution because firms are unlikely to risk greater damages than necessary in the event of an erroneous attribution.[111] At the same time, the availability of disruptive/destructive options would enable more firms to attack—and eventually disable—an attacker's system in the same way that Facebook handled the Koobface "Mothership." Though some critics may balk at sanctioning destructive capabilities along with disruptive ones, a strong argument can be made that the threat of losing control over one's system and data may deter an attacker more than the mere possibility of a victim seeking to ascertain the attacker's identity and disrupt the attack.[112] The difference is particularly pronounced in the case of attackers outside US jurisdiction, who are not likely to be

[109] The amendment could also clarify that federal law does not prohibit in-network actions in any capacity. Indeed, the House of Representatives has recently passed two bills that appear to explicitly authorize in-network activity. *See* National Cybersecurity Protection Advancement Act of 2015, H.R. 1731 at § 3, *available at* https://www.congress.gov/bill/114th-congress/house-bill/1731/text; Protecting Cyber Networks Act, H.R. 1560 at § 3(d)(3). Commentators have suggested that these measures authorize "hacking back." *See* Center for Democracy and Technology, *Cybersecurity Information Sharing Bills Fall Short on Privacy Protections*, CDT INSIGHTS (Apr. 22, 2015), https://cdt.org/insight/cybersecurity-information-sharing-bills-fall-short-on-privacy-protections/. However, it appears that both bills authorize only in-network actions. H.R. 1560 provides that "a private entity may, for a cybersecurity purpose, operate a defensive measure that is operated on and is limited to . . . an information system of such private entity." H.R. 1560 at § 3(d)(3). H.R. 1731 explicitly states that "a non-Federal entity . . . may, for cybersecurity purposes, operate a defensive measure that is applied to . . . an information system of such non-Federal entity." *See* H.R. 1731 at § 3.

[110] An example might be reviewing client connection logs or other identifying data on a machine that the adversary is using to bounce traffic; *see* Oracle, *Tracking Client Requests through Directory Proxy Server and Directory Server Access Logs* (Sun Directory Server documentation, 2010), https://docs.oracle.com/cd/E19424-01/820-4811/track_requests/.

[111] Jay P. Kesan & Ruperto Majuca, *Optimal Hackback*, 84 CHI.-KENT L. REV. 831, 837 (2010).

[112] Gerry Smith, *"Hacking Back" Could Deter Chinese Cyberattacks, Report Says*, HUFFINGTON POST (May 22, 2013), http://www.huffingtonpost.com/2013/05/22/hacking-back-chinese-cyberattacks_n_3322247.html.

prosecuted even if their victims accurately identify them.[113] Additionally, destructive measures will permit a firm to destroy stolen trade secrets. Finally, destructive measures can undermine an adversary's short- to mid-term capabilities, consequently reducing the risk that the adversary will continue attacking firms after the initial attack has been disrupted.[114]

Robust Statutory Damages That Can Ensure an Optimal Incentive Structure

The amendment would enforce those limitations by granting a private right of action for operators of wrongfully targeted systems. To avoid liability, the defendant would have the burden to show either that the plaintiff was the initial attacker or else that (1) the defendant's active defense measures were limited to observation and access tactics, (2) the initial attacker was routing traffic through the plaintiff's network at the time of the active defense action, and (3) obtaining the plaintiff's cooperation in tracing the initial attacker was impracticable.

To be sure, the attribution problem will occasionally prevent operators of wrongfully targeted networks from bringing lawsuits against firms engaged in active defense. However, firms will likely engage in active defense when the value of doing so exceeds the risk of liability times the potential damages,[115] so Congress could offset the attribution problem's effect on liability risk by imposing relatively stiffer statutory damages.[116] In this way, the amendment would maintain an incentive structure under which firms will use active defense tactics only when they have an appropriate degree of confidence in the identity of their

[113] *Id.*

[114] That broader deterrent effect is the reason this paper rejects the idea that disruption or destruction must be proportional to the harm to the victim network. Harms imposed by an attacker are likely distributed over a wide range of targets, and insufficient deterrence would result if the few firms to successfully engage the attacker were constrained to a proportional response. *Contra* Huang, *Self-Help Privilege*, *supra* note 66 at 1259.

[115] Messerschmidt, *Hackback, supra* note 68 at 321.

[116] A. Mitchell Polinsky & Steven Shavell, *Punitive Damages: An Economic Analysis*, 111 HARV. L. REV. 869, 874 (1998).

targets.[117] Additionally, the amendment could require firms to identify themselves at the conclusion of their active defense operation unless they have obtained authorization from a law enforcement agency to retain anonymity, thereby enabling owners of wrongfully targeted networks to take legal action if necessary.

Moreover, it seems unlikely that the prospect of high damages would unduly dissuade risk-averse smaller firms over the long term. As network security increasingly becomes a booming sector of the economy, insurers may offer coverage for liability incurred during active defense campaigns on a similar model to the medical and legal malpractice insurance markets today, thereby allowing smaller firms to engage in the practice without fearing financial ruin.[118] Furthermore, it seems unlikely that active defense insurance would cancel out the deterrent effect of higher damages, because firms that abuse the coverage to undertake legally dubious hacking campaigns would soon find themselves uninsurable.

The Active Defense Proposal Applied

Imagine that a system administrator at a bank notices that the bank's internal network is responding slowly. The administrator logs the network traffic and determines that an unusual amount of data is traversing the network. The bank's security team investigates and discovers that an intruder has breached the network and is attempting to copy a database containing sensitive accountholder information.

[117] *Id*. Further economic analysis will need to be done to determine the appropriate dollar figures for the statutory penalties, but the deterrence concepts seem clear enough.

[118] That is, like malpractice insurance, active defense insurance would permit firms to engage in socially useful but occasionally dangerous activities. For an example of insurers adapting to new liability markets, consider the current insurance firm rush to develop offerings for data breach liability. *See* Noah Buhayar et al., *JPMorgan's Data Breach Reveals Growth Market for Insurers*, BLOOMBERG (Oct. 9, 2014), http://www.bloomberg.com/news/2014-10-09/jpmorgan-s-data-breach-reveals-growth-market-for-insurers.html.

Under the current framework, the system administrator has not violated the CFAA by logging the traffic on the bank's internal network because this was done with the bank's authorization. After that, however, the security team is mostly confined to other in-network actions, such as attempting to identify and close the security hole and thereby boot the attacker off of the network. In doing so, the team might use tools like honeypots to distract the attacker or sandtraps to slow the attacker down.

This paper's proposal enables the security team to go further in defending its network. Under the amendment, the security team could apply tracebacks and beacon files to uncloak the attacker. If the team could attribute the attack with sufficient certainty to reassure the bank's decisionmakers that the risk of liability was low, the team could then attempt to decommission the attacker such that the attacker could not complete the operation against the bank—or any other targets. The security team might use a rootkit to compromise the attacker's system and remove any software that the attacker might have used in the attack, along with any confidential information that the attacker might have succeeded in extracting from the bank's network. The security team might also seek to lock the attacker out of its own system or otherwise obstruct the attacker's ability to continue using the system as a tool to attack others. Under the proposal, these actions would all be privileged, provided that they were used against an aggressor.

The bank might decide, however, that it merely wants to identify the attacker and then relay the information to the appropriate authorities. By doing so, the bank would avoid any potential liability for wrongly damaging a third party's computer in the event of a mistaken identification. Either option—disabling the attacker's system or identifying and reporting the attacker—provides social benefits that extend beyond the company involved. Furthermore, the party in the best position to evaluate the risk of mistaken identification—and to undertake the associated risk of liability—is empowered to make that decision. Thus, the proposal leverages profit motives to achieve the greatest possible social gains while minimizing the risk of damage to third-party systems following a mistaken attribution.

To be sure, this proposal is not a magic bullet—for example, it would likely not have provided cover for the Kraken researchers discussed in the previous section because the researchers would have had to disrupt or destroy data on the compromised intermediary systems infected by Kraken malware. Accordingly, Congress may consider supplementing the CFAA amendment with more targeted solutions for specific recurring scenarios such as botnet research. Network security doubtless poses complex challenges, but with estimates placing the price tag on global network insecurity in the hundreds of billions of dollars,[119] policymakers should be seeking to adopt balanced solutions sooner rather than later. This proposal would represent a major step forward in adapting our network security laws to 21st-century reality.

VI. Conclusion

This paper has sought to address several difficult questions associated with the active defense debate. As security increasingly becomes integral to consumer welfare and a strong economy, this paper submits that policymakers should avoid unilaterally disarming innocent parties' front line of defense and instead should enact a liability regime under which firms are permitted to use active defenses.

[119] CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES, NET LOSSES: ESTIMATING THE GLOBAL COST OF CYBERCRIME (June 2014), *available at* http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf.