NOTE

Proposing a Self-Help Privilege for Victims of Cyber Attacks

*Shane Huang**

ABSTRACT

As the Internet occupies increasingly important functions in modern society, cyber attacks pose an increasingly serious threat to private companies and ordinary citizens. Sophisticated hackers threaten the nation's military and foreign policy interests and can destabilize the nation's financial, telecommunications, and energy sectors. In order to combat these threats, Congress has enacted laws specifically criminalizing hacking, and courts have fashioned doctrines for finding liability for tortious Internet activity. These legal tools, however, provide inadequate protection against today's sophisticated hackers. Developed decades ago, these doctrines are difficult to apply with respect to hostile criminal organizations or foreign state actors. Indeed, legal ambiguity creates an uncertain legal environment that deters legitimate security professionals from using a full range of defenses against unknown attackers.

Congress should amend the Computer Fraud and Abuse Act to grant a limited self-help privilege to victims of cyber attacks. Providing legal clarity in this fashion would allow legitimate security organizations to adopt more proactive defenses for themselves and for ordinary Internet users. Information sharing would improve between the private entities closest to the action

* J.D., May 2014, The George Washington University Law School. This Note would not have been possible if not for the connections made through The George Washington University's Cyber Security Policy and Research Institute. The author also thanks Professors Brian D. Smith, Orin S. Kerr, and Robert W. Tuttle for their assistance in developing and refining the ideas in this Note. Finally, the author especially wishes to thank the editorial board of *The George Washington Law Review* for working tirelessly in preparing this Note for publication.

and the government agencies responsible for securing American interests on the Internet. This proposal would result in better situational awareness for private and public security organizations, as well as a more secure Internet for everyone.

TABLE OF CONTENTS

INTRODUCTION

On a single day in August 2012, the world's largest oil producer helplessly watched as a computer infection destroyed the files on about 30,000 computers[1]—or approximately three-quarters of its office computers.[2] The victim, Aramco, was able to continue oil production without interruption, but the attack disabled its internal office network for more than a week.[3]

The Aramco attack was the most severe of its kind in the past few years, during which large cyber attacks have become routine. In January 2012, hackers successfully copied the names, email addresses, billing and shipping addresses, and passwords of 24 million customers of online retailer Zappos.[4] By summer 2012, dating website eHarmony, music website last.fm, and professional networking website LinkedIn had suffered similar breaches.[5] In 2013, hackers successfully compromised customer information for 50 million LivingSocial customers[6] and 50 million Evernote customers.[7] During the height of the 2013 holiday shopping season, hackers stole information for approximately

---

1 *Aramco Says Cyberattack Was Aimed at Production*, N.Y. TIMES, Dec. 10, 2012, at B2 [hereinafter N.Y. TIMES, *Aramco*].

2 Nicole Perlroth, *Cyberattack on Saudi Firm Disquiets U.S.*, N.Y. TIMES, Oct. 24, 2012, at A1.

3 N.Y. TIMES, *Aramco*, *supra* note 1, at B2.

4 Mathew J. Schwartz, *Zappos Hack Exposes Passwords*, DARKREADING (Jan. 17, 2012, 10:27 AM), http://www.darkreading.com/attacks-and-breaches/zappos-hack-exposes-passwords/d/d-id/1102297?.

5 Nicole Perlroth, *Lax Security at LinkedIn Is Laid Bare*, N.Y. TIMES, June 11, 2012, at B1.

6 Julianne Pepitone, *50 Million Customers Hit in LivingSocial Hack*, CNNMONEY (Apr. 26, 2013, 5:47 PM), http://money.cnn.com/2013/04/26/technology/security/livingsocial-hack/.

7 Graham Cluley, *Evernote Hacked—Almost 50 Million Passwords Reset After Security Breach*, NAKED SECURITY (Mar. 2, 2013), http://nakedsecurity.sophos.com/2013/03/02/evernote-hacked-almost-50-million-passwords-reset-after-security-breach/.

40 million debit and credit card accounts from the national retailer Target.[8] These attacks are not isolated incidents and show no signs of going away.

Unfortunately, legal ambiguity in antihacking laws stifles the ability of security professionals to properly investigate and respond to these cyber threats, which has exacerbated the problem for American businesses and consumers alike. Security professionals, uncertain about the legal permissibility of proactive technical solutions, are forced to adopt passive, reactive postures on their own networks. In addition, when circumstances are sufficiently dire to warrant more aggressive responses, fear of legal repercussions discourages coordination and disclosure with outside parties. In order to improve the United States' cybersecurity posture, Congress should amend the Computer Fraud and Abuse Act ("CFAA")[9] to allow for a limited self-help privilege in exigent circumstances.

Part I of this Note introduces the rising threat of cyber attacks over the Internet. Part II discusses the current legal framework regarding unauthorized or unwanted Internet activity. Part III demonstrates that the current law is ambiguous regarding private sector counterattacks, and that this uncertainty paralyzes legitimate security researchers and hampers current efforts to combat cyber threats on the Internet. Part IV discusses prior proposals to give a self-help privilege, each of which falls short of fully solving the problem. Part V then proposes that Congress codify a limited counterattack privilege in order to resolve the ambiguity in current law and give actors a clear legal framework to design effective cybersecurity procedures. Finally, Part VI analyzes historical counterattacks under the proposed legal framework and demonstrates that this proposal would resolve current legal ambiguity.

I. THE RISING PROBLEM OF CYBER ATTACKS

A range of threats face computers on the Internet. All users are potentially susceptible to infection by broad exploits that indiscriminately target ordinary computers for infection. In addition, high value targets face the persistent threat of highly targeted, highly sophisticated attacks, which are known as "advanced persistent threats."[10]

---

8 Brian Krebs, *Target Hackers Broke In via HVAC Company*, KREBS ON SECURITY (Feb. 5, 2014, 1:52 PM), http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/.

9 Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030 (2012).

10 DMITRI ALPEROVITCH, MCAFEE, REVEALED: OPERATION SHADY RAT 2 (2011).

A. *Advanced Persistent Threats*

In December 2009, Google made news by engaging in an unconventionally aggressive response to a security incident involving a "theft of intellectual property."[11] In recent years, large western corporations have complained of frequent breaches and compromises of their valuable intellectual property,[12] but Google noticed that these attackers were targeting its "crown jewels," including the highly sensitive source code for its password systems securing millions of accounts.[13] Google "began a secret counteroffensive" and gained access to the immediate source of the attacks—a server located in Taiwan, used to disguise the mainland Chinese attackers.[14] With this access, Google uncovered a large-scale operation targeting at least thirty-three other companies.[15] Google's security experts were stunned by the sophistication and scale of the attacks, which the computer security community named "Operation Aurora."[16]

Many security researchers and government officials have concluded that the actual perpetrators of Operation Aurora were hackers sponsored by the Chinese government. Researchers arrived at this conclusion in part because the sophistication of the attack suggested a state sponsor, and because the attackers appeared to be most interested in eavesdropping on email messages by Chinese political dissidents.[17] In response, Google withdrew its search service from mainland China.[18]

Since the discovery of Operation Aurora, security researchers have uncovered other large-scale attacks staged behind intermediary computers. For example, a coordinated five-year campaign of attacks, named "Operation Shady RAT," compromised the secrets of at least seventy-one victims in fourteen countries, including major defense contractors, government entities, and even international sporting agencies.[19] In late 2012 and early 2013, Middle Eastern activists at-

---

11 David Drummond, *A New Approach to China*, GOOGLE OFFICIAL BLOG (Jan. 12, 2010), http://googleblog.blogspot.com/2010/01/new-approach-to-china.html.

12 *See* ALPEROVITCH, *supra* note 10, at 2.

13 *E.g.*, John Markoff, *Hackers Said to Breach Google Password System*, N.Y. TIMES, Apr. 20, 2010, at A1.

14 David E. Sanger & John Markoff, *U.S. Treads Lightly in Wake of Google's Loud Stance on China*, N.Y. TIMES, Jan. 15, 2010, at A1.

15 *Id.*

16 *See, e.g.*, Michael Joseph Gross, *Enter the Cyber-Dragon*, VANITY FAIR, Sept. 2011, at 222, *available at* http://www.vanityfair.com/culture/features/2011/09/chinese-hacking-201109.

17 *Id.*

18 Drummond, *supra* note 11.

19 ALPEROVITCH, *supra* note 10, at 4. The name "Operation Shady RAT" is derived from

tacked the availability of U.S. banking websites by routing distributed denial-of-service ("DDoS") attacks through "remotely hijacked" data centers.[20] The New York Times has reported that its own internal networks have been hacked through "compromised computer systems registered to universities" throughout the United States.[21] Sophisticated hackers use compromised intermediary computers as a matter of routine in order to mask their own identities.[22]

B. *Less Sophisticated Cyber Attacks Still Affect Ordinary Internet Users*

Although many cyber attacks target governments or corporations, ordinary users also suffer consequences from malicious Internet activity. For example, malicious actors frequently target large numbers of ordinary users' computers for the purpose of coordinating large-scale fraudulent computer activities.[23] These ecosystems of compromised computers are known as "botnets."[24] The creators of botnets generally exploit vulnerabilities in commonly used software to silently infect large numbers of computers, which are known as "drones" or "zombies."[25] These infected computers then seek out orders from a "command and control" server, which coordinates the be-

---

the industry term RAT, which stands for "Remote Access Tool" or "Remote Access Trojan." *Id.* at 3. The targeting of international sporting agencies, such as the World Anti-Doping Agency and the International Olympic Committee, led investigators to conclude that a state actor was involved in the attacks. *Id.* at 6. The organizations and countries targeted in the operation have led some to suspect that this state actor was likely China. Michael Joseph Gross, *Exclusive: Operation Shady RAT—Unprecedented Cyber-Espionage Campaign and Intellectual-Property Bonanza*, VANITY FAIR (Aug. 2, 2011), http://www.vanityfair.com/culture/features/2011/09/operation-shady-rat-201109.

20 Nicole Perlroth & Quentin Hardy, *Bank Hacks Were Work of Iranians, Officials Say*, N.Y. TIMES, Jan. 9, 2013, at B1.

21 Nicole Perlroth, *Hackers in China Attacked The Times for Last 4 Months*, N.Y. TIMES, Jan. 31, 2013, at A1.

22 *See* MANDIANT, APT1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS 39 (2013), *available at* http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf. The security firm Mandiant has also collected recorded video evidence of hackers remotely controlling American computers to engage in their hacking operations from their base of operations in Shanghai. *See* MandiantCorp, *APT1: Exposing One of China's Cyber Espionage Units*, YOUTUBE (Feb. 18, 2013), http://www.youtube.com/watch?v=6p7FqSav6Ho.

23 *See* Tyler Moore, Richard Clayton & Ross Anderson, *The Economics of Online Crime*, J. ECON. PERSP., Summer 2009, at 3, 5 (explaining that "botnet herders" manage large numbers of compromised computers and "rent[ ] them out to spammers, phishermen, and other crooks").

24 Jan Kok & Bernhard Kurz, *Analysis of the BotNet Ecosystem*, *in* 10TH CONFERENCE OF TELECOMMUNICATION, MEDIA AND INTERNET TECHNO-ECONOMICS (CTTE) (2011), *available at* http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5897957.

25 *Id.*

havior of the entire network of infected devices.[26] Distributing the infection across multiple networks and geographical regions increases the anonymity and the resilience of the botnets.[27] Botnet operators then use the herds for nefarious purposes, such as displaying ads,[28] stealing passwords or valuable financial information, or sending spam.[29] As a result, the ordinary users of these compromised computers are also vulnerable to fraud and extortion, because the botnet operators have the ability to capture passwords, bank account information, and the contents of their communications.[30] Some botnets are also used to conceal the origins of malicious Internet traffic and protect the identities of scammers, extortionists, and traffickers of child pornography.[31] Botnets also enable DDoS attacks, which generally flood a target with a large number of requests so that the target service or computer is made unavailable to legitimate users.[32] The end result is that computer infection enables much of the social harm caused by malicious behavior on the Internet—from traditional crimes like child pornography, extortion, and fraud to computer-specific crimes like hacking, spam, and cyber vandalism.

---

26 *Id.*

27 *Id.* Some botnets may be updated to listen to new servers in the event an old command and control server is taken down by law enforcement authorities. *See* Jesse Hicks, *Down the Sinkhole: Inside the Kelihos.B Takedown*, VERGE (Apr. 30, 2012, 2:10 PM), http://www.theverge.com/2012/4/30/2971958/kelihos-b-botnet-takedown-crowdstrike.

28 *See* Jim Edwards, *This Is What It Looks Like When a Click-Fraud Botnet Secretly Controls Your Web Browser*, BUSINESS INSIDER (Nov. 27, 2013, 4:18 PM), http://www.businessinsider.com/this-is-what-it-looks-like-when-a-click-fraud-botnet-secretly-controls-your-web-browser-2013-11.

29 *See* GA. TECH INFO. SEC. CTR., EMERGING CYBER THREATS REPORT 2011 3 (2010), *available at* http://www.mobileactivedefense.com/wp-content/uploads/2010/10/gtisc_report_2010.pdf.

30 Kok & Kurz, *supra* note 24, at 3.

31 *See* Moore, Clayton & Anderson, *supra* note 23, at 5–6.

32 *See* Mindi McDowell, *Security Tip (ST04-015): Understanding Denial-of-Service Attacks*, U.S. COMPUTER EMERGENCY READINESS TEAM (Nov. 4, 2009), http://www.us-cert.gov/cas/tips/ST04-015.html (last updated Feb. 6, 2013). DDoS attacks are best understood as a subset of these denial-of-service attacks, where many discrete entities individually interact with the target in seemingly innocuous ways such that the aggregate effect overwhelms the target's ability to process these interactions. *See id.* These types of cyber DDoS attacks have similar mechanisms to analogous noncyber DDoS attacks in the physical world. *See, e.g.*, Improv Everywhere, *Best Buy Uniform Prank*, YOUTUBE (Nov. 7, 2011), http://www.youtube.com/watch?v=KgUIbPfhSuo (demonstrating a noncyber DDoS where a large number of volunteers arrive at a store wearing clothes similar to the employee uniform, confusing legitimate customers about which personnel are actual employees); SPARTACUS (Universal Pictures 1960) (demonstrating a noncyber DDoS when a large number of slave rebels falsely self-identify as the slave leader "Spartacus" in order to shield the real Spartacus from identification and special punishment).

C. *The Common Thread: Innocent Intermediaries and the Attribution Problem*

These computer intrusions share a common tactic—the use of unknowing intermediaries' computers to hide the true origins of attacks. Sophisticated and unsophisticated attackers alike choose to leverage existing infections in order to hide their own identities.[33] As a result, researchers struggle to properly identify the specific computer or computers from which an attack originates.[34] Moreover, even knowing the source computer may not necessarily reveal the identity of the computer's owner, the identity of the hacker at the keyboard, or even the precise geographic location of the computer itself.[35] Cybersecurity experts commonly describe the difficulty of identifying the true actor behind an attack as "the attribution problem."[36] Therefore, any proposed legal solutions to hacking problems must account for the difficulty of attribution.[37] Specifically, policymakers should consider the interests of the innocent intermediaries who are also victims of cyber attacks.

The attribution problem makes it difficult for cyber attack victims to pursue their attackers using traditional legal process, especially across jurisdictional boundaries.[38] From service of process to pretrial discovery to meeting one's burden of proof, difficulties in identifying the computers and people behind attacks provide potential plaintiffs with such onerous procedural burdens that the problem of attribution effectively shields attackers from legal consequences, regardless of the attackers' actual liability under substantive law.[39]

---

33 *See* David D. Clark & Susan Landau, *Untangling Attribution*, 2 HARV. NAT'L SECURITY J. 323, 329 (2011) (noting that attackers "[have] usually taken care to be several degrees removed from the machines doing the actual attack").

34 *See id.* at 323.

35 *See id.* at 324.

36 *See, e.g., id.*; Scott J. Shackelford & Richard B. Andres, *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem*, 42 GEO. J. INT'L L. 971, 979 (2011).

37 Determining the identity of Internet attackers is often difficult, and it is nearly impossible to determine with sufficient confidence to successfully win a civil lawsuit. *See, e.g., Planning for the Future of Cyber Attack Attribution: Hearing Before the Subcomm. on Tech. & Innovation of the H. Comm. on Sci. & Tech.*, 111th Cong. 90–95 (2010) (statement of Robert K. Knake, International Affairs Fellow in Residence, Council on Foreign Relations) [hereinafter *Planning for the Future of Cyber Attack Attribution*].

38 *See* Clark & Landau, *supra* note 33, at 344–45.

39 Although the international nature of the Internet raises important issues of international law, jurisdiction, evidence, and procedure, a full analysis of these issues is beyond the scope of this Note. The procedural and jurisdictional issues here are relevant to this Note's analysis of substantive domestic law because the attribution problem is an important mechanism

II. CURRENT LAW RELATING TO HACKING

Several substantive areas of law govern unauthorized or unanticipated uses of computers on the Internet. Hackers may face criminal liability under the CFAA,[40] as well as under state computer hacking statutes.[41] Furthermore, hackers may face civil liability under the CFAA, state statutes, or state tort law.

A. The Computer Fraud and Abuse Act

1. The CFAA Forbids Hacking and Likely Does Not Provide a Privilege for Defending One's Property

The CFAA criminalizes the hacking of privately owned computers in several contexts. An attacker would violate the CFAA if the attacker intentionally accessed a "protected computer" without authorization, or exceeded authorized access, and then performed one of the following: obtained information, fraudulently obtained anything of value, or caused damage.[42] The CFAA does not define "authorization"[43] or "obtain information,"[44] so courts have generally applied the plain meanings of these words.[45] The CFAA also prohibits other offenses concerning government-owned computers[46] or national security information,[47] but this Note focuses on unauthorized remote access involving private parties and privately owned computers.

The CFAA does not expressly provide for defenses for necessity, duress, or defense of property, and it is unclear whether courts would recognize any such defenses. The mere absence of a statutory provision for self-help, however, does not necessarily indicate that the defense is not available.[48] When Congress creates a criminal statute that

---

by which incentives have become misaligned in the substantive law. *See* discussion *infra* Part III.A.

40 *See* 18 U.S.C. § 1030(a) (2012).

41 *See generally Computer Crime Statutes*, NAT'L CONF. ST. LEGISLATURES, http://www.ncsl.org/issues-research/telecom/computer-hacking-and-unauthorized-access-laws.aspx (last updated June 27, 2014) (listing the computer hacking statutes of all fifty states).

42 18 U.S.C. § 1030(a)(2), (a)(4), (a)(5).

43 *See id.* § 1030(a), (e).

44 *See id.* § 1030(e).

45 *See, e.g.*, United States v. Cioni, 649 F.3d 276, 283–84 (4th Cir. 2011) (holding that attempting to log into another person's email account and read their emails was "clearly" a violation of § 1030(a)(2)(C)'s prohibition against obtaining information through unauthorized access); LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1132 (9th Cir. 2009) (holding that "authorization," not separately defined in the CFAA, simply means the ordinary, plain dictionary definition of the word).

46 18 U.S.C. § 1030(a)(3).

47 *Id.* § 1030(a)(1).

48 *Cf., e.g.*, Dixon v. United States, 548 U.S. 1, 12–13 (2006) (holding that federal courts

is silent on common law defenses, courts must determine whether and how Congress intended the defenses to apply.[49] For modern statutory crimes that do not have close analogies to any common law crime, statutory silence on a defense creates even more ambiguity, because courts would be less able to rely on analogous common law doctrines in determining how common law defenses would fit with new crimes. Some scholars argue that this ambiguity means that courts ought to be more reluctant to extend common law defenses to nontraditional crimes.[50] Moreover, the CFAA's civil action provisions make the statute even less clear by raising the possibility that common law tort defenses may apply as well. Congress's silence on whether the CFAA includes defenses for self-defense, necessity, or defense of property has led to an ambiguity that discourages strong responses by legitimate computer security professionals.[51]

2. *The CFAA Covers Access to Nearly All Computers*

Throughout two decades of amendments, Congress has expanded the scope of the CFAA to cover nearly all networked computers in the world. Prior to 1984, federal law enforcement prosecuted computer crimes under the mail and wire fraud statutes.[52] However, Congress expressed concern that federal jurisdiction under these statutes left gaps in the law where certain types of computer fraud would not be punishable under federal law.[53] In response, Congress passed the Counterfeit Access Device and Computer Fraud and Abuse Act of

---

must "effectuate the duress defense as Congress may have contemplated it" (internal quotation marks omitted)); United States v. Oakland Cannabis Buyers' Coop., 532 U.S. 483, 490–91 (2001) (dictum) (discussing, without reaching a conclusion, the possibility that a necessity defense might be implied in some federal criminal statutes).

49 *See Dixon*, 548 U.S. at 12–13; *Oakland Cannabis Buyers' Coop.*, 532 U.S. at 490–91; *see also* Orin Kerr, *Does a "Cyber Self-Help" Defense Exist, and Would It Be a Good Idea?*, VOLOKH CONSPIRACY (Apr. 11, 2007, 5:32 PM), http://www.volokh.com/archives/archive_2007_04_08-2007_04_14.shtml#1176327133.

50 *See* Kerr, *supra* note 49 (arguing that the CFAA is "quite different" from the federal criminal statutes in *Dixon* and other cases where courts have allowed common law defenses such as necessity or duress, because violation of the CFAA is not a traditional crime—and the CFAA was therefore not enacted with a "background sense that [common law] defenses would apply"—and because the CFAA already lists other defenses in its statutory language).

51 *See* discussion *infra* Part III.A.

52 *See, e.g.*, United States v. Seidlitz, 589 F.2d 152, 153 (4th Cir. 1978) (applying the wire fraud statute to a defendant who had used interstate phone transmissions to fraudulently access a computer system).

53 *See* H.R. REP. NO. 98-894, at 6 (1984) (noting with alarm that in two serious computer access fraud cases, "had the access telephone calls not gone across [s]tate lines, the U.S. prosecutor would not have been able to use the wire fraud statute").

1984.[54] The law was later renamed the Computer Fraud and Abuse Act,[55] and Congress eventually broadened the statute to cover any computer "used in or affecting interstate or foreign commerce or communication."[56] Because of this broad language, the CFAA now applies to any computer that is connected to the Internet[57]—possibly even when the computer is located outside of the territory of the United States.[58] The Internet's rapid pace of growth in recent decades has therefore extended the reach of the CFAA to approximately one billion devices within the United States and ten billion devices worldwide.[59]

3. *Consequences of Violating the CFAA*

The CFAA carries a broad range of potential punishments depending on the type of violation. For a first-time conviction, unauthorized access of information from protected computers is punishable by imprisonment of up to one year,[60] and therefore qualifies as a Class A misdemeanor.[61] For extortion or fraudulent acquisition of more than $5,000 of value, the penalty increases to up to five years imprisonment,[62] or a Class D felony.[63] A first-time conviction of causing damage through unauthorized access carries a penalty of up to ten years, five years, or one year depending on whether the damage is—respec-

---

54 Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, 98 Stat. 2190 (codified as amended at 18 U.S.C. § 1030 (2012)).

55 Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213 (codified as amended at 18 U.S.C. § 1030).

56 18 U.S.C. § 1030(e)(2)(B).

57 *See, e.g.*, United States v. Trotter, 478 F.3d 918, 921 (8th Cir. 2007) ("With a connection to the Internet, the [victim's] computers were part of a system that is inexorably intertwined with interstate commerce and thus properly within the realm of Congress's Commerce Clause power." (internal quotation marks omitted)).

58 *See, e.g.*, United States v. Ivanov, 175 F. Supp. 2d 367, 373 (D. Conn. 2001) ("[T]here is clear evidence that the [CFAA] was intended by Congress to apply extraterritorially."). *Ivanov* involved a defendant who was physically present in Russia while hacking Connecticut computers through servers in the state of Washington. *Id.* at 368–70. It is unclear whether courts would find that the CFAA's definition of "protected computer" would extend to overseas computers, but the plain language of the statute appears to include even foreign computers. *See* 18 U.S.C. § 1030(e)(2).

59 *VNI Forecast Highlights*, CISCO, http://www.cisco.com/web/solutions/sp/vni/vni_forecast_highlights/index.html (last visited Aug. 18, 2014).

60 18 U.S.C. § 1030(c)(2)(A).

61 *Id.* § 3559(a)(6).

62 *Id.* § 1030(c)(3)(A).

63 *Id.* § 3559(a)(5).

tively—intentional, reckless, or neither.[64] Repeat convictions carry enhanced criminal penalties as well.[65]

Under certain circumstances, the CFAA provides a civil cause of action that allows victims to recover damages or seek equitable relief from violators of the CFAA.[66] Specifically, the statute allows victims to sue when the violation causes a loss of at least $5,000; modifies or impairs medical examination, diagnosis, treatment, or care; causes physical injury to any person; or threatens public health or safety.[67]

4. *The CFAA Overlaps with State Statutes*

All fifty states have their own antihacking statutes[68] that are substantially similar to the federal CFAA.[69] The dormant Commerce Clause limits states' ability to regulate Internet activity in ways that are not substantially similar to those used by the federal government or other states because the Internet's architecture does not easily allow for purely intrastate regulation.[70] As a result, the state statutes generally cannot criminalize behavior not already covered by the CFAA.[71]

B. *Common Law Torts Applied to Computer Access*

1. *Trespass to Chattels*

In recent decades, courts have revived the common law doctrine of trespass to chattels to address the growing problem of unsolicited Internet communications. Trespass to chattels applies to actions that either "dispossess[ ] another of the chattel" or "us[e] or intermeddl[e] with a chattel in the possession of another."[72] "Intermeddling" re-

---

64 *Id.* § 1030(c)(4)(A), (B), (G).

65 *Id.* § 1030(c)(1)(B), (2)(C), (3)(B), (4)(C)–(D).

66 *Id.* § 1030(g).

67 *Id.* § 1030(c)(4)(A)(i)(I)–(IV).

68 *See Computer Crime Statutes*, *supra* note 41.

69 *See, e.g.*, CAL. PENAL CODE § 502(c) (West 2010) (forbidding "access[ ] . . . without permission"); N.Y. PENAL LAW § 156.05 (McKinney 2010) (forbidding "access[ ] . . . without authorization").

70 *See, e.g.*, Psinet, Inc. v. Chapman, 362 F.3d 227, 240 (4th Cir. 2004) (describing as "nearly impossible" Virginia's attempt to regulate the Internet locally without impermissibly burdening interstate commerce); Am. Libraries Ass'n v. Pataki, 969 F. Supp. 160, 181 (S.D.N.Y. 1997) (striking down a New York Internet law on Commerce Clause grounds, reasoning that "[r]egulation by any single state can only result in chaos . . . subjecting Internet users to conflicting obligations").

71 *See Psinet*, 362 F.3d at 240; *Pataki*, 969 F. Supp. at 181.

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

quires intentional physical contact,[73] and courts have held that electronic signals are sufficiently physically tangible to satisfy this requirement.[74] In 1997, a federal district court held that under Ohio law, the bulk sending of unsolicited email, or "spam," sufficiently interfered with an email server's processing power and storage space to diminish the server's value, and that the email server's owner could thus sustain a cause of action for trespass to chattels.[75] Further, the court held that the victim could sue for nonphysical damages caused by such a trespass.[76]

Using a similar rationale, courts have applied the trespass to chattels doctrine to unwanted computer access as well. In *Register.com, Inc. v. Verio, Inc.*,[77] the Second Circuit upheld the application of New York's trespass to chattels doctrine to repeated bulk queries of a public database.[78] The court in *Register.com* based its decision on the fact that the defendant's continuous, automated behavior "consumed a significant portion of the capacity of Register's computer systems" and thus "impaired [their] condition, quality, or value."[79] Some courts have also followed this reasoning and broadened the application of the trespass to chattels doctrine to even intangible damage to computer servers.[80] However, the more recent trend is for courts to find that this type of trespass liability requires not only continuous and repeated access, but also a consumption of a significant amount of computer resources.[81] When the unwanted computer activity comes

---

73 *Id.* § 217 cmt. e.

74 *See, e.g.*, CompuServe Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1021 (S.D. Ohio 1997); Thrifty-Tel, Inc. v. Bezenek, 54 Cal. Rptr. 2d 468, 473 n.6 (Cal. Ct. App. 1996).

75 *CompuServe*, 962 F. Supp. at 1022.

76 *See id.* at 1023 (holding that a spammer could be liable to an email provider for the diminution of value provided through its email service, even in the absence of physical damage to any equipment).

77 Register.com, Inc. v. Verio, Inc., 356 F.3d 393 (2d Cir. 2004).

78 *Id.* at 404–05 (finding district court did not abuse discretion in determining that the use of automated querying software was a trespass to chattels, because "[the Defendant's] use of search robots, consisting of software programs performing multiple automated successive queries, consumed a significant portion of the capacity of Register's computer systems").

79 *Id.* at 404 (quoting RESTATEMENT (SECOND) OF TORTS § 218(b) (1965)).

80 *See, e.g.*, Snap-On Bus. Solutions Inc. v. O'Neil & Assocs., Inc., 708 F. Supp. 2d 669, 679 (N.D. Ohio 2010) (finding that a defendant's automated program with a high volume of queries could constitute "sufficient evidence to permit a reasonable trier [of fact] to conclude that [the defendant's program] either impaired the servers' condition, quality, or value or deprived [the plaintiff] of their use for a substantial time"); eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1070–72 (N.D. Cal. 2000) (finding that a high volume of repeated, automated queries on plaintiff's website caused sufficient impairment of the website server's condition to grant a preliminary injunction, even though eBay claimed no physical damage).

81 *Compare eBay*, 100 F. Supp. 2d at 1071 (holding that 80,000–100,000 automated queries

through a public service or one that the defendant was otherwise authorized to use, the person alleging harm usually must show that they suffered some burden to the computer itself as a result of the action[82]—or, at the very least, demonstrate that a "[specter] of . . . [other parties] joining the fray" could harm the plaintiff's business through degraded computer performance.[83] In summary, current courts are likely to find trespass to chattels liability only in cases where repeated access actually causes degradation in computer performance, as in a denial-of-service attack.[84]

2. *Nuisance and Unwanted Computer Activity*

Some scholars have argued that trespass to chattels is a poor doctrinal fit for the problem of spam or unwanted computer access and propose instead that courts should apply common law nuisance doctrine to electronic "intrusions."[85] Traditionally, the law of trespass protects "the right to exclusive possession of property," but the law of nuisance protects "the interest in use and enjoyment of property."[86] Electronic signals from remote sources do not dispossess the owner of the computer, and very few electronic attacks actually rise to the level of "intermeddling" that would be "equivalent to physical seizure of the chattel or similar deprivation of its use."[87] Further, the line of cases applying trespass to chattels to electronic intrusions traces its

---

per day, accounting for approximately one to two percent of eBay's traffic, harmed the "condition, quality, or value" of eBay's computer servers), *and* CompuServe Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1022 (S.D. Ohio 1997) (holding that continuous, automated sending of spam constituted an actionable trespass to chattels), *with* Ticketmaster Corp. v. Tickets.com, Inc., No. 99CV7654, 2000 WL 1887522, at *4 (C.D. Cal. Aug. 10, 2000) (holding that the relatively small volume of traffic from Tickets.com's automated crawlers did not meet the threshold for harming the condition, quality, or value of Ticketmaster's servers necessary to grant a preliminary injunction), *aff'd*, 2 F. App'x 741 (9th Cir. 2001), *and* Intel Corp. v. Hamidi, 71 P.3d 296, 306 (Cal. 2003) (holding that a few thousand unsolicited messages was a "minuscule" number compared to ordinary commercial traffic and did not satisfy the "condition, quality, or value" requirement to qualify as a trespass to chattels).

82 *See Ticketmaster*, 2000 WL 1887522, at *4 (finding in that particular case that mere repeated and continuous access did not rise to the standard of an "obstruction of its basic function"); *Intel*, 71 P.3d at 307 (rejecting the theory that loss of employee productivity was a "measurable loss from the use of its computer system").

83 *Ticketmaster*, 2000 WL 1887522, at *4.

84 *See supra* note 32 and accompanying text.

85 *E.g.*, Dan L. Burk, *The Trouble with Trespass*, 4 J. SMALL & EMERGING BUS. L. 27, 29, 53 (2000); Adam Mossoff, *Spam—Oy, What a Nuisance!*, 19 BERKELEY TECH. L.J. 625, 647–48 (2004).

86 Mossoff, *supra* note 85, at 647 (internal quotation marks omitted).

87 Burk, *supra* note 85, at 34.

doctrinal origins back to an unauthorized telephone access case,[88] where the court relied primarily on cases concerning real property and not personal property.[89] Scholars have argued that this reliance on trespass to land cases ignores a key distinction: courts have long recognized an "interest in inviolability" in real property but not in personal property.[90] These scholars argue that a more appropriate common law doctrine is nuisance, with its focus on an owner's interest in the enjoyment and use of property.[91]

Recognizing flaws in the trespass to chattels doctrine, at least as applied in the context of electronic activity, courts have begun to impose a more stringent standard in trespass to chattels cases[92]—quietly borrowing doctrines and concepts from nuisance law.[93] Still, courts have not actually applied nuisance law to computers, in part because courts appear reluctant to expressly endorse the use of real property doctrines on virtual spaces on the Internet.[94] In addition, nuisance law may have failed to garner much interest simply because of the greater body of case law analyzing trespass to chattels on the Internet.[95] Although common law nuisance has not been used in electronic intrusion cases, nuisance law is relevant for its self-help or summary

---

88 Thrifty-Tel, Inc. v. Bezenek, 54 Cal. Rptr. 2d 468 (Cal. Ct. App. 1996). In *CompuServe Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015 (S.D. Ohio 1997), the first case to apply trespass to chattels doctrine to computers, the court relied heavily on the reasoning in *Thrifty-Tel*. *See id.* at 1021–22.

89 *Thrifty-Tel*, 54 Cal. Rptr. 2d at 473 n.6.

90 *See* Burk, *supra* note 85, at 33–34 (noting that even the real property cases cited in *Thrifty-Tel* involved enough contamination by particles to effectively dispossess the plaintiff owners of their land).

91 *See, e.g.*, *id.* at 53–54; Mossoff, *supra* note 85, at 646–47; Steven Kam, Note, Intel Corp. v. Hamidi: *Trespass to Chattels and a Doctrine of Cyber-Nuisance*, 19 BERKELEY TECH. L.J. 427, 447–48 (2004) (arguing that nuisance is superior to trespass for electronic tort cases because nuisance law gives courts greater flexibility to consider aggregate harm and benefits, especially to third parties, when finding liability or ordering remedies).

92 *See* discussion *supra* Part II.B.1.

93 *E.g.*, Intel Corp. v. Hamidi, 71 P.3d 296, 306 (Cal. 2003); *see also* Mossoff, *supra* note 85, at 643–45 (discussing the "doctrinal confusion" caused by the *Intel* court imposing nuisance law's "substantial interference" test in a trespass to chattels analysis); Kam, *supra* note 91, at 443–45 (observing that the *Intel* opinion "emphasizes utilities and harms in a manner reminiscent of the balancing tests in the nuisance doctrine").

94 *See Intel*, 71 P.3d at 309–10 (rejecting the application of real property doctrines to the Internet, despite the "familiar metaphor of the Internet as a physical space," because at its core, the Internet is made up of computers, which are "personal property, not realty").

95 *See* John Edward Sharp, Comment, *There Oughta Be a Law: Crafting Effective Weapons in the War Against Spyware*, 43 HOUS. L. REV. 879, 921 (2006) (noting that arguments in favor of computer nuisance "arrive[d] too late," as "computer trespass is already making inroads as a cause of action").

abatement doctrine, which provides a framework for proposing a statutory right of self-help to victims of cyber attacks.

3. *A Limited Self-Help Privilege in Nuisance Law*

In certain circumstances, owners of real property are entitled to abate nuisances without resorting to formal legal proceedings.[96] Generally, the private privilege arises in cases concerning disputes between neighbors regarding adjacent parcels of land. When exercised by a private party, this self-help privilege is subject to several conditions: (1) the nuisance must give rise to an urgent or extreme necessity where the exigencies of the case will not allow delay;[97] (2) the remedy is confined to doing only what is necessary—and no more—to abate the nuisance;[98] (3) the person exercising the privilege must be able to do so without a breach of peace;[99] and (4) the privilege must be exercised within a reasonable time, without a large enough delay to allow resort to legal process.[100]

Moreover, one who chooses to exercise this self-help privilege "acts at his own peril and assumes all liability for exceeding the right."[101] The appropriate degree of care depends on the exigency of the need, and "a greater degree of care is required for summarily abating a nuisance in the absence of an emergency or imminent peril

---

96 *See* 58 AM. JUR. 2D *Nuisances* §§ 364–368 (2012).

97 *See, e.g.*, Cook Indus., Inc. v. Carlson, 334 F. Supp. 809, 816 (N.D. Miss. 1971) (finding no privilege in part because "[t]here was no urgency in their situation"); Martin v. Martin, 246 S.W.2d 718, 720 (Tex. Civ. App. 1952) (finding no privilege when the nuisance-abater waited over a year to act).

98 *See, e.g.*, *Cook Indus.*, 334 F. Supp. at 816 (holding that an effort to dam a drainage ditch, as a "maneuver to gain publicity and community support for their position," was well outside the scope of any self-help privilege); Fick v. Nilson, 220 P.2d 752, 753–54 (Cal. Dist. Ct. App. 1950) (holding that even though a landowner was privileged to cut overhanging branches or intruding tree roots, the landowner exceeded this privilege when he cut down entire trees); Md. Tel. & Tel. Co. v. Ruth, 68 A. 358, 360–61 (Md. 1907) (holding that the takedown of a telephone pole was privileged, even when causing damage to the mounted transformer, because any other method of takedown would have risked personal injury).

99 *See, e.g.*, *Cook Indus.*, 334 F. Supp. at 815 (stating that Mississippi recognizes an individual's right of self-abatement "provided he is able to do so without provoking a breach of the peace" (citing Lindsey v. Shaw, 49 So. 2d 580, 584 (Miss. 1950))); *Md. Tel. & Tel. Co.*, 68 A. at 360–61 (holding that there was no "breach of the peace" when there was sufficient notice to all parties that a takedown of a telephone pole would occur, and when the takedown did not risk physical injury to anyone).

100 *See, e.g.*, *Martin*, 246 S.W.2d at 720 (holding that a landowner's willful destruction of a regularly leaking sewage line was not privileged, because over a year had passed between the first sewage leak and the eventual destruction of the line, and the owner had enough time to resort to legal process).

101 *Cook Indus.*, 334 F. Supp. at 815.

to the [person exercising self-help] or his property."[102] This privilege is entirely optional and only applies in a narrow set of circumstances where the benefits to a party outweigh the harm to another. Also, proper exercise of this self-help privilege is unlikely to lead to retaliation and escalation between two parties, because the limits in scope and timing would still allow courts to find fault in cases of escalating disputes.[103]

III. CURRENT U.S. HACKING LAW DISCOURAGES THE RESPONSIBLE USE OF THE BEST AVAILABLE TECHNICAL SOLUTIONS TO A CYBER THREAT

Ambiguous legal standards and the threat of harsh penalties have not stopped security professionals from engaging in some legally questionable tactics, but the legal uncertainty has chilled their ability to share information or protect a broader portion of the public.[104] These security professionals have pioneered several innovative tactics in the past decade—engaging in their own counterattacks,[105] sinkhole operations, and ex parte in rem seizures of malicious computers and domains.

A. Harsh Criminal and Civil Penalties Disproportionately Deter Legitimate Organizations from Legally Questionable Network Access

The severe criminal and civil penalties for hacking create a dynamic where large American corporations are deterred from engaging in legally ambiguous counterattacks but malicious hackers are not de-

---

102 *Id.* at 815–16; *see also Md. Tel. & Tel. Co.*, 68 A. at 361 ("The interest of the party menaced by a nuisance should govern in determining the degree of care and expense to be observed in protecting from injury the objects constituting the nuisance during their removal by him.").

103 *See, e.g.*, *Fick*, 220 P.2d at 753 (sympathizing with nuisance-abater's position and recognizing his privilege but nonetheless finding that he exceeded his privilege and was therefore liable for damages).

104 *See* 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, 46 (2013) ("While a dialog has started to take shape with recent pronouncements by policymakers acknowledging the need to apply traditional notions of self-defense in cyber operations, meaningful guidance has not yet developed that would allow a stakeholder in the commercial community to freely take action that might be necessary to protect itself." (footnote omitted)).

105 This Note uses the term "counterattack" to encompass any unauthorized access by victims against their attackers, which other authors have described using the terms "hackback" or "counterstrike." This Note also uses "self-help" to describe the legal privilege to engage in counterattacks. In addition, this Note's use of the term "counterattack" includes read-only access and other activities involving little or no damage.

terred because of the low risk of being caught. Effective deterrence depends on the certainty and immediacy of negative consequences, as well as the severity of the negative consequences.[106] With the difficulty of attribution, hackers are unlikely to face negative consequences for their actions.[107] Further, the severity of civil penalties or criminal fines is low for those defendants who have few assets within the reach of domestic courts.

On the other hand, the deterrence effect is high against the legitimate corporations who are usually the victims of these attacks. These corporations maintain more complete business records and are under continuous public scrutiny, so they face a higher likelihood of being punished for any controversial or legally ambiguous activity.[108] Rich entities with deep pockets would potentially stand to lose a large amount from fines or monetary judgments, so the severity of punishment would be higher as well.[109] The end result is that the overall structure of U.S. hacking law does little to deter criminals and foreign governments, but leaves U.S. corporations overly cautious and unwilling to publicly respond in kind.

B. Counterattacks Are Already Occurring and Are Arguably Illegal

1. Google's Response to Operation Aurora May Have Violated the CFAA's Criminal Provisions, but It Did Not Give Rise to Civil Liability

Google's response to Operation Aurora[110] may have violated the CFAA's prohibition against "intentionally access[ing] a computer

106 *See, e.g.*, D.A. ANDREWS & JAMES BONTA, THE PSYCHOLOGY OF CRIMINAL CONDUCT 444–45 (5th ed. 2010) (summarizing a large body of research on the conditions of effective punishment and finding a broad consensus behind the importance of immediacy of punishment and perceived certainty of punishment).

107 *See* discussion *supra* Part I.C.

108 For example, Google has faced public scrutiny from consumer groups and governments amidst allegations that its mapping and imaging programs intercepted wireless communications in violation of the Wiretap Act. *See In re* Google Inc. St. View Elec. Commc'ns Litig., 794 F. Supp. 2d 1067, 1070–72 (N.D. Cal. 2011) (summarizing class action plaintiffs' allegations that Google had driven vehicles on public streets and had intercepted Wi-Fi communications), *aff'd sub nom.* Joffe v. Google, Inc., 746 F.3d 920 (9th Cir. 2013).

109 As discussed in the previous footnote, Google has faced controversy over its interception of wireless communications even though legal experts disagree on whether Google even violated any law. *See supra* note 108. Notably, Google has entered into a settlement agreement with the attorneys general of thirty-eight states and the District of Columbia, which requires Google to maintain a complex privacy program, submit to privacy audits, conduct a public education campaign, and pay $7 million to the states. *See* David Streitfeld, *Google Concedes Drive-by Prying Violated Privacy*, N.Y. TIMES, Mar. 13, 2013, at A1.

110 *See* discussion *supra* Part I.A.

without authorization . . . and thereby obtain[ing] . . . information from any protected computer."[111] Google gained access to a server in Taiwan and collected information about the nature of the attacks, the perpetrators of the attacks, and other victims of the attacks.[112] The Taiwanese server was connected to the Internet and, despite being located outside of the United States and its territories, was within the CFAA's definition of a "protected computer."[113] Without permission from the server's owner to access the logs, Google's intentionally accessing the server fits into the plain meaning of "without authorization."[114] In addition, the viewing and analysis of the logs is similar to logging into another user's email account to read messages and would have qualified as "obtaining information."[115] As discussed above, the legal ambiguity surrounding self-help means that raising such a self-help defense would be unlikely to succeed.[116]

Under this set of facts, Google would probably have met the requirements for Class A misdemeanor liability but not civil liability under the CFAA. Google obtained information without authorization from a protected computer, which carries a penalty of imprisonment up to one year and qualifies as a Class A misdemeanor.[117] Google's actions do not appear to have triggered civil liability under the CFAA, which requires a more tangible harm than simple access and the obtaining of information.[118] Google's actions do not appear to have damaged any computers, interfered with medical treatment, caused physical injury, or created a threat to public safety.[119]

---

111 18 U.S.C. § 1030(a)(2) (2012).

112 Sanger & Markoff, *supra* note 14.

113 *See, e.g.*, United States v. Ivanov, 175 F. Supp. 2d 367, 374 (D. Conn. 2001) (holding that the CFAA protects computers outside of the United States and its territories).

114 18 U.S.C § 1030(a)(2); *see also* LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1132 (9th Cir. 2009) (holding that "authorization," not separately defined in the CFAA, simply meant the ordinary dictionary definition of the word).

115 18 U.S.C. § 1030(a)(2)(C); *see also* United States v. Cioni, 649 F.3d 276, 283–84 (4th Cir. 2011) (holding that logging into another person's email account and reading emails was "clearly" a violation of § 1030(a)(2)(C)'s prohibition against obtaining information through unauthorized access).

116 *See* discussion *supra* Part II.A.1.

117 *See supra* notes 60–61 and accompanying text.

118 *See* 18 U.S.C. § 1030(c)(4)(A)(i)(I)–(V), (g) (authorizing civil actions against violators of the CFAA when the violation causes more than $5,000 in damage, interferes with medical diagnosis or treatment, causes physical injury, creates a threat to public safety, or damages government computers).

119 *See supra* note 67 and accompanying text.

Computer-related trespass to chattels generally requires a higher threshold of damage than merely reading or copying files once.[120] In order to maintain an action for trespass to chattels under California law, the continuous and repeated consumption of computer resources must actually degrade the performance of the computer.[121] Google's counterattack did not involve continuous, repeated access, and the counterattack itself occurred sometime in the month between Google's discovery of the attack and Google's announcement of the response.[122] Thus, any civil action against Google for the counterattack, whether under the CFAA or under state tort law, would be unlikely to succeed.

In summary, Google's actions probably constituted a criminal misdemeanor but did not expose Google to civil liability under either the CFAA or state tort law. A similar analysis would apply to any other counterattack in which the counterattacker merely copied information or accessed logs without actually degrading the services on the intermediary computer.

2. *The Federal Government's Implicit Approval of Google's Actions Demonstrates a Gap in the Law*

Despite the probability that Google may have committed a federal crime in responding to the Operation Aurora attack, Google is unlikely to face charges from federal prosecutors. After uncovering details of the attack, including its likely Chinese state sponsorship, Google notified law enforcement and intelligence officials of its findings.[123] After these briefings, the Secretary of State subtly indicated the executive branch's approval of Google's actions by turning attention instead to China's behavior—essentially communicating that there would be no criminal investigation into Google's actions and

120 *See* discussion *supra* Part II.B.1.

121 *See* Intel Corp. v. Hamidi, 71 P.3d 296, 306 (Cal. 2003) (holding that a few thousand unsolicited messages was "minuscule" compared to ordinary commercial traffic and did not satisfy the "condition, quality, or value" threshold required to qualify as a trespass to chattels). Although forum non conveniens law is outside the scope of this Note, the California Supreme Court's holding in *Intel* is especially relevant, as it would be binding authority in the jurisdiction most likely to survive a forum non conveniens motion to dismiss, because Google's own counterattack personnel and equipment are located in California. *See* Piper Aircraft Co. v. Reyno, 454 U.S. 235, 242 (1981) (holding that the locations of witnesses and evidence are important factors in forum non conveniens analysis); Stangvik v. Shiley Inc., 819 P.2d 14, 20–21 (Cal. 1991) (holding that in California courts, a corporate defendant's principal place of business is presumptively a convenient forum).

122 Sanger & Markoff, *supra* note 14.

123 *Id.*

implying that China was an impediment to "[t]he ability to operate with confidence in cyberspace."[124] Later that month, Secretary Clinton gave another speech about Internet freedom, specifically naming Google as a positive force for "internet and information freedom" and calling upon American companies to "make a principled stand" and fight censorship.[125] The State Department simultaneously released Secretary Clinton's speech translated into seven foreign languages—including Chinese.[126] With this speech following so quickly after Google's announcement of Operation Aurora and the aggressive counterinvestigation, the executive branch implicitly endorsed Google's actions throughout the attack and response.

The circumstantial evidence suggesting Chinese state sponsorship behind Operation Aurora may have made it easier for the government to publicly support Google, but the order of events indicates that Google had to engage in its counterattacking activity before the full scope and sophistication of the Operation Aurora attacks became known.[127] In other words, Google made a decision to engage in activity that was of questionable legality before it had indication that the results of such activity would earn government approval.

This approach, under which the victim must first engage in possibly criminal conduct and uncover evidence of government interest before seeking out government cooperation and approval, carries a considerable amount of legal risk for prospective counterattackers. Potential counterattackers would expose themselves to liability before the nature of the initial attack is apparent. In addition, the risk of criminal prosecution may cause counterattackers to be overly reluctant to share their findings with other security professionals or government agencies—even if the investigation uncovers information of interest to defense, intelligence, and law enforcement agencies.

---

124 Hillary Rodham Clinton, U.S. Sec'y of State, Statement on Google Operations in China (Jan. 12, 2010), *available at* http://www.state.gov/secretary/20092013clinton/rm/2010/01/135105.htm.

125 Hillary Rodham Clinton, U.S. Sec'y of State, Remarks on Internet Freedom (Jan. 21, 2010), *available at* http://www.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm.

126 *See id.* (listing translated transcripts available in Arabic, Chinese, French, Persian, Russian, Spanish, and Urdu).

127 *See* Sanger & Markoff, *supra* note 14 (reporting that Google first engaged in a "secret counteroffensive" and then reported its findings to law enforcement and intelligence officials *after* "[s]eeing the breadth of the problem" from the Taiwanese server's logs).

3. *Other Entities Also Engage in Counterattacking*

Many other legitimate security professionals are also engaging in counterattacks to investigate or mitigate attacks from malicious actors.[128] Security software vendors sell tools capable of real-time hackback.[129] In early 2013, Mandiant, a computer security firm, published a comprehensive report compiling intelligence on a particular "prolific" hacker group and concluding that this group was "likely government-sponsored" and possibly a unit within the Chinese military.[130] Much of the evidence that was shared with the public consisted of videos surreptitiously recorded from the hackers' computer sessions—including videos of the hackers performing tasks on their own networks.[131] Detailed statistics are not available, in large part because the legal ambiguity discourages candid discussion of the topic within the computer security community.[132]

C. *Legal Restrictions Limit the Effectiveness of Anti-Botnet Strategies*

The legal ambiguity surrounding counterattacks affects the security of ordinary Internet users as well—even ordinary users who lack the means or desire to engage in their own counterattacks. The security professionals responsible for safeguarding ordinary users on the Internet often encounter legal limits that hinder their ability to protect ordinary computers.

One strategy for combating malware on personal computers is to engage in a "sinkhole" takedown operation. Many botnets operate in a decentralized fashion, and may be configured to update the contact information for the command and control servers so that the infected bots begin taking commands from a new server.[133] This design gives the malicious botnet operator resilience against targeted attacks directed at a single weak link.[134] Resilience against targeted attacks, however, opens the botnet to another type of vulnerability: legitimate

---

128 *See Black Hat Survey: 36% of Information Security Professionals Have Engaged in Retaliatory Hacking*, REUTERS (July 26, 2012, 11:00 AM), http://www.reuters.com/article/2012/07/26/idUS184869+26-Jul-2012+BW20120726.

129 *See* Andy Oram, *Symbiot on the Rules of Engagement*, ONLAMP.COM (Mar. 10, 2004), http://www.onlamp.com/pub/a/security/2004/03/10/symbiot.html (interviewing a vendor who strongly advocated the use of his company's software to engage in "counter-strike capabilities," even against infected intermediary computers).

130 MANDIANT, *supra* note 22, at 2–3.

131 *See* MandiantCorp, *supra* note 22.

132 *See* discussion *supra* Part III.A–B.

133 Hicks, *supra* note 27.

134 *See id.* ("Infected machines typically receive commands from other infected machines—

security professionals, also known as "white hats," can sometimes successfully mimic the update command so that the infected bots listen for commands from servers within the control of the white hats.[135] The white hats then use this botnet control to prevent the infected computers from receiving any further malicious commands.[136]

A serious limitation of this tactic is that legitimate security organizations are unwilling to actually cure the infection on these bots.[137] Legal uncertainty discourages these security organizations from taking the technically trivial step of patching the infected computers and removing the malware.[138] Instead, the infected computers sit quarantined and wait for malicious commands that never come, and the white hats must fund the cost of indefinitely maintaining a nonmalicious botnet controller.[139] The ordinary Internet user is harmed by the continued existence of a malware infection, and resolving the legal ambiguity would allow those in a position to cure the infection to easily do so.

Another anti-botnet tactic is to use the courts to physically seize the command and control servers or seize their addresses.[140] In these cases, security organizations file complaints in federal court, sometimes under the civil RICO statute,[141] and seek ex parte temporary and permanent injunctions.[142] Tying together all the malicious servers into an alleged racketeering conspiracy gives the court and the plain-

---

this makes it more difficult to 'decapitate' the network by eliminating a single command-and-control server.").

135 *See id.* ("If researchers can crack the communications protocol used among the peers, they can create 'poison' data that will propagate through the whole botnet. The data forces all peers to connect to a single machine. That machine, of course, belongs to the white hats, who now control the botnet.").

136 *See id.*

137 *See id.* ("The sinkhole only shifts control of the botnet; it doesn't cure the zombie computers.").

138 *See id.* (noting that sticky legal and ethical questions leave security researchers hesitant to actually "push an update . . . [to] remove the offending software").

139 *See id.*; Adi Robertson, *FBI Says 360,000 DNSChanger-Infected Computers May Lose Web Access in July*, VERGE (Apr. 23, 2012, 4:51 PM), http://www.theverge.com/2012/4/23/2969730/fbi-dnschanger-server-shutdown-date-july-9th (explaining that the FBI maintained clean botnet servers for almost a year after taking down DNSChanger botnet).

140 *See, e.g.*, Tim Cranton, *Cracking Down on Botnets*, OFFICIAL MICROSOFT BLOG (Feb. 24, 2010, 6:16 PM), http://blogs.technet.com/b/microsoft_blog/archive/2010/02/25/cracking-down-on-botnets.aspx.

141 Racketeer Influenced and Corrupt Organizations (RICO) Act, 18 U.S.C. §§ 1961–1968 (2012).

142 *See, e.g.*, Amended Complaint, Microsoft Corp. v. Does 1–39, No. 12-cv-01335 (SJ/RLM) (E.D.N.Y. June 29, 2012); Proposed Order for Permanent Injunction, Microsoft Corp. v. Does 1–39, No. 12-cv-01335 (SJ/RLM) (E.D.N.Y. Nov. 28, 2012).

tiff the legal tools to take down an entire botnet at once. Using legal process, these plaintiff security organizations ultimately obtain court orders authorizing U.S. Marshals to physically seize the servers and transfer them to the plaintiffs' technical experts for further analysis.[143]

A similar variation on this strategy is to seize the addresses of the servers, especially when the servers are physically outside of the territory of the United States but use domain names within the United States' jurisdiction.[144] These domain name seizures then have the effect of severing the communications links between the botnet itself and the botnet controller.

These ex parte seizures are a powerful weapon in the fight against consumer malware, but they suffer from limitations as well. As with the sinkhole tactics discussed above, the underlying malware infections on the botnet's computers are left intact.[145] In addition, this legal process cannot reach servers physically located outside of the United States that do not use United States domains.[146] These jurisdictional gaps mean that these ex parte seizures followed by permanent injunctions are valuable tools for fighting malware controlled

143 *See* Dennis Fisher, *Microsoft, FireEye Take Down Notorious Rustock Botnet*, THREATPOST (Mar. 18, 2011, 12:59 PM), http://threatpost.com/microsoft-fireeye-take-down-notorious-rustock-botnet-031811 (describing the seizure of servers).

144 Domain names are the familiar Internet addresses that resolve to the actual computer providing the service. For example, "www.google.com" resolves to a physical computer located in one of Google's data centers. The rightmost segment of the address, set aside with a period, is called the "top level domain." The top level domains ".com," ".net," ".org," and many others are administered by U.S. organizations and are subject to legal process under United States law. *See, e.g.*, *Ex Parte* Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction at 3–5, Microsoft Corp. v. Does 1–27, No. 1:10:cv156 (LMB/JFA) (E.D. Va. Feb. 22, 2010) (finding good cause to believe that unnamed defendants had "engaged in illegal activity using .com Domains which are maintained by the top level domain registry Verisign, located in the United States and the Eastern District of Virginia," and ordering Verisign to hold the domains in escrow).

145 *See* Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 HARV. J.L. & TECH. 429, 444 (2012) ("[I]nterrupting the controller's ability to issue commands to the infected computers . . . [is] generally only [a] temporary measure[ ] because the zombie computers remain infected.").

146 *See* Lilian Edwards, *Dawn of the Death of Distributed Denial of Service: How to Kill Zombies*, 24 CARDOZO ARTS & ENT. L.J. 23, 45 (2006) ("[E]ffective legal action may be extremely difficult to take against either criminals lurking in foreign jurisdictions or teen hackers with few or no resources. Just as it is difficult to prosecute zombie masters under criminal law, civil law actions are also likely to be ineffective in curbing their activities."). Some other countries have followed the United States' lead and have engaged in similar seizures of domains within their respective jurisdictions. *See, e.g.*, Brian Krebs, *Polish Takedown Targets 'Virut' Botnet*, KREBS ON SECURITY (Jan. 18, 2013, 10:59 AM), http://krebsonsecurity.com/2013/01/polish-takedown-targets-virut-botnet (reporting that the Polish domain registrar NASK had seized twenty-three Polish domains in a botnet takedown).

from within the United States, but that these tactics alone are insufficient to combat the widespread problem of malware across international borders.[147]

IV. PREVIOUSLY PROPOSED LEGAL SOLUTIONS FALL SHORT

A. *Imposing Tort Liability to Give a Defense of Property Privilege Is an Imprecise Solution*

Some scholars have suggested applying a negligence or nuisance theory with respect to computer owners who allow their computers to become infected with malware.[148] This way, victims of cyber attacks would be privileged under state tort law to respond with their own mitigating or preemptive counterattacks—even against innocent intermediaries—whenever the social benefit outweighs the cost.[149] These proposed solutions fall short in two ways: many computer infections are not the result of negligence, and common law doctrines would not address the criminal and civil liability stemming from antihacking statutes.

1. *Many Infections Are Not the Result of Negligence*

A substantial number of innocent intermediaries would not meet the traditional definition of negligence.[150] Specifically, the most problematic element of negligence would be proving that a computer owner has failed to meet the appropriate standard of care.[151] With regard to ordinary computer owners' duties, any standard of care

147 *Cf.* Krebs, *supra* note 146 (expressing doubt that seizing Polish domain names would have a long-term effect against a botnet that also uses Russian domain names "outside the reach" of the Polish authorities).

148 *See, e.g.*, Burk, *supra* note 85, at 53–54 (advocating for the application of nuisance principles to the Internet for activities that are more intrusive than beneficial); Stephen E. Henderson & Matthew E. Yarbrough, *Suing the Insecure?: A Duty of Care in Cyberspace*, 32 N.M. L. REV. 11, 16–18 (2002) (analyzing both the duty and standard of care involved in protecting one's own computer against becoming a staging ground for attacks under a negligence analysis); T. Luis de Guzman, Comment, *Unleashing a Cure for the Botnet Zombie Plague: Cybertorts, Counterstrikes, and Privileges*, 59 CATH. U. L. REV. 527, 551–54 (2010) (arguing that owners of infected bots should be held liable to DDoS victims under a negligence theory).

149 *See* RESTATEMENT (SECOND) OF TORTS §§ 64, 87 (1965) (outlining privileges of self-defense against negligent conduct and defense of chattels against dispossessory acts); de Guzman, *supra* note 148, at 556.

150 *See generally* RESTATEMENT (SECOND) OF TORTS § 281(b) (1965).

151 *See* Kesan & Hayes, *supra* note 145, at 499 ("Under the common law, it would likely be difficult to hold any intermediary party liable in tort for harm caused by a DDoS attack. First, it is unclear whether any intermediary party owes a duty of care to the ultimate victim."); *see also* Edwards, *supra* note 146, at 48–49 (discussing reasonable foreseeability problems with imposing a new duty of security on home computer users).

strict enough to give victims a self-help privilege under negligence law would also unfairly categorize many ordinary users as negligent.[152]

As discussed above, the attackers of greatest interest to the security community are known for their technical sophistication and patience.[153] If full time security employees at dedicated computer security corporations, defense contractors, and Silicon Valley giants cannot reliably secure their systems against all attacks,[154] ordinary users could not reasonably be expected to protect their computers from all infections—especially against zero-day attacks.[155] At best, ordinary users could be expected to secure their computers against publicly known malware.[156] Proponents of a negligence standard acknowledge the unfairness of holding "personal users" to the standard "required to establish military-grade systems."[157] Unfortunately, some botnets exploit zero-day vulnerabilities, so malware would still infect the computers of owners who do meet a reasonable standard of care.[158]

Because falling victim to a malware infection does not always stem from negligence, a potential counterattacker would often have to make a decision based on incomplete information. For example, an attack could exploit a zero-day vulnerability and infect certain computers (nonnegligent zombies). If the vendor later patches the vulnerability, but not all users apply the update, unpatched systems will still become infected and join the botnet (negligent zombies). If the

---

152 *See* Edwards, *supra* note 146, at 48–49 ("Does a home PC user really foresee that their failure to install Microsoft patches will lead to WorldPay being taken out by a DDOS attack?"). *See generally* RESTATEMENT (SECOND) OF TORTS § 282 (1965) ("[N]egligence is conduct which falls below the standard established by law for the protection of others against unreasonable risk of harm.").

153 *See* discussion *supra* Part I.A (discussing "advanced persistent threats").

154 *See* discussion *supra* Part I.A.

155 A "zero-day" attack is an attack that exploits a vulnerability that was not previously known to the vendor or the security community. *See* Leyla Bilge & Tudor Dumitras, *Before We Knew It: An Empirical Study of Zero-Day Attacks in the Real World*, *in* PROCEEDINGS OF THE 2012 ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY 833 (2012), *available at* http://dl.acm.org/citation.cfm?id=2382196.2382284. In contrast, some attacks take advantage of the fact that some computers do not have all the latest security patches applied and exploit known vulnerabilities on these systems. *Id.*

156 *See* de Guzman, *supra* note 148, at 556 n.196 (hinting at a distinction between zero-day vulnerabilities and known vulnerabilities by discussing the reasonableness of expecting a user to apply a fix to a known vulnerability once a "reasonable user would have become aware that a fix was available").

157 Henderson & Yarbrough, *supra* note 148, at 17.

158 *See, e.g.*, Brian Krebs, *Crimeware Author Funds Exploit Buying Spree*, KREBS ON SECURITY (Jan. 7, 2013, 12:05 AM), http://krebsonsecurity.com/2013/01/crimeware-author-funds-exploit-buying-spree/.

botnet attacks a victim, the victim will be unable to distinguish between the "nonnegligent" zombies and the "negligent" zombies. Legally speaking, the victim would be privileged to counterattack against the negligent zombies but not the nonnegligent zombies[159]—replacing legal ambiguity with factual ambiguity and eliminating any practical gain from this privilege.

2. *The CFAA and Other Statutes Still Apply to Counterattacks Even If Privileged Under State Tort Law*

Even if courts could create a workable standard for a computer owner's standard of care, or were to apply nuisance doctrine to the Internet, state tort law would not change the applicability of the federal CFAA statute, which does not provide a counterattack privilege. Federal law preempts state law when the two conflict,[160] so a privilege under state tort law would not protect a counterattacker from negative legal consequences. As discussed above, the CFAA criminalizes any counterattacks, including some counterattacks that cause no damage.[161] From the perspective of a potential counterattacker, a state tort privilege would provide little reassurance when the very same actions violate federal criminal law. Therefore, giving counterattackers a state tort privilege would not give sufficient legal cover to make a practical difference in a counterattacker's risk calculus.

B. *Giving Counterattack Power Only to Government Agencies Would Inefficiently Stretch Government Resources*

Other legal scholars have argued that only the government should have the right to counterattack against hackers.[162] A variation of this proposal involves giving the government the authority to deputize private entities to engage in cyber operations on behalf of U.S. interests.[163] Any deputization framework would fit well into the na-

159 *See supra* note 149 and accompanying text.

160 McCulloch v. Maryland, 17 U.S. (4 Wheat.) 316, 406 (1819).

161 *See* discussion *supra* Part II.A.1.

162 *See, e.g.*, Susan W. Brenner & Leo L. Clarke, *Civilians in Cyberwarfare: Conscripts*, 43 VAND. J. TRANSNAT'L L. 1011, 1033–34, 1037 (2010) (arguing that offensive civilian counterattacks in a cyberwar context would risk "punitive reprisals" and would "erode[ ] the distinction between combatants and noncombatants" in the law of armed conflict); Orin S. Kerr, *Virtual Crime, Virtual Deterrence: A Skeptical View of Self-Help, Architecture, and Civil Liability*, 1 J.L. ECON. & POL'Y 197, 205–06, 213 (2005) (arguing that a private self-help privilege would pose a danger to innocent third parties).

163 *See, e.g.*, Zach West, Note, *Young Fella, If You're Looking for Trouble I'll Accommodate You: Deputizing Private Companies for the Use of Hackback*, 63 SYRACUSE L. REV. 119, 139–41 (2012).

tion's overall cybersecurity policy and would probably improve the United States' resilience against cyber attacks.[164] However, a deputization policy should be seen as only one of several complementary policies for improving security on the Internet, because deputization alone will not be enough to protect the United States' interests.

Limiting private counterattacks to only those deputized by the government would effectively require government approval before any counterattack operation would be lawful. Requiring that all privileged counterattack operations first meet government approval suffers from fundamental weaknesses in efficiency and efficacy: private sector actors are already responsible for their own computer security measures, the nature of the government's interest may not become apparent until after a counterattacker successfully accesses a hostile system, and the government lacks the resources to investigate all attacks.

1. *The Government Already Expects Private Actors to Take Responsibility for Securing Their Own Networks*

Although governments, software vendors, hardware manufacturers, and security organizations can and do provide services for improving security on the Internet, government officials agree that the ultimate responsibility for securing computer systems lies with the computers' owners.[165] As it stands now, the government expects computer owners to take steps to protect their own networks and their own data.[166] After Google fell victim to Operation Aurora, Google's security team was surprised to discover that the National Security Agency ("NSA") did not provide protection to privately owned computer networks, even from foreign state-sponsored attacks.[167] Current law therefore leaves the private sector to fend for itself without granting an analogous level of power.

Giving the government the exclusive power to authorize counterattacks would create mismatched incentives where the authority to counterattack is assigned to a separate party from the cost-bearing

---

164 *See id.* at 141–44 (analyzing the relative strengths of the government and the private sector and arguing that a deputy relationship would leverage each side's respective strengths).

165 *See* THE WHITE HOUSE, CYBERSPACE POLICY REVIEW 17 (2009), *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf (emphasizing the private sector's responsibility because it "designs, builds, owns, and operates most of the network infrastructures that support government and private users alike").

166 *See id.* at 17–19.

167 *See* Gross, *supra* note 16, at 225 (quoting a former White House official as saying: "After Google got hacked, they called the N.S.A. in and said, 'You were supposed to protect us from this!' The N.S.A. guys just about fell out of their chairs. They could not believe how naïve the Google guys had been.").

victim. With such an incentive scheme, the government would likely be overly reluctant to exercise its counterattack power.[168] Moreover, the private sector as a whole has substantial cybersecurity expertise, which government officials stress is an important part of our nation's cybersecurity posture.[169]

Further, the borderless Internet has created an environment in which the practical distinctions between the private and public sectors have blurred. Large multinational corporations often fill roles traditionally reserved for nation states, and they may need analogous powers traditionally reserved for nation states—such as the inherent right of self-defense against state-sponsored attacks.[170] This dynamic weakens the rationale for reserving counterattack powers solely for the government and its chosen deputies.

2. *The Full Extent of the Government's Interest Might Not Be Known Before the Private Actor Investigates the Origin of an Attack*

In addition to private sector entities naturally having a more immediate, direct interest in fighting their attackers, the government should allocate its own resources efficiently by focusing attention towards attacks that are already known to affect a government interest. Giving private sector entities the power to proactively investigate computers outside their network would give the government more complete intelligence on the origin, nature, and scope of attacks—before the government invests resources into an investigation. Armed with better data collected by the private sector, the government should be able to efficiently allocate resources to attacks that have the most effect on federal interests—attacks with implications for foreign policy, national and homeland security, and national economic stability. Similarly, any deputizing process where the government gives private parties the authorization to engage in hackback would still require government involvement at a preliminary, low-information

168 *See* Ross Anderson et al., *Incentives and Information Security*, *in* ALGORITHMIC GAME THEORY 633, 633 (Noam Nisan et al. eds., 2007) ("Systems are particularly prone to failure when the person guarding them is not the person who suffers when they fail.").

169 *See* Brenner & Clarke, *supra* note 162, at 1071–73 (observing that the private sector has a vastly larger pool of computer security professionals than does the military or civilian government).

170 Gross, *supra* note 16, at 234 (quoting Michael Hayden, former Director of the National Security Agency, as saying: "Because of their size, [large multinational corporations] actually are making decisions that have the impact of the kinds of decisions made in the halls of government. Google is not a state. But what constitutes Google's inherent right of self-defense in this new environment against this kind of attack?").

stage of the investigation.[171] In a situation where the private sector lacks the legal authority to conduct a robust investigation and where the government does not have the means to investigate every private sector attack, the government would have to make decisions on how to allocate resources without fully understanding which attacks directly implicate its interests.

V. SOLVING THE PROBLEM OF CYBER ATTACKS BY GRANTING A LIMITED SELF-HELP PRIVILEGE IN THE CFAA

A. Congress Should Create a Self-Help Privilege with Important Restrictions

The nature of the interests involved points towards a specific solution for resolving the current legal ambiguity surrounding counterattacks—creating a statutory, limited self-help privilege for victims of cyber attacks. Specifically, Congress should amend the CFAA to codify a self-help privilege with the following requirements: (1) the counterattack must be necessary and proportional to the threat being mitigated or prevented; (2) the counterattack must be in response to an ongoing or repeated attack; (3) the counterattacker must submit a good-faith justification and notification to the government; and (4) the counterattacker must assume strict liability for all damage to third parties, and liability for all negligently caused unnecessary damage to the original attacker. Moreover, Congress should expressly preempt state law, giving anyone who counterattacks within the proposed limitations a defense to criminal prosecution or tort liability in state courts.

B. The Proposed Codified Counterattack Privilege Would Resolve Current Legal Ambiguity

Codifying this counterattack privilege in the CFAA would immediately resolve ambiguity in the law and would provide a uniform, consistent framework to apply in cases in which these issues arise in United States courts. By systematically checking the counterattackers' compliance with each of the express elements of the privilege, courts would be able to analyze facts using a test designed specifically for cyber attacks, instead of trying to fit centuries-old common law doctrines to modern computer activity. Similarly, attorneys for security companies and multinational Internet corporations would be able

171 *See* West, *supra* note 163, at 140–41 (noting need for DOJ involvement and investigation prior to decision to deputize private company and grant authorization for hackback).

to effectively counsel clients on how to design procedures to successfully and lawfully defend their own networks against cyber threats.

In addition, federal preemption of state law would clear up ambiguity in state law, especially when interstate jurisdictional issues do not give clear answers. Express preemption would save potential counterattackers the burden of the highly fact-intensive inquiry of determining which state's laws potentially apply to their actions.

C. *Authority Would Reside with the Actors Who Will Bear the Costs of Both Action and Inaction*

This proposal aligns incentives so that the same party who bears the costs of inaction would also have the authority to act. As the law currently stands, and under some proposals, those in the private sector are confined to their own networks while simply hoping that the government will investigate outside of the victim's network. This arrangement decouples the government's decisionmaking authority from the private sector's costs. Instead, the cost-bearing victim should have some additional authority to go beyond its own network to investigate and mitigate its risk from external attacks.[172] For counterattacks, granting authority to those cost-bearing private entities would properly align incentives between costs and responsibility.

At the same time, any counterattackers who may take actions under a self-help proposal must bear the costs of their own actions.[173] This proposed self-help framework would incentivize doing only what is necessary to prevent, mitigate, or investigate an attack. By imposing strict liability for damage done to third parties in a counterattack, this proposal would encourage counterattackers to exercise a high standard of care.[174]

D. *Actors Would Be Encouraged to Share Information, Including Findings from Counterattack Operations*

This proposal would encourage open communication throughout the security community, to include communication between the pri-

---

172 *See, e.g.*, R. H. Coase, *The Problem of Social Cost*, 3 J.L. & ECON. 1, 11 (1960); Richard A. Posner, *A Theory of Negligence*, 1 J. LEGAL STUD. 29, 33 (1972).

173 Liability would internalize any negative externalities associated with these counterattack actions and prevent actions with a net aggregate cost to the participants on the network. *See, e.g.*, Posner, *supra* note 172, at 33 (analyzing that a rational actor will avoid imposing costs that exceed the actor's benefit when the actor is liable for those costs); *see also* SPIDER-MAN (Columbia Pictures 2002) ("With great power comes great responsibility.").

174 *See* Mark Geistfeld, *Negligence, Compensation, and the Coherence of Tort Law*, 91 GEO. L.J. 585, 619 (2003).

vate sector and appropriate government agencies.[175] As discussed above, the legal ambiguity surrounding counterattacks discourages transparency in the security community, depriving the defenders of computer networks of the information they need to effectively combat sophisticated attackers.[176] Moreover, with the threat of prosecution lifted, the computer security community would be more willing to share threat information with one another, including information about the effectiveness of various counterattack tactics.[177]

By requiring disclosure of all privileged counterattacks to the government, this proposal also opens communication between the private sector and the government, which could use these disclosures to improve awareness over the cyber threat landscape. In this way, this proposal would complement other proposals that encourage greater partnership and information sharing between the public and private sectors.[178]

E. This Self-Help Privilege Accommodates Concerns Raised Against Previous Counterattack Proposals

This proposal would address common criticisms levied against previous counterattack proposals: that a counterattack privilege would risk an endless cycle of escalating retribution between cyber attackers, that a privilege is dangerous in a world where attribution of attacks is difficult, and that a privilege would not deter attackers.

Earlier proposals to create self-help privileges have been criticized as being counterproductive in an environment in which attribution is difficult.[179] One danger is that this privilege would encourage "bankshot" attacks—where an attacker disguises himself so that the victim retaliates against an innocent third party.[180] Former NSA Senior Counsel Joel Brenner has noted that even a purely defensive booby-trap tactic, where potential victims place malware in their own decoy files, could backfire in the event that the attacker decides to intentionally cause harm by opening the booby-trapped file from inside the compromised network of either the victim or an innocent third party.[181]

---

175 *See* discussion *supra* Part III.B.2.

176 *See* discussion *supra* Part III.B.2.

177 *See* discussion *supra* Part III.B.2.

178 *See* THE WHITE HOUSE, *supra* note 165, at 17–19.

179 *See* discussion *supra* Part I.C.

180 *See* Kerr, *supra* note 162, at 205–06.

181 Joel Brenner, Former Senior Counsel, National Security Administration, Address at The George Washington University Cyber Security Policy and Research Institute and Depart-

This Note's proposal, however, contains several strong mechanisms for preventing third party injury and a cycle of escalating retribution. These criticisms have mostly focused on proposals allowing for destructive counterattacks,[182] while the exigency, necessity, and notification requirements of this Note's proposal would strongly discourage any disabling or damaging counterattack actions. The focus of the current proposal is on prevention, mitigation, and investigation; and white hat professionals have already exhibited strong reservations against any actions that may have irreversible consequences.[183] As with nuisance disputes between neighbors, courts would not endorse unnecessarily harmful behavior, and any counterattacker would act "at his own peril and assume[ ] all liability for exceeding the right."[184] In other words, this proposal gives a very limited privilege that would cover access but not damage in most cases.

Moreover, early notification to the government would allow it to step in when it believes a private counterattack risks harm to government interests, especially in regard to foreign relations, national security, or homeland security. Escalation and retribution between two privileged counterattackers would be highly unlikely if they have to report their privileged counterattacks to a common authority.

Critics have also correctly pointed out that a counterattack privilege would not deter attackers,[185] but this proposal does not rely on deterrence to achieve its goals. Because attribution is difficult,[186] the proposed counterattack privilege would provide for very little protection from liability for intentionally causing damage in a counterattack. Merely investigating the origins of an attack may be sufficient to enable the victim of an attack to thwart any continuing attack, and the counterattacker would lose any privilege to cause damage once the

---

ment of Computer Science: America the Cyber-Vulnerable (Jan. 24, 2013); *cf.* Bruce P. Smith, *Hacking, Poaching, and Counterattacking: Digital Counterstrikes and the Contours of Self-Help*, 1 J.L. ECON. & POL'Y 171, 185–87, 195 (2005) (distinguishing retaliatory cyber counterattacks from spring gun traps in large part because cyber counterattacks would involve greater discretion and discrimination).

182 *See* Smith, *supra* note 181, at 180–81 (assuming without discussion that counterstrikes will involve "collateral damage" to third parties).

183 *See* Hicks, *supra* note 27 (reporting a contentious debate in the security community about the fear of "pushing code onto someone else's machine and something [going] wrong," described as "very, very bad").

184 Cook Indus., Inc. v. Carlson, 334 F. Supp. 809, 815 (N.D. Miss. 1971) (defining the narrow scope of the self-help privilege in abating a nuisance).

185 *See, e.g.*, *Planning for the Future of Cyber Attack Attribution*, *supra* note 37.

186 *See supra* note 37 and accompanying text.

exigency of the threat has passed.[187] Under this proposal, victims of cyber attacks would be better equipped to defend themselves without the need to deter bad actors.

Further, even in the event of harm to innocent third parties, this proposal facilitates fair compensation from the counterattacker. The strict liability regime would make the substantive liability inquiry relatively straightforward. The governmental notification requirement would pave the way for streamlined evidentiary discovery.

Similarly, actions that exceed the scope of this privilege would still allow for an orderly recovery of damages—especially when compared to the difficulties involved in ordinary hacking cases where identities are uncertain.[188] Nonetheless, such suits between an actual attacker and counterattacker would probably be rare, because the first attacker would expose themselves to potential counterclaims by filing a complaint.[189]

F. This Proposal Complements Other Counterattack Proposals

Giving a self-help privilege to victims of cyber attacks does not preclude other policy proposals. This self-help privilege would work well alongside proposals advocating government-appointed deputies who are authorized to engage in their own offensive cyber attacks.[190] This Note's proposal gives a very limited privilege to counter attack only when justified by necessity and exigency, and it imposes strict liability for damage to innocent third parties.[191] A deputization scheme could give a stronger privilege with the government's express approval, either by privileging more aggressive actions or by applying a more forgiving liability standard. In this way, the private cyber attack victim would have an immediate self-help privilege to conduct a preliminary investigation through harmless access to the attacking computer. With a better understanding of the situation, the private party could then make its case for government deputization to engage in a destructive attack, either alone or in concert with the govern-

187 *See* discussion *supra* Part II.B.3.

188 *See supra* note 37 and accompanying text.

189 *See* FED. R. CIV. P. 13(a)(1)(A) (requiring that a pleading state as a counterclaim any claim "aris[ing] out of the [same] transaction or occurrence"); FED. R. CIV. P. 13(b) (allowing a pleading to "state as a counterclaim against an opposing party any claim that is not compulsory").

190 *See* West, *supra* note 163, at 139–43.

191 *See* discussion *supra* Part V.A.

ment.[192] As a whole, this self-help privilege proposal and the deputization proposal would both serve the same goal of encouraging proactive but responsible defenses on the Internet.

VI. Application of the Proposed Privilege to Previously Encountered Scenarios

A. *Google's Response to Operation Aurora Provides a Model for Counterattack Actions Under the Proposed Privilege*

Google's response to Operation Aurora followed each of the requirements outlined in the proposed privilege. Google responded to a serious emergency, took only the necessary and proportional steps to mitigate the threat, and notified the government.[193] Google responded to a serious breach by a sophisticated attacker who had accessed Google's high-value password-management source code—potentially giving access to "the keys to the kingdom."[194] Indeed, the exigency and severity of the threat posed in this attack is evident from Google's extraordinary response—where the cofounder of the company personally extended job offers to over 100 security professionals in an aggressive recruiting campaign.[195] Meanwhile, the "secret counteroffensive" to copy information from the Taiwanese server went no further than what was absolutely necessary to identify the threat and mitigate its effects.[196] Google shared the information, including evidence of attacks on other victims, with government intelligence and law enforcement agencies.[197] Google even briefed the Secretary of State on the attack.[198]

B. *Sinkhole Operations and RICO Ex Parte Seizures Could Go Further and Actually Cure Botnet Infections*

For widespread botnet attacks targeting ordinary consumers' computers, this privilege would also create a solid legal basis for removing malware infections without each computer owner's knowledge. Not only would security professionals be able to isolate botnets

---

192 *See* West, *supra* note 163, at 141 (discussing how private and government security teams could coordinate their responses in concert with one another).

193 Although it is unclear whether Google counterattacked before or after notifying the government, its candor and cooperation with the government suggest that Google would have complied with a notice requirement had such a requirement been in the statute at the time.

194 Gross, *supra* note 16, at 225.

195 *See id.* at 226 (reporting that Google offered hiring bonuses of up to $100,000).

196 Sanger & Markoff, *supra* note 14.

197 *Id.*

198 Gross, *supra* note 16, at 226.

from their controllers, as they are able to do today,[199] they would be able to go further and actually install updates to remove the underlying malware itself. Although the security teams pushing such updates may risk liability for inadvertent damage under this proposal, the proposal does not mandate that they actually assume such a risk. Instead, this proposal grants security teams a lawful option for assuming the risk if they so choose. To manage their liability risk, some researchers may opt for a hybrid approach, where they first try to notify the computer owners of the malware infection and wait a reasonable time period before pushing an involuntary update on the unresponsive owners.

C. *A Counterattack Privilege Would Encourage Open Communication Between Security Experts from Both the Public and Private Sectors*

Finally, this counterattack privilege would foster communication between the public and private sectors. As discussed above, counterattack statistics are unreliable because the legally questionable status of such activities makes security professionals reluctant to publicize them.[200] White hat security professionals who currently engage in counterattacks would be able to tailor their counterattack behavior to the proposed statutory framework and share their lessons with a central public knowledge repository. Moreover, the government would be able to aggregate statistics and form a more complete picture of the cyber-threat landscape. The government, through information sharing, would be able to coordinate more active responses by private party actors. The greater availability of communication between interested actors in the cybersecurity world would improve the overall security posture of all users of the Internet, both public and private.

CONCLUSION

The proposal in this Note is designed to be only one of many strategies for improving the nation's cybersecurity posture. Resolving legal ambiguity by applying a proposed uniform standard to private-party actions on the Internet—an international, interstate communications network—would serve as a starting point for further development of national cybersecurity strategy. Technical experts could design proactive procedures to comply with this uniform standard, instead of worrying about ambiguously drafted laws of all the separate

199 *See* discussion *supra* Part III.C.

200 *See* discussion *supra* Part III.B.3.

jurisdictions within the United States. Policymakers could take advantage of the information-sharing aspects of the proposal and use the data to outline better-defined roles for the different players in the cybersecurity community—whether private sector, civilian public sector, or military public sector.