Authorized Investigation: A Temperate Alternative to Cyber Insecurity

Casey M. Bruner[*]

"Wage war honorably.
You may be obliged to wage war but not to use poison arrows."[1]
-Baltasar Gracián

I. INTRODUCTION

In 2011, "Operation Shady RAT" became universally known as one of the most widespread and pervasive cyber espionage campaigns ever discovered.[2] The security breach, which persisted over a five-year period, infected more than seventy organizations worldwide including: federal and state government entities, high-tech and communications businesses, thirteen different national defense contractors, and the International Olympic Committee, among others.[3] The Operation Shady RAT vulnerability promulgated the way most computer viruses do: through an email and an attachment.[4] An employee of one of the infected defense contractors received an email with an Excel file attached.[5] The file contained a

---

[*] Casey Bruner is a J.D. Candidate at Seattle University School of Law. He previously served as Project Manager for the National Bureau of Asian Research (NBR) and for the Commission on the Theft of American Intellectual Property (IP Commission). The views, opinions, and policy recommendations contained in this paper are his alone and do not necessarily reflect the views of NBR, the IP Commission, or any other organization.

1. BALTASAR GRACIÁN, THE ART OF WORLDLY WISDOM 67 (Joseph Jacobs trans., Dover Publications 2005) (1653).

2. *See* DMITRI ALPEROVITCH, MCAFEE, REVEALED: OPERATIONS SHADY RAT (2011), http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf; *see also* WILLIAM C. HANNAS ET AL., CHINESE INDUSTRIAL ESPIONAGE: TECHNOLOGY ACQUISITION AND MILITARY MODERNIZATION 220 (2013) (stating that some experts believe that the "Shady RAT" vulnerability originated in China).

3. ALPEROVITCH, *supra* note 2, at 2.

4. Hon Lau, *The Truth Behind the Shady RAT*, SYMANTEC SECURITY RESPONSE BLOG (Aug. 4, 2011), http://www.symantec.com/connect/blogs/truth-behind-shady-rat.

5. Kelly Jackson Higgins, *'Operation Shady RAT' Attackers Employed Steganography*, DARK READING (Aug. 11, 2011, 2:42 PM), http://www.darkreading.com/attacks-breaches/operation-shady-rat-attackers-employed-s/231400084.

list of high-level executives that recently attended a popular industry event—useful information the employee was likely to open.[6] When opened, the file initiated backdoor communications with the hackers' server allowing the hackers to access the contractor's system and establish more footholds, ensuring long-term network access.[7] With this access, hackers were able to steal trade secrets, specifications and designs for classified defense technology, and anything else they were able to find on the compromised organizations' servers.[8] While the pervasiveness of Operation Shady RAT may be shocking for some, experts insist that this was merely one operation and that cyber espionage is a threat that affects nearly every industry and every country—the only ones immune to attack are those without anything valuable to steal.[9]

In another striking example, the McAfee security company discovered an extensive cyber espionage campaign, dubbed "Night Dragon," which targeted global oil, energy, and petrochemical companies.[10] Night Dragon was more narrowly focused than Operation Shady RAT, in that it specifically targeted "sensitive competitive proprietary operations and project-financing information with regard to oil and gas field bids . . . ."[11] The perpetrators of the Night Dragon operation were seeking information on the amount of money major oil and energy companies would be bidding on various projects around the world. Armed with this information, a country's state-owned enterprises could theoretically underbid their competitors by one dollar on each contract, effectively pushing the competition out of the market and taking all of the work.[12]

The vulnerability of our networks and computers, as evidenced by these and other attacks, is resulting in the loss of petabytes[13] of valuable information, costing the U.S. economy billions of dollars, weakening its ability to defend its own people, and compromising the integrity and reliability of its critical infrastructure.[14] Why is this such a pervasive and seemingly unfixable problem? What should be done about it? In response

---

6. *Id.*

7. ALPEROVITCH, *supra* note 2, at 2.

8. *Id.*

9. *See id.*

10. *See* McAfee Foundstone Professional Services & McAfee Labs, *Global Energy Cyberattacks: "Night Dragon"*, MCAFEE (Feb. 10, 2011), http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf.

11. *Id.* at 3.

12. The Night Dragon attacks are believed by many security experts to have originated in China and could have been perpetrated on behalf of Chinese state-owned energy companies. *See* HANNAS ET AL., *supra* note 2, at 220.

13. A petabyte is 1,000,000 gigabytes.

14. *See infra* Part III.B.

to these questions, many security experts have concluded that the purely defensive network protection measures of the past are insufficient and are now urging private industries and governments to supplement their security protocols with "active defense" or "hack-back" cyber defense tools.[15] Hack-back is a method of cybersecurity that involves some level of retaliation, or "counterstrike," against the hacker.[16] While the desire for hack-back measures is understandable given the magnitude of the problem, the practice is fraught with potential collateral damage and privacy concerns.[17] Nonetheless, some individuals and organizations have already begun to implement this legally questionable practice.[18]

This Note aims to show that legal structures created to protect the Internet in its original form are completely insufficient to protect what the Internet has become. This antiquated legal framework is exacerbating the problem. The breadth of activity that the current law restricts severely limits the remedies that cyberattack victims can pursue, and it must be updated.[19] While full hack-back may prove necessary in the long run, I argue for a more temperate initial response to the problem—I call this response "authorized investigation." Specifically, the Computer Fraud and Abuse Act should be amended to allow victims access to their attackers' computers for purposes of investigation without incurring criminal and civil liability.

Part II of this Note provides a brief overview of the foundations, original purposes, and philosophies that surrounded the inception of the Internet and the legal framework that developed as a result. Part III discusses current cyberthreats, and the damage these threats can do to our economic and national security infrastructures. Part IV discusses proposed methods of stopping and deterring cyberattacks, ranging from purely defensive measures to full-blown hack-back. Finally, Part V proposes a model of "authorized investigation," which would grant victims

---

15. *See generally* Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace,* 25 HARV. J.L. & TECH. 415 (2012); Shane McGee et al., *Adequate Attribution: A Framework for Developing a National Policy for Private Sector Use of Active Defense*, 8 J. BUS. & TECH. L. 1 (2013); Jan E. Messerschmidt, *Hackback: Permitting Retaliatory Hacking by Non-State Actors as Proportionate Countermeasures to Transboundary Cyberharm*, 52 COLUM. J. TRANSNAT'L L. 275 (2013).

16. *See infra* Part IV.B.

17. *See* McGee et al., *supra* note 15, at 43.

18. Stewart Baker, *RATs and Poison: Can Cyberespionage Victims Counterhack?*, SKATING ON STILTS (Oct. 13, 2012), http://www.skatingonstilts.com/skating-on-stilts/2012/10/us-law-keeps-victims-from-counterhacking-intruders.html. *See also* Jeremy Wagstaff, *More Companies Hacking Back at Cyber Attackers*, LAS VEGAS REV.-J. (Feb. 9, 2015, 1:36 PM), http://www.reviewjournal.com/business/more-companies-hacking-back-cyber-attackers.

19. *See infra* Part II.A.

of cyberattacks limited authorization to access and investigate computers used in the attack.

II. BACKGROUND

In 1972, at the Hilton Hotel in downtown Washington, D.C., a group of scientists, engineers, and researchers came together for the first ever International Computer Communications Conference. Also in attendance was a government engineer, Robert Kahn, who worked for the Advanced Research Project Agency (ARPA)—a small unit established by President Eisenhower to pursue scientific advancement beyond short-term military need.[20] More simply, ARPA was created to ensure that the U.S. military possessed the world's most advanced technology.[21] Kahn was there to demonstrate ARPA's newest achievement: a group of twenty computers, all networked together and able to communicate with each other through a revolutionary "packet switching" technology—ARPANET, the first computer network, was born.[22]

ARPANET, which would eventually develop into the Internet as we know it today, was the brainchild of a small network consisting of the federal government, universities, and research centers.[23] Its initial functions were exclusively to facilitate collaborative research and scientific advancement and to help facilitate long-range governmental and military communications, particularly in times of national security crises.[24] In fact, commercial Internet use was banned until 1992.[25] In the mid-1990s—after the commercial Internet ban was lifted—computers and Internet use and access was only practically accessible to a few.[26] The limitations on the type and quantity of Internet users—as well as the

---

20. *See* Department of Defense Advanced Research Projects Agency, Number 5105.15 (Dep't of Defense Feb. 7, 1958) ("In accordance with the provisions of the National Security Act of 1947, . . . there is established in the Office of the Secretary of Defense the Department of Defense Advanced Research Projects Agency. . . . The Agency shall be responsible for the direction or performance of such advanced projects in the field of research and development as the Secretary of Defense shall [designate] . . . .").

21. ARPA is still in existence but is now known as DARPA. *See ARPA-DARPA: The Name Chronicles*, DARPA, http://www.darpa.mil/About/History/ARPA-DARPA__The_Name_Chronicles.aspx (last visited Feb. 19, 2015).

22. *See Brief History of the Internet*, INTERNET SOC'Y, http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet (last visited Feb. 14, 2015).

23. RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT 82 (2011).

24. *Id.*; *see also* JOEL BRENNER, GLASS HOUSES: PRIVACY, SECRECY, AND CYBER INSECURITY IN A TRANSPARENT WORLD 15 (2013).

25. CLARKE & KNAKE, *supra* note 23, at 82.

26. *Id.*

assumption that the Internet would be used only for morally upright purposes—led to an intentionally "lawless" and "government-free" Internet.[27]

As the Internet grew in breadth and accessibility, early attempts at government regulation were treated with great hostility. One of the early, significant attempts to regulate the Internet and its content was the Communications Decency Act of 1996 (CDA).[28] The CDA was intended to protect children from obscene, indecent, and pornographic material on the Internet.[29] Advocates for "open-Internet" argued that the CDA's criminal provisions were overly broad and violated the First Amendment to the Constitution.[30] After the President signed the legislation, John Perry Barlow, an early open-Internet advocate, responded in his now famous speech called the "Declaration of the Independence of Cyberspace," by proudly and defiantly declaring to governments around the world, "Your legal concepts . . . do not apply to us."[31] The only governance necessary to rule the Internet, according to Barlow, would come "from ethics, enlightened self-interest, and the commonweal . . . ."[32]

This idea—that a system this complex could intentionally exclude governance and operate on the naïve belief that its users would act ethically absent the rule of law—is one that has restricted the government from maintaining any real order online and has removed all traces of the centuries old common law defense-of-self and defense-of-property concepts, both of which are well-established in both criminal[33] and civil law.[34] As a result, the legal framework that exists, built on a handful of

27. One of the four principles set out by Robert Kahn for how information transition would take place over the networks was "[t]here should be no global control at the operations level." *Id.* Additionally, Larry Roberts, who wrote the code for an early version of the transmission protocol, knew the code was insecure. *Id.* at 83. However, at the time, the network was so small that it was not a concern. *Id.*

28. *See* Telecommunications Act of 1996, Pub. L. No. 104-104, tit. 5, 110 Stat. 56, 133–43 (1996).

29. Reno v. ACLU, 521 U.S. 844, 859 (1997) ("[The law] prohibits the knowing transmission of obscene or indecent messages to any recipient under 18 years of age.").

30. The law was, in fact, declared unconstitutional by the Supreme Court. *See id.*

31. John Perry Barlow, *A Declaration of the Independence of Cyberspace*, ELEC. FRONTIER FOUND. (Feb. 8, 1996), https://projects.eff.org/~barlow/Declaration-Final.html.

32. *Id.*

33. *See* RICHARD J. BONNIE ET AL., CRIMINAL LAW 425 (2d ed. 2004) ("In general, one who is free from fault may use force to defend his or her person or property against harm threatened by the unlawful act of another if: (i) the person cannot avoid the threatened harm without using defense force or giving up some right or privilege; and (ii) the force used for this purpose is not excessive in view of the harm which it is intended to prevent.").

34. *See* VICTOR E. SCHWARTZ ET AL., PROSSER, WADE AND SCHWARTZ'S TORTS: CASES AND MATERIALS 112 (12th ed. 2010) ("As in the case of self-defense, the privilege to defend property is limited to the use of force reasonably necessary to the situation as it appears to the defendant.").

broad, ambiguous statutes and little case law, tips the balance of power unquestionably in favor of those who intend to use the Internet for harm. Additionally, there is little remedial action available to responsible users who are wronged. Criminal statutes do little to deter cybercriminals, while law-abiding citizens are unable to legally defend themselves. Had stronger governance of the Internet been allowed early on, perhaps there would be more effective policing of cybercrime today. Alternatively, had the Internet been left without "legal concepts," in a Hobbesian state, private individuals would have the ability to defend themselves without fear of criminal prosecution or civil suit. Ironically, by aiming for the middle ground, and trusting that only "good" people would use the Internet, the current system appears to be a combination of the worst of both worlds.

A handful of statutes now govern the way users, good or bad, may act in the cyberspace realm; two of these statutes are the Computer Fraud and Abuse Act (CFAA)[35] and the Electronic Communications Privacy Act (ECPA).[36] Also relevant are the Economic Espionage Act of 1996 (EEA)[37] and section 1637 of the National Defense Authorization Act of 2015.[38] Each of these statutes, in its own way, tips the scale of network defense in favor of cybercriminals and cyberspies and against those trying to protect their own networks.

A. The Computer Fraud and Abuse Act

The CFAA criminalizes a wide variety of actions related to the unauthorized access or misuse of computers.[39] In its broadest provision, the CFAA provides: "Whoever . . . intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any *protected computer* . . . shall be punished . . . ."[40] The statute defines "protected computer" as "a computer . . . which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States . . . ."[41] Experts have aptly noted that the statute covers nearly any computer connected to the Internet from any location.[42] Because any unauthorized access, or any activity that exceeds authorization, is a viola-

35. 18 U.S.C. § 1030 (2008).

36. 18 U.S.C. § 2510 (2002); 18 U.S.C. § 2701 (2002); 18 U.S.C. § 3121 (2001).

37. 18 U.S.C. § 1831 (2013).

38. National Defense Authorization Act of 2015, Pub. L. No. 113-291, § 1637, 128 Stat. 3292 (2014).

39. 18 U.S.C. § 1030 (2008).

40. *Id.* § 1030(a) (emphasis added).

41. *Id.* § 1030(e)(2)(B).

42. Kesan & Hayes, *supra* note 15, at 492.

tion of the statute, it appears interaction with *any* computer without authorization is a violation of the CFAA.[43] In a striking example of the CFAA's immense breadth, federal prosecutors, attempting to find novel avenues to combat the growing and serious epidemic of cyberbullying, argued that Lori Drew violated the CFAA when she created a MySpace account under the name and profile picture of a fictitious person[44]—a violation of MySpace's Terms of Service (ToS).[45] However, after the jury returned a guilty verdict, the trial judge overturned the conviction and declared the interpretation of the law invalid under the void-for-vagueness doctrine.[46]

In addition to the CFAA's overly broad criminal provisions, the Act also provides for a civil cause of action, allowing the victim to sue the hacker for any violation of the CFAA's felony provisions for compensatory damages or equitable relief.[47] However, these claims can only be brought against a *known* violator.[48] Given the current state of traceback technology,[49] and the stringent service of process requirements for international actors, the CFAA is unlikely to have any significant deterrent effect or provide any substantial relief to victims of cyberattacks. The CFAA does, however, dissuade legitimate actors from acting in self-defense because they fear potential criminal prosecution for nearly any retaliatory measures taken.

Finally, in a brief nod to cyber defense, the CFAA grants a very limited exemption to law enforcement agencies for the purpose of criminal investigation, yet it provides no investigative authority to the actual victims of cyberattacks.[50] Therefore, a company that was attacked, and

---

43. Stewart Baker, *RATs and Poison II—The Legal Case for Counterhacking*, SKATING ON STILTS (Oct. 13, 2012, 2:33 PM), http://www.skatingonstilts.com/skating-on-stilts/2012/10/rat-poison-the-legal-case-for-counterhacking.html.

44. United States v. Drew, 259 F.R.D. 449, 452 (C.D. Cal. 2009). Drew allegedly, with others, created a profile of "Josh Evans," who began an online relationship with Megan Meier. *Id.* Later, "Josh" began bullying Megan. *Id.* Megan later committed suicide. *Id.*

45. *Id.* at 454. MySpace's terms of service require that "all registration information you submit is truthful and accurate . . . ." *Id.* Therefore, according to the prosecutors, submitting *any* false registration information to MySpace was a criminal act under the CFAA. *Id.*

46. *Id.* at 467 ("In sum, if any conscious breach of a website's terms of service is held to be sufficient by itself to constitute intentionally accessing a computer without authorization or in excess of authorization, the result will be that section 1030(a)(2)(C) becomes a law 'that affords too much discretion to the police and too little notice to citizens who wish to use the [Internet].'") (quoting City of Chicago v. Morales, 527 U.S. 41, 64 (1999)).

47. Kesan & Hayes, *supra* note 15, at 491.

48. *See id.* at 494.

49. Current traceback technology currently boasts, at best, 87% accuracy. However, tracing an attacker is often made more difficult, and more inaccurate, by anti-tracing measures such as IP-spoofing. *Id.* at 481–82.

50. 18 U.S.C. § 1030(f) (2008).

potentially had valuable trade secrets or sensitive customer information stolen, may not interact with the hacker's computer in an "unauthorized" manner without facing criminal liability. Clearly, the CFAA provides little disincentive to criminal actors, but severely limits the defensive remedies available to those who wish to operate within the law.

B. The Electronic Communications Privacy Act

The ECPA prohibits:

> (1) the interception of wire, oral, or electronic communications (wiretapping); (2) access to the content of stored electronic communications and to communications transaction records; and (3) the use of trap and trace devices and pen registers.[51]

Generally, the ECPA prohibits the interception or monitoring of phone and Internet communication.[52] However, the ECPA does provide some exemptions, including a general exemption for phone and Internet service providers who intercept, disclose, or use information while engaged in any activity that is "a necessary incident to the rendition of his service[,]" such as "mechanical or service quality control checks."[53] Thus, while an Internet service provider can monitor traffic over its network to ensure that its services are working correctly, an Internet service provider may not, absent a court order, share this information with law enforcement.[54] As a result, service providers can sometimes see—in real time—cyberattacks happening over their networks, but cannot do anything about it; additionally, the U.S. intelligence community, which has proprietary intelligence on current cyberthreats, cannot share this information with industry actors.[55] The result is a worldwide network where cybercriminals can move about and conduct their activities, while neither private service providers nor intelligence communities may inform the other about what is happening.

The proposed Cyber Intelligence Sharing and Protection Act (CISPA) intends to eliminate this legal barrier to communication be-

---

51. *See* EDWARD C. LIU ET AL., CONG. RESEARCH SERV., R42409, CYBERSECURITY: SELECTED LEGAL ISSUES 20 (2013) (footnotes omitted), *available at* https://www.fas.org/sgp/crs/misc/R42409.pdf.

52. *Id.*

53. 18 U.S.C. § 2511(2)(a)(i) (2008).

54. *Id.* § 2511(2)(a)(ii).

55. U.S. HOUSE REPRESENTATIVES PERMANENT SELECT COMM. ON INTELLIGENCE, THE ROGERS-RUPPERSBERGER CYBERSECURITY BILL (H.R. 624) 1 (2013), *available at* http://intelligence.house.gov/sites/intelligence.house.gov/files/images/BackgrounderApril172013.pdf.

tween industry and government.[56] CISPA would grant Internet service providers and government agencies limited authority to share anonymous cyberthreat information with each other to better protect their networks.[57] Congressional consideration of CISPA, like other Internet-related laws, has been met with great hostility from many privacy advocates, despite the bill's extensive civil protection and privacy measures.[58] Because CISPA passage and implementation would only allow for better coordination against cyberthreats—without increasing the tools for defense against those threats—it will only marginally help secure cyberspace.[59] While better information sharing is necessary, it is only part of the solution.

C. The Economic Espionage Act

Congress responded to the rise in international intellectual property theft by passing the EEA of 1996.[60] When President Clinton signed the legislation, he stated that the new law "will help us crack down on acts like software piracy and copyright infringement that cost American businesses billions of dollars in lost revenues. And it will advance our national security."[61]

In actuality, the law has little to do with piracy, copyright infringement, or national security. The EEA criminalized two distinct actions: (1) economic espionage, and (2) the theft of trade secrets.[62] Economic espionage is defined as stealing, misappropriating, or receiving trade secrets while "intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent . . . ."[63] Trade secret theft, on the other hand, is defined as stealing, misappropriating, or

---

56. U.S. HOUSE REPRESENTATIVES PERMANENT SELECT COMM. ON INTELLIGENCE, MYTH V. FACT: H.R. 624, THE CYBER INTELLIGENCE SHARING AND PROTECTION ACT (CISPA) (2013), *available at* http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/cispamythvfact04172013.pdf.

57. *See id.*

58. *See The NSA's Favorite Anti-Privacy Law, CISPA, Is Back*, FIGHT FOR THE FUTURE, http://www.cispaisback.org/ (last visited Feb. 20, 2015).

59. As of this writing, CISPA failed to pass the 113th Congress. With the retirement of Representative Mike Rogers, the bill's primary advocate, it seems unlikely to pass in the next Congress.

60. *See* 18 U.S.C. § 1831 (2013).

61. William J. Clinton, Statement on Signing the Economic Espionage Act of 1996 (Oct. 11, 1996), *available at* http://www.presidency.ucsb.edu/ws/?pid=52087.

62. *See* 18 U.S.C. § 1831 (2013); 18 U.S.C. § 1832 (2012).

63. 18 U.S.C. § 1831 (2013).

receiving trade secrets "with intent to convert [the] trade secret . . . to the economic benefit of anyone other than the owner thereof . . . ."[64]

Although the EEA could be used to bring criminal charges against hackers, doing so is problematic for a number of reasons. The first problem is attribution. Like many civil actions proposed as cybertheft deterrents, it is extremely difficult to identify the perpetrator of a cyberattack; it is difficult to sue someone who you cannot identify. Without additional investigative tools, identifying the hacker is unlikely to happen with the level of certainty required to bring criminal charges under the EEA.

Even if the hacker could reasonably be identified, adequate service of process is problematic. This has been problematic for prosecutors under the EEA even when the alleged espionage was committed in the physical world.[65] Most cases classified as cyber espionage originate overseas, with a disproportionate amount coming from China and Russia.[66] In one case of Chinese industrial espionage, federal prosecutors attempted to serve a Chinese company for trade secret theft by serving the company's U.S. subsidiary.[67] The trial court judge found that service was improper and quashed the indictment.[68]

More recently, the U.S. Department of Justice indicted five Chinese hackers for their cyberspying.[69] It is widely assumed that no prosecutions will take place because of similar jurisdictional issues.[70] With most of the defendants outside of the United States, the EEA is unlikely to result in significant prosecutions and will therefore provide little deterrent effect to cyberspies. As a whole, the EEA has been largely ineffective and has not resulted in any significant international or economic cyber espionage deterrence.

D. Section 1637 of the National Defense Authorization Act of 2015

At the end of 2014, Congress gave the Obama Administration another tool to combat industrial and economic espionage in cyberspace. The National Defense Authorization Act of 2015 contained a small pro-

64. 18 U.S.C. § 1832 (2012).

65. *See* United States v. Pangang Grp. Co., Ltd., 879 F. Supp. 2d 1052, 1056 (N.D. Cal. 2012).

66. *See* VERIZON, 2013 DATA BREACH INVESTIGATIONS REPORT 22 (2013), *available at* http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf.

67. *Pangang Grp. Co.*, 879 F. Supp. 2d at 1056.

68. *Id.* at 1069.

69. RICHARD J. ELLINGS, NAT'L BUREAU ASIAN RESEARCH, FIVE CHINESE MILITARY OFFICERS INDICTED. NOW WHAT? (May 22, 2014), *available at* http://nbr.org/downloads/pdfs/ETA/Ellings_FiveIndicted_052214.pdf.

70. *Id.*

vision expanding the President's authority under the International Emergency Economic Powers Act.[71] Under this new authority, the President can list people, companies, or organizations that fit the statute's definition of cyberspies and ban them from sending or receiving payments through the U.S. financial system.[72]

This legislation intends to change the incentive structure in countries known to engage in economic espionage in cyberspace.[73] While the new power may be useful on some level, the attribution problem persists. As discussed later in this Article, it is nearly impossible to identify the perpetrators of most cyberattacks.[74] If we do not know who is doing the hacking, we do not know whom to sanction.

* * * *

These legal provisions, and the cyberlaw landscape generally, have created an extremely fragile and unhealthy system on which we have built our entire economic, national security, and critical infrastructure systems.[75] This system is plagued with a wide variety of cyberthreats detrimental to both individuals and the country as a whole.

III. TYPES OF CYBERTHREATS & THEIR EFFECTS

A. Types of Threats

The number of threats that exist in cyberspace are as numerous and varied as the people therein. However, the motivations for cyberattacks can generally be broken down into three categories: hacktivism, economic, and espionage.[76]

1. Hacktivism

Individuals engaged in hacktivism, known as "hacktivists," are generally hackers motivated by ideological beliefs, not by material benefit.[77] Sometimes, however, they are simply honing their hacking skills, or

71. 50 U.S.C. §§ 1701–1707 (2014).

72. National Defense Authorization Act of 2015, Pub. L. No. 113-291, § 1637, 128 Stat. 3292 (2014).

73. *Testimony of Former U.S. Senator Slade Gorton Before the House Energy & Commerce Committee,* IP COMMISSION (July 9, 2013), http://www.ipcommission.org/press/Gorton_Testimony_070913.pdf.

74. *See infra* Part IV.B.

75. Joel Brenner, former senior counsel at the National Security Agency, uses the metaphor of a "glass house" to describe the Internet and related systems. *See generally* BRENNER, *supra* note 24.

76. *See* VERIZON, *supra* note 66, at 20–21.

77. *Id.* at 21.

even hacking for "fun and epic lulz," as one security firm put it.[78] While hacktivists have often been classified as low-level "script-kiddies," hacktivism is becoming increasingly sophisticated.[79]

One of the best-known examples of hacktivism is the widely publicized saga of WikiLeaks, Julian Assange, and Anonymous. Assange founded WikiLeaks in 2007[80] and spent the next several years publishing state and corporate secrets that were, at best, embarrassing and at worst, highly compromising to the safety and security of individuals worldwide.[81] In 2010, WikiLeaks released its largest trove of secrets to date: the Afghan War Diary, a "compendium of over 91,000 reports covering the war in Afghanistan from 2004 to 2010."[82] Many groups—including some who do not generally see eye to eye on the issue of security leaks—criticized the uncensored information dump as irresponsible.[83]

The backlash against WikiLeaks, and against Assange's professional and personal conduct, was widespread.[84] A number of countries, including WikiLeaks' home country of Iceland, quickly became "unfriendly" to the Internet icon.[85] Meanwhile, PayPal froze the accounts of donors to WikiLeaks, and many banks refused to process transactions for the group, including Bank of America, MasterCard, Visa, and others.[86] Hacktivists from around the globe came to WikiLeaks and Assange's defense. At the forefront of the counter-campaign was the cyberanarchist group known as Anonymous,[87] who launched "Operation Avenge Assange."[88] Using an advanced Distributed Denial of Service (DDOS) attack, Anonymous was able to temporarily take down PayPal, Master-

78. *Id.*

79. *See* AKAMAI, THE STATE OF THE INTERNET 3D QUARTER, 2012 REPORT 5 (David Belson ed., 2012).

80. BRENNER, *supra* note 24, at 171. As Julian Assange said, "I am the heart and soul of this organization, its founder, philosopher, spokesperson, original coder, financier, and all the rest." *Id.* at 173.

81. For example, included in the 2010 release of the Afghan War Diary were the names of many Afghan citizens who cooperated with NATO forces and exposed members of the Taliban during the ongoing conflict. Shortly after the leaks, the Taliban announced that they had set up a commission to discover the identities of those spying for NATO. *Id.* at 172.

82. *Id.* at 171.

83. Examples include Reporters Without Borders and the head of the NSA. *Id.* at 172.

84. In August 2010, the Swedish government issued an arrest warrant for Assange alleging the rape of two women. *Id.* at 174.

85. *Id.* at 173.

86. *Id.* at 175.

87. "We are Anonymous. We do not forgive. We do not forget. Expect us." *Id.*

88. *Id.*

Card, Bank of America, a Swiss bank, and the office of the Swedish prosecutor.[89]

The most recent example of hacktivism came at the end of 2014. Sony Pictures intended to release the movie "The Interview" on Christmas Day. The movie was a fictional portrayal of an absurd assassination attempt of North Korean leader Kim Jong Un. In preemptive retaliation, North Korean hackers attacked Sony Pictures Entertainment, obtaining private emails, personal employee information, and more.[90]

Regardless of their motivations, or the sometimes-laudable nature of their actions,[91] hacktivists are defined by their lack of interest in financial gain. Instead, they are interested in pushing a social agenda at any cost and they do so in a cyberworld that gives them freedom with little fear of criminal charges. Even the U.S. courts have begun to realize what little power they have over amorphous, non-state cyberactors.[92]

2. Economic Crime

Cyberattacks classified as financial crimes represent, by far, the highest percentage of online threats.[93] Organized crime groups conduct most of these illicit activities.[94] In the short-term, these cybercriminals target ATMs, point of sale (POS) machines, and desktops to commit payment fraud and steal identities.[95] A recent example of this type of hack is the data breach of retail store Target's POS terminals.[96] In a nineteen-day security breach over the high-volume holiday shopping season, hackers pilfered data from approximately 70 million customers.[97]

---

89. *Id.*

90. Ellen Nakashima, *U.S. Attributes Cyberattack on Sony to North Korea*, WASH. POST (Dec. 19, 2014), http://www.washingtonpost.com/world/national-security/us-attributes-sony-attack-to-north-korea/2014/12/19/fc3aec60-8790-11e4-a702-fa31ff4ae98e_story.html.

91. For example, in June 2013, Anonymous attempted to hack the North Korean government in an attempt to learn more about their military and weapons systems. *See* Max Fisher, *Hacker Group Anonymous is No Match for North Korea*, WASH. POST (June, 27, 2013), http://www.washingtonpost.com/blogs/worldviews/wp/2013/06/27/hacker-group-anonymous-is-no-match-for-north-korea/.

92. *See* Bank Julius Baer & Co. Ltd. v. WikiLeaks, 535 F. Supp. 2d 980, 984 (N.D. Cal. 2008) (court finding it lacked subject matter jurisdiction and dissolving its own temporary restraining order). The decision unlocked the wikileaks.org domain and re-enabled the website. *Id.* The court could not accurately determine the citizenship of the defendants and, therefore, was unable to establish subject matter jurisdiction. *Id.*

93. *See* VERIZON, *supra* note 66, at 6.

94. *Id.*

95. *Id.* at 20, 22 tbl.1.

96. Mathew J. Schwartz, *Target Breach Widens: 70 Million Warned*, DARK READING (Jan. 10, 2014, 11:50 AM), http://www.darkreading.com/attacks-and-breaches/target-breach-widens-70-million-warned/d/d-id/1113392.

97. *Id.*

Although security breaches on par with the Target breach may seem few and far between, it is likely that similar attacks will increase in frequency due to recent technology changes. In April 2014, Microsoft ended support for Windows XP, including software updates and security patches.[98] Although this is standard practice for businesses,[99] due to its stability, Windows XP has been the preferred operating system for specialized machines including POS systems, medical devices, and many others.[100] After April 2014, however, security holes that are discovered will go unpatched, leaving these systems vulnerable.[101]

The long-term goal of cybercriminals is to convert the information they gather to cash.[102] The majority of financial attacks originate from the United States or Eastern European countries such as Romania, Bulgaria, and the Russian Federation.[103] Because a sophisticated cyberattack requires a significant amount of effort and skill, and the value of a stolen identity may not be immediately recognizable, it would seem that cyber financial crime is not a lucrative business. However, some of these criminal operations are so vast, and the volume of information gathered so great, the data retrieved generates millions of dollars.

The most notable example of organized cybercrime is the former international syndicate known as Shadowcrew. Co-founded by Andrew Mantovani, Shadowcrew was an online marketplace and hacker forum where members could learn the trade, obtain people's personal identification, sell the information to other identity thieves, and launder their money.[104] It was a one-stop-shop for cybercriminals and identity thieves. Before the Secret Service took down Shadowcrew in 2004, the group acquired 1.5 million stolen credit card numbers and caused over $4 million in real losses to credit card companies.[105] While the Shadowcrew takedown was largely hailed as a win for those cracking down on online criminal activity, it is important to remember that the Shadowcrew web-

98. *See* Maxim Weinstein, *The Dinosaur in the Room*, DARK READING (Dec. 5, 2013, 9:42 AM), http://www.darkreading.com/sophoslabs-insights/the-dinosaur-in-the-room/240164462; *Windows XP Support Has Ended,* MICROSOFT, http://windows.microsoft.com/en-us/windows/end-support-help (last visited Feb. 9, 2015).

99. *See* MICROSOFT, *supra* note 98. As a business creates new software, at some point it needs to devote fewer resources to the software of the past.

100. Weinstein, *supra* note 98.

101. *Id.*

102. *See* VERIZON, *supra* note 66, at 20.

103. *Id.* at 21.

104. Indictment, United States v. Mantovani, No. 2:04CR00786, 2004 WL 3609591 (D.N.J. 2004).

105. *Id.*

site had nearly 4,000 members—the 2004 indictment charged only nineteen of them, and nine years later, three remain at large.[106]

3. State-Sponsored Economic Espionage & Trade Secret Theft

Espionage between governments is nearly as old as government itself.[107] Economic and industrial espionage between companies is also nothing new.[108] Companies have long sought each other's secrets in order to gain an economic advantage in the marketplace.[109] However, espionage campaigns waged by state intelligence organizations for the purpose of helping their country's economic actors gain an advantage in the marketplace are relatively new. These state intelligence organizations are especially prevalent in the cyber realm.

Unlike the widespread nature of cyber financial criminals, and the first-world nature of hacktivists, state-sponsored cyber espionage is concentrated in a few countries that have both the capability to effectively wage such a campaign and state involvement in industrial markets. The countries most culpable for state-sponsored economic espionage are China and Russia.[110]

China's national leaders considered the beginning of the 21st century to be an opportunity to generate significant national economic growth.[111] To help facilitate this growth, Chinese intelligence services sought to exploit a variety of ways to steal trade secrets.[112] A 2011 report by the Office of the National Counter Intelligence Executive describes

---

106. *See* Lucian Constantin, *Alleged Shadowcrew Member Extradited to U.S. 9 Years After Cybercrime Forum Takedown*, PCWORLD (July 2, 2013, 5:20 AM), http://www.pcworld.com/article/2043498/alleged-shadowcrew-member-extradited-to-the-us-nine-years-after-forum-takedown.html.

107. "[I]t is only the enlightened ruler and the wise general who will use the highest intelligence of the army for purposes of spying, and thereby they achieve great results. . . . Spies are a most important element in war, because on them largely depends an army's ability to move." SUN TZU, THE ART OF WAR 99 (Lionel Giles trans., Dover Publ'ns 2002)

108. *See, e.g.*, DENNIS C. BLAIR ET AL., COMM'N ON THEFT AM. INTELL. PROP., THE IP COMMISSION REPORT, 40 (2013), *available at* http://ipcommission.org/report/IP_Commission_Report_052213.pdf.

109. *Id.*

110. *See* OFFICE OF THE NAT'L COUNTERINTELLIGENCE EXEC., FOREIGN SPIES STEALING US ECONOMIC SECRETS IN CYBERSPACE: REPORT TO CONGRESS ON FOREIGN ECONOMIC COLLECTION AND INDUSTRIAL ESPIONAGE, 2009–2011 4 (Oct. 2011), *available at* http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf; *see also* CONG.-EXEC. COMM'N ON CHINA, 2012 ANNUAL REPORT 139 (Oct. 12, 2012), *available at* www.gpo.gov/fdsys/pkg/CHRG-112shrg76190/pdf/CHRG-112shrg76190.pdf ("Chinese spy agencies have conducted a 'far-reaching industrial espionage campaign' in a range of industries, including biotechnology, telecommunications, nanotechnology, and clean energy.").

111. *See* OFFICE OF THE NAT'L COUNTERINTELLIGENCE EXEC., *supra* note 110, at 5.

112. *See* CONG.-EXEC. COMM'N ON CHINA, *supra* note 110, at 139.

Chinese actors as "the world's most active and persistent perpetrators of economic espionage."[113] This disproportionate participation by Chinese trade secret thieves is particularly evident in cyberspace. Industry reports estimate that 96% of cyberattacks classified as "espionage cases,"[114] and one-third of those classified as "attack traffic,"[115] originate in China. China has held the top spot for attack traffic since 2011.[116]

Similarly, Russia, due to its "high dependence on natural resources, the need to diversify its economy, and the belief that the global economic system is tilted toward [the United States]," has begun using human intelligence, cyber espionage, and other operations to "collect economic information and technology to support [its] economic development and security."[117] However, while registering third in attack traffic, Russia accounts for only roughly 5% of total attack traffic.[118] As opposed to China, most of Russia's cyberattacks were financially motivated and affiliated with organized crime, not a state-sponsored agency.[119] Unfortunately, experts believe that both China and Russia will remain "aggressive and capable collectors of sensitive US economic information and technologies, particularly in cyberspace."[120]

B. Effects of Cyber Insecurity

1. Economic Implications

The economic losses due to cyber insecurity are significant. First, victims of cyberattacks suffer direct economic loss. In the Shadowcrew example discussed previously, the group was able to obtain *only* 1.5 million fake credit cards resulting in $4 million dollars in real losses.[121] In a more recent sophisticated attack against Heartland Payment Systems (a credit card processing company for merchants) hackers were able to obtain 130 million credit and debit card numbers.[122] One can only speculate at the real losses suffered by the Heartland attack.

---

113. *See* OFFICE OF THE NAT'L COUNTERINTELLIGENCE EXEC., *supra* note 110, at 5.

114. VERIZON, *supra* note 66, at 21.

115. *See id.*; *See also* AKAMAI, *supra* note 79, at 4 fig. 1.

116. *See* AKAMAI, *supra* note 79, at 5.

117. *See* OFFICE OF THE NAT'L COUNTERINTELLIGENCE EXEC., *supra* note 110, at 5.

118. *See* AKAMAI, *supra* note 79, at 4.

119. *See* VERIZON, *supra* note 66, at 22.

120. *See* OFFICE OF THE NAT'L COUNTERINTELLIGENCE EXEC., *supra* note 110, at ii.

121. Indictment, United States v. Mantovani, No. 2:04CR00786, 2004 WL 3609591 (D.N.J. 2004).

122. BRENNER, *supra* note 24, at 41.

Second, companies and research institutions lose economically valuable assets, such as trade secrets, that are difficult to quantify. In 2013, the cybersecurity firm Mandiant[123] released a report exposing the persistent and ongoing cyber espionage campaigns waged by a "likely government-sponsored" group in China, now known as "Unit 61398."[124] Since 2006, Unit 61398 has compromised 141 companies spanning twenty major industries.[125] The intelligence that the group obtained included "technology blueprints, proprietary manufacturing processes, test results, business plans, pricing documents," and other information.[126] In one case, the group took 6.5 terabytes of information from a single company over a ten-month period.[127] However, as Mandiant points out: "The activity we have directly observed likely represents only a small fraction of the cyber espionage" that the group conducted.[128]

Government officials have confirmed how prevalent the theft of trade secrets has become. General Keith Alexander, Director of the National Security Agency (NSA) and Commander of the U.S. military's newly established Cyber Command (CYBERCOM), stated that cyber espionage "represents the greatest transfer of wealth in history."[129]

Third, the indirect cost of cyber insecurity is the increased investment that companies and individuals must make to protect their data from cyberthreats.[130] These costs are particularly damaging to small businesses because they incur nearly four times the per capita cost of dealing with cyberattacks than large organizations.[131]

Finally, the most tangible loss is the loss of broad economic growth and employment. The U.S. International Trade Commission (USITC) estimated that in 2009, trade secret theft by China alone cost the United

123. Mandiant was recently acquired by FireEye. Press Release, Mandiant, FireEye Announces Acquisition of Mandiant (Jan. 4, 2014), *available at* https://www.mandiant.com/news/release/fireeye-announces-acquisition-of-mandiant/.

124. MANDIANT, APT1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS 2, *available at* http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf (last visited Feb. 19, 2015).

125. *Id.* at 3.

126. *Id.*

127. *Id.*

128. *Id.* at 2.

129. Emil Protalinski, *NSA: Cybercrime is the 'Greatest Transfer of Wealth in History'*, ZDNET (July 10, 2012, 4:13 PM), http://www.zdnet.com/article/nsa-cybercrime-is-the-greatest-transfer-of-wealth-in-history/.

130. *See generally* PONEMON INST., SECOND ANNUAL COST OF CYBER CRIME STUDY (2011), *available at* http://www.ponemon.org/local/upload/file/2011_2nd_Annual_Cost_of_Cyber_Crime_Study%20.pdf.

131. *See id.* at 13.

States as much as $2.4 billion.[132] The effect of international intellectual property (IP) infringement on employment is striking: the USITC report further estimated that if IP protection against China improved substantially, the U.S. economy would see an increase of 2.1 million jobs.[133] Furthermore, the IP Commission estimates that the United States loses $300 billion annually due to lost intellectual property.[134]

2. National Security Implications

The national security implications of an insecure cyber network are just as significant, and in some ways more alarming, than the economic implications. The prevalence of insecure networks and compromised technology may threaten the United States' ability to protect itself against its enemies.

There are several ways cyber insecurity is undermining our national security infrastructure. First, many of our military technology secrets are drained through insecure networks. Operation Shady RAT, as discussed above, penetrated thirteen different defense contractors.[135] These defense contractors were infected for periods ranging from one month to twenty-one months.[136] Significant amounts of classified military technology specifications can be pilfered over a twenty-one month period. Suffice it to say, our military technology will not remain effective if our enemies know how the technology works and how to shut it down.

Second, a significant amount of military technology is built using compromised technology. A 2012 study conducted by the U.S. Senate Armed Services Committee discovered 1,800 cases where counterfeit electronic parts were used in military technology.[137] The total number of counterfeit parts likely exceeds one million.[138] These counterfeit parts are used in various products, including missile defense systems, Air Force planes and helicopters, and thermal sights for the Army.[139] The Commit-

---

132. U.S. INT'L TRADE COMM'N, CHINA: EFFECTS OF INTELLECTUAL PROPERTY INFRINGEMENT AND INDIGENOUS INNOVATION POLICIES ON THE U.S. ECONOMY 3-9 (May 2011), *available at* http://www.usitc.gov/publications/332/pub4226.pdf.

133. *Id.* at 4-4.

134. BLAIR ET AL., *supra* note 108, at 2. It is important to note that this figure also includes intellectual property lost through non-cyber means.

135. ALPEROVITCH, *supra* note 2, at 4.

136. *Id.* at 7.

137. Press Release, U.S. Comm. on Armed Servs., Senate Armed Services Committee Releases Report on Counterfeit Electronic Parts (May 21, 2012), *available at* http://www.armed-services.senate.gov/press-releases/senate-armed-services-committee-releases-report-on-counterfeit-electronic-parts.

138. *Id.*

139. *Id.*

tee concluded, "The use of counterfeit electronic parts in defense systems can . . . risk national security . . . ."[140] "[M]ost experts cannot look at a complicated computer chip and determine whether there is an extra piece [of code] here or there, a physical trapdoor."[141] Thus, these counterfeit parts could provide access points for hackers to exploit during conflicts.

Finally, the use of vulnerable technology and the inability to maintain secure networks is a liability in future military conflicts, as cyberwarfare tactics are already being used in armed conflict.[142] In 2008, during Israel's "Operation Cast Lead," a cyberwar erupted between Israeli and Arabic state-sponsored hackers.[143] Also in 2008, Russia invaded Georgia in response to Georgia's attack on South Ossetia.[144] Just before Russia began the armed conflict, a variety of cyberattacks began against Georgian websites.[145] Since the servers connecting Georgia to the outside world—located in Russia and Turkey—were disabled or flooded with attack traffic, Georgia lost connection to news and information sources, was unable to communicate through email, and had to shut down its banking system.[146] The resulting confusion and lack of intelligence made it difficult for Georgia to counter the Russian army.[147] Finally, it is suspected that North Korea has begun testing its own cyberwarfare capabilities by attacking government sites in the United States and South Korea.[148] Without secure networks, one can only imagine what cyberwarfare tactics would be employed if two world powers entered armed conflict.[149]

Some have argued that large-scale cyberwarfare could not occur between large militaries because of mutually assured destruction; the same argument explains why militaries keep from engaging in nuclear war.[150] However, because of the unique speed of cyberwar and its ability to disrupt communications and intelligence, there may be an incentive to at-

---

140. *Id.*

141. CLARKE & KNAKE, *supra* note 23, at 95.

142. *See generally id.* at ch. 3.

143. JEFFREY CARR, INSIDE CYBER WARFARE: MAPPING THE CYBER UNDERWORLD 2 (Mike Loukides ed., 2d ed. 2011).

144. *Id.* at 3.

145. *Id.*

146. CLARKE & KNAKE, *supra* note 23, at 19.

147. *Id.*

148. *See* CARR, *supra* note 143, at 4.

149. *See* Kevin Pollpeter*, Controlling the Information Domain: Space, Cyber, and Electronic Warfare*, *in* STRATEGIC ASIA 2012-2013: CHINA'S MILITARY CHALLENGE 163, 172 (Ashley Tellis & Travis Tanner eds., 2012) ("Cyberwarfare has emerged as the most pernicious threat from China. In recent years, Chinese cyberwarfare units and civilian hackers have most likely conducted widespread and effective espionage against targets around the world.").

150. CLARKE & KNAKE, *supra* note 23, at xi.

tack first if armed conflict seems imminent.[151] Unless steps are taken now to better secure U.S. networks, national security efforts may be undermined or seriously frustrated in a large-scale conflict.

3. Critical Infrastructure

In 2007, an electricity generator in Alaska began to vibrate at unusual speeds.[152] It continued to do so until the turbines blew apart causing the system to shut down.[153] Although it appeared the damage was the result of an explosive, it was really caused by hackers miles away.[154] Luckily, this event was later identified as "Project AURORA," an experiment by Idaho National Laboratory designed to test the security of our critical infrastructure.[155] Even though this was an authorized, controlled experiment, it is indicative of the damage hackers could do to critical U.S. infrastructure.

In the United States, manufacturing controls, electricity grids, banking and financial systems, telecommunications systems, air traffic control systems, water supplies, sewage systems, and countless other critical infrastructure systems are electronically operated. Most of these electronically-operated systems are integrated into a larger system, which is vulnerable to attack. The National Intelligence Council has acknowledged that cyberattacks on critical infrastructure could be seen by our enemies as a way to attack the United States at home.[156] Whether by accident, terrorist attack, or the hands of bored script kiddies, the loss of any of these systems—even for brief periods—could result in serious human and economic costs.

The threat to critical infrastructure around the globe was one of the biggest criticisms against the "hacktivist" group Anonymous.[157] In a 2010 information dump, the group released a secret list of worldwide critical infrastructure, including locations of hydroelectric plants, pharmaceutical companies that manufacture smallpox and other vaccines, and undersea cables that connect the world's communication system.[158] While pieces of this information may have been publicly accessible from various sources, broadcasting all of it in one place, to some, provided a

151. *Id.*
152. BRENNER, *supra* note 24, at 93.
153. *Id.*
154. *Id.*
155. *Id.*
156. CARR, *supra* note 143, at 9–10.
157. BRENNER, *supra* note 24, at 174.
158. *Id.*

blueprint for terrorists on how to do the most damage.[159] The threat against our critical infrastructure is significant, and damage to this infrastructure would affect all other aspects of our social, economic, and political structures. Without secure networks, it is only a matter of time before we experience a catastrophic loss of one of these essential systems.

IV. PROPOSED SOLUTIONS

A. Passive Defense

The law significantly limits what actions people may take in self-defense against hackers, and criminal enforcement of cybercrime is rare. As a result, most Internet users—from private individuals to high-tech defense contractors—attempt to secure their computers and networks using passive defense alone. Passive defense actions usually fall into one or more of four categories: (1) controlling system access; (2) limiting data access; (3) security administration; and (4) secure system design.[160] Some basic defensive actions include: requiring usernames and passwords, installing anti-virus software and spam-filters, and encrypting sensitive data. These passive defense methods are the functional equivalent of locking the door and hiding your valuables to deter burglars from entering your house. However, without an effective police force or a right of self-defense, it is only a matter of time before the burglars kick down your door.

In order for passive measures to secure a system, they must work 100% of the time; otherwise, hackers will just keep trying until they succeed.[161] In fact, experts have begun to argue that passive measures alone are inadequate for long-term security.[162] These defensive measures are particularly inadequate against "zero-day" vulnerabilities—newly coded threats that are unknown to software manufacturers and security professionals.[163] Anti-virus software works by keeping a catalogue of known virus code. When files that contain known malicious code are opened, the anti-virus stops their execution. A newly coded zero-day virus and an accidental opening of an attachment is all that is required to circumvent even the most sophisticated passive defense networks. Without the ability to defend yourself and your property, and without belief that the po-

159. *Id.*
160. Kesan & Hayes, *supra* note 15, at 470.
161. *Id.* at 471.
162. *Id.*
163. *Id.* at 472.

lice are on their way, it is only a matter of time before that burglar picks the lock.

One version of passive defense that has garnered attention is the idea of a "public health model" of cyber defense.[164] Proponents of the public health model suggest that the best way to secure the Internet as a whole is to ensure the "health" of each of its citizens.[165] Many cyberattacks are committed using computers that belong to unassuming third parties—also known as "Botnets."[166] For example, a DDOS attack uses thousands of these computers to repeatedly send packets of information to a network server.[167] The information overload crashes the server, which is unequipped to deal with the deluge of data. This type of attack is how Anonymous was able to bring down financial institutions.[168] The hackers had access to thousands of "unhealthy" computers that, at some point, were infected with malicious software that allowed the hacker to access their system and send these data packets. In contrast, DDOS attacks would be extremely difficult to execute if all computers online were updated with the last anti-virus definitions and were clear of malware because the hackers no longer have their "zombie army" or botnet.

There are two major difficulties encountered when implementing a public health model. First, the model relies on the active and willing participation of all users. Each Internet participant must actively invest in the latest security software, continually check for software patches,[169] and knowledgably and actively avoid less reputable and potentially infectious Internet sites. As one security expert put it: security does not work when it is left in the hands of the user.[170]

Second, the public health model assumes that viruses and exploits occur naturally and independently; it does not account for actors actively generating zero-day threats in order to overcome established defenses. To take the public health metaphor to an extreme, this would be like combatting a series of anthrax filled envelopes by instructing citizens to

---

164. *See generally* SCOTT CHARNEY, MICROSOFT, COLLECTIVE DEFENSE: APPLYING PUBLIC HEALTH MODELS TO THE INTERNET (2010).

165. *Id.* at 5 ("For a society to be healthy, its members must be aware of basic health risks and be educated on how to avoid them.").

166. CLARKE & KNAKE, *supra* note 23, at 282 ("Botnet: A network of computers that have been forced to operate on the commands of an unauthorized remote user . . . .").

167. *Id.* at 284 ("Distributed Denial of Service (DDOS): A basic cyber war technique often used by criminals and other nonstate actors in which an Internet site, a server, or a router is flooded with more requests for data than the site can respond to or process.").

168. BRENNER, *supra* note 24, at 175.

169. New strains of Malware appear faster than one every second. *Id.* at 34.

170. *Id.* at 38.

eat right, exercise, and take their vitamins. While public health models should be employed online, and may help prevent attacks from low-level hackers, something more needs to be done about high-level threats that continually engineer new vulnerabilities.

B. Hack-Back/Active Defense

Due to the widespread security risks that exist in the cyberworld, and the apparent inability of the government and private actors to stop these attacks, many security experts have begun advocating for some form of "active defense," or hack-back.[171] Unleashing these tools, proponents argue, would further two broad aims: (1) deterring hackers by punishing them with unacceptably high costs; and (2) preventing attackers from succeeding in their current or future attacks.[172]

Active defense or hack-back generally involves three steps: (1) detecting the intrusion; (2) tracing the intruder; and (3) some form of counterstrike.[173] For the most part, the first two steps of active defense are generally accepted as legal means of network security. Detecting an intrusion, which is usually done within one's own network or computer, does not lead to any legal trouble. Because the CFAA only limits unauthorized activity, as long as you have authorization to be on the system, you may act as you see fit, and it is nearly impossible to violate the CFAA.

The second step—tracing and identifying the intruder—is where the idea of hack-back, or mitigative counterstriking, becomes technologically complicated. Usually, attackers are traced using some form of traceroute technology.[174] However, depending on the type of traceroute, correctly identifying the hacker happens, at best, 80% of the time.[175] Attribution rates drop dramatically if the hacker is spoofing his IP address, and the rates become decrease even further if the hacker is using a third-party command and control system.[176]

---

171. *See* BLAIR ET AL., *supra* note 108, at 83; Baker, *supra* note 18; Kesan & Hayes, *supra* note 15, at 474; McGee et al., *supra* note 15.

172. Kesan & Hayes, *supra* note 15, at 433.

173. Some distinguish active defense and hack-back; for the purposes of this paper, they are considered synonymous, with both being defined as described. *See id.* at 434.

174. Kesan & Hayes, *supra* note 15, at 481; *see also* McGee et al., *supra* note 15, at 12.

175. *See* Kesan & Hayes, *supra* note 15, at 481.

176. "'Command and Control' (C&C) servers are centralized machines that are able to send commands and receive outputs of machines part of a botnet." *Command and Control Server*, RADWARE, http://security.radware.com/knowledge-center/DDoSPedia/command-and-control-server/ (last visited April 2, 2015).

The inability to regularly identify the hacker makes the third step—some form of counterstrike—difficult. Counterstriking can range from things as simple as turning over the supposed hacker to law enforcement, to damaging the system to prevent it from perpetrating future attacks.[177]

Hack-back has some obvious appeal. First, hack-back allows an individual to respond quickly to attacks perpetrated on his or her network, resulting in less network downtime and greater productivity. Second, it increases the cost of hacking and makes hackers less effective by creating barriers to entry—potentially causing some hackers to exit the game due to ineffectiveness.

However, some argue that this would lead to a number of undesirable results, mostly resulting from the problem of attribution. Where full hack-back was allowed (i.e. damaging or "locking" a hacker's systems), one can imagine a scenario where victims of cyber espionage discover an attack on their system and begin hack-back protocols, only to discover that they damaged the personal computer of an innocent third party used by the hacker. Thus, a free for all vigilante framework would likely result in significant collateral damage to innocent third parties. Even proponents of mitigative counterstriking acknowledge that the current state of technology, particularly in respect to identifying hackers, may not be sufficient to allow for permissive counterstriking.[178]

V. AN ALTERNATIVE: AUTHORIZED INVESTIGATION

This paper suggests a moderate alternative to hack-back proposals. Under a model of authorized investigation, section (a)(2) of the CFAA—the ban on unauthorized access for the purpose of obtaining information—should be amended to grant victims of cyberattacks criminal and civil immunity for the limited purpose of investigating their attackers. In practice, this would mean that network security professionals, businesses, or even private individuals who are technologically competent, would be able to use necessary means to: (1) access the attacking computer; and (2) gather information about the attack, its perpetrator, its origin, and its purpose—nothing more.

Opponents of this limited authorization will certainly cite the same concerns they have regarding hack-back. First, they will argue that accurate attribution remains a problem and could damage their systems. However, the proposed limited exemption would leave the rest of the CFAA in effect, including civil and criminal actions for damaging sys-

177. *See* Kesan & Hayes, *supra* note 15, at 481.

178. Kesan & Hayes, *supra* note 15, at 483.

tems. If individuals are found abusing their authority and damaging systems, prosecutors could bring criminal charges or citizens could file suit for compensatory damages. Second, opponents will likely argue that, even if damage is not a consideration, allowing individuals and organizations to access third-party systems violates the third party's privacy. However, as one expert noted, once an innocent third party's system is taken over and used by a hacker for illicit purposes, the privacy of the user has already been seriously violated.[179]

Allowing cybervictims to access and investigate the systems of their attackers provides many benefits, both on the individual and societal level. First, allowing access helps to further the goals of attribution. While inspecting a system, network investigators would be able to determine if the computer in question was the system that perpetrated the attack or if it was a command and control system taking advantage of an innocent third party. In the case of an innocent third party, investigators could use the network logs to determine where the true hacker resides.[180]

Second, these investigations could reveal data about the tools and exploits the hackers are using in their attacks. Network administrators could use this information to further secure passive defense systems from future attack.

Third, the ability to more accurately identify hackers could generate significant deterrent effects. "Name and shame" tactics are especially effective in some scenarios. By publicly declaring who the attackers are and who they work for, international political pressure could be placed on the origin country to prosecute hackers. Countries would no longer be able to hide behind plausible deniability—claiming that the hackers are not in their country. Also, the President's new authority allows him to impose sanctions on those known to engage in cyber espionage.[181] Attribution may be the key to securing the Internet. Any tool that can responsibly increase attribution rates should be seriously considered.

Fourth, in addition to identifying the hacker, investigators could identify for whom the hacker works and determine whether the attack was an act of state-sponsored espionage or corporate espionage. Furthermore, investigators can more accurately determine who should ultimately be held accountable for the attack.

Fifth, this proposal aids defensive models by working to create "healthier" Internet users. Identifying infected third parties could encour-

179. Baker, *supra* note 18.

180. The vast details of Operation Shady RAT were uncovered after investigators at McAfee were able to inspect an infected command and control server. ALPEROVITCH, *supra* note 2, at 3.

181. *See supra* notes 71–72 and accompanying text.

age users to clean their systems by informing them of the vulnerabilities and damage they are causing.

Finally, granting statutory authority for investigations could help prevent more drastic self-help methods. Some companies and individuals, frustrated at the futility of defensive measures, have already begun utilizing mitigative counterstriking and hack-back. The potential collateral damage, and the potential shadow wars due to vigilantism, could be avoided by granting users a little of the authority network experts seek.

In summary, authorizing investigative procedures to organizations and individuals that have been attacked allows for greater attribution and defense while limiting the risk of collateral damage to innocent third parties. Although some advocate for more aggressive measures, authorized investigation would allow for increased security while testing the water for greater individual action.

VI. CONCLUSION

We stand in a valley of moderation, and we are being attacked on all sides. The legal system that developed around the Internet is insufficient to protect what it has become. What was designed as a collaborative tool for a small set of researchers is now the backbone for nearly everything in modern society. The Internet manages our food distribution systems, our water supply, our electric grids, our missile defense networks, and more. We use the Internet to manage both our personal 401(k)s and the New York Stock Exchange. The Internet is where we file health insurance claims and purchase health plans—sending our private medical information across unknown servers. The same system that generated unprecedented technological development and economic growth over recent decades is also a system under attack. Hacktivists, cybercriminals, and state-sponsored cyberspies use the Internet to steal identities, pilfer trade secrets, crash websites, and divulge national security secrets. Countries are lacing servers and private computers with backdoors and corrupt code waiting to supplement armed attack with cyberwar.

While current laws have brought about some successful attempts at maintaining an orderly cyberspace, attribution and procedural problems continue to ensure that most hackers are never held accountable for their actions. As a result, many cyber experts are now advocating for a system that permits hack-back, allowing private individuals and organizations to defend themselves. Others worry that this practice will result in collateral damage to innocent third parties because of these same attribution problems. A very limited criminal and civil exemption allowing victims of cyberattacks to investigate their attackers could solve many issues while limiting third-party collateral damage. By allowing victims to access

their attacker's computer without authorization and obtain information, victims are able to gather the intelligence needed to defend themselves, help secure the system more broadly, shed light on the attacker and his or her motives, and increase the cost to hackers, all while limiting the potential for third-party collateral damage. Finally, a legally-authorized, limited hack-back could stem the tide of growing cyber vigilantism while providing a test case by which we can judge future cyber self-defense proposals.