# ACTIVE CYBER DEFENSE CERTAINTY: A DIGITAL SELF-DEFENSE IN THE MODERN AGE

Hardik Gandhi*

## I. INTRODUCTION

Imagine a world where your personal information can be accessed for any reason. Well unfortunately, this is the reality. It is the reality because cybersecurity (the measures that can be taken to protect a computer or computer system from unauthorized access or attack) is in a state of disarray. Currently, hackers are seldom prosecuted while major corporations frequently bear the burden for failing to secure data in an arms-race environment.[1] Equifax, HBO, and Yahoo fell victim to some of the largest breaches in history.[2] Certain actors use the internet as a cloak for their identity to evade tracking.[3] The current law is outdated, limits entities in their defensive measures, and presents far more issues than it resolves.[4] As a result, we are now entering an age many refer to as the "Code War," where the *agents of chaos*, using digital means, can destabilize the real world.[5]

* Hardik Gandhi graduated in May 2019 with his Juris Doctor degree. He thanks his late mother for the gift of grit. And to Toronto, the city that raised him, for teaching him to value people by the depth of their actions and not the color of their skin or the mistakes of their forefathers.

1. Roger A. Grimes, *Why It's So Hard to Prosecute Cybercriminals?*, CSO (DEC. 6, 2016), https://www.csoonline.com/article/3147398/why-its-so-hard-to-prosecute-cyber-criminals.html [https://perma.cc/F7NH-MAAZ].

2. *See generally*, Tom Kemp, *What Do Equifax, HBO, Uber and Yahoo All Have in Common?*, CENTRIFY (Feb. 1, 2018), https://blog.centrify.com/identity-breaches/ [https://perma.cc/R4CM-HQFY].

3. *See* Alex Lockie, *The US's Most Secretive Intelligence Agency Was Embarrassingly Robbed and Mocked by Hackers*, BUS. INSIDER (Nov. 13, 2017, 8:05 AM), https://www.businessinsider.com/nsa-embarrassingly-robbed-mocked-by-shadow-brokers-2017-11 [https://perma.cc/4JQM-6HA3].

4. Grimes, *supra* note 1.

5. Phil Richards, *Beyond Patch: Be a Security Vigilante*, CSO (Apr. 19, 2018),

Thinking large corporations, healthcare providers, and government entities will adequately protect their information, people willingly give it up.[6] But the law only allows entities to sit and wait for an attack. Though entities may have a stout defense and a strong secondary, cyber attackers often find the end zone. Hackers are able to readily adapt, finding vulnerabilities faster than the defenders are able to locate them. And unfortunately, Congress still relies on law formulated over three decades ago when the digital landscape was in its infancy.[7] Investigations drag on, and ultimately only a small number of hackers are prosecuted.[8] There are over 4,000 cyberattacks every day, indicating that a change in the cybersecurity landscape is desperately needed.[9] As a result, Congress is considering active cyber self-defense as a solution—one that deters cybercrimes.[10]

Common law self-defense, a justified use of force against an unprovoked imminent threat of harm, has long been a western tradition. It was established in English common law by Sir Edward Coke in the 17th century and arrived to the United States in the 18th century.[11] Its presence has prevented harm and empowered people, proving to be a significant benefit to society. Coupled with the right tools, self-defense—the castle doctrine or stand your ground—has afforded citizens an avenue of self-help against those who wish to do harm. In fact, "57% of felons polled agreed 'criminals are more worried about meeting an armed victim than they are about running into the police.'"[12] FBI crime statistics between

https://www.csoonline.com/article/3268976/nation-state-attacks-the-cyber-cold-war-gets-down-to-business.html [https://perma.cc/C5QF-TTB7].

6. Steve Olenski, *For Consumers, Data Is a Matter of Trust*, FORBES (Apr. 18, 2016, 9:35 AM), https://www.forbes.com/sites/steveolenski/2016/04/18/for-consumers-data-is-a-matter-of-trust/#33b47b7c78b3 [https://perma.cc/2ZLK-6FXM].

7. Grimes, *supra* note 1.

8. *Id.*

9. Jorge Reye, *Business Cyber Attacks Top 4,000 Per Day: Your Guide to Ransomware*, CYBERSECURITY (Nov. 30, 2016), http://www.entrepreneaur.com/article/284724 [http://perma.cc/9PU2-L8CF].

10. Paul Rosenzweig, *Next Steps for U.S. Cybersecurity in the Trump Administration: Active Cyber Defense*, HERITAGE FOUND. (May 5, 2017), https://www.heritage.org/cybersecurity/report/next-steps-us-cybersecurity-the-trump-administration-active-cyber-defense [https://perma.cc/C7LH-8HV8].

11. Jim Powell, *Edward Coke: Common Law Protection for Liberty*, FOUND. FOR ECON. EDUC. (Nov. 1, 1997), https://fee.org/articles/edward-coke-common-law-protection-for-liberty/ [https://perma.cc/PN9P-MDWM].

12. GUY SMITH, GUN FACTS VERSION 6.2 30 (2013) (quoting JAMES D. WRIGHT & PETER H. ROSSI, THE ARMED CRIMINAL IN AMERICA: A SURVEY OF INCARCERATED FELONS

2000 and 2010 show that "homicide incidents decreased over 5%, robbery decreased 10%, and aggravated assaults decreased 15%" after states enacted self-defense laws.[13]

This information suggests active self-defense has a deterrent effect on crime—an effect that would be vital in the digital world. Allowing active self-defense would make hacking more challenging, and in turn, hackers would be less likely to engage in it. The U.S. Senate Armed Services Committee published a report stating that "[d]espite ever-improving network defenses, the diverse possibilities for remote hacking intrusions, supply chain operations to insert compromised hardware or software, and malevolent activities by human insiders will hold nearly all [information and communications technology] systems at risk for years to come."[14] Allowing a rogue nation or malicious hacker to employ a denial-of-service attack would disrupt all internet-related services for a major corporation.[15] Using backdoor vulnerability to steal sensitive credit-card information is also clearly disruptive.[16] One thing is clear, a solution, buried within the Computer Fraud and Abuse Act (CFAA), is needed.

The solution to rampant cyber threats is to arm entities with legal rights so they have the ability and confidence to defend themselves when faced with a serious threat. In recognizing a legal self-defense, the Active Cyber Defense Certainty Act (ACDC) presents a powerful solution analogous to physical self-defense.[17] A counter-strike, within the appropriate legal scope, will deter hackers, help identify hackers, increase prosecution, and ultimately reduce crime itself. The ACDC does require some refining to ensure it is not misappropriated as a right to engage in economic espionage or other forms of hacking. However, the benefits of the ACDC, when applied to the right situation, are invaluable.

Therefore, this Note will analyze the contemporary anti-hacking

27 (1985)).

13. Howard Nemerov, *No, Castle Doctrine Does Not Increase Violent Crime*, TRUTH ABOUT GUNS (Jul. 12, 2013), http://www.thetruthaboutguns.com/2013/07/daniel-zimmerman/no-castle-doctrine-does-not-increase-violent-crime/ [https://perma.cc/PR36-67ZJ].

14. JAMES R. CLAPPER, SENATE ARMED SERVS. COMM., STATEMENT FOR THE RECORD: WORLDWIDE THREAT ASSESSMENT OF THE US INTELLIGENCE COMMUNITY 1 (Feb. 26, 2015), https://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf [https://perma.cc/E95U-Z7YM].

15. Mehmud Abliz, *Internet Denial of Service Attacks and Defense Mechanisms* 3, U. OF PITTSBURG (March 2011), https://people.cs.pitt.edu/~mehmud/docs/abliz11-TR-11-178.pdf [https://perma.cc/6PVV-KQ2W].

16. *Id.*

17. *See* Active Cyber Defense Certainty Act, H.R. 4036, 115th Cong. (2017).

framework under the CFAA along with the applicable portions of the Digital Millennium Copyright Act (DMCA). This Note will also discuss the present technological advancements in society and the crucial need for revised legislation. Finally, this Note will argue in support of ethical hacking under the proposed ACDC and discuss many of its undesirable consequences.

## II. HISTORY

The ability to communicate and access vast amounts of information from practically anywhere can single handedly be attributed to the information revolution. The evolution of the internet began in the 1960s during the Cold War.[18] Fearing the Soviets could destroy telephone lines and cripple communication, the American government searched for ways to "communicate and share data" without restraint.[19] Therefore, the Department of Defense formed the Advanced Research Projects Agency (ARPA).[20] And J.C.R. Licklider, a Massachusetts Institute of Technology scientist, worked with the ARPA to develop a concept known as the "galactic network."[21]

In 1965, the ARPA developed ARPANET, the network that became the basis for the internet.[22] It utilized a packet-switching network, which broke data into blocks before sending it to another computer.[23] Four years later, the first attempt at communicating data over the internet was a partial success when a computer at University of California, Los Angeles and another at Stanford were able to communicate the first two letters of the word "LOGIN."[24] Thereafter, the ARPANET project quickly began to evolve.[25]

In 1986, the National Science Foundation Network (NSFNet) took over the work of ARPANET.[26] That same year, NSFNet connected live

18. *The Invention of the Internet*, HIST. (Jul. 30, 2010), http://www.history.com/topics/inventions/invention-of-the-internet [https://perma.cc/7XJX-7QLP].
19. *Id.*
20. *Id.*
21. *Id.*
22. *Id.*
23. *Id.*
24. *Id.*
25. *Id.*
26. *See* Aaron Schwabach, Internet and the Law: Technology, Society, and Compromises xxi (2d ed. 2014).

supercomputer centers.[27] The evolution of NSFNet heavily overlapped with the creation of the personal computer.[28] A major breakthrough occurred when computer scientist Vinton Cerf developed a set of procedures for the "world's mini-networks to communicate with one another."[29] This development was coined the "Transmission Control Protocol."[30] Finally, in 1991, Tim Berners-Lee invented the everlasting "WWW"—the World Wide Web—an abode of boundless information accessible to anyone.[31]

Today the internet is used to engage in video conferencing, purchase products worldwide, watch videos, access insurmountable information, share our lives through social media, listen to music anywhere, and even remotely perform surgeries from 400 kilometers away.[32] It is one of the fastest growing revolutions in modern society. But rapid progress is often coupled with new challenges—setbacks. The law needs to be modernized to compete with the technological world's seemingly unstoppable maturation.

## III. TECHNICALITIES

"[T]he [i]nternet is a global network of computers" where each computer has a distinctive address—an internet protocol (IP) address.[33] Any request, from the playback of a Netflix video to visiting a website, is broken down into packets and communicated to the appropriate IP address.[34] Once a packet reaches its destination, usually through the most efficient route, it is put back into sequence using predetermined markers.[35]

27. *Id.*

28. *A Brief History of NSF and the Internet*, NAT'L SCI. FOUND., https://www.nsf.gov/news/news_summ.jsp?cntn_id=103050 [https://perma.cc/WT7S-LHYL].

29. *The Invention of the Internet*, *supra* note 18.

30. *Id.*

31. *Id.*

32. Rose Eveleth, *The Surgeon Who Operates from 400km Away*, FUTURE (May 16, 2014), http://www.bbc.com/future/story/20140516-i-operate-on-people-400km-away [https://perma.cc/YGX4-CWYU].

33. Rus Shuler, *How Does the Internet Work?*, (2002) https://web.stanford.edu/class/msande91si/www-spr04/readings/week1/InternetWhitepaper.htm [https://perma.cc/6ESR-7EWV].

34. *See id.*

35. *See What Is TCP/IP and How Does It Work?*, TECH JUNKIE (Jan. 9, 2017), https://www.techjunkie.com/what-is-tcpip-and-how-does-it-work/ [https://perma.cc/A3D5-GKT6].

This results in a delivered message, access to a website, or video playback.[36] Endpoints, such as computers and smartphones, are known as clients.[37] And rules that dictate communication, particularly data transfers between systems, are known as protocols.[38] Clients use a specific protocol to access servers that store information at a physical location, on a physical device, and in binary form.[39]

Different protocols accomplish different things.[40] Protocols are stacked upon each other with each layer performing a precise function.[41] This stacked approach allows communication to be flexible and efficient.[42] Computers communicate using IP addresses via an internet service provider (ISP).[43] A hardwired connection allows a computer to communicate with its ISP.[44] Hundreds of thousands of miles of submarine communication cables run under oceans, connecting internet-accessible devices across the world.[45]

The internet consists of transmission control protocol (TCP) and IP—TCP/IP collectively.[46] The TCP/IP protocol has four distinct layers: the application layer, the transport layer, the internet layer, and the network interface layer.[47] The application layer is the front-end program being used, such as the web browser.[48] The transport layer divides data into packets and directs it to certain applications on a computer.[49] The internet

36. *See id.*

37. Jonathan Strickland, *How Does the Internet Work?*, HOWSTUFFWORKS (May 2, 2010), https://computer.howstuffworks.com/internet/basics/internet.htm [https://perma.cc/C78G-39R6].

38. Shuler, *supra* note 33.

39. *See* Corey Nachreiner, *Understanding IP Addresses and Binary*, WATCHGUARD https://www.watchguard.com/wgrd-resource-center/security-fundamentals/understanding-ip-addresses-and-binary [https://perma.cc/PN9X-LWR7].

40. Shuler, *supra* note 33.

41. *Id.*

42. *Id.*

43. *Id.*

44. *IP 101: The Basics of IP Addresses*, https://whatismyipaddress.com/ip-basics [https://perma.cc/VBC3-XFDP] (last visited April 12, 2019).

45. Nick Routley, *Map: The World's Network of Submarine Cables*, VISUAL CAPITALIST (Aug. 24, 2017), https://www.visualcapitalist.com/submarine-cables/ [https://perma.cc/8FM4-W7MZ].

46. *How TCP/IP Works*, MICROSOFT (Oct. 7, 2009), https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc786128 (v=ws.10) [https://perma.cc/SZ3A-KV4A].

47. *Id.*

48. *Id.*

49. *Id.*

layer directs packets to a specific computer using the proper IP address.[50] Lastly, the network layer is the hardwired interface that converts binary-packet data to network signals, which sends and receives the information.[51]

Vulnerability arises when hackers attempt to access sensitive information that major corporations and other entities have collected.[52] Most companies will collect a customer's personal information, such as credit-card numbers, and attempt to store it on a *secure* server.[53] Secure servers are the physical embodiment of the "cloud."[54] They transmit all the stored information via an IP address and allow authorized users remote access to stored information.[55] Cloud computing is an emerging trend and will likely shape the future of computing and data storage. What this illustrates is that, unlike the physical world where biological markers (one's face, fingerprints, or footprints) are used to identify individuals, a hacker leaves no such trace. In fact, all an IP address tells us is that a certain computer was used at a certain location—it tells us nothing about *who* used it.[56]

## IV. CURRENT DEFENSE MEASURES

Large enterprises invest millions into equipping themselves with the latest cyber-security preventative measures.[57] Different laws govern the financial, healthcare, and energy sectors, imposing certain industrial standards and responsibilities concerning cyber security.[58] The Gramm-Leach-Billey Act governs the financial sector, the Health Information Portability and Accountability Act governs healthcare entities, and the

50. *Id.*

51. *Id.*

52. Christian de Looper, *How Hackers Are Really Getting Your Data, and What You Can Do to Keep It Safe*, TECHRADAR (June 20, 2016), http://www.techradar.com/news/internet/how-hackers-are-really-getting-your-information-and-what-you-can-do-to-keep-it-safe-1323706 [https://perma.cc/FV7A-RKTR].

53. *See* Bradley Mitchell, *Servers Are the Heart of the Internet*, LIFEWIRE (Oct. 22, 2018), https://www.lifewire.com/servers-in-computer-networking-817380 [https://perma.cc/JW95-XDDT].

54. *See id.*

55. *See id.*

56. *How TCP/IP Works*, *supra* note 46.

57. Ms. Smith, *Cyber Attacks Cost U.S. Enterprises $1.3 Million on Average in 2017*, CSO (Sept. 20, 2017, 7:43 AM), https://www.csoonline.com/article/3227065/security/cyber-attacks-cost-us-enterprises-13-million-on-average-in-2017.html [https://perma.cc/BL9Y-M5A8].

58. JEFF KOSSEFF, CYBERSECURITY LAW 105 (2017).

Federal Energy Regulatory Agency governs critical energy infrastructure.[59] Although their specific standards differ, each industry requires administrative, technical, physical, and organizational protections.[60]

Administratively, organizations must have procedures in place to prevent a data breach, train employees on best practices, and limit each user's privileges.[61] For example, a company may require passwords to include capitals, numbers, and other characters; require periodical system updates; and e-mail warnings regarding security threats.[62] While this seems elementary, Christopher Correa, the former scouting director for the St. Louis Cardinals, was able to guess a former employee's weak password; and he used it to gain access into the Houston Astros' database.[63] Afterwards, Mr. Correa was charged with "violating federal hacking laws as part of a cyberespionage campaign."[64]

Now there are three different ways to protect against cyberattacks: 1) technical protection, 2) physical protection, and 3) organizational protection. Technical protection includes software related security, like firewalls, that prevent outsiders from initiating code-based attacks.[65] This also involves using secure front-end webpages, the latest anti-virus software, traffic monitoring, and software configuration to minimize threats.[66]

On the other hand, physical protection refers to how hardware, servers, and computers are physically guarded so no one can simply walk in and steal data, or even worse, cause structural damage.[67] For instance, a power plant facility may require key-card access to server rooms, be monitored by 24/7 surveillance, and require biological identification.[68] This is

59. *Id*.
60. *Id.* at 105–31.
61. *12 Best Cyber Security Practices in 2017*, EKRAN SYS. BLOG (Feb. 22, 2017), https://www.ekransystem.com/en/blog/best-cyber-security-practices [https://perma.cc/AGP3-3JDD].
62. *Id.*
63. Andrea Peterson, *This Basic Security Mistake Led to the Houston Astros Hack That Shook Baseball*, WASH. POST (July 19, 2016), https://www.washingtonpost.com/news/the-switch/wp/2016/07/19/this-basic-security-mistake-led-to-the-houston-astros-hack-that-shook-baseball/?utm_term=.baaa73b42a3f [https://perma.cc/UHG6-XQUH].
64. *Id.*
65. *See* KOSSEFF, *supra* note 58, at 119.
66. *Id.*
67. *Id.* at 127–31.
68. Marc Blitz, Lecture on Industry Responsibilities Cyber Security Law, Oklahoma

necessary to prevent hackers from nonchalantly walking into a server location, deploying malicious codes from a USB, and then effortlessly walking out.[69]

Finally, organizational protection encompasses a contractual obligation, including procedures for each entity affiliated within the industry to follow in the event of a breach. Procedures might entail communication of data breaches to the public, "[c]ommunication protocols with law enforcement[,] [i]solation procedures for the infected computer[,] [and] [i]solation procedures for devices that have not been infected, such as those for stopping the backup synchronization schedule."[70]

## V. BREAKING INTO THE VAULT: HACKING SECURE SERVERS

Imagine a secure server as a bank vault. Now imagine a team of highly trained individuals orchestrating an elaborate plan to break in and escape with millions, or even billions. Conversely, hacking into a server requires a lot less man power. A tech-savvy sixteen-year-old sitting at home in his pajamas—half-way around the world—can bypass a server with the correct software.[71]

"Data is increasingly more valuable to steal and sell, and most importantly, the tools that grift are rarely noticed. A successful infection within the right computer can provide a steady stream of private data for years without raising any red flags."[72] An obvious solution would be to prevent the infection all together. But as technological safeguards develop, so do the means of bypassing the safeguards.

Hackers use different types of software attacks—viruses, worms, Trojan horses, phishing scams, ransomware, spyware, and many more—to break through a computer network's defense.[73] Software security, like

City University School of Law (Nov. 2017).

69. *Id.*

70. Jorge Rey, *Business Cyber Attacks Top 4,000 Per Day: Your Guide to Ransomware*, ENTREPRENEUR (Nov. 30, 2016), https://www.entrepreneur.com/article/284754 [https://perma.cc/PN6G-2VZP].

71. Blitz, *supra* note 68.

72. *Hacking Publicly Traded Companies and the US Government to Steal Data & Money*, PLATTE RIVER NETWORKS (June 5, 2017), https://platteriver.com/post/hacking-publicly-traded-companies-us-government-steal-data-money/ [https://perma.cc/HR2E-ZWFR].

73. *See* Kim Komando, *5 Ways Hackers Attack You (and How to Counter Them)*, USA TODAY (July 19, 2013, 8:07 AM), https://www.usatoday.com/story/tech/columnist/

firewalls, minimize certain damages depending on the type of attack. A distributed-denial-of-service (DDoS) attack overloads a network with requests causing a digital traffic jam, which results in website and service outages.[74] In 2014, a group called "Lizard Squad" used a DDoS attack to take down Sony's PlayStation network,[75] Microsoft's Xbox Live network,[76] and potentially North Korea's internet access.[77]

Viruses, worms, and Trojan horses delivered through infected e-mails or infected clicks on downloads and advertisements can cause data and software corruption.[78] Even worse, certain worms are "self-replicating" and can spread swiftly.[79] For example, the "Love Bug worm" spread throughout the United States via e-mail "affecting government computers at Congress, the White House, and the Pentagon" resulting in "$10 billion in economic damages by overwriting files and corrupting data."[80]

Phishing, an exploitation of trust using social engineering, sends out a mass amount of fake e-mails in hopes the recipient will input his credentials into a website that seems authentic but actually sends the individual's credentials to the hacker.[81] These websites can replicate bank providers, e-mail providers, Facebook, or virtually any business that requires a username and password.[82] For example, if someone requests banking information after claiming to be a long-lost relative who left a hefty sum of money, chances are this is a phishing attempt.

komando/2013/07/19/hacker-attack-trojan-horse-drive-by-downloads-passwords/2518053/ [https://perma.cc/H5RM-LYGV].

74. Laura Hautala, *That Massive Internet Outage, Explained*, CNET (Oct. 21, 2016, 5:24 PM), https://www.cnet.com/how-to/what-is-a-ddos-attack/ [https://perma.cc/J78Z-7SET].

75. Dave Smith, *Why Hacker Gang 'Lizard Squad' Took Down Xbox Live and PlayStation Network*, BUS. INSIDER (Dec. 26, 2014, 8:49 AM), http://www.businessinsider.com/why-hacker-gang-lizard-squad-took-down-xbox-live-and-playstation-network-2014-12 [https://perma.cc/2LKB-RPHG].

76. *Id.*

77. Cecilia Kang et al., *North Korean Web Goes Dark Days After Obama Pledges Response to Sony Hack*, WASH. POST (Dec. 22, 2014), https://www.washingtonpost.com/business/economy/north-korean-web-goes-dark-days-after-obama-pledges-response-to-sony-hack/2014/12/22/b76fa0a0-8a1d-11e4-9e8d-0c687bc18da4_story.html?utm_term=.0f4735de5abb [https://perma.cc/5C2J-R7GR].

78. Robert W. Hahn & Anne Layne-Farrar, *The Law and Economics of Software Security*, 30 HARV. J.L. & PUB. POL'Y 283, 288–89 (2006).

79. *Id.*

80. *Id.* at 289.

81. *Id.* at 290.

82. *Id.*

Ransomware hijacks a computer through a security vulnerability, "overwrit[es] the affected system's master boot record, [and] then encrypts the master file table, which is the part of the filesystem that serves as sort of a roadmap for the hard drive."[83] The year 2017 saw the rise of "NotPetya," a ransomware that "infect[ed] . . . computers in more than 100 countries," costing companies like "Merck more than $300 million in Q3 alone."[84] Moreover, spyware infects nearly "three-quarters of all corporate machines;" it embeds itself into a computer where it pries and collects data on the user's activities, such as "internet sites visited, financial data, and passwords."[85]

Poorly designed software can also lead to a breach.[86] For example, many programs have buffers or temporary storage allocations.[87] When hackers inject codes into the buffer, an overflow can occur.[88] If this happens, there can be corruption of data and execution of unsigned codes.[89] Hackers will also attempt to dodge software security through a *backdoor* to gain administrative privileges or root access.[90] This "superuser" clearance allows a hacker to accomplish anything within the target computer's capability.[91] A backdoor breach can allow a hacker to deliver a malicious payload.[92]

Finally, zero-day exploits, often in the form of a backdoor, are flaws

83. Josh Fruhlinger, *Petya Ransomware and NotPetya Malware: What You Need to Know Now*, CSO (Oct. 17, 2017, 2:59 AM), https://www.csoonline.com/article/3233210/petya-ransomware-and-notpetya-malware-what-you-need-to-know-now.html [https://perma.cc/6ZH3-V97B].

84. Alison DeNisco Rayome, *The Top 10 Worst Ransomware Attacks of 2017, So Far*, TECHREPUBLIC (Oct. 31, 2017, 5:43 PM), https://www.techrepublic.com/article/the-top-10-worst-ransomware-attacks-of-2017-so-far/ [https://perma.cc/HA8P-QCNQ].

85. Hahn & Layne-Farrar, *supra* note 78, at 291.

86. *Id.* at 292.

87. *Id.*

88. *Id.*

89. *Id.*

90. *Id.* at 291. Backdoors are created by programmers who created the actual program. The programmer is typically the only one who knows of this hidden access, which allows him or her easy access to the program or even the entire computer system. *Id.* at 291–92 n.49.

91. Matt Miller, *What Is Least Privilege & Why Do You Need It?*, BEYONDTRUST (Nov. 17, 2016), https://www.beyondtrust.com/blog/entry/what-is-least-privilege [https://perma.cc/A9L3-BRTC].

92. John E. Dunn, *Security Flaws of the Year 2016 – Breaches, Backdoors and Anti-Virus Gone Wrong*, TECHWORLD (Dec. 31, 2015), https://www.techworld.com/security/security-flaws-of-year-2016-breaches-backdoors-anti-virus-gone-wrong-3632708/ [https://perma.cc/QDJ5-5YV7].

in the software that no one is aware of and "for which no [security] patch exists."[93] These exploits are useful because they provide "the capability to penetrate any device in the world running the affected software until the developer rolls out a software update that patches the security flaw."[94] Many enterprises use the same business-managements software, so a small zero-day exploit could have a wide-spread, negative impact.[95] In fact, zero-day exploits are so popular that an entire part of the Darknet—(a portion of the internet that is accessible using a "specific software and a dedicated browser")[96]—TheRealDeal Market focused on "brokering hackers' zero-day attack methods."[97] Hackers can also potentially transfer data from a secure server to a remote location where the data can then be manipulated or sold. Further, if the target computer is used to maintain power grids or control military weapons, physical destruction can astoundingly occur.[98]

In addition, "[i]f the attackers [have] access to names, birthdays, addresses and [s]ocial [s]ecurity numbers, it means that information can be easily used to carry out identity theft schemes."[99] This information is usually sold on the Darknet.[100] A commonality among all of these methods is that they require and use the internet to facilitate attacks. Without the internet, a majority of these schemes would fail.

## VI. COMPUTER FRAUD AND ABUSE ACT

In 1984, Congress promulgated the Computer Fraud and Abuse Act

93. *See* Ahmed Ghappour, *Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web*, 69 STAN. L. REV. 1075, 1110 (2017).

94. *Id.*

95. *See id.*

96. Claire Reilly, *Dark Web 101: Your Guide to the Badlands of the Internet*, CNET (Nov. 29, 2017, 5:45 PM), https://www.cnet.com/news/darknet-dark-web-101-your-guide-to-the-badlands-of-the-internet-tor-bitcoin/ [https://perma.cc/L7BT-65JX].

97. Andy Greenberg, *New Dark-Web Market Is Selling Zero-Day Exploits to Hackers*, WIRED (Apr. 17, 2015, 6:25 AM), https://www.wired.com/2015/04/therealdeal-zero-day-exploits/ [https://perma.cc/G6RJ-9WXK].

98. Andy Greenberg, *'Crash Override': The Malware That Took Down a Power Grid*, WIRED (June 12, 2017, 8:00 AM), https://www.wired.com/story/crash-override-malware/ [https://perma.cc/5DG3-697Q].

99. Chad Terhune, *Anthem Hack Exposes Data on 80 Million*, L.A. TIMES (Feb. 5, 2015, 10:56 AM), http://www.latimes.com/business/la-fi-anthem-hacked-20150204-story.html [https://perma.cc/4S3W-TWDP].

100. Reilly, *supra* note 96.

(CFAA), which regulated the access of information on the computer.[101] The CFAA was "[o]riginally designed to protect computers having a specified federal interest, such as national security, financial records, and government property," but it has evolved over time.[102] Today, the CFAA "allow[s] private entities to assert a civil cause of action[,] obtain compensatory damages and . . . equitable relief," and protect computers "used in interstate or foreign commerce or communication."[103]

It aims to protect sensitive information by prosecuting those who access this information without authorization or who exceed their authorization.[104] Code-based hacking, denial-of-service attacks, bypassing access restriction, and accessing information on an employer's computer contrary to the company's policy were all been found to be in violation of the CFAA.[105] Pursuant to 18 U.S.C. § 1030, it is illegal to obtain security information, compromise confidentiality, access a government computer, damage information, traffic passwords, threaten to damage a computer, or make any attempts thereof without authorization.[106]

A protected computer is one

> (A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or
> (B) which is used in . . . interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States.[107]

However, Congress failed to adequately define *authorization*, generating a split in interpretation.[108] A broad interpretation of the CFAA allows

101. James Juo, *Split Over the Use of the CFAA Against Disloyal Employees*, 61 FED. LAW. 50, 51 (2014).
102. *Id.*
103. *Id.*
104. *Id.* at 51–52 (citing 18 U.S.C. § 1030(e)(2) (Supp. II 1997)).
105. *See id*. at 52–53.
106. 18 U.S.C. § 1030 (2012).
107. *Id.* § 1030(e)(2)(A)–(B).
108. Juo, *supra* note 101, at 51–52.

prosecution under "code-based[,] . . . contract-based[,] and norms-based violations."[109] Code-based violations occur when hackers use software to circumvent the security in order to access information they do not have authority to access.[110]

In *United States v. Rodriguez*, the Eleventh Circuit held the CFAA broadly applied to individuals who violate a company's administrative policies regarding access to information.[111] Mr. Rodriguez was charged under § 1030(a)(2)(B) of the CFAA for using his credentials as a teleservice representative to access the "personal records of [seventeen] different individuals for nonbusiness reasons."[112] He was able to gain access to "any person's social security number, address, date of birth, father's name, mother's maiden name, amount and type of social security benefit received, and annual income."[113]

In contrast, the Ninth Circuit, en banc, adopted a narrow definition of *exceeds authorized access* in *United States v. Nosal*.[114] In *Nosal*, the court wanted to refrain from "transform[ing] the CFAA from an anti-hacking statute into an expansive misappropriation statute."[115] The defendant, a former employee of an executive search firm, convinced his former colleagues to use their valid "log-in credentials to download source lists, names and contact information from a confidential database on the company's computer" so that he could start his own business.[116] The court noted that the CFAA was intended to cover hackers who use code-based violations to "circumvent[] the security measures" rather than individuals who misappropriate information using valid credentials.[117] The Ninth Circuit also found that "the CFAA did not give a private party's use policies the force of law" because allowing such "could impose unexpected burdens on [the] defendants."[118]

The most high-profile conviction under the CFAA was of internet activist Aaron Swartz.[119]

109. KOSSEFF, *supra* note 58, at 163.
110. *Id.*
111. United States. v. Rodriguez, 628 F.3d 1258, 1260 (11th Cir. 2010).
112. *Id.*
113. *Id.*
114. 676 F.3d 854, 863–64 (9th Cir. 2012).
115. *Id.* at 857.
116. *Id.* at 856.
117. *Id.* at 858.
118. Juo, *supra* note 101, at 52.
119. Kim Zetter, *Hacker Lexicon: What Is the Computer Fraud and Abuse Act?*, WIRED (Nov. 28, 2014, 6:30 AM), https://www.wired.com/2014/11/hacker-lexicon-computer-

> Mr. Swartz [was] a well-known figure in Internet academic circles [who] created a site called Infogami that later merged with the social news site Reddit. He [was] also a founder and director of the nonprofit group Demand Progress, which calls itself a political action group hoping to change public policy . . . relat[ing] to the [i]nternet.[120]

Swartz also co-founded the Rich Site Summary (RRS Feed), a popular news and information aggregator and feed.[121] He believed that academic journals should be free to the public.[122]

In 2010, Swartz used the Massachusetts Institute of Technology's (M.I.T) *open campus* to access and download millions of files from the Journal Storage (JSTOR), a digital repository for academic journals that "[l]ibraries and universities pay a subscription fee to . . . access."[123] Local police used surveillance technology to catch Swartz as he needed to be physically present on the M.I.T. campus to download the files.[124]

However, Swartz did not *hack* in a conventional sense "because he did not use parameter tampering, break a CAPTCHA, or do anything more complicated than automate a process that download[ed] a file in the same manner as clicking 'Save As' from a browser."[125] Even so, this conduct was in violation of JSTOR's terms of service, which "prohibit[s] [the] downloading or exporting [of] documents using automated computer programs."[126]

Swartz was charged with multiple counts under the CFAA, including knowingly and intentionally defrauding a protected computer, intentionally accessing a computer without authorization; and "as a result of such conduct[,] recklessly caused damage" to the institution he was accused of stealing from.[127]

---

fraud-abuse-act/ [https://perma.cc/8PU8-3VM2].

120. Nick Bilton, *Internet Activist Charged in M.I.T. Data Theft*, N.Y. TIMES (July 19, 2011, 12:54 PM), https://bits.blogs.nytimes.com/2011/07/19/reddit-co-founder-charged-with-data-theft/ [https://perma.cc/9VE2-BAN7].

121. Caroline Bankoff, *Reddit Co-Founder and JSTOR Hacker Aaron Swartz*, INTELLIGENCER (Jan. 12, 2013), http://nymag.com/daily/intelligencer/2013/01/jstor-hacker-aaron-swartz-commits-suicide.html [https://perma.cc/KWB9-KD9D].

122. Juo, *supra* note 101, at 52.

123. *Id.*

124. *Id.*

125. *Id.* at 52–53.

126. *Id.* at 52.

127. Superseding Indictment at 12–14, United States v. Swartz, No. 1:11-CR-10260-

The circuit split and the arguably erroneous indictment of Aaron Swartz suggests the CFAA is unable to confidently prosecute cybercrimes in today's world. The need to modernize the CFAA is evident. The inclusion of an exemption for ethical-hacking and self-defense could prove to be advantageous to the overall deterrence of cyber-crimes.

## VII. THE DIGITAL MILLENNIUM COPYRIGHT ACT

Along with the CFAA, the DMCA is used to prosecute hackers.[128] Congress enacted the DMCA "in 1998 as an anti-piracy statute effectively making it illegal to circumvent copy protections designed to prevent pirates from duplicating digital copyrighted works and selling or freely distributing them."[129] *Circumvention* "means to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner."[130] Protection under the DMCA was needed "to make digital networks [a] safe place[] to disseminate and exploit copyrighted materials."[131]

For protection, copyright owners use Digital Rights Management (DRM)—a scheme of technological restrictions that control the access and usage of digital media.[132] Denuvo, a DRM software, offers anti-tampering, anti-cheating, and optical media protection for games, business to business software, electronic books, and video playback.[133] Steam, Amazon, Origin, Apple, and Google Play Store use this technology to prevent hackers and pirates from accessing copyright content for free.[134]

Though the DMCA protects against the circumvention of technical protection measures and access controls, it does not protect against the

NMG (Sept. 12, 2012).

128. Kim Zetter, *Hacker Lexicon: What Is the Digital Millennium Copyright Act?*, WIRED (June 6, 2016, 7:00 AM), https://www.wired.com/2016/06/hacker-lexicon-digital-millennium-copyright-act/ [https://perma.cc/6K7U-7KG3].

129. *Id.*

130. 17 U.S.C.A § 1201(a)(3)(A) (West 1999).

131. KOSSEFF, *supra* note 58, at 202 n.183 (quoting S. Rep. No. 105-190, at 2 (1998)).

132. Paul Gil, *Why Is DRM So Controversial with Music and Movie Artists?*, LIFEWIRE (Oct. 5, 2018), https://www.lifewire.com/why-is-drm-so-controversial-2483185 [https://perma.cc/4ZRD-RWRY].

133. *Denuvo Software Solutions*, IRDETO, https://www.denuvo.com/ [https://perma.cc/3GYZ-RK9H].

134. *See id.*

subsequent use of the materials once accessed.[135] There are three provisions under 17 U.S.C. § 1201 that apply directly to hackers: "Section (a)(1) prohibits the act of circumventing technology that controls access to copyrighted material. Section (a)(2) prohibits trafficking in technology that facilitate circumvention of access [to] control measures. Section (b)(1) prohibits trafficking in technology that facilitate circumvention of measures that protect against copyright infringement."[136]

Unlike the CFAA, the DMCA does not apply to individuals who merely violate user agreements.[137] In *I.M.S. Inquiry Mgmt. Sys., Ltd. v. Berkshire Info. Sys., Inc.*, the defendant used valid login credentials obtained from a third party to copy content from the plaintiff's web-based system.[138] The court concluded this did not constitute evasion under the DMCA.[139]

### *A. Cost Associated with Security and Breaches*

IBM Security defines *data breach* as "an event in which an individual's name and a medical record and/or a financial record or debit card is potentially put at risk—either in electronic or paper format."[140] The financial impact of security breaches is substantial, reaching an average of "$1.3 million for enterprises and $117,000 for small [to] medium-sized businesses."[141] In addition, large enterprises spend nearly $25 million on information technology security, which is expected to increase over the coming years.[142] "[H]ealth care organizations had an average cost of $380 [per lost or stolen record, and] in financial services the average cost was $245 [per record]. Media ($119), research ($101) and public sector ($71)

135. KOSSEFF, *supra* note 58, at 202.

136. *Id.* (emphasis omitted).

137. *What is the DMCA?*, WINSTON & STRAWN LLP (2019), https://www.winston.com/en/legal-glossary/dmca.html [https://perma.cc/D2QP-WX48].

138. I.M.S. Inquiry Mgmt. Sys., Ltd. v. Berkshire Info. Sys., Inc., 307 F. Supp. 2d 521, 523 (S.D.N.Y. 2004).

139. *Id.* at 532–33.

140. *2017 Cost of Data Breach Study: Global Overview*, IBM (June 2017), https://www.ibm.com/downloads/cas/ZYKLN2E3 [https://perma.cc/QN76-4RXL].

141. Ms. Smith, *supra* note 57.

142. *See Measuring Financial Impact of IT Security on Businesses: IT Security Risks Report 2016*, KASPERSKY LAB 5 (2016), https://go.kaspersky.com/rs/802-IJN-240/images/Kaspersky%20Lab%20Report_IT%20Security%20Economics_GLOBAL_final.pdf [https://perma.cc/RTR8-XRXW].

had the lowest average cost per lost or stolen record."[143] However, because only one in five incidents are publicly disclosed, the financial impact is likely more severe.[144]

For example, Home Depot fell victim to a cyberattack in 2014.[145] Credit information and e-mails of nearly 56 million customers were exposed as a result.[146] Hackers used stolen logins to access Home Depot's network, and they inserted a malware stealing data from point-of-sale machines.[147] This breach resulted in approximately $179 million in settlement costs.[148] That year retail stores were prime targets.[149] Because credit card information is of value on the black market, corporations like Michael's, Sally Beauty Supply, P.F. Chang's, Goodwill Industries, SuperValu, The UPS store, Jimmy John's, Dairy Queen, Staples, and Kmart were all victims of cyberattacks.[150]

In addition, the summer of 2017 proved to be a rough one for Equifax—a consumer-credit-reporting-agency.[151] On July 29, 2017, Equifax discovered a data breach affecting the data of 143 million customers.[152] A flaw in Apache Struts, "a free, open-source . . . framework" used to create web applications,[153] allowed hackers to access Equifax's dispute portal "where Equifax . . . customers go to log issues with their credit reports."[154] The stolen information consisted of "[credit-card] numbers of around 209,000 U.S. consumers and certain dispute

143. *2017 Cost of Data Breach Study: Global Overview*, *supra* note 140.

144. *Damage Control: The Cost of Security Breaches, IT Security Risks Special Report Series*, KASPERSKY LAB 2, https://media.kaspersky.com/pdf/it-risks-survey-report-cost-of-security-breaches.pdf [https://perma.cc/PML6-862C] (last visited April 12, 2019).

145. CLAPPER, *supra* note 14, at 1.

146. *Id.*

147. Brett Hawkins, *Case Study: The Home Depot Data Breach*, SANS INST. (Jan. 2015), https://www.sans.org/reading-room/whitepapers/breaches/case-study-home-depot-data-breach-36367 [https://perma.cc/4FP5-GH5K].

148. *Cost of a Retail Data Breach: $179 Million for Home Depot*, WEBTITAN (Mar. 14, 2017), https://www.webtitan.com/blog/cost-retail-data-breach-179-million-home-depot/ [https://perma.cc/YYY4-568U].

149. Hawkins, *supra* note 147.

150. *Id.*

151. Jackie Wattles & Selena Larson, *How the Equifax Data Breach Happened: What We Know Now*, CNN BUS. (Sep. 16, 2017, 4:06 PM), http://money.cnn.com/2017/09/16/technology/equifax-breach-security-hole/index.html [https://perma.cc/2KPV-8QA8].

152. *Id.*

153. *Apache Struts*, STRUTS, https://struts.apache.org/ [https://perma.cc/4DR9-GLA2] (last visited April 12, 2019).

154. Wattles & Larson, *supra* note 151.

documents with personal identifying information of around 182,000 U.S. consumers."[155] The breach cost Equifax $87.5 million in expenses.[156] On April 4, 2018, a Massachusetts state court ruled that the state will be able to pursue its claim: "Equifax breached its legal duties to address all reasonably foreseeable risks to its data security and to implement reasonably up-to-date fixes to its software," because it "knew or should have known by March 2017 that a serious security vulnerability existed in computer code that the company used in its systems but failed to patch or upgrade its software to eliminate it."[157] Moreover, Equifax still faces "class action lawsuits and investigations by the U.S. Federal Trade Commission and various state attorneys generals."[158]

Lastly, "NotPetya," a malware, and "Petya", a ransomware, caused world-wide financial damage and service disruption in 2016 and 2017.[159] This system-wide disruption cost Merck, a pharmaceutical giant, a loss of $135 million in revenues "directly related to the cyberattack."[160]

In allowing only ineffective and passive measures of defense, the current law is a financial burden on companies. Allowing a company to strike back by using a team of *ethical hackers* could cost hundreds of thousands of dollars, but this could prove to be the more cost-effective option in the long-run.

## VIII. THE ACTIVE CYBER DEFENSE CERTAINTY ACT

Even with defenses in place, there are still around 1.5 million cyberattacks annually, totaling 4,000 per day.[161] Symantec, a firm

155. Yashaswini Swamynathan, *Equifax Reveals Hack That Likely Exposed Data of 143 Million Customers*, REUTERS (Sep. 7, 2017, 3:53 PM), https://uk.reuters.com/article/us-equifax-cyber/equifax-reveals-hack-that-likely-exposed-data-of-143-million-customers-idUKKCN1BI2VK [https://perma.cc/RWE5-XH2M].

156. Stacy Cowley, *Equifax Faces Mounting Costs and Investigations from Breach*, N.Y. TIMES (Nov. 9, 2017), https://www.nytimes.com/2017/11/09/business/equifax-data-breach.html [https://perma.cc/P5R8-H5RB].

157. Nate Raymond, *Massachusetts Can Sue Equifax Over Data Breach, Judge Rules*, REUTERS (Apr. 4, 2018, 2:00 PM), https://www.reuters.com/article/us-equifax-cyber/massachusetts-can-sue-equifax-over-data-breach-judge-rules-idUSKCN1HB2QQ [https://perma.cc/B3DN-9UZ9].

158. *Id.*

159. Fruhlinger, *supra* note 83.

160. Jessica Davis, *Petya Cyberattack Cost Merck $135 Million in Revenue*, HEATHCARE IT NEWS (Oct. 27, 2017, 2:00 PM), http://www.healthcareitnews.com/news/petya-cyberattack-cost-merck-135-million-revenue [https://perma.cc/U384-T8GX].

161. *These Cybercrime Statistics Will Make You Think Twice About Your Password:*

specializing in cybersecurity, reported that in the last eight years 7.1 billion identities have been exposed via data breaches.[162] The Equifax scenario alone shows the gravity of legal implications for disarming a company and preventing it from utilizing active defense measures.

Because technological advances are without rest, cyberspace can never have a norm; it remains in a state of unpredictability. Consequently, the cost of passive defense is extensive. Therefore, an active approach is necessary, but companies face an uphill battle in defending against cyberattacks. Investigators are seldom able to locate the attackers through the anonymity of the internet.[163] The CFAA prosecutes all forms of hacking, preventing companies from utilizing the best form of defense—offense. Massive walls have historically been used to keep harm out or delay attacks. But once that wall fails, your only option is to wait until the attack is over, hope nothing is taken, and then try to rebuild. Meanwhile, attackers have likely seized your valuables and are now in a place that is frequently unreachable by law. Attackers are thus effectively immune from punishment.

Legal authority allows individuals facing a threat of unlawful force or harm to counteract that threat with self-defense. The ACDC aims to bring this same level of protection to the digital world.[164] "Hack back, . . . sometimes called hack counter[-]strike" is a form of incidence response that is most appropriate given the nature and rise of cyberattacks.[165] The ACDC is an amendment that acts as a defense when companies that have fallen victim to cyberattacks activate a similar form of unauthorized access against the perpetrator's computer.[166] Although this form of vigilantism

*Where's the CSI Cyber Team When You Need Them?*, CBS (Mar. 3, 2015, 7:00 AM), http://www.cbs.com/shows/csi-cyber/news/1003888/these-cybercrime-statistics-will-make-you-think-twice-about-your-password-wheres-the-csi-cyber-team-when-you-need-them-/ [https://perma.cc/5396-QS97].

162. Shaun Aimoto et al., *Internet Security Threat Report*, SYMANTEC 10 (April 2017), https://www.symantec.com/security-center/threat-report [https://perma.cc/9HVS-MM3J].

163. Maggie Koerth-Baker, *Why Global Hackers Are Nearly Impossible to Catch*, LIVESCIENCE (June 19, 2008), https://www.livescience.com/2627-global-hackers-impossible-catch.html [https://perma.cc/VWP8-CTTA].

164. Press Release, Tom Graves, Congressman, Rep. Tom Graves Proposes Cyber Self Defense Bill, (Mar. 3, 2017), https://tomgraves.house.gov/news/documentsingle.aspx?DocumentID=398726 [https://perma.cc/GDW3-DUQE].

165. Corey E. Thomas, *Hacking Back Will Hold Companies Back*, NACD: BOARDTALK (Sep. 14, 2017), https://blog.nacdonline.org/posts/hacking-back-hold-back [https://perma.cc/Y7RT-7GEY].

166. *Id.*

could be abused, its benefits far outweigh its detriment given that the "private sector organizations looking to hack back . . . , unlike governments, . . . typically do not have the large-scale, sophisticated intelligence gathering programs needed to accurately attribute cyberattacks to the correct actor."[167]

Alternatively, the National Cyber Investigative Joint Task Force (NCIJTF) is currently charged with "coordinat[ing], integrat[ing], and shar[ing] information to support cyber threat investigations[;] supply[ing] and support[ing] intelligence analysis for community decision-makers[;] and provid[ing] value to other ongoing efforts in the fight against the cyber threat to the nation."[168] The NCIJTF's main concern is cyber-terrorism and attacks to critical infrastructure.[169] The task force is made up of more than twenty agencies "from across law enforcement, the intelligence community, and the Department of Defense."[170] However, this task force is not able to monitor all private companies that are being actively hacked.[171]

The current approach to cyberattacks presents a high-reward-low-risk scenario for most hackers. Congress is aware of the threats cyberattacks pose "to the national security and economic vitality of the United States."[172] Because perpetrators use the internet as a shield to engage in these attacks, prosecution is untimely and deterrence is minimal.[173] Threats, in turn, only upsurge.[174] Congressional findings suggest that implementing stronger "cyber defensive practices, including enhanced training, strong[er] passwords, and routine updating and patching [of] computer systems," can prevent attacks.[175] But an active cyber-defense technique would empower both individuals and companies to form more successful cyber-defense strategies.

167. *Id.*
168. *National Cyber Investigative Joint Task Force*, FBI, https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force [https://perma.cc/638D-8PAB] (last visited Apr. 12, 2019).
169. Peter Purton, *Cyber Crime: How Are Governments Protecting Businesses Worldwide?*, AEROHIVE NETWORKS BLOG (June 15, 2016), https://blog.aerohive.com/cyber-crime-how-are-governments-protecting-businesses-worldwide/ [https://perma.cc/LW59-N4TU].
170. *National Cyber Investigative Joint Task Force*, *supra* note 168.
171. *See id.*
172. Active Cyber Defense Certainty Act, H.R. 4036, 115th Cong. at 2 (2017).
173. *Id.*
174. *Id.*
175. *Id.* at 3.

The ACDC allows "an entity that is a victim of a persistent unauthorized intrusion of the individual entity's computer" to use any method or measure to gather information to share with law enforcement or to disrupt continued unauthorized activity against the victim's own network.[176] However, the ACDC does not allow the destruction of stored information, physical injury to another, or harm to public health.[177]

For example, during the DDoS attack on Sony, Sony PlayStation Network could have employed a counter attack, allowing them to track the location from which the high volume of traffic was originating.[178] Acknowledging this would discourage many future attacks because hackers would know they cannot hide behind the internet's anonymity. Active cyber-defense would allow companies to embed tracking codes or self-destruction codes so that when information is stolen the codes would either identify the hacker's location or delete all of the stolen data. However, currently the ACDC only allows companies to use a counter-strike to obtain identification information concerning a hack's origin.[179] The latter proposition, employing malicious code to destroy the stolen data, exemplifies how a digital self-defense could be used. However, the nature and use of the ACDC created many debates within the legal and technology community, hinging on whether a right to self-defense against hackers can be effectively controlled and regulated without creating chaos.

### *A. Debate*

Proponents of hacking argue that "criminal and state-run hackers are only getting better, and that because they risk little by attacking purely defensive systems, they will simply persist until they succeed."[180] Some even argue that to actively deter hackers, companies should be allowed to insert malicious codes into the hacker's machine, going beyond exposing their identity.[181] This sort of retaliation can be a slippery slope. But with the number of daily cyberattacks rising and the increase in digitally stored

176. *Id.* at 6–7.
177. *Id.* at 7.
178. *See* Smith, *supra* note 75.
179. Active Cyber Defense Certainty Act, H.R. 4036, 115th Cong. at 5 (2017).
180. Max Fisher, *Should the U.S. Allow Companies to 'Hack Back' Against Foreign Cyber Spies?*, WASH. POST (May 23, 2013), https://www.washingtonpost.com/news/worldviews/wp/2013/05/23/should-the-u-s-allow-companies-to-hack-back-against-foreign-cyber-spies/?utm_term=.8ae6683154a9 [https://perma.cc/LM5A-H5DS].
181. *Id.*

information, such direct measures may be necessary and the only means of protection. Those who understand the digital world know that most current measures failed. Look at Denuvo—its protection was shattered within months of its release.[182] Now, many of the applications it protects appear on peer-to-peer and torrent networks, free for use.[183]

The ACDC only shields defenders from criminal liability, so companies that cause severe damage in defense of a cyberattack are still liable for civil damages.[184] Further, the highly skilled individuals who utilize an active cyber-defense attack are only allowed to retaliate after providing a preemptive review of the threat.[185] In criminal law, physical self-defense has long been recognized—it is a universally accepted principle. Self-defense has improved security and confidence in many citizens.[186] Why can't the same principle be afforded in the digital world?

Well, critics argue the ACDC will lead to a chaotic internet environment allowing companies to use self-defense as a pretense.[187] Certain terms in the statute, such as *persistent*, are vague and could "refer to the time on a network in relation to a particular intrusion, or to a series of intrusions, or both."[188] Additionally, the ACDC provides no solution where the attack is based from outside of the country.[189] Or worse, "[w]hat if a system is being attacked by the public Port Address Translation/Network Address Translation address of an organization?"[190] As a result, this would give the attacker access to every system in that public port.[191] Allowing entities to hack back in these situations is likely

182. Allegra Frank, *It Took Just 24 Hours to Crack Shadow of War's DRM*, POLYGON (Oct. 12, 2017, 12:39 PM), https://www.polygon.com/2017/10/12/16464616/middle-earth-shadow-of-war-drm-cracked-denuvo [https://perma.cc/9SVG-5BG6].

183. *See id.*

184. Chris Cook, *Hacking Back in Black: Legal and Policy Concerns with the Updated Active Cyber Defense Certainty Act*, JUST SECURITY (Nov. 20, 2017), https://www.justsecurity.org/47141/hacking-black-legal-policy-concerns-updated-active-cyber-defense-certainty-act/ [https://perma.cc/W2JZ-85JL].

185. *Id.*

186. *See* SMITH, *supra* note 12, at 30; Nemerov, *supra* note 13.

187. Cook, *supra* note 184.

188. *Id.*

189. Matthew Pascucci, *Active Cyber Defense Certainty Act: Should We 'Hack Back'?*, SEARCHSECURITY, http://searchsecurity.techtarget.com/opinion/Active-Cyber-Defense-Certainty-Act-Should-we-hack-back [https://perma.cc/AL43-MMJX] (last visited April 12, 2019).

190. *Id*.

191. Kelson Lawrence, *NAT and PAT – What's the Difference?*, BOSON (Feb. 8, 2011), http://blog.boson.com/bid/53313/NAT-and-PAT-What-s-the-Difference

to cause more harm than good.[192] Further, some critics suggest implementing "a better threat intelligence and cybersecurity organization that can act as a governing body when attacks like these occur."[193] However, under the current CFAA law such an organization would be unable to prevent attacks and would merely act as a post-theft analysis and liability agency.

In 2015, President Obama signed the Cybersecurity Information Sharing Act (CISA), trying to remedy the situation.[194] Unfortunately, CISA was nothing more than a temporary *patch* to the larger problem. The CISA "authorizes entities to share cyber threat indicators and defensive measures with each other and with [The Department of Homeland Security], with liability protection."[195]

Access Now, a digital civil-liberties group, argues that the CISA creates "[a] world where a company is forced to betray its users in order to protect them," deeming the law "backward[s]."[196] Much of Silicon Valley opposed the bill because it "allow[ed] companies to monitor users and share their information with the government without a warrant, while offering a backdoor that circumvents any laws that might protect users' privacy."[197]

This author contests that the greater problem with the CISA stems from the *limitations* on defensive measures. The law sacrifices a constitutional right to privacy[198] for the minuscule ability to use defensive

[https://perma.cc/AL43-MMJX].

192. Pascucci, *supra* note 189.

193. *Id.*

194. Thomas F. Duffy, *Cybersecurity Information Sharing Act of 2015*, CTR. FOR INTERNET SECURITY (May 2016), https://www.cisecurity.org/newsletter/cybersecurity-information-sharing-act-of-2015/ [https://perma.cc/F7J2-L4R8].

195. *Id.*

196. *CISA Security Bill Passes Senate with Privacy Flaws Unfixed*, WIRED (Oct. 27, 2015, 5:30 PM), https://www.wired.com/2015/10/cisa-cybersecurity-information-sharing-act-passes-senate-vote-with-privacy-flaws/ [https://perma.cc/FW8Z-ZKC8].

197. *Id.*

198. *See* Griswold v. Connecticut, 381 U.S. 479 (1965). In a landmark decision, Justice Douglas articulated the existence of an implied right to privacy when considering "the 'spirit' of the First Amendment (free speech), Third Amendment (prohibition on the forced quartering of troops), Fourth Amendment (freedom from searches and seizures), Fifth Amendment (freedom from self-incrimination), and Ninth Amendment (other rights), as applied against the states by the Fourteenth Amendment." Alex McBride, *The Supreme Court, Expanding Civil Rights, Landmark Cases, Griswold v. Connecticut (1965)*, THIRTEEN, https://www.thirteen.org/wnet/supremecourt/rights/landmark_griswold.html [https://perma.cc/PB82-TKHH] (last visited Apr. 29, 2019).

measures against cyber threats. The CISA's immunity from civil liability does not offer any protections or solutions to protect sensitive data when its defensive measures only include "identiy[ing] certain malicious activity, [implementing] firewall rules that successfully block certain internet traffic, and [using] techniques for screening incoming email traffic for suspicious content."[199] An ACDC type amendment to the CISA may be enough to balance the public interest in data protection and cybercrime deterrence against the greater interest of a right to privacy.

Further, because multiple computers may be used to route the attack, verifying the source of an attack is difficult; consequently, the entity using the counter measure may not be able to identify the source's IP address.[200] To confront this issue, the ACDC allows counter actions against an "entity's computer that is not under the ownership or primary control of the attacker but has been used to launch or obscure the origin of the persistent [cyberattack]."[201] The ACDC needs a technical upgrade, restriction of the defense mechanism to approved entities, a stringent probable-cause requirement, and a limit on the hacking back to the location identification when public sector access points are used.

Finally, utilizing the ACDC would violate surveillance statutes like the "Wiretap Act, the Electronic Communications Privacy Act, and the Pen Register Trap and Trace statute" because it requires companies to monitor the attacker's network.[202] The Wiretap Act prevents anyone from monitoring communications without consent, while the Electronic Communications Privacy Act prevents entities from releasing private and sensitive information to unauthorized users.[203] Entities engaging in active cyber-defense measures would inevitably violate one or both of these laws. Now the ACDC includes a voluntary preemptive-review clause that allows entities to gain FBI authorization prior to utilizing their defense measures.[204] In addition, the entity's own system does the monitoring and

199. Joseph Moreno & Keith Gerver, *Potential Risks and Rewards of Cybersecurity Information Sharing Under CISA*, CADWALADER (Jul. 21, 2016), http://www.cadwalader.com/resources/clients-friends-memos/potential-risks-and-rewards-of-cybersecurity-information-sharing-under-cisa [https://perma.cc/GF77-HNAC].

200. Cook, *supra* note 184.

201. *Id.*

202. *Id.*

203. 18 U.S.C. §§ 2701–2702 (2012).

204. Andrea Little Limbago, *The 'Hacking Back' Bill Isn't the Answer to Cyberattacks*, WAR ON ROCKS (Oct. 31, 2017), https://warontherocks.com/2017/10/the-hacking-back-bill-isnt-the-solution-to-cyberattacks/ [https://perma.cc/9H2E-5VKZ].

only involves third parties when there is an intrusion via cyberattack. The law should not protect wrongdoers at the cost of the wronged party.

### *B. Penetration Testing*

Beyond providing defense mechanisms, legalized hacking also allows for much needed ethical-penetration testing. "White hat" hackers are "ethical hacker[s] who expose[] vulnerabilities in computer systems to improve cybersecurity, rather than compromise it."[205] For example, German cryptographers were able to find flaws in Whatsapp, an encrypted end-to-end communication application used world-wide.[206] The ethical hackers were proficient in identifying the system's flaws, accessing Whatsapp's servers, and adding unauthorized members to groups, eroding the groups' confidentiality.[207]

Prosecutors have countlessly attempted to pursue charges against ethical hackers. The President of Network Installation Computer Services, Scott Moulten, conducted a penetration test while installing a connection between a local 911 Center and Cherokee County, Georgia.[208] While scanning the networks, Moulten gained access to a "Cherokee County web server that was owned and maintained by VC3, a South Carolina-based IT firm."[209] Although Moulten terminated the scan immediately, he was arrested and charged under the CFAA.[210] Instances like this exemplify why the current model of the CFAA is outdated and debilitating to entities that want to improve their own security. Thus, entities are left with no choice but to wait for—and endure—security attacks that divulge their fragilities. Permitting a carve-out in the law would allow for real-life defense testing. For example, the legislature could incorporate the

205. Donna Lu, *When Ethical Hacking Can't Compete*, ATLANTIC (Dec. 8, 2015), https://www.theatlantic.com/technology/archive/2015/12/white-hat-ethical-hacking-cybersecurity/419355/ [https://perma.cc/RE5L-LJNR].

206. Andy Greenberg, *Whatsapp Security Flaws Could Allow Snoops to Slide into Group Chats*, WIRED (Jan. 10, 2018, 7:00 AM), https://www.wired.com/story/whatsapp-security-flaws-encryption-group-chats/ [https://perma.cc/VGQ2-8EZB].

207. Shannon Liao, *Researchers Found a Way into WhatsApp Group Chats – But Facebook Says It's Not a Problem*, VERGE (Jan. 10, 2018, 6:26 PM), https://www.theverge.com/2018/1/10/16873606/whatsapp-security-gap-end-to-end-encryption-hack [https://perma.cc/T2QX-5UNR].

208. Kevin Poulsen, *Port Scans Legal, Judge Says*, SECURITYFOCUS (Dec. 18, 2000), https://www.securityfocus.com/news/126 [https://perma.cc/DJQ6-J68K].

209. *Id.*

210. *Id.*

following language into the ACDC as a safe zone to enable white-hat hacking: "Entities who employ others to test their cyber defenses, or entities who breach a private, secured cyber-defense purely to improve the security are not in violation of this Act."

The need for legalized hacking, whether in the form of a counter measure or to test an entity's cybersecurity protocols, is necessary to improve security in the digital world and deter the inexhaustible attacks that plague modern society. Alongside breach, the costs associated with retaining security measures crossover into the hundreds of millions. Entities' financial stakes are dramatically disproportionate to the legal consequences violators face. However, this incongruity does not mean or suggest that investigatory practices need to be revved up. Unless law enforcement can travel faster than information can on the internet, allocating time and resources towards heightened investigation would be futile. Once the hacker steals sensitive data, the data becomes accessible on a black market in a matter of minutes. Because self-defense is successful in deterring crime in the physical world, a parallel should be applied in the digital world.

## IX. PROPOSITION

The Facebook breach clearly demonstrates the need for legislation that allows companies to actively protect sensitive data.[211] The breach occurred when an app developer sold the personal information, information the developer gained lawfully through Facebook's app policies, of 50 million users to the political data firm Cambridge Analytica.[212] The Facebook CEO acknowledged that his company did not "take a broad enough view of [its] responsibilit[ies]."[213] During Mr. Zuckerberg's congressional hearing, he said that

> it's not enough to give people tools to sign into apps, we have to

211. Kevin Granville, *Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens*, N.Y. TIMES (Mar. 19, 2018), https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html [https://perma.cc/7H4E-79YA].

212. *Id.*

213. Justin Carissimo et al., *Mark Zuckerberg Testimony: Facebook CEO Open to Regulation*, CBS NEWS (Apr. 10, 2018, 8:03 PM), https://www.cbsnews.com/live-news/watch-mark-zuckerberg-testimony-senate-judiciary-commerce-committee-facebook-data-breach-today-live/ [https://perma.cc/6S2M-XNMS].

> ensure that all of those developers protect people's information too. It's not enough to have rules requiring they protect information, it's not enough to believe them when they tell us they're protecting information—we actually have to ensure that everyone in our ecosystem protects people's information.[214]

During the hearing, Congress posed a challenge to online companies warning that "[i]f Facebook and other online companies will not or cannot fix the privacy invasions, then we are going to have to—we the Congress."[215] However, it was alarming that Congress did not understand the technical and social parameters of how the internet, Facebook, and, specifically, personal-data collection works. But all "seem to agree they want to fix something about Facebook. They just [had] no idea what."[216] Herein lies the problem, if Congress is ill-equipped to understand and "agree on the problem, [then] it might be hard to agree on the solution."[217]

Legalized hacking, a form of offensive active-incident response, is the type of broader responsibilities and information protection that can help solve this issue. Companies would hire cybersecurity counter-strike experts or cybersecurity firms whose job would surpass monitoring threats on the network. A counter-strike expert would be used only in the event that a hacker is able to bypass the technological-defense barriers. In such cases, an active defense would trace the time, origin, method, and intent of the attack. A DDoS attack would require an active port, and most other live attacks would require an active IP address, which are traceable.[218] The counter-strike agent would report this information to the appropriate authorities. Depending on the type of attack, this information should allow investigators to infer the hacker's intent. For example, if ransomware is used, the intent of the hacker is likely to extort money in exchange for decrypting sensitive information.

214. *Hard Questions: Q&A with Mark Zuckerberg on Protecting People's Information,* FACEBOOK NEWSROOM (Apr. 4, 2018), https://newsroom.fb.com/news/2018/04/hard-questions-protecting-peoples-information/ [https://perma.cc/Q3XR-86X4].

215. Carissimo et al., *supra* note 213.

216. Emily Stewart, *Lawmakers Seem Confused about What Facebook Does – and How to Fix It*, VOX (Apr. 10, 2018, 7:50 PM), https://www.vox.com/policy-and-politics/2018/4/10/17222062/mark-zuckerberg-testimony-graham-facebook-regulations [https://perma.cc/ZFX4-4VLL].

217. *Id.*

218. Adarsh Verma, *What Is a DDoS Attack?*, FOSSBYTES (Aug. 17, 2015), https://fossbytes.com/what-is-a-ddos-attack-how-ddos-attack-works/ [https://perma.cc/RA54-6XHM].

Lastly, when sensitive data is stolen, two options should be available. First, companies should be allowed to not only encrypt data but also inject malicious code as a precautionary measure. This would render an unauthorized hacker's computer useless and send a location back to the owner of the data. Alternatively, the companies should have the option to counter-strike and delete or retrieve the data while embedding malicious code into the attacker's computer, ceasing the attack mid-transfer. These are differing methods to the same end. The counter-strikers ultimate goal is to find the hacker and bring them to justice rather than take part in vigilantism. The deterrence lies in exposing their identity and prosecuting them.

The scope of the statute should be limited to registered entities or entities that are government-certified *ethical hackers*. In addition, the skill to hack back is not something that is easily learned, so the general population would not be able to use it as effectively as physical self-defense. These limitations go to the nature of the threat itself, which is primarily aimed at large corporations. It is not this Note's suggestion that the ACDC become a full-fledged self-defense mechanism for anyone to use. Rather, it should be a restrictive mechanism that gives entities a greater chance at success.

Interestingly enough, the concept of hacking back is not entirely novel when it comes to investigating cybercrimes. In the past, law enforcement used hacking tools "to pursue criminal suspects who have anonymized their communications on the dark web."[219] For example, to apprehend the creator of Silk Road, a digital marketplace that "facilitate[s] black market transactions" through the use of a cryptographic communication protocol, investigators posed as fake consumers but were unable to beat the decryption system.[220] It was only the creator's human error, signing his original identity on a public website long before Silk Road became active, which led to his arrest.[221]

Further, Federal Rules of Criminal Procedure 41(b)(6) allows for a judge in a criminal investigation to issue a search warrant to remotely access or hack an electronic device and "seize . . . information located *within or outside* that district if . . . the district where the media or information is located has been concealed through technological

219. Ghappour, *supra* note 93, at 1075.
220. *Id.* at 1077–78.
221. *Id.* at 1078.

means."[222] This allows for law enforcement to use "network investigative technique[s]" such as "remotely accessing and installing malware on a computer without the permission of its owner or operator. . . . and converting it into a surveillance device."[223] This is the very essence of what the ACDC allows private entities to do, but it is in the form of self-defense rather than investigation of potential cyber-criminals. Because private entities are in a better position to protect their own interest, the use of such hacking tools should not only be limited to government purposes.

Paradoxically, a leak from within the U.S. National Security Agency exposed the government's involvement in the weaponizing of exploits and the "hoarding of hacking tools."[224] The tools include exploits that inject code into target assets. For instance, log keys copy target data, hack into e-mail servers, change time-stamps, and run malicious code.[225] The government, through the use of these tools, acknowledges that an active approach in the digital world is necessary and effective.

Finally, individuals should be allowed to register as *ethical hackers* after undergoing a rigorous background check. This would improve the art of cyber-defense and, more significantly, would provide those committed to penetration testing a legal safe-harbor. Hackers currently use the Darknet, among other forums, to communicate vulnerabilities and hacks with each other.[226] Allowing *ethical hackers* to do the same would balance the scales and limit the opportunities criminal hackers have in finding a zero-day exploit. Most importantly, allowing ethical hacking would give the federal government control over entities that can exercise such skill over interstate commerce.

Cyberattacks are on the rise, and at this moment, almost all aspects of society are vulnerable. Digital integrity is becoming synonymous with physical integrity; therefore, protection is needed. How do entities who maintain large amounts of sensitive data defend themselves from constant, innovative, and intrusive attacks? The ACDC presents a solution to the

222. Fed. R. Crim. P. 41(b)(6) (emphasis added).

223. Ghappour, *supra* note 93, at 1079.

224. Matt Day, *Microsoft Criticizes Government Creation of Hacking Tools Used in Global Cyberattack*, SEATTLE TIMES (May 14, 2017, 1:58 PM), https://www.seattletimes.com/business/microsoft/microsoft-criticizes-government-creation-of-hacking-tools-used-in-global-cyberattack/ [https://perma.cc/AVG5-HZ3Y].

225. Devin Coldewey, *Names and Definitions of Leaked CIA Hacking Tools*, TECHCRUNCH (Mar. 9, 2017), https://techcrunch.com/2017/03/09/names-and-definitions-of-leaked-cia-hacking-tools/ [https://perma.cc/DH2C-Y4JV].

226. Greenberg, *supra* note 97.

problem. It allows for digital self-defense in a predominantly digital era analogous to the common-law right to physical self-defense. Because the internet has revolutionized modern society, the laws governing such conduct on the internet must catch up.