South Dakota Law Review

Volume 65 | Issue 3

2020

Spoiling for a Fight: Hacking Back with the Active Cyber Defense Certainty Act

Alice M. Porch

Recommended Citation
Alice M. Porch, *Spoiling for a Fight: Hacking Back with the Active Cyber Defense Certainty Act*, 65 S.D. L. Rev. 467 (2020).
Available at: https://red.library.usd.edu/sdlrev/vol65/iss3/6

SPOILING FOR A FIGHT: HACKING BACK WITH THE ACTIVE CYBER DEFENSE CERTAINTY ACT

ALICE M. PORCH†

Cybersecurity breaches are happening all the time. While hackers continue to attack computers on the Internet, organizations need to protect their networks to secure the data they collect. Congress conducted an investigation of the hacking problem and found that more deterrence is necessary to stop cybercriminals. To create a solution, United States House Representative Tom Graves sponsored a bill, along with a bipartisan group of cosponsors, called the Active Cyber Defense Certainty ("ACDC") Act. The ACDC Act would update the Computer Fraud and Abuse Act to allow organizations to take active cyber defense measures that go beyond the boundaries of their own networks. Although the bill has good intentions, there are critics in the technology industry that fear the ACDC Act would create more problems.

I. INTRODUCTION: FIGHTING HACKERS

In 2007, Michel Cukier, assistant professor of mechanical engineering at the University of Maryland, wanted to profile the behavior of hackers who randomly attack computers using unsophisticated methods.[1] To collect data, Cukier and his graduate students set up four Linux[2] computers with Internet access and weak security.[3] They discovered that the computers were almost constantly under attack, mostly from hackers using "brute force" hacking techniques.[4] The research showed that hackers launched their random attacks using basic software-

† Alice Porch has a Juris Doctor from the Stetson University College of Law and is a licensed attorney in Florida. She is a Certified Information Privacy Professional ("CIPP/US"), a Certified Ethical Hacker ("C|EH"), and has the CompTIA Security+ certification. The author thanks Stan Porch, a Certified Information Systems Security Professional ("CISSP"), for offering his technical knowledge and experience to review this article. The author also thanks the dedicated members of the *South Dakota Law Review* for reviewing and publishing this article.

[1] Michel Cukier, *Study: Hackers Attack Every 39 Seconds*, UNIV. OF MD. A. JAMES CLARK SCH. OF ENG'G (Feb. 9, 2007), https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds. Michel Cukier is an assistant professor of mechanical engineering at the A James Clark School of Engineering at the University of Maryland and "an affiliate of the School's Center for Risk and Reliability and Institute for Systems Research." *Id.*

[2] "Linux is the best-known and most-used open source operating system." *What Is Linux?*, OPENSOURCE.COM, https://opensource.com/resources/linux (last visited Feb. 1, 2020). An operating system "is software that sits underneath all of the other software on a computer, receiving requests from those programs and relaying these requests to the computer's hardware." *Id.*

[3] Cukier, *supra* note 1.

[4] *Id.*

aided techniques such as "dictionary attacks"[5] to guess passwords by running through lists of common words.[6]

Almost a decade later, ransomware emerged as the fastest growing threat that targets all types of users by taking their files hostage.[7] Ransomware is a type of malware that locks users out of their systems, encrypts their files with algorithms that are nearly impossible to break, and then demands a payment to unlock their files.[8] A United States interagency technical guide reported that every day since January 1, 2016, an average of 4,000 ransomware attacks occurred, which was an increase of 300% from 2015.[9] By 2019, ransomware attacks affected "more than 70 state and local governments" in the United States.[10] Even worse, new strains of ransomware include a threat to publish stolen files on the Internet if the victim refuses to pay the ransom.[11]

In recent years, Supervisory Control and Data Acquisition ("SCADA") hacking of industrial control systems has become a major concern in the evolving world of cyber wars.[12] SCADA devices "control nearly every type of industrial system such as the electrical grid, power plants, manufacturing systems, sewage and water systems, oil and gas refineries and nearly every type of industrial system."[13] The manipulation and control of these industrial systems though SCADA hacking "could itself become a weapon."[14]

To empower organizations to protect themselves from hackers, in 2017, United States House Representatives, Rep. Tom Graves (a Republican from Georgia) and Rep. Kyrsten Sinema (a Democrat from Arizona), introduced the Active Cyber Defense Certainty Act ("ACDC Act"), H.R. 4036, into the 115th Congress.[15] Along with its sponsor, Rep. Graves, H.R. 4036 had nine bipartisan

[5] *Id.*; *Dictionary Attacks*, HACKSPLAINING.COM, https://www.hacksplaining.com/glossary/dictionary-attacks (last visited Dec. 8, 2019).

[6] Cukier, *supra* note 1. The "A Clark School study is one of the first to quantify the near-constant rate of hacker attacks of computers with Internet access—every 39 seconds on average—and the non-secure usernames and passwords we use that give attackers more chance of success." *Id.*

[7] *How to Protect Your Networks from Ransomware*, U.S. COMPUT. EMERGENCY READINESS TEAM 2 https://www.us-cert.gov/sites/default/files/publications/RansomwareExecutiveOne-PagerandTechnicalDocument-FINAL.pdf (last visited Feb. 2, 2020).

[8] *Id.*

[9] *Id.*

[10] Alfred Ng, *Ransomware Froze More Cities in 2019. Next Year Is a Toss-Up,* CNET (Dec. 5, 2019), https://www.cnet.com/news/ransomware-devastated-cities-in-2019-officials-hope-to-stop-a-repeat-in-2020/.

[11] Brian Krebs, *Ransomware Gangs Now Outing Victim Businesses That Don't Pay Up*, KREBS ON SEC. (Dec. 16, 2019), https://krebsonsecurity.com/2019/12/ransomware-gangs-now-outing-victim-businesses-that-dont-pay-up/.

[12] OTW, *SCADA Hacking: Why YOU Should Study SCADA/ICS Hacking*, HACKERS-ARISE (Sept. 2, 2019), https://www.hackers-arise.com/post/2017/06/30/scada-hacking-why-you-should-study-scadaics-hacking.

[13] *Id.*

[14] *Id.*

[15] Active Cyber Defense Certainty Act, H.R. 4036, 115th Cong. (2017); Press Release, Congressman Tom Graves, Rep. Tom Graves Formally Introduces Active Cyber Defense Bill (Oct. 13, 2017), https://tomgraves.house.gov/news/documentsingle.aspx?DocumentID=398840.

cosponsors, but it did not become law.[16] In 2019, Rep. Graves reintroduced the ACDC Act under H.R. 3270 with Rep. Josh Gottheimer (a Democrat from New Jersey), and this time it has eighteen bipartisan cosponsors.[17] The bill would make "targeted changes" to the 1986 Computer Fraud and Abuse Act ("CFAA") "to allow use of limited defensive measures that exceed the boundaries of one's network" to monitor, identify, and stop hacking attacks.[18] Currently, the CFAA does not make exceptions for the use of defensive actions to prevent attacks other than taking preventative measures, such as installing anti-virus software.[19] Rep. Graves believes that the passage of the ACDC Act could be "the most significant update to the CFAA since its enactment."[20]

Cyber breaches are getting out of control, and the proposed ACDC Act aspires to give the private sector a tactic to fight cybercrime. Although the bill intends to give organizations a way to fight back against hackers, critics worry that instead of stopping cybercrime, it may create more problems and potential liabilities for organizations.[21] If passed, the Act could leave organizations with the feeling that they are fighting outlaws in a cyber-version of the Wild West.

Part II of this article examines how organizations protect their networks and then explores existing issues such as the arrests of security researchers.[22] Part III evaluates the relevant parts of the CFAA, examines information sharing, and breaks down the ACDC Act to analyze how effective it would be for preventing hacking attacks.[23] Part IV looks to the future of cybersecurity by analyzing the pros and cons of passing the ACDC Act and offers possible solutions to make the law more effective.[24]

II. PROTECTING COMPUTER NETWORKS

A. BEST PRACTICES

Organizations have the responsibility of protecting their networks from intruders by adhering to the best practices in their industries. Although best practices are based around voluntary actions, state breach notification laws establish a duty for organizations to use reasonable procedures and practices to

[16] Active Cyber Defense Certainty Act, H.R. 4036, 115th Cong. (2017).

[17] Active Cyber Defense Certainty Act, H.R. 3270, 116th Cong. (2019); Press Release, Congressman Tom Graves, Graves, Gottheimer Introduce the Active Cyber Defense Certainty Act (June 13, 2019), https://tomgraves.house.gov/news/documentsingle.aspx?DocumentID=401122 [hereinafter Press Release, Graves, Gottheimer Introduce ACDC Act].

[18] Press Release, Graves, Gottheimer Introduce ACDC Act, *supra* note 17.

[19] *Id.*

[20] *Id.*

[21] *See infra* Part IV (analyzing the ACDC Act and offering possible solutions to make the Act more effective).

[22] *See infra* Part II (exploring how organizations protect their networks, as well as discussing current issues).

[23] *See infra* Part III (evaluating the CFAA and breaking down the ACDC Act).

[24] *See infra* Part IV (analyzing the ACDC Act and offering possible solutions to make the Act more effective).

secure their data.[25] The National Institute of Standards and Technology ("NIST") promotes a "Cybersecurity Framework" that is based on five primary functions: Identify, Protect, Detect, Respond, and Recover.[26] These functions work together to create a "successful and holistic cybersecurity program."[27] The International Organization for Standardization ("ISO") established ISO 27001, which contains detailed standards for information security that is accepted internationally as a "de facto" cybersecurity framework.[28] The ISO standard provides guidance for organizations to review, measure, and audit their cybersecurity programs so they can take corrective actions and make improvements.[29]

An effective cybersecurity program should balance security measures with safety concerns.[30] The concept of "defense in depth" aims to secure an organization's assets by establishing multiple layers of security controls.[31] For example, to protect the physical environment, the "first line of defense" involves implementing administrative, technical, and physical controls.[32] Administrative controls include facility design, employee management, and emergency response.[33] Technical controls include access limits, intrusion detection, and system audits.[34] Physical controls include perimeter security, locks, and guards.[35]

As an example of defensive measures, a "robust" network defense should include an Intrusion Detection System ("IDS") and an Intrusion Prevention System ("IPS") solution.[36] Conceptually, an IDS captures and analyzes data packets in real time to detect malicious traffic, which is called "promiscuous" mode, and it works with other network devices, such as routers and firewalls.[37] In contrast, an IPS monitors traffic and provides protection in real time by not

[25] *Data Security Laws, Private Sector*, NAT'L CONF. OF STATE LEGISLATURES (May 29, 2019), http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx.

[26] *The Five Functions*, NIST, https://www.nist.gov/cyberframework/online-learning/five-functions (last updated Aug. 10, 2018).

[27] *Id.*

[28] Dejan Kosutic, *Which One to Go With – Cybersecurity Framework or ISO 27001?*, ADVISERA: THE ISO 27001 & ISO 22301 BLOG (Feb. 24, 2014), https://advisera.com/27001academy/blog/2014/02/24/which-one-to-go-with-cybersecurity-framework-or-iso-27001/. ISO/IEC 27001:2013 is a part of the ISO/IEC 27000 international family of standards. ISO 27001 is a certifiable standard that formally specifies an Information Security Management System ("ISMS"), which is regularly reviewed and audited. ISO 27001 has a key objective to ensure the confidentiality, integrity, and availability for critical data assets. On the other hand, ISO 27002 is not a "formal certification, but it provides best practice recommendations for information security management policies." *ISO/IEC 27001:2013*, INT'L STANDARDS ORG., https://www.iso.org/standard/54534.html (last visited Jan. 14, 2020); *Information Security & Compliance (ISO 27001)*, WILKINS CONSULTING, http://www.wilkins-consulting.com/security-compliance.html (last visited Jan. 14, 2020).

[29] Kosutic, *supra* note 28.

[30] David Hutter, *Physical Security and Why It Is Important*, SANS INST., 11 (Jun. 10, 2016), https://www.sans.org/reading-room/whitepapers/physical/physical-security-important-37120.

[31] *Id.*

[32] *Id.*

[33] *Id.*

[34] *Id.*

[35] *Id.*

[36] Catherine Paquet, *Network Security Using Cisco IOS IPS*, CISCO PRESS (June 8, 2009), http://www.ciscopress.com/articles/article.asp?p=1336425.

[37] *Id.*

allowing packets to enter the network on its trusted side, which is called "inline" mode.[38] There are different types of IDS/IPS sensors such as signature based, policy based, anomaly based, and honeypot based.[39] These concepts are combined into an Intrusion Detection and Prevention System ("IDPS") that "consists of more than one application or hardware device and incorporates more than just detection" and involves three network defense functions: "prevention, detection, and response."[40]

B. PENETRATION TESTING

A cyber breach can leave an organization exposed to legal liabilities and "are frequently the result of vulnerabilities that could have been fixed for a relatively low cost."[41] To identify weaknesses in a network, an organization should conduct a risk assessment that includes a penetration ("pen") test.[42] Organizations routinely allow security researchers, also referred to as "pen testers," to reveal security gaps in their networks by using "brute force" hacking methods.[43] A pen tester is considered to be a "white hat or good hacker" who is trained to "think like a bad guy" with the end goal of improving the security practices of an organization "to prevent theft and damage."[44]

The purpose of a pen test is to figure out how a cybercriminal could harm an organization's computer systems and applications.[45] A pen test involves multiple phases that include planning, reconnaissance, scanning, exploitation, risk analysis, recommendation, and report generation.[46] An efficient pen test helps to identify various attack vectors so an organization can prioritize correcting any misconfigurations and improve the time to respond to a security incident.[47]

When researchers engage in reconnaissance and set up network defenses, an organization must maneuver through a "fog of legal and ethical uncertainty" that surrounds a maze of federal and state laws regarding computer crimes and privacy protections.[48] Generally, a pen tester needs express written permission by the targeted organization to conduct security tests along with a detailed agreement that

[38] *Id.*

[39] *Id.*

[40] RANDY WEAVER, DAWN WEAVER & DEAN FARWOOD, GUIDE TO NETWORK DEFENSE AND COUNTERMEASURES 266 (Cengage Textbook, Kindle Edition 2014).

[41] Steve King, *Why Penetration Tests Are So Essential*, DATA BREACH TODAY (Jan. 13, 2020), https://www.databreachtoday.com/blogs/penetration-tests-are-so-essential-p-2850.

[42] *Id.*

[43] *Id.*; EC-Council, *Purpose of Intelligence-Led Penetration and Its Phases – 1*, EC-COUNCIL|BLOG (Dec. 27, 2019), https://blog.eccouncil.org/purpose-of-intelligence-led-penetration-and-its-phases-1/.

[44] Brianna White, *Your Next Move: Penetration Tester*, COMPTIA (Oct. 20, 2017), https://www.comptia.org/blog/your-next-move-penetration-tester.

[45] EC-Council, *supra* note 43.

[46] *Id.*

[47] *Id.*

[48] Aaron J. Burstein, *Conducting Cybersecurity Research Legally and Ethically,* 1 (Apr. 5, 2008), https://static.usenix.org/events/leet08/tech/full_papers/burstein/burstein.pdf.

includes the rules of engagement during the project; otherwise, the pen tester may end up in trouble with law enforcement and also face civil liabilities.[49]

A Florida case from 2016 demonstrates the need for an express agreement to conduct pen testing. An independent security researcher, David Levin, found a vulnerability in the website for the Lee County Elections in Florida.[50] To announce his findings, Levin appeared in a video posted on YouTube.com with Dan Sinclair, a candidate running against Sharon Harrington, the Supervisor of Elections.[51] In the video, Levin demonstrated how he used a SQL injection[52] attack to access usernames and passwords in the website's database.[53]

Harrington reported the hacking incident to the Florida Department of Law Enforcement ("FDLE").[54] The FDLE served Levin with a search warrant and took his cellphone and laptops belonging to him and his wife.[55] As a result of the investigation, the FDLE arrested Levin and charged him with "three third-degree-felony counts of property crimes."[56] While Levin faced prosecution, Harrington accused Sinclair of creating a publicity stunt.[57]

A written contract for pen testing should include details of the rules of engagement, which may require notification to law enforcement. In 2019, two pen testers employed by Coalfire, a security firm, tripped an alarm at the Dallas County Courthouse in Iowa.[58] Within three minutes, police officers arrived and found the pen testers walking around the building, taking pictures, and manipulating doors.[59] One of the pen testers explained to a deputy that they were authorized to conduct a vulnerability study.[60] Instead of letting them go, the officers arrested the pen testers and charged both with "third-degree burglary and possession of burglary tools."[61] The Des Moines Register revealed that the

[49] Corey Nachreiner, *Pen-Tester Arrested - Daily Security Byte EP. 260*, at 1:30-40, YOUTUBE (May 9, 2016), https://www.youtube.com/watch?v=ckX6BYNdGw4.

[50] Ben Brasch, *Lee Elections Website Hacking Involves Elections Supervisor Candidate*, NEWS-PRESS (Feb. 10, 2016), https://www.news-press.com/story/news/2016/02/08/lee-elections-website-hacked-supervisor-elections-candidate/80025004/.

[51] *Id.*

[52] *Id. See* J.M. Porup, *What Is SQL Injection? How SQLi Attacks Work and How to Prevent Them*, CSO (Oct. 2, 2018), https://www.csoonline.com/article/3257429/what-is-sql-injection-how-sqli-attacks-work-and-how-to-prevent-them.html ("SQL injection is a type of attack that can give an adversary complete control over your web application database by inserting arbitrary SQL code into a database query.").

[53] Brasch, *supra* note 50.

[54] *Id.*

[55] *Id.*

[56] Ben Brasch, *Estero Man Arrested for Hacking Into State, Lee Elections Website*, NEWS-PRESS (May 4, 2016), https://www.news-press.com/story/news/crime/2016/05/04/estero-man-arrested-hacking-into-state-lee-elections-website-david-levin-dan-sinclair/83921672/.

[57] *Id.*

[58] Anna Spoerre, *State Employees Authorized Courthouse 'Penetration,' Urged Sheriff Not to Make Burglary Arrests, Records Show*, DES MOINES REG. (Sept. 19, 2019), https://www.desmoinesregister.com/story/news/crime-and-courts/2019/09/18/iowa-courts-dallas-county-courthouse-coalfire-contract-judicial-branch-test-security-ia-crime-arrest/2356047001/.

[59] *Id.*

[60] *Id.*

[61] *Id.*

judicial branch had a contract with Coalfire "to test the 'adequacy and effectiveness' of security" at various buildings in Iowa, which included the Dallas County Courthouse.[62] The contract included a physical security test using methods such as tailgating, dumpster diving, and picking locks; however, the state court administrators announced that they "did not intend, or anticipate, those efforts to include the forced entry into a building."[63]

Several weeks later, the county attorney had the charges against the pen testers reduced to criminal trespass.[64] Coalfire's CEO, Tom McAndrew, was not satisfied, and he wrote in a press release that "The ongoing situation in Iowa is completely ridiculous, and I hope that the citizens of Iowa continue to push for justice and common sense."[65] McAndrew expected the charges to be dropped after "the Iowa Supreme Court Chief Justice apologized and admitted mistakes were made . . . ."[66] He emphasized that Coalfire's pen testers "were simply doing the job that Coalfire was hired to do," and the job was similar in nature to one they conducted three years earlier for the Iowa State Judicial Branch and had "done hundreds of times around the world for similar clients."[67] He further explained that physical testing was part of active pen testing as "a best practice and a common engagement," and the judicial branch confirmed the pen tests for specific locations through multiple documented conversations.[68]

III. COMBATING COMPUTER CRIMES

A. THE COMPUTER FRAUD AND ABUSE ACT

In 1984, Congress addressed federal computer-related crimes when it enacted the Comprehensive Crime Control ("CCC") Act to prosecute the unauthorized access of computers.[69] However, Congress continued to investigate the emerging threat of computer crimes and amended the CCC Act by passing the Computer Fraud and Abuse Act ("CFAA") in 1986.[70] The goal of the CFAA was to strike a balance between the interests of the federal government and the ability of the states to prosecute computer crimes.[71]

[62] *Id.*

[63] *Id.*

[64] Alex Schuman, *Coalfire CEO Says Dallas County Courthouse Doors Were Unlocked*, KCCI 8 NEWS DES MOINES (Oct. 30, 2019), https://www.kcci.com/article/coalfire-ceo-lambasts-dallas-county-sheriff-in-scathing-statement/29639404.

[65] *Coalfire CEO Tom McAndrew Statement*, COALFIRE (Oct. 29, 2019), https://www.coalfire.com/News-and-Events/Press-Releases/Coalfire-CEO-Tom-McAndrew-statement.

[66] *Id.*

[67] *Id.*

[68] *Id.*

[69] 18 U.S.C. § 1030 (1984); OFFICE OF LEGAL EDUC. EXEC. OFFICE FOR U.S. ATTORNEYS, *Prosecuting Computer Crimes*, 1 (2010), https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf [hereinafter *Prosecuting Computer Crimes*].

[70] *Prosecuting Computer Crimes*, *supra* note 69.

[71] *Id.*

Criminal offenses in the CFAA require that the defendant access a computer "without authorization" or "exceed authorized access" of a computer.[72] The CFAA does not define the term "without authorization," but its legislative history reflects an expectation that "persons who access computers 'without authorization' will typically be outsiders (e.g., hackers)."[73] In addition to criminal penalties, the CFAA allows a victim to pursue a civil action against the violator, and the remedies include "compensatory damages and injunctive or other equitable relief."[74]

B. THE CYBERSECURITY INFORMATION SHARING ACT OF 2015

The Cybersecurity Information Sharing Act of 2015 ("CISA") provides protection from liability under its provisions for sharing "cyber threat indicators and defensive measures" with government and private entities.[75] Under CISA, parties may use defensive measures such as "an action, device, procedure, signature, technique, or other measure applied to an information system," but CISA does not allow the parties to "hack back" to gain unauthorized access to another network.[76] Participating in CISA is voluntary, and the federal government cannot force parties to share information.[77]

CISA authorizes entities to monitor their information system for cybersecurity purposes.[78] Generally, CISA's liability protections apply to information sharing conducted with Information Sharing and Analysis Centers ("ISACs") and Information Sharing and Analysis Organizations ("ISAOs").[79] CISA provides an exemption for violating antitrust laws for two or more private organizations "to exchange or provide a cyber threat indicator or defensive measure, or assistance relating to the prevention, investigation, or mitigation of a

[72] *Id.* at 5. In the CFAA under 18 U.S.C. § 1030(a)(2)(C), the term "protected computer" is commonly used in many prosecutions and "is a statutory term of art that has nothing to do with the security of the computer." *Id.* at 4. A protected computer is defined under 18 U.S.C. § 1030(e)(2) and "covers computers used in or affecting interstate or foreign commerce and computers used by the federal government and financial institutions." *Id.* A protected computer also covers "an individual using a computer" who "contacts or communicates with an Internet website." *Id.*

[73] *Id.* at 5.

[74] *Id.* at 3.

[75] 6 U.S.C. §§ 1501-1510 (2015); *Cybersecurity Information Sharing Act – Frequently Asked Questions*, U.S. COMPUT. EMERGENCY READINESS TEAM, 1, https://www.us-cert.gov/sites/default/files/ais_files/CISA_FAQs.pdf (last visited Jan. 1, 2020) [hereinafter *Cybersecurity Information Sharing Act – FAQs*].

[76] 6 U.S.C. § 1501(7)(A) (2015); Jasper L. Tran, *Navigating the Cybersecurity Act of 2015*, 19 CHAP. L. REV. 483, 487 (2016).

[77] Tran, *supra* note 76, at 486.

[78] 6 U.S.C. § 1503(a) (2015).

[79] *Cybersecurity Information Sharing Act – FAQs*, *supra* note 75, at 2. ISACs provide "sector-specific collaboration" for critical infrastructure sectors, and ISAOs provide "practice sharing networks" for a combination of public and private sector organizations. ACSC Staff, *ISACS vs ISAOs: Supporting the Cybersecurity Information Sharing Ecosystem*, ADVANCED CYBER SEC. CTR. (Nov. 26, 2018), https://www.acscenter.org/blog/isac-vs-isao-supporting-the-cybersecurity-information-sharing-ecosystem.

cybersecurity threat."[80] The information shared under CISA's provisions is exempt from disclosure under federal, state, tribal, or local laws.[81] CISA also contains a non-waiver of privilege where "sharing information with the federal government does not waive privileges," but it does not have this provision for sharing with companies, state governments, or local governments.[82]

The Department of Homeland Security ("DHS") offers a free Automated Indicator Sharing ("AIS") service that enables participants from the private sector to exchange cyber threat indicators with the federal government "at machine speed."[83] Threat indicators include pieces of information such as a phishing email sender or a malicious IP address.[84] The DHS created AIS as part of an ecosystem for private companies and federal agencies to share attempted compromises in real time to reduce cyberattacks.[85] To ensure privacy, DHS has applied "careful measures" that are regularly tested to protect civil liberties with the goal of minimizing data collection and only retaining information related to a threat.[86] These measures include processes that protect personally identifiable information ("PII") such as an automated analyzer that deletes PII not related to a cyber threat along with human review of certain indicators.[87]

CISA requires oversight by multiple government entities that review the effectiveness of the statute.[88] Every two years, CISA requires a joint report to Congress on the actions taken to accomplish its objectives by the "appropriate Federal entities," which includes the "Departments of Commerce, Defense, Energy, Homeland Security, Justice, and the Treasury, and the Office of the Director of National Intelligence (ODNI)" that are "in consultation with the Inspector General of the Intelligence Community and the Council of Inspectors General on Financial Oversight."[89]

[80] 6 U.S.C. § 1503(c) (2015).

[81] *Id.* § 1503(d)(4)(B)(ii); Brad S. Karp, *Federal Guidance on the Cybersecurity Information Sharing Act of 2015*, HARV. LAW SCH. FORUM ON CORP. GOVERNANCE (Mar. 3, 2016), https://corpgov.law.harvard.edu/2016/03/03/federal-guidance-on-the-cybersecurity-information-sharing-act-of-2015/.

[82] Karp, *supra* note 81.

[83] *Automated Indicator Sharing (AIS)*, U.S. DEP'T OF HOMELAND SEC. CISA, https://www.us-cert.gov/ais (last visited Jan. 6, 2020) [hereinafter *Automated Indicator Sharing (AIS)*].

[84] *Id.* "An IP address (short for Internet Protocol address) is used to identify computers on the Internet. It works like a return address would on a piece of mail." *About IP Addresses*, GOOGLE, https://support.google.com/websearch/answer/1696588?hl=en (last visited Jan. 15, 2020) [hereinafter *About IP Addresses*].

[85] *Automated Indicator Sharing (AIS)*, *supra* note 83.

[86] *Id.*

[87] *Id.*

[88] Office of the Inspector General of the Intelligence Community, *Unclassified Joint Report on the Implementation of the Cybersecurity Information Sharing Act of 2015*, 1 (Dec. 19, 2019), https://www.oversight.gov/sites/default/files/oig-reports/Unclassified%2020191219_AUD-2019-005-U_Joint%20Report.pdf.

[89] *Id.*

The 2019 report found that the sharing of cyber threats and defensive measures has improved, but there are multiple areas that need improvement.[90] The report identified barriers that hinder information sharing such as restrictive classifications that limit sharing, communication hurdles that reduce speed, and liability uncertainties that impact private sector participation.[91] For non-government entities, the report revealed there is a minimal use of the AIS capability for sharing cyber threats.[92] An investigation by auditors found that the cyber threat indicators lacked the context necessary for entities to know what actions to take.[93] To increase participation, DHS launched the AIS Engagement Plan to target and recruit partners to overcome the challenges that entities have with sharing information.[94]

C. THE PROPOSED ACTIVE CYBER DEFENSE CERTAINTY ACT

The ACDC Act presents "congressional findings" about cyber-enabled crimes to justify adding exceptions to the CFAA for battling cyberattacks.[95] Congress found that cyber-related crimes posed a "severe threat to the national security and economic vitality of the United States."[96] The investigation revealed that law enforcement has a difficult time responding and prosecuting cybercrime; although computer hacking is an almost constant threat, the Department of Justice ("DOJ") prosecuted only 165 computer fraud cases in 2017.[97]

Congress determined from its findings that the current situation in cyberspace is unacceptable, and cybercrime will continue to be further incentivized without deterrence.[98] The ACDC Act's sponsor, Rep. Graves, believes the Act will be an effective solution because it "unties the hands of law-abiding defenders to use new techniques to thwart and deter attacks, while also providing legal certainty for industry experts to innovate, which could spur a new generation of tools and methods."[99] Although the Act creates exceptions from prosecution under the CFAA, it also states that a victim of cybercrime should first report the incident to authorities.[100] Also, the Act emphasizes that citizens and organizations should improve their cyber breach preventative measures, such as updating computer systems and using strong passwords.[101]

[90] *Id.*; Akshaya Asokan, *Cybersecurity Data Sharing: A Federal Progress Report*, DATA BREACH TODAY (Jan. 3, 2020), https://www.databreachtoday.com/cybersecurity-data-sharing-federal-progress-report-a-13575.

[91] Office of the Inspector General, *supra* note 88, at 3.

[92] *Id.* at 11.

[93] *Id.*

[94] *Id.*

[95] Active Cyber Defense Certainty Act, H.R. 3270, 116th Cong. § 2 (2019).

[96] *Id.* § 2(1).

[97] *Id.* § 2(2).

[98] *Id.* § 2(2)-(3).

[99] *ACDC Explainer 2019*, U.S. HOUSE OF REPRESENTATIVES, 1-2, https://tomgraves.house.gov/uploadedfiles/acdc_explainer_2019.pdf (last visited Dec. 21, 2019) [hereinafter *ACDC Explainer 2019*].

[100] Active Cyber Defense Certainty Act, H.R. 3270, 116th Cong. § 2(4) (2019).

[101] *Id.* § 2(5).

The ACDC Act would modify the CFAA to state that using "active cyber defense measures" would not be a violation of the law. An "active cyber defense measure" is defined in the Act as "consisting of accessing without authorization the computer of the attacker to the defender's own network to gather information."[102] An attacker is "a person or an entity that is the source of the persistent unauthorized intrusion into the victim's computer."[103] The purpose of using the measure is to establish attribution of hackers to inform authorities, to disrupt persistent unauthorized activity, and to monitor the behavior of the hacker for improving cyber defense techniques.[104]

The intention of the ACDC Act is to protect a "defender" against prosecution for using a cyber defense that could violate the CFAA.[105] The Act defines a defender as "a person or an entity that is a victim of a persistent unauthorized intrusion of the individual entity's computer."[106] However, the Act does not apply to a civil action, so an entity or defender can be held liable for damages caused to others.[107]

The congressional findings emphasize the dangers involved with the use of active cyber defenses. The ACDC Act aims to provide "legal certainty" to organizations "by clarifying the type of tools and techniques that defenders can use that exceed the boundaries of their own computer network."[108] The findings warn that defenders would need to "exercise extreme caution" so they do not violate a law of another nation where an attacker's computer is located.[109] Also, to avoid escalating a cyber incident, only "qualified defenders" should use an active cyber defense technique where the end goal is to uncover the identity of the attacker.[110] To accomplish this goal, a defender must have "a high degree of confidence in attribution" before using any active methods.[111]

The core idea of the ACDC Act is to establish attribution of a hacker.[112] The Act modifies the CFAA to create an "exception" for a defender using attributional technology, such as a program, code, or command "that beacons or returns locational or attributional data in response to a cyber intrusion in order to identify the source of an intrusion."[113] The Act further explains that attributional data is "digital information such as log files, text strings, time stamps, malware samples, identifiers such as user names and Internet Protocol addresses, and metadata or other digital artifacts gathered through forensic analysis."[114]

[102] *Id.* § 4(3)(B)(i)(II).
[103] *Id.* § 4(3)(C).
[104] *Id.* § 4(3)(B)(i)(II)(aa)-(cc).
[105] *Id.* § 4(1).
[106] *Id.* § 4(3)(A).
[107] *Id.* § 4(2).
[108] *Id.* § 2(11).
[109] *Id.* § 2(9).
[110] *Id.* § 2(10).
[111] *Id.*
[112] *ACDC Explainer 2019*, *supra* note 99, at 1.
[113] Active Cyber Defense Certainty Act, H.R. 3270, 116th Cong. § 3(1) (2019).
[114] *Id.* § 3(2).

Attribution is important to track down cybercriminals so they can be prosecuted.[115] The Act allows defenders to perform a "deep reconnaissance" with the goal to attribute blame to the source behind a hacking attack.[116] As a result, a cyber defender could "follow the bread crumbs" back to the origin of the attack, and then the defender would be able to turn over the information to law enforcement so the hacker could be prosecuted.[117]

According to the congressional findings, the use of active cyber defense methods "when properly applied" would improve defenses and prevent cybercrime.[118] The findings acknowledged that private entities need a way to restrain the growing threat of cyber-enabled crimes that thrive on the dark web,[119] which is a hidden section of the Internet that is not indexed by search engines.[120] To provide guidance, the DOJ would need to establish the "proper protocol" for defenders to access the dark web and retrieve stolen private property, such as intellectual property and financial records.[121] The findings by Congress also recognized that although federal agencies need to prioritize cyber incidents that affect national security, the agencies have the potential to assist the private sector by responding to reports of cybercrime activity in a timely manner; otherwise, organizations are left with "significant uncertainty" about cyber threats and cannot adequately protect themselves.[122]

The ACDC Act has been referred to as the "hack back" law.[123] Rep. Graves objects to the term "hack back" as describing the purpose of the bill.[124] In reality, the bill actually authorizes a defender to respond to a cyberattack using an "active defense."[125] In comparison, the strategy of an active defense is not about going into someone else's territory.[126] Historically, militaries used an "active defense" strategy to take action based upon monitoring the environment and

[115] *Cyber Attribution*, TECHTARGET, https://searchsecurity.techtarget.com/definition/cyber-attribution (last visited Dec. 21, 2019).

[116] *ACDC Explainer 2019*, *supra* note 99, at 1.

[117] *Id.* at 1-2.

[118] Active Cyber Defense Certainty Act, H.R. 3270, 116th Cong. § 2(6) (2019).

[119] Darren Guccione, *What Is the Dark Web? How to Access It and What You'll Find*, CSO (July 4, 2019), https://www.csoonline.com/article/3249765/what-is-the-dark-web-how-to-access-it-and-what-youll-find.html. The dark web provides encrypted communications and "requires the use of an anonymizing browser called Tor" to be accessed. *Id.* *See* Marcus, *infra* note 211 (discussing how Tor works and why it is useful).

[120] Active Cyber Defense Certainty Act, H.R. 3270, 116th Cong. § 2(7) (2019).

[121] *Id.*

[122] *Id.* § 2(8).

[123] Shannon Vavra, *Congress to Take Another Stab at 'Hack Back' Legislation*, CYBERSCOOP (June 13, 2019), https://www.cyberscoop.com/hack-back-bill-tom-graves-offensive-cybersecurity/.

[124] Patrick Howell O'Neill, *Rep. Graves: 'Active Defense' Bill Will Launch a New Industry*, CYBERSCOOP (Nov. 27, 2017), https://www.cyberscoop.com/tom-graves-active-defense-hack-back-bill-new-industry/.

[125] *Id.* *See also* Robert M. Lee, *DFIR Summit 2016: Leveraging Cyber Threat Intelligence in an Active Cyber Defense*, at 04:10-04:41 (SANS Digital Forensics and Incident Response, July 22, 2016), https://www.youtube.com/watch?v=ea50SyPBDBo&feature=youtu.be (defining the term "active defense" as it relates to cybersecurity).

[126] *Id.*

adapting over time.[127] However, the Act expands the scope of an active defense by allowing defenders to go beyond their networks to monitor intruders, deploy beacons, disrupt cyberattacks, and retrieve or destroy stolen files.[128]

The ACDC Act forbids an action that intentionally harms another's information or recklessly causes a "physical injury or financial loss."[129] A defender cannot create "a threat to the public health or safety" or exceed "the level of activity required to perform reconnaissance on an intermediary computer" when tracking down the intruder.[130] This includes intentional "intrusive or remote access into an intermediary's computer" or actions that cause a person or entity to experience a persistent disruption with their Internet connectivity that results in damages.[131] Additionally, the defender cannot take an action that impacts national security or disrupts government entities.[132]

In the ACDC Act, the ability of a defender to utilize "self-help" for retrieving stolen property without causing harm is based on a historical concept.[133] The idea that individuals could "regain possession of their rightful and legal property without resorting to a formal judicial process" appeared in the Roman Empire and progressed into English law.[134] In the United States, the concept evolved into the common law, and Congress formalized a standard under the Uniform Conditional Sales Act where the concept was codified in the Uniform Commercial Code ("UCC").[135] Section 9-609 of the UCC established a formal process to recover secured property as long as the repossession does not "breach the peace," and most states have adopted this section into their statutes.[136]

Under the ACDC Act, a defender must notify the FBI National Cyber Investigative Joint Task Force and receive an acknowledgment from the FBI before engaging in an active cyber defense measure.[137] The notification must explain the type of cyber breach that the victim experienced and how the defender plans to preserve evidence of the cyber intrusion.[138] To provide FBI oversight, the defender must disclose the intended target of the active cyber defense measure and explain the steps to avoid damage to intermediary computers that are not owned by the attacker.[139]

If passed, the ACDC Act would launch a pilot program that would allow the FBI to coordinate with other federal agencies to establish a "voluntary preemptive

[127] *Id.*

[128] *ACDC Explainer 2019*, *supra* note 99, at 1.

[129] Active Cyber Defense Certainty Act, H.R. 3270, 116th Cong.§ 4(3)(B)(ii)(I)-(II) (2019).

[130] *Id.* § 4(3)(B)(ii)(III)-(IV).

[131] *Id.* § 4(3)(B)(ii)(V)-(VI).

[132] *Id.* § 4(3)(B)(ii)(VII).

[133] Ryan McRobert, Comment, *Defining "Breach of the Peace" in Self-Help Repossessions*, 87 WASH. L. REV. 569, 569 (2012).

[134] *Id.*

[135] *Id.* at 569-70.

[136] *Id.*

[137] Active Cyber Defense Certainty Act, H.R. 3270, 116th Cong.§ 5(1) (2019).

[138] *Id.* § 5(2).

[139] *Id.*

review of active defense measures" for a two-year period.[140] A defender could submit a proposed measure to the program and receive an assessment of how well it conforms to federal law.[141] This would allow the defender to amend the measure and improve its technical operation.[142] Based on available resources, the FBI could prioritize the guidance it offers to defenders.[143] Each year, the Act would require that the DHS and the DOJ, along with other relevant federal agencies, deliver a report to Congress that details the effects of the law and how it has deterred cybercrime.[144]

The annual report would include eight key activities that affect cybercriminal deterrence. First, the report would track "the number of computer fraud cases reported by United States citizens and United States businesses to FBI Field Offices, the Secret Service Electronic Crimes Task Force, the Internet Crimes Complaint Center ("IC3") website, and other Federal law enforcement agencies."[145] Second, the report would show the number of computer fraud crime investigations from public reporting and specific crimes from independent inquiries.[146] Third, the report would present the number of cybercrime cases prosecuted under the CFAA.[147] Fourth, the report would show crimes that originated from United States suspects and foreign suspects.[148] Fifth, the report would track the number of "dark web cybercriminal marketplaces and cybercriminal networks" that law enforcement disabled.[149] Sixth, the report would give an estimate of the financial damages in the United States caused by cyberattacks and ransomware.[150] Seventh, the report would show how many law enforcement personnel investigated and prosecuted cybercrimes.[151] Eighth, the report would disclose how many active cyber defense notifications were filed and provide "a comprehensive evaluation of the notification process and voluntary preemptive review pilot program."[152]

D. HONEYPOTS

The ACDC Act allows an organization to monitor the actions of an attacker "to assist in developing future intrusion prevention or cyber defense

[140] *Id.* § 6(a).
[141] *Id.* § 6(b).
[142] *Id.*
[143] *Id.* § 6(c).
[144] *Id.* § 7.
[145] *Id.* § 7(1).
[146] *Id.* § 7(2).
[147] *Id.* § 7(3).
[148] *Id.* § 7(4).
[149] *Id.* § 7(5).
[150] *Id.* § 7(6).
[151] *Id.* § 7(7).
[152] *Id.* § 7(8).

techniques."[153] Monitoring could include deploying a honeypot,[154] which is a type of defense where a decoy system is placed on a network that is set up to lure hackers so their attempts to gain unauthorized access can be observed.[155] A honeypot can be a passive server that appears vulnerable to attacks, or it can have an active function that interacts with the network or other computers.[156]

The ACDC Act has the potential to make organizations more at ease with using a honeypot, but there could be other legal issues outside the CFAA. A honeypot should be closely monitored; if a hacker uses it to launch attacks or commit crimes, the organization could be held liable. Importantly, organizations using a honeypot could potentially expose themselves to civil and criminal penalties because state and federal statutes have provisions that may restrict the right to monitor intruders.[157]

The Electronic Communications Privacy Act ("ECPA") of 1986 includes the Stored Communications Act ("SCA"),[158] and it also updated the Federal Wiretap Act of 1968 ("Wiretap Act").[159] The ECPA protects wire, oral, and electronic communications in real time, in transit, and in storage.[160] The ECPA applies to email, stored data, and telephone conversations.[161] Over the years, the ECPA has been updated to make clarifications and to keep pace with new technologies.[162]

A honeypot may have a privacy concern because it monitors and records all the activity that is happening on the device, so the gray areas of the ECPA could apply to its operation.[163] In addition to criminal penalties, the ECPA has a private right of action, which allows a person or corporation to seek relief for communications that are intercepted or unlawfully accessed.[164] Government

[153] *Id.* § 4(1)(3)(B)(i)(II)(cc); *ACDC Explainer 2019*, *supra* note 99, at 1.

[154] Caleb Townsend, *What Is a Honeypot?*, U.S. CYBERSECURITY MAGAZINE, https://www.uscybersecurity.net/honeypot/, (last visited Jan. 13, 2020). "The metaphor of a bear being attracted to a pot of honey is deeply rooted in early folklore." *Id.*

[155] *Honeypot (Computing)*, TECHTARGET, https://searchsecurity.techtarget.com/definition/honey-pot (last visited Dec. 22, 2019).

[156] *Honeypot*, MGMT. MANIA, https://managementmania.com/en/honeypot (last visited Jan. 12, 2020).

[157] Richard P. Salgado, *How to Avoid Federal Wiretap Act Issues with a Honeypot Network Security System*, TECHTARGET (July 2003), https://searchsecurity.techtarget.com/feature/How-to-avoid-federal-Wiretap-Act-issues-with-a-honeypot-network-security-system.

[158] 18 U.S.C. §§ 2701-10 (1986). The SCA is part of the "Stored Wire and Electronic Communications and Transactional Records Access." *Id.*

[159] 18 U.S.C. § 2511 (1968) (amended 1986); *Privacy & Civil Liberties*, U.S. DEP'T OF JUSTICE OFFICE OF JUSTICE PROGRAMS, https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285 (last updated Apr. 23, 2019).

[160] *Id.*

[161] *Id.*

[162] *Id.*

[163] Jerome Radcliffe, *CyberLaw 101: A Primer on US Laws Related to Honeypot Deployments*, SANS INST., 6 (Feb. 1, 2007), https://www.sans.org/reading-room/whitepapers/legal/cyberlaw-101-primer-laws-related-honeypot-deployments-1746.

[164] Ian Walden & Anne Flanagan, *Honeypots: A Sticky Legal Landscape*, 29 RUTGERS COMPUT. & TECH. L.J. 317, 340 (2003).

agencies must also follow the Fourth Amendment, which requires a warrant for searches unless there is no "reasonable expectation of privacy."[165]

An organization should analyze the types of data it collects in a honeypot. The ECPA defines the "contents" of a "wire, oral, or electronic communication" to mean "any information concerning the substance, purport, or meaning of that communication."[166] Courts have held that "non-content" would cover addressing information and user records such as billing data.[167] Under these definitions, courts have determined that IP addresses and the "To" and "From" fields in e-mail messages are non-content information, but the "Subject" field is considered to be content.[168]

The Wiretap Act prohibits anyone from intercepting the content of an electronic communication unless an exception applies, and a few of these exceptions could apply to the operation of a honeypot.[169] The service provider exception would apply when a network operator engages in any activity for "the protection of the rights or property," but it is difficult to predict how a court would apply this exception to honeypots.[170] The party to a communication exception allows "a person acting under color of law" to intercept an electronic communication "where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception."[171] The trespasser exception allows a computer owner or operator to authorize the interception of a computer trespasser's communications.[172] A Patriot Act amendment provided some insight into the meaning of "computer trespasser" as including "any person who accesses a protected computer" without authorization.[173] In the past, law enforcement has relied on the party to a communication exception to monitor the activity of hackers, and courts have recognized "owners" as being "parties."[174]

The Pen Register and Trap and Trace Device statute prohibits a real-time interception of the non-content parts of an electronic communication, but it contains a service provider exception that is similar to the ECPA and Wiretap Act.[175] However, once the non-content data are placed into storage, the data becomes subject to the SCA, which applies to providers of "electronic communications service to the public" and prevents them from disclosing a

[165] Salgado, *supra* note 157.

[166] 18 U.S.C. § 2510(8) (1968) (amended 1986).

[167] Burstein, *supra* note 48, at 2.

[168] *Id.*

[169] Salgado, *supra* note 157.

[170] 18 U.S.C. § 2511(2)(a)(i) (1968) (amended 1986); Salgado, *supra* note 157.

[171] 18 U.S.C. § 2511(2)(c) (1968) (amended 1986).

[172] *Id.* § 2511(2)(i)(I).

[173] U.S. Department of Justice, Computer Crime and Intellectual Property Section, *Field Guidance on New Authorities that Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001*, § 217, 10-11 (last visited Dec. 29, 2019); Salgado, *supra* note 157. *See also Prosecuting Computer Crimes*, *supra* note 72 (explaining the term "protected computer").

[174] Walden, *supra* note 164, at 345.

[175] 18 U.S.C. § 3121(a)-(b) (1986); Burstein, *supra* note 48, at 2-3.

communication.[176] While the SCA imposes few restrictions on using the data within the collecting organization, the data is subject to restrictive disclosure rules.[177]

Security experts promote the use of honeypots to serve as an "early-warning system" that is deployed with an IDS/IPS system.[178] Research gathered from honeypot networks, or honeynets, determined that the best way to lower the risk of violating a communications privacy statute is to incorporate them into production systems and networks.[179]

IV. FIGHTING CYBERCRIME

A. THE PROS AND CONS OF THE ACDC ACT

The ACDC Act attempts to solve the growing problem of cybercrime by updating the CFAA. Currently, organizations use a variety of methods to defend their computer networks. Inside a network, an organization must be aware of privacy laws that govern the monitoring of electronic communications. Once a defense strategy goes outside the network, a defender risks breaking the CFAA. While pen testing targets the vulnerabilities inside a network, the Act would authorize defensive actions that go outside an organization's network.

Supporters of the ACDC Act believe that the proposed law could solve the hacking problem by equipping organizations with a method of self-defense.[180] As a benefit, allowing organizations to take active cyber defense measures would "balance the scales" by limiting the opportunities for hackers to discover a zero-day exploit.[181]

The ACDC supporters offer some valuable points that are worthy of consideration as hacking skills are become commonplace among security professionals. Over the years, hacking competitions have become a popular way for security enthusiasts to learn real-word hacking techniques within a fun environment.[182] Corporations host their own hacking events that include competitions such as Capture the Flag ("CTF") contests, which have existed for

[176] Burstein, *supra* note 48, at 3.

[177] *Id.*

[178] Catherine Paquet, *Network Security Using Cisco IOS IPS,* CISCOPRESS (June 8, 2009), http://www.ciscopress.com/articles/article.asp?p=1336425.

[179] Burstein, *supra* note 48, at 2. *See also Honeynet*, TECHTARGET, https://searchsecurity.techtarget.com/definition/honeynet (last visited Dec. 24, 2019) (defining "honeynet").

[180] *ACDC Explainer 2019*, *supra* note 99, at 2; Hardik Gandhi, *Active Cyber Defense Certainty: A Digital Self-Defense in the Modern Age*, 43 OKLA. CITY U. L. REV. 279, 308 (2019).

[181] Gandhi, *supra* note 180, at 308. A zero-day exploit is an unknown vulnerability that exposes a software or hardware flaw before anyone realizes the problem and leaves no opportunity for early detection. *What Is a Zero-Day Exploit?* FIREEYE, https://www.fireeye.com/current-threats/what-is-a-zero-day-exploit.html (last visited Jan. 14, 2020).

[182] David Strom, *10 Questions to Answer Before Running a Capture the Flag (CTF) Contest*, CSO (Mar. 6, 2018), https://www.csoonline.com/article/3257659/10-questions-to-answer-before-running-a-capture-the-flag-ctf-contest.html.

decades.[183] For example, the DEFCON show began in 1996 and has attracted thousands of participants.[184] Now, there are competitions held all over the world that includes a diversity of white hat hackers from corporate employees to high school students.[185]

CTF is an information security competition where contestants solve a variety of challenges that include scavenger hunts, programming exercises, and server hacking.[186] With a goal to capture a flag, CTFs test a participant's skill with different types of challenges, which include cryptography ("decrypting or encrypting a piece of data"), steganography ("finding information hidden in files or images"), binary ("reverse engineering or exploiting a binary file"), web ("exploiting web pages to find the flag"), and Pwn[187] ("exploiting a server to find the flag").[188]

Besides hackings contests, new scanning tools have emerged that assist hackers with finding targets. Shodan, which is known as the "world's most scary search engine" is a "pretty amazing" searching tool like Google, but it finds things such as banner information[189] and protocols such as FTP,[190] HTTP,[191] RDP,[192] SSH,[193] and SNMP[194] services.[195] A basic Shodan search can find "results by country, network, operating system(s), and port(s)."[196] Shodan's "deep web" search capabilities can seek out "Internet of Things, as it is able to locate refrigerators, alarms, security cameras, webcams, wearables, and any other

[183] *Id.*

[184] *Id.*

[185] *Id.*

[186] Atan, *What Is CTF and How to Get Started!*, DEV (Mar. 28, 2019), https://dev.to/atan/what-is-ctf-and-how-to-get-started-3f04.

[187] "Pwn" or "own" is defined as "[a]n act of dominating an opponent." *Pwn*, URBAN DICTIONARY, https://www.urbandictionary.com/define.php?term=pwn (last visited Jan. 11, 2019). This term "dates back to the days of WarCraft" when a game designer misspelled "own" as "pwn" on a map. *Id.* The term became a popular way to mean that a player has been "pwned" or "owned." *Id.*

[188] Atan, *supra* note 186.

[189] Banner grabbing is "a passive information gathering tool." *Banner Grabbing (Search)*, HACKER TARGET, https://hackertarget.com/banner-grabbing/ (last visited Jan. 11, 2020). A banner shows a simple text message of versions of services running on a network by querying a port. *Id.*

[190] FTP stands for "File Transfer Protocol" that transfers files over the Internet. *FTP*, TECHTERMS (Jan. 30, 2015), https://techterms.com/definition/ftp.

[191] HTTP stands for "Hypertext Transfer Protocol" that transfers data over the Internet and "defines commands and services used for transmitting webpage data." *HTTP*, TECHTERMS (May 28, 2015), https://techterms.com/definition/http.

[192] RDP stands for "Remote Desktop Protocol" that "makes it possible to view another computer's desktop on your computer." *Remote Desktop*, TECHTERMS (Sept. 18, 2008), https://techterms.com/definition/remotedesktop.

[193] SSH stands for "Secure Shell" that securely communicates with another computer using encryption. *SSH*, TECHTERMS (Oct. 25, 2006), https://techterms.com/definition/ssh.

[194] SNMP stands for "Simple Network Management Protocol" that is used for "exchanging management information between network devices." *SNMP*, TECHTERMS (Oct. 11, 2007), https://techterms.com/definition/snmp.

[195] Henry Dalziel, *Shodan Explained*, CONCISE AC (Dec. 16, 2019), https://www.concise-courses.com/shodan-explained/; OnlineCmag Team, *Shodan, The More Dangerous Alternative to Google*, ONLINECMAG (Aug. 5, 2019), http://www.onlinecmag.com/shodan/.

[196] Dalziel, *supra* note 195.

connected device."[197] Shodan continues to get "better and better at what it is designed to do" and has become a "must-know" for those that work in the cybersecurity field.[198]

Although the increase of hacking knowledge among information security professionals may serve as an argument for passing the ACDC Act, there are many critics of the Act within the profession. Critics of the Act believe its passage could be "dangerous" and would "only make matters much worse" along with creating unintended consequences.[199] The critics express concern that computers targeted for launching an attack could be innocent organizations that are unaware they were compromised.[200] Also, most companies do not possess the abilities or resources to take on sophisticated attackers.[201]

As a major concern, an organization could find itself confronting hackers from another nation, and if things go wrong, the situation could escalate into a threat to national security.[202] Nation-state hacking groups are growing more powerful as they develop the tools and techniques that allow them to "loot hundreds of millions in cash" and steal intellectual property.[203] In 2019, Microsoft warned that nation-state hackers pursued or breached the accounts of 10,000 people.[204] Microsoft revealed that most attacks, around 84%, targeted businesses, and the remaining attacks, around 16%, targeted personal email accounts.[205] Meanwhile, Optiv Security released its 2019 Cyber Threat Intelligence Estimate report revealing that top industries are being targeted including retail, healthcare, and financial institutions.[206] The report revealed that nation-state hackers and cybercriminals are becoming more successful by learning from each other's techniques such as attempting to spoof each other to confuse investigators.[207] CheckPoint Software Technologies also warned that government agencies were "especially vulnerable" to the criminal methods of nation-state

[197] OnlineCmag Team, *supra* note 195.

[198] Dalziel, *supra* note 195.

[199] Carolyn Crandall, *Hacking Back: Simply a Bad Idea*, DARKREADING (Sept. 24, 2018), https://www.darkreading.com/threat-intelligence/hacking-back-simply-a-bad-idea/a/d-id/1332856; Martin Giles, *Five Reasons "Hacking Back" Is a Recipe for Cybersecurity Chaos*, MIT TECH. REVIEW (June 21, 2019), https://www.technologyreview.com/s/613844/cybersecurity-hackers-hacking-back-us-congress/.

[200] Giles, *supra* note 199.

[201] *Id.*

[202] *Id.*

[203] Tom Foremski, *Report: Nation State Hackers and Cyber Criminals Are Spoofing Each Other*, ZDNET (Oct. 4, 2019), https://www.zdnet.com/article/optiv-report-nation-state-hackers-and-cyber-criminals-are-spoofing-each-other/.

[204] Tom Warren, *Microsoft Has Warned 10,000 People That Nation-State Hackers Are Targeting Them*, THE VERGE (July 18, 2019), https://www.theverge.com/2019/7/18/20698982/microsoft-nation-state-hackers-warning-2019.

[205] *Id.*

[206] *Optiv Security Releases Cyber Threat Intelligence Estimate Report to Increase Understanding of Cyber Threat Landscape, Offer Best Practices*, OPTIV (Oct. 1, 2019), https://www.optiv.com/press-releases/optiv-security-releases-cyber-threat-intelligence-estimate-report-increase; Foremski, *supra* note 203.

[207] Foremski, *supra* note 203.

attackers.[208] The attackers use techniques such as spear phishing[209] to distribute fake documents containing useful information in government formats, but when users view the documents, their computers become infected with malware.[210]

Tracking down a hacker can be complicated and may present hurdles that are beyond the capabilities of an organization. While the ACDC Act would allow a defender to "follow the breadcrumbs," the reality is that hackers often compromise a series of computers to make the breadcrumb trail longer between the target and their own computer. For example, a hacker could compromise systems in different countries that do not cooperate very well with each other to effectively cover the hacker's tracks because prosecution is more difficult. Also, a hacker could use the Tor browser to create a "daisy chain" effect.[211] As a result, accessing the logs of compromised computers in the chain may be impossible.

The technology industry voiced concerns over a proposed hacking law that resembled parts of the proposed ACDC Act. In 2018, Georgia's Governor, Nathan Deal, vetoed S.B. 315 "that would have criminalized unauthorized access of computer systems and allowed companies to 'hack back' in defense against breaches."[212] The veto happened as a result of opposition to the bill by information security firms and major technology companies.[213]

The origin of S.B. 315 came from a controversy that followed after a security researcher, Logan Lamb, discovered "major security issues in Georgia's election systems."[214] Lamb reported a flaw in Kennesaw State University's Center for Election Systems that left the unencrypted data of millions of Georgia voters exposed on the Internet.[215] A year later, another researcher, Chris Grayson, found that the hole remained open, and the data was still accessible.[216] After the hole was closed, FBI agents visited Lamb and "determined he had done nothing wrong"; however, the information security community feared that the language of the proposed bill would have made Grayson and Lamb's actions a crime.[217]

[208] *Rancor: The Year of the Phish*, CHECK POINT RESEARCH (Sept. 22, 2019), https://research.checkpoint.com/2019/rancor-the-year-of-the-phish/ [hereinafter *Rancor: The Year of the Phish*]; Foremski, *supra* note 203.

[209] Spear phishing is when criminals send malware in "emails to specific and well-researched targets while purporting to be a trusted sender." Dan Swinhoe, *What Is Spear Phishing? Why Targeted Email Attacks Are So Difficult to Stop*, CSO (Jan. 21, 2019), https://www.csoonline.com/article/3334617/what-is-spear-phishing-why-targeted-email-attacks-are-so-difficult-to-stop.html.

[210] *Rancor: The Year of the Phish*, *supra* note 208; Foremski, *supra* note 203.

[211] Adam Marcus, *Privacy Solutions Part 8: The Best Anonymizer Available: Tor, the TorButton & TorBrowser*, THE TECH. LIBERATION FRONT (Nov. 10, 2009), https://techliberation.com/2009/11/10/privacy-solutions-part-8-the-best-anonymizer-available-tor-the-torbutton-torbrowser/. Tor is "a sophisticated anonymizer [that] can obscure the identity of any one web user by pooling requests from large numbers of users across a 'daisy chain' of proxy servers-thus effectively anonymizing the user's identity." *Id.*

[212] Sean Gallagher, *Georgia Governor Vetoes Cyber Bill That Would Criminalize "Unauthorized Access,"* ARS TECHNICA (May 9, 2018), https://arstechnica.com/tech-policy/2018/05/georgia-governor-vetoes-cyber-bill-that-would-criminalize-unauthorized-access/.

[213] *Id.*

[214] *Id.*

[215] *Id.*

[216] *Id.*

[217] *Id.*

Tripwire, "an industry-leading provider of threat detection and remediation," was concerned about the language in S.B. 315, so the Chief Technology Officer, David Meltzer, sent a letter to Governor Deal to oppose the bill. [218] In the letter, Meltzer expressed concern about the "vague definitions" in the bill such as if "legitimate business activity" included services such as vulnerability testing.[219] Meltzer also explained in the letter that the bill would "not promote good security practices."[220] Further, Meltzer stated that if the bill became law, the company would reexamine whether it should continue conducting security research in Georgia.[221]

The S.B. 315 controversy revealed that major technology companies were not ready to endorse the "active defense" concept in the ACDC Act. Google and Microsoft expressed concern over the bill's provision that exempted "cybersecurity active defense measures that are designed to prevent or detect unauthorized computer access."[222] In a joint letter to Governor Deal, Google and Microsoft executives criticized the provision because it would broadly authorize "hacking back" that was "highly controversial within cybersecurity circles" and would create an "undefined guise of cybersecurity"[223] The executives pointed out that the provisions "could easily lead to abuse and be deployed for anticompetitive, not protective purposes."[224] The executives also added that passing the bill into law would make Georgia into a "laboratory for offensive cybersecurity practices" that other jurisdictions have not authorized.[225]

B. POSSIBLE SOLUTIONS

As cyber adversaries become more advanced, information sharing methods must operate at "wire speed" to detect and prevent cyber threats.[226] In the past, collaboration among security professionals was usually focused on manual interactions that lacked contextual information, but to provide faster intelligence, organizations must be able to exchange information using automated tools.[227] The use of open-community-driven standards such as "the Trusted Automated Exchange of Indicator Information (TAXII), Cyber Observable Expression

[218] Andrea Flanagan, *Why We Believe Georgia's S.B. 315 Bill Will Increase Cybersecurity Risk*, TRIPWIRE, INC. (Apr. 26, 2018), https://www.tripwire.com/state-of-security/government/why-we-believe-georgias-s-b-315-bill-will-increase-cybersecurity-risk/.

[219] *Id.*

[220] *Id.*

[221] *Id.*

[222] Gallagher, *supra* note 212.

[223] *Id.*

[224] *Id.*

[225] *Id.* (click on "Google and Microsoft executives" hyperlink).

[226] Koen Van Impe, *How STIX, TAXII and CybOX Can Help with Standardizing Threat Information*, SEC. INTELLIGENCE (Mar. 26, 2015), https://securityintelligence.com/how-stix-taxii-and-cybox-can-help-with-standardizing-threat-information/.

[227] *Id.*

(CybOX) and Structured Threat Information Expression (STIX)" will have an important place in the future of information sharing.[228]

As a solution for helping organizations understand how to stay ahead of cyber threats, the ACDC Act could create a government-private sector partnership that works along with the information sharing provisions of CISA. An organization would be required to become a member to receive the benefit of the Act's protections. The partnership could also create educational programs that offer certifications to use active cyber defenses after a qualified individual meets educational requirements, completes extensive training, and passes a rigorous background check.[229]

V. CONCLUSION

If passed, the ACDC Act may create a new age of cyber retribution with defenders who are eager to pursue a hacker.[230] Allowing organizations to deploy an active cyber defense may seem like a fair way to stop hackers, but this "eye-for-an-eye form of justice" could have terrible consequences.[231] For example, when a defender launches a counterattack to pursue a hacker, the route may lead into an innocent system within the hacker's chain of IPs that mask the real origin of the attack.[232] As a result, the hacker could make a hospital computer appear to be the source of the attack.[233] When chasing the hacker, the defender could possibly cause a disruption to the hospital, which could be devastating if the computer supported critical services.[234]

While the proposed ACDC Act offers a much-needed awareness of the problem with cyber threats, the bill leaves many gaps. To make this law into an effective solution, it needs the endorsement of industry executives, government officials, and security professionals. Otherwise, the law could leave a cloud of confusion that creates more questions than answers to the growing problem of cybercrime.

[228] *Id.*

[229] Gandhi, *supra* note 180, at 308.

[230] A defender that has an "eager desire" to fight is "spoiling for a fight." *Spoil (Verb), Intransitive Verb*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/spoil (last visited Feb. 5, 2020). Ironically, the Australian rock band AC/DC has a song titled "Spoilin' for a Fight" from the 2008 *Black Ice* Album. Chris Jones, *AC/DC Black Ice Review*, BBC, https://www.bbc.co.uk/music/reviews/86f9/ (last visited Feb. 5, 2020).

[231] Greg Nojeim & David Snead, *Letting Cyberattack Victims Hack Back Is a Very Unwise Idea*, WIRED (July 22, 2017), https://www.wired.com/story/letting-cyberattack-victims-hack-back-is-a-very-unwise-idea/. The Code of Hammurabi, section 196 states, "If a man put out the eye of another man, his eye shall be put out. [An eye for an eye]." L. W. King (trans.), *The Code of Hammurabi*, YALE LAW SCH. LILLIAN GOLDMAN LAW LIBRARY – THE AVALON PROJECT, https://avalon.law.yale.edu/ancient/hamframe.asp (last visited Feb. 1, 2020).

[232] Nojeim & Snead, *supra* note 231. *See About IP Addresses*, *supra* note 84 (explaining how an IP address works).

[233] Nojeim & Snead, *supra* note 231.

[234] *Id.*