DELEGATING HACKING BACK: PMC-STYLE, FACILITY-CLEARED CYBER CONTRACTORS UNDER CFAA § 1030(F)

Sophia Stener*

Ransomware attacks on American organizations threaten the U.S.'s national security and economic stability. Under the Computer Fraud and Abuse Act (CFAA), private organizations are prohibited from taking self-help measures, such as "hacking back," to defend against attacks. Instead, American organizations must rely on law enforcement, which is under-resourced and over-burdened, to respond to an attack. Twice, Congress has declined to amend the CFAA to allow organizations to hack back under the Active Cyber Defense Certainty Act (ACDC Act), citing concerns over attribution, foreign policy implications, and immunity. This Note proposes a new framework for enabling organizations to hack back that would not require amending the CFAA.

This Note proposes that the federal government create a regulated industry of private "hack back contractors" that may conduct active cyber defense operations on behalf of victim organizations while remaining under the oversight of federal entities like the Federal Bureau of Investigation (FBI) or Department of Homeland Security (DHS). This Note argues that: (i) the law enforcement exception of the CFAA provides private organizations the legal authorization to hack back when delegated to do so by U.S. law enforcement and points to two recent federal district court cases that support this reading of the statute; and (ii) this proposal is congruent with the U.S.'s existing policy on private military contractors (PMCs) and granting of facility security clearances (FCLs).

* J.D. Candidate 2026, Columbia Law School; B.A. 2022, Columbia University. Thank you to Professor Matthew Waxman, Professor Talia Gillis, and Major Michelle Lukomski, J.A., U.S. Army, in providing such thoughtful feedback and comments. Finally, thank you to the Columbia Business Law Review Board and Staff for their work in preparing this Note for publication.

INTRODUCTION

Ransomware has emerged as a critical threat to American national security and economic stability. Despite this growing threat, private organizations currently face severe legal constraints when responding to attacks. Under the Computer Fraud and Abuse

Act (CFAA),[1] private organizations are prohibited from taking offensive remedial action or "hacking back" against actors who steal or encrypt their data and systems.[2] As a result, companies are left with limited recourse beyond paying ransoms, reporting incidents to overburdened federal agencies, or shuttering their operations.[3]

The existing legal framework, as it is widely understood, inadequately protects American businesses and critical infrastructure from the rapidly evolving threat of ransomware. In 2017 and then again in 2019, the Active Cyber Defense Certainty Act (ACDC Act) was introduced in Congress to curtail this threat.[4] The ACDC Act would have amended the CFAA to permit private-sector hacking back.[5] The Act did not advance beyond committee in either session despite attracting significant discussion.[6] Even if

[1] *See* 18 U.S.C. § 1030 for the most updated codification.

[2] While there has never been a federal case prosecuting hacking back, there are several persuasive authorities which suggest that the same provisions of the CFAA that prohibit hacking also prohibit hacking back. *See, e.g.*, 18 U.S.C. § 1030(a)(5); *see also* PETER G. BERRIS, CONG. RSCH. SERV., CYBERCRIME AND THE LAW: COMPUTER FRAUD AND ABUSE ACT (CFAA) AND THE 116TH CONGRESS, R46536 at 1, 30 (Sep. 21, 2020) (cautioning that "[r]egardless of the victim's motive" it is possible that "accessing, modifying, or damaging a computer it does not own or operate" will "violate federal law and possibly also the laws of many states and foreign countries, if the accessed computer is located abroad . . ."") (citing U.S. DEP'T OF JUSTICE, BEST PRACTICES FOR VICTIM RESPONSE AND REPORTING OF CYBER INCIDENTS 23 (2018), https://www.justice.gov/criminal/criminal-ccips/file/1096971/dl?inline=#page=23 [https://perma.cc/4UNV-2VC8].

[3] Abeerah Hashim, *6 Times Hackers Forced Companies To Go Bankrupt & Shut Down*, PRIVACYSAVVY (Aug. 23, 2024), https://privacysavvy.com/security/business/6-times-hackers-forced-companies-to-go-bankrupt-shut-down/ [https://perma.cc/8ZJM-HKS5]; Catalin Cimpanu, *Company Shuts Down Because of Ransomware, Leaves 300 Without Jobs Just Before Holidays*, ZDNET (Jan. 3, 2020), https://www.zdnet.com/article/company-shuts-down-because-of-ransomware-leaves-300-without-jobs-just-before-holidays/ [https://perma.cc/GR7N-5Z8C].

[4] Active Cyber Defense Certainty Act, H.R. 4036, 115th Cong. (2017); Active Cyber Defense Certainty Act, H.R. 3270, 116th Cong. (2019).

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

[6] *See* discussion *infra* Part II.C; *see also* Study on Cyber-Attack Response Options Act, S. 2292, 117th Cong. (2021) (directing the Department of Homeland Security to study and report on the potential benefits and risks of

either attempt had worked, the solution proposed by the ACDC Act would have been inadequate, as the ACDC Act, as proposed, failed to address legitimate concerns regarding foreign policy implications, technical capabilities, and oversight mechanisms.[7]

This Note argues that the CFAA's law enforcement exception provides private organizations with limited authorization to hack back when delegated to do so by U.S. law enforcement. Drawing from historical precedents in American military contracting and recent case law interpretations of the CFAA's exception for law enforcement,[8] this Note proposes a novel solution: the creation of a regulated industry of private "hack-back contractors" operating under government supervision through facility security clearances (FCLs).[9] The proposed framework would enable vetted cybersecurity firms to obtain appropriate clearances and conduct active cyber defense operations on behalf of victim organizations while remaining under the oversight of federal agencies like the Federal Bureau of Investigation (FBI) or Department of Homeland Security (DHS).[10] This approach addresses the key limitations of previous proposals by ensuring that hack-back operations are conducted by technically qualified entities with appropriate consideration for diplomatic and legal implications. By establishing this new industry of cyber contractors, the United States could leverage private sector expertise and resources to counter ransomware threats while maintaining necessary government supervision.

This Note proceeds as follows. Part I discusses the nature and scale of ransomware attacks, the relevant threat actors, and the threat these attacks pose to the U.S.'s national security and economic stability. Part II outlines the current legal landscape for combating ransomware attacks and explains why previous attempts to authorize limited hacking-back under the ACDC Act have failed. Part III proposes a new framework for hack-back contractors, drawing support from recent case law interpreting the CFAA's exception for law enforcement under 18 U.S.C. § 1030(f) and

amending the CFAA to allow private organizations to take proportional actions in response to an unlawful network breach).

[7] *See* discussion *infra* Part II.C.2.

[8] 18 U.S.C. § 1030(f).

[9] *See infra* Part III.A.

[10] *See infra* Part III.B.

historical precedents of modern private military contractors. Part III also offers practical considerations in the implementation of this framework and highlights areas for further legal scholarship. Part IV concludes with recommendations for policymakers.

I. THE RANSOMWARE CRISIS

In February 2024, Change Healthcare—one of the U.S.'s primary payment cycle management services—was hit with the largest ransomware attack on a healthcare company to date.[11] Billing systems at medical practices stopped working and insurance claims ceased processing.[12] Suddenly, offices rushed to check patients in with pen and paper.[13] BlackCat (ALPHV), a known Russian cybercrime gang, sought $22 million in ransom from Change Healthcare's parent company, UnitedHealth Group, in exchange for the nightmare ending.[14] The company complied, but the cost of the attack has totaled far greater than just this payment alone. To date, UnitedHealth Group has spent over $5.7 billion in connection with the February 2024 attack.[15]

---

[11] Zack Whittaker, *How the Ransomware Attack at Change Healthcare Went Down: A Timeline*, TECHCRUNCH (Jan. 27, 2025), https://techcrunch.com/2025/01/27/how-the-ransomware-attack-at-change-healthcare-went-down-a-timeline/ [https://perma.cc/3HZ7-YQ7J].

[12] *Id.*

[13] *See*, *e.g.*, *The Change Healthcare cybersecurity breach: Impact on healthcare providers*, NIXON PEABODY LLP (Nov. 12, 2025), https://www.nixonpeabody.com/insights/alerts/2025/11/12/change-healthcare-cybersecurity-breach-impact-on-healthcare-providers [https://perma.cc/E6SJ-36N3] (describing the "costly manual solutions" deployed in response to the attack).

[14] *See* Whittaker, *supra* note 11.

[15] Steve Alder, *Change Healthcare Increases Ransomware Victim Count to 192.7 Million Individuals*, HIPPA J. (Aug. 6, 2025), https://www.hipaajournal.com/change-healthcare-responding-to-cyberattack/ [https://perma.cc/2KCQ-PCZR] (To alleviate the cost of the attack to providers, UnitedHealth Group established a temporary financial assistance program of no-interest loans, which has paid out over $5.7 billion so far.); *UnitedHealth Group Reports 2024 Results,* UNITEDHEALTH GRP. 3 (Jan. 16, 2025), 2025-16-01-uhg-reports-fourth-quarter-results.pdf [https://perma.cc/6SJ6-VMBT]; *UnitedHealth Group Re-Establishes Full Year Outlook and Reports Second Quarter 2025 Results*, UNITEDHEALTH GRP. 12 (July 29, 2025), unh-reestablishes-full-year-outlook-and-reports-second-quarter-2025-results.pdf [https://perma.cc/52VP-UC6W].

Similar stories litter our newsfeeds: a $25 million ransom in an attack targeting the car dealership technology provider, CDK Global;[16] a $30 million attack on casino conglomerate MGM Resorts International;[17] a ransomware attack on one of Starbuck's software vendors that left the coffee giant calculating its baristas wages by hand;[18] and numerous attacks on municipal and state governments, including in New York,[19] Minnesota,[20] and Nevada.[21] In October of 2025, Oracle and Google confirmed that top executives at various companies had been targeted with ransom demands after hackers claimed to have stolen sensitive data via Oracle's business applications.[22] The demands are part of a growing

[16] AJ Vicens, *Wallets Tied to CDK Ransom Group Received $25 Million Two Days After Attack*, CYBERSCOOP (July 12, 2024), https://cyberscoop.com/cdk-ransom-blacksuit-25-million/ [https://perma.cc/Y6WS-GKT9].

[17] Robert McMillan & Katherine Sayre, *The Audacious MGM Hack That Brought Chaos to Las Vegas*, WALL ST. J. (Mar. 29, 2024), https://www.wsj.com/tech/cybersecurity/mgm-hack-casino-hackers-group-0366c641 [https://perma.cc/J7C8-H9VT].

[18] Sean Lyngaas, *Starbucks Forced to Pay Its Baristas Manually Because of a Ransomware Attack on Third-Party Software*, CNN BUS. (Nov. 25, 2024), https://www.cnn.com/2024/11/25/tech/starbucks-ransomware-attack [https://perma.cc/S88Y-HVDX].

[19] Nick Reisman et al., *New York Was Struggling Toward a Budget Deal. Then Hackers Made It Worse.*, POLITICO (Apr. 17, 2024), https://www.politico.com/news/2024/04/17/cyberattack-new-york-budget-00152885 (on file with Columbia Business Law Review); Anthony Izaguirre, *Cyberattack Hits New York State Government Office*, NBC N.Y. (Apr. 17, 2024), https://www.nbcnewyork.com/news/local/cyberattack-hits-new-york-state-government-office/5329681/ [https://perma.cc/HMG6-ZNNQ].

[20] Samantha Fischer, *MN National Guard Deployed; St. Paul Declares State of Emergency in Response to Cyberattack*, KARE 11 (July 29, 2025), https://www.kare11.com/article/news/local/mn-national-guard-deployed-st-paul-declares-state-of-emergency-in-response-to-cyberattack/89-e8ce8c3f-7ad6-43f6-8e22-af62c6392e2d [https://perma.cc/R6T7-CBG5].

[21] Alyssa Bethencourt, *Nevada Ransomware Attack Marks First-of-its-Kind Statewide Shutdown*, ABC 13 KTNV (Aug. 30, 2025), https://www.ktnv.com/news/nevada-ransomware-attack-marks-first-of-its-kind-statewide-shutdown [https://perma.cc/4EG5-S4SK].

[22] Raphael Satter & A.J. Vicens, *Google Says Hackers Are Sending Extortion Emails to Corporate Executives*, REUTERS (Oct. 2, 2025), https://www.reuters.com/business/google-says-hackers-are-sending-extortion-emails-executives-2025-10-02/ [https://perma.cc/5K9G-VXTL]; Raphael Satter, *Oracle Says Hackers Are Trying to Extort Its Customers*, REUTERS (Oct. 3, 2025), https://www.reuters.com/business/oracle-says-hackers-are-trying-extort-its-customers-2025-10-03/ [https://perma.cc/98G8-TQUV].

trend towards double or triple extortion.[23] Cumulatively, these ransomware attacks are emblematic of a rapidly growing crisis that has led some experts to consider ransomware to be "the [number one] challenge of threat event attacks that industrial, public, and private organizations are facing" today.[24]

A. *The Scale and Nature of Ransomware Attacks*

Every year, the number of ransomware attacks carried out on U.S. organizations increases,[25] and the total cost of these attacks is only expected to grow.[26] One estimate of the average cost of a ransomware attack is around $4.88 million, with recovery costs averaging a few million dollars as well,[27] and the cost of these attacks is increasing every year.[28] A ransomware attack occurs when a malicious actor identifies a vulnerability in an organization's

[23] *See* discussion *infra* Part I.B.2.

[24] DIETMAR P.F. MÖLLER, GUIDE TO CYBERSECURITY IN DIGITAL TRANSFORMATION 275 (2023), https://doi.org/10.1007/978-3-031-26845-8_6#DOI [https://perma.cc/5MFH-RZPP].

[25] Carly Page, *Record-Breaking Ransoms and Breaches: A Timeline of Ransomware in 2024*, TECHCRUNCH (Dec. 27, 2024), https://techcrunch.com/2024/12/27/record-breaking-ransoms-and-breaches-a-timeline-of-ransomware-in-2024/ [https://perma.cc/3UVC-JECQ]. The article notes that 2024 was another "record-breaking year" and that "data theft and extortion attacks continue to increase dramatically, both in terms of frequency and sophistication." *Id.*

[26] *See, e.g.*, *The Cost of Cyber Theft to the U.S. Economy in 2024*, CIPHERTEX DATA SEC. (May 24, 2024), https://ciphertex.com/2024/05/24/the-cost-of-cyber-theft-to-the-u-s-economy-in-2024/ [https://perma.cc/M3WT-7RX9]; Nivedita James Palatty, *The Staggering Cost of Cyberattacks: How Much Money Do Businesses Actually Lose*, ASTRA (June 14, 2023), https://www.getastra.com/blog/security-audit/cost-of-cyberattacks/ [https://perma.cc/QNP3-JLJE]; Steve Morgan, *Cybercrime To Cost The World $10.5 Trillion Annually By 2025*, CYBERSECURITY VENTURES (Nov. 13, 2020), https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/ [https://perma.cc/69ZL-EWEF].

[27] Chantelle Golombick, *The True Cost of Cyber Attacks in 2026 and Beyond*, EXPRESSVPN BLOG (Sep. 7, 2025), https://www.expressvpn.com/blog/the-true-cost-of-cyber-attacks-in-2024-and-beyond/ [https://perma.cc/3XYX-4VX3].

[28] In 2023, the average ransomware payment demanded more than doubled, while the median ransom payment quintupled. *See The 2024 Malware and Ransomware Defense Report,* SPYCLOUD 12 (2024), https://spycloud.com/resource/2024-malware-ransomware-defense-report/ [https://perma.cc/WK3C-EJ4W].

information technology (IT) infrastructure,[29] utilizes that vulnerability to encrypt an organization's data, and demands payment (a ransom), often in the form of cryptocurrency, from that organization in return for a key to decrypt the data.[30] Put simply, by deploying ransomware, a malicious actor can effectively lock an organization out of its systems and demand payment in exchange for handing back the keys.[31]

There are an ever-increasing number of cyberattack strategies but a limited set of preemptive security measures to protect against attacks.[32] To thwart attacks, organizations can

[29] *See* JOHN P. CARLIN & GARRETT M. GRAFF, DAWN OF THE CODE WAR: AMERICA'S BATTLE AGAINST RUSSIA, CHINA, AND THE RISING GLOBAL CYBER THREAT 50 (PublicAffairs, 2018) ("Most hacks—even the most damaging ones—have come through relatively unsophisticated means exploiting obvious vulnerabilities: software patches that haven't been installed, weak or default passwords protecting sensitive data, or 'phishing' techniques where a user clicked a nefarious link . . . .").

[30] 6 U.S.C. § 650(22)(A)–(B); *see also America Under Cyber Siege: Preventing and Responding to Ransomware Attacks: Hearing Before the S. Comm. on the Judiciary*, 117th Cong. 2 (2021) (statement of Bryan A. Vorndran, Assistant Dir., FBI Cyber Div.) ("These ransom payments are typically requested in the form of virtual currency, like Bitcoin.").

[31] Using asymmetric encryption, hackers create unique mathematically linked "key pairs," making it practically impossible for an organization to decrypt its data without the hacker's decryption key. While quantum computing may eventually address this challenge, such technology is still years away from being accessible. *See, e.g.*, Tom Olzak, *Will Symmetric and Asymmetric Encryption Withstand the Might of Quantum Computing?*, SPICEWORKS (June 14, 2021), https://www.spiceworks.com/it-security/data-security/articles/will-symmetric-and-asymmetric-encryption-withstand-the-might-of-quantum-computing/ [https://perma.cc/K5DD-MSDC].

[32] *See* Kurt Baker, *12 Most Common Types of Cyberattacks*, CROWDSTRIKE (May 13, 2024), https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/common-cyberattacks/ [https://perma.cc/29QG-3C9V]. Examples of some cyberattack types are malware, including ransomware, trojans, spyware, worms, and rootkits; Distributed Denial-of-Service (DDoS) attacks; phishing; spoofing; identity-based attacks; code injection attacks; DNS tunneling; and IoT-based attacks. Artificial intelligence (AI) is also making the threat landscape more difficult to predict and making it easier for malicious actors to launch attacks. In 2025, a prominent American artificial intelligence service, Anthropic, revealed that Chinese hackers had used its technology to automate cyberattacks. *See Disrupting the First Reported AI-Orchestrated Cyber Espionage Campaign*, ANTHROPIC (Nov. 13, 2025), https://www.anthropic.com/news/disrupting-AI-espionage [https://perma.cc/L6KM-MUZF].

pursue a handful of preemptive security measures.[33] Still, it is impossible to be prepared for every type of potential attack, and once an attack has occurred, organizations have few options for recourse. Organizations can report attacks to the Federal Bureau of Investigation (FBI), but many choose not to do so, given that (i) response times can average over 280 days[34] and (ii) doing so would expose them to reputational, privacy, and other legal risks like class action litigation.[35] The Computer Fraud and Abuse Act (CFAA) further constrains organizations by prohibiting self-help measures, such as "hacking back," against the cybercriminals who steal or encrypt their data and systems.[36] Consequently, in the wake of a ransomware attack, organizations typically have two options: (i) pay the ransom to receive the decryption key and regain access to their systems; or (ii) refuse to pay and instead rely on backups to return to normal operations. Most organizations are unable to rely on backups alone, as the malicious code may be present on the backup, and backups have themselves become a target of ransomware.[37] Therefore, many resort to paying ransoms in the hopes of being able to decrypt their encrypted systems. However, not every

[33] *See* Lana Kontseva, *Ransomware: Still a Threat in 2025?*, UNDERDEFENSE (June 26, 2024), https://underdefense.com/blog/ransomware-still-a-threat-in-2024/ [https://perma.cc/SB4D-7ABR] ("[B]y taking proactive measures and remaining vigilant, organizations and individuals can significantly reduce their risk of falling victim to this ever-evolving threat."). Organizations also can and should develop a Disaster Recovery Plan (DRP) to mitigate the time their systems are down and thus the revenue they would lose in the wake of an attack. *See* Möller, *supra* note 24, at 292.

[34] *See* IBM CORP., *2024 Cost of Data Breach Report* 27 (July 2024) (stating that the average response time can be significantly reduced if a victim organization has an established relationship with law enforcement prior to an attack).

[35] *See* Brad S. Karp, *Federal Guidance on the Cybersecurity Information Sharing Act of 2015*, HARV. L. 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/ [https://perma.cc/FME5-QS5H]; *see also* Daniel Lange, *CISA 2015 – Present*, 32 ALB. L.J. SCI. & TECH. 72, 78 (2022).

[36] *See* BERRIS, *supra* note 2; 18 U.S.C. § 1030(a)(5) (2020).

[37] ProLion Team, *Why Backups Won't Save You From Ransomware*, PROLION (July 2025), https://prolion.com/blog/backups-and-ransomware/ [https://perma.cc/BS3B-Y2A3] (noting that backups are increasingly active targets of ransomware).

malicious actor will send the requisite decryption key despite receiving payment.[38] In other cases, such as that of Colonial Pipeline in 2021, hackers have provided organizations with a decryption key, but the speed at which the key can decrypt is so slow that the organization must rely on their out-of-date backups anyway.[39]

With organizations largely at the mercy of hackers, it is important to understand who these malicious hackers are and just how destructive they can be. Ransomware attacks threaten more than just a company's profit margins and reputation. Given the interdependency between the government and the private sector today, the collateral impact of these attacks extends to the country's economy and national security at large.

B. *The Threat Landscape: Who's Behind the Attacks*

John Carlin, the former Assistant Attorney General for National Security under the Obama Administration, has posited that the U.S. is currently engaged in a sort of Code War.[40] Unlike the Cold War, where "we confronted a single, locatable adversary with a defined ideology, today we confront online a world beset by anonymity and vulnerabilities."[41] On a daily basis, both private and public organizations are subject to attacks from "nation-states, terrorists, criminals, hacktivists, or [even] single individuals seeking fun, profit, or destruction."[42] Malicious hackers range from criminal

[38] In 2016, Kansas Heart Hospital paid hackers a ransom for the decryption key. However, the hackers refused to provide the decryption key without a subsequent payment. *See* Linn Foster Freedman, *Kansas Heart Hospital Pays Ransom but Attackers Renege on Their Word*, DATA PRIVACY + CYBERSECURITY INSIDER (June 1, 2016), https://www.dataprivacyandsecurityinsider.com/2016/06/kansas-heart-hospital-pays-ransom-but-attackers-renege-on-their-word/ [https://perma.cc/SP8E-47VC].

[39] William Turton et al., *Colonial Pipeline Paid Hackers Nearly $5 Million in Ransom*, BLOOMBERG (May 13, 2021), https://www.bloomberg.com/news/articles/2021-05-13/colonial-pipeline-paid-hackers-nearly-5-million-in-ransom (on file with Columbia Business Law Review).

[40] *See generally* CARLIN & GRAFF, *supra* note 29.

[41] *Id.* at 44.

[42] *Id.*

masterminds[43] and state-sponsored terrorists[44] to rebellious teenagers.[45] Indeed, it has never been easier to become a hacker capable of deploying ransomware.

1. *Three Categories of Attackers*

Malicious hackers conducting cyberattacks can be classified into three categories: (i) nation-state adversaries; (ii) state-sponsored groups; and (iii) rogue actors.

The U.S. government has voiced its concern about several nation-state adversaries that threaten national security[46] by conducting advanced persistent threat (APT) activities.[47] In particular, the Cybersecurity & Infrastructure Security

[43] *E.g.*, Sean Lyngaas, *U.S. Offers $10 Million Reward for Info on Russian Hacker Accused of Cyberattack on Major U.S. Police Department*, CNN (May 16, 2023), https://www.cnn.com/2023/05/16/politics/us-reward-russian-hacker/index.html [https://perma.cc/XNE6-WN53]; Press Release, U.S. Dep't of Just., Romanian National Sentenced to 20 Years in Prison in Connection with NetWalker Ransomware Attacks Resulting in the Payment of Millions of Dollars in Ransoms (Dec. 19, 2024), https://www.justice.gov/usao-mdfl/pr/romanian-national-sentenced-20-years-prison-connection-netwalker-ransomware-attacks [https://perma.cc/4CRJ-EWHD].

[44] *See*, *e.g.*, *Nation-State Cyber Actors*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors [https://perma.cc/S8RC-VVBP] (cautioning that advanced persistent threat (APT) activity is on the rise); *The New Frontline of Geopolitics: Understanding the Rise of State-Sponsored Cyber Attacks*, SENTINELONE BLOG (Aug. 16, 2023), https://www.sentinelone.com/blog/the-new-frontline-of-geopolitics-understanding-the-rise-of-state-sponsored-cyber-attacks/ [https://perma.cc/GEC2-DWCU] (noting that nation-state-sponsored cyberattacks are on the rise and that China, Russia, North Korea, and Iran are leading the charge); Edvardas Mikalauskas, *The World's Most Dangerous State-Sponsored Hacker Groups*, CYBERNEWS (Dec. 10, 2021), https://cybernews.com/editorial/the-worlds-most-dangerous-state-sponsored-hacker-groups/ [https://perma.cc/9XTD-G5YE].

[45] *See* Sean Lyngaas, *Homeland Security Report Details How Teen Hackers Exploited Security Weaknesses in Some of the World's Biggest Companies*, CNN (Aug. 10, 2023), https://www.cnn.com/2023/08/10/politics/-dhs-hacking-report/index.html [https://perma.cc/66AR-HT2R]; *see also* Robert McMillan & Jenny Strasburg, *This Teenage Hacker Became a Legend Attacking Companies. Then His Rivals Attacked Him.*, WALL ST. J. (Oct. 3, 2024), https://www.wsj.com/tech/cybersecurity/arion-kurtaj-hacker-468e6cad [https://perma.cc/66YY-YMUF].

[46] CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, *supra* note 44.

[47] *Id.*

Administration (CISA) has warned that China, Russia, North Korea, and Iran all pose serious cybersecurity threats, as they focus on "espionage, data theft, and network/system disruption or destruction."[48] Nation-state adversaries directly employ military or government agents to conduct these APT activities. For example, the U.S. government and its partners have attributed APT activities to Russia's Foreign Intelligence Service (SVR) and military intelligence agency (GRU)[49] and the Chinese military.[50]

However, there is another method that nation-state adversaries use to attack U.S. organizations: funding state-sponsored groups. State-sponsored hacking groups are not directly part of the military or intelligence apparatus of a nation-state adversary. Instead, state-sponsored groups are financially backed by a national government.[51] Attacks are typically linked to the political or economic goals of the sponsoring state, such as stealing

[48] *Id.*

[49] *Russia Cyber Threat Overview and Advisories*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/russia [https://perma.cc/35GB-7DUB] (last visited May 12, 2026); *SVR Cyber Actors Adapt Tactics for Initial Cloud Access*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (Feb. 26, 2024), https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-057a [https://perma.cc/EUP6-NVH9]; *Five Russian GRU Officers and One Civilian Charged for Conspiring to Hack Ukrainian Government*, U.S. DEP'T OF JUST. (Sep. 5, 2024), https://www.justice.gov/opa/pr/five-russian-gru-officers-and-one-civilian-charged-conspiring-hack-ukrainian-government [https://perma.cc/7DKN-8K2H].

[50] *U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage*, U.S. DEP'T OF JUST. (May 19, 2014), https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor [https://perma.cc/FBF3-SGAA] (The Justice Department indicted five China's People Liberation Army (PLA) Unit 61398 officers for hacking or attempting to hack into U.S. nuclear power, metals, and solar products entities.); Jim Finkle et al., *U.S. accuses China of cyber spying on American companies*, REUTERS (Nov. 20, 2014), https://www.reuters.com/article/us-cybercrime-usa-china-idUSKCN0J42M520141120/ [https://perma.cc/YR8L-67UL]. A critical constraint of DOJ cases like the one against the five PLA Unit 61398, also known as APT1, is that the U.S. government cannot extradite or compel these individuals to stand trial in the United States. *See id.*

[51] Jacque de la Riviere, *Rogue Nations: An Assessment of State-Sponsored Cyberattacks*, CYBER DEF. MAG. (June 24, 2024), https://www.cyberdefensemagazine.com/rogue-nations-an-assessment-of-state-sponsored-cyberattacks/ [https://perma.cc/568W-JT8X].

intellectual property or influencing public opinion. In more insidious cases, state-sponsored groups can spy on or disrupt critical infrastructure. For example, in 2024, the FBI confirmed that Salt Typhoon, a Chinese government-backed hacking group, successfully hacked into at least eight telecommunications firms in the United States, including AT&T and Verizon.[52] But, as Congressmen Eric Swalwell (D–Calif.) points out, adversaries such as "China, Russia, and Iran . . . are only the tip of the iceberg[,]" as we also "have rogue cyber actors who are capable of targeting and disrupting" American organizations.[53]

In the last decade, rogue actors motivated by profit, ideology, chaos, and even bragging rights have emerged as key ransomware attackers. Even people with very few coding skills can be effective at debilitating organizations with ransomware. Highly-skilled ransomware operators now offer ransomware as a service (RaaS) on the dark web.[54] RaaS is a cybercrime business model

---

[52] Aamer Madhani, *White House says at least 8 telecom firms, dozens of nations impacted by China hacking campaign*, AP NEWS (Dec. 4, 2024), https://apnews.com/article/china-hack-us-telecoms-salt-typhoon-88cabc592dae2fa870772c5ce4ace5ea [https://perma.cc/RTX9-932J; The Pub. Safety and Homeland Sec. Bureau, *Fact Sheet: Implications of Salt Typhoon Attack and FCC Response*, FED. COMMC'NS COMM'N (Dec. 5, 2024), https://docs.fcc.gov/public/attachments/DOC-408015A1.pdf. (on file with Columbia Business Law Review). It is not yet clear whether Salt Typhoon is explicitly operating as a part of the People's Republic of China (PRC) or whether the group is affiliated with China's Ministry of State Security, also known as APT40. Still, it is widely believed to be at a minimum state-sponsored. *See, e.g.*, Sarah Krouse, Robert McMillan & Dustin Volz, *China-Linked Hackers Breach U.S. Internet Providers in New 'Salt Typhoon' Cyberattack*, WALL ST. J. (Sep. 26, 2024), https://www.wsj.com/politics/national-security/china-cyberattack-internet-providers-260bd835 [https://perma.cc/46RK-HC75].

[53] *Securing Operational Technology: A Deep Dive Into The Water* Sector Hearing Before the Subcomm. on Cybersecurity and Infrastructure Prot. of the H. Comm. On Homeland Sec., 118th Cong. 3 (Feb. 6, 2024) (statement of Rep. Eric Swalwell (D–CA)).

[54] Kurt Baker, *Ransomware as a Service (RaaS) Explained How It Works and & Examples*, CROWDSTRIKE (Jan. 30, 2023), https://www.crowdstrike.com/en-us/cybersecurity-101/ransomware/ransomware-as-a-service-raas/ [https://perma.cc/VQT2-533R]. Moreover, Malware as a Service (MaaS) is another business model used for selling malware, including ransomware. For purposes of brevity, only RaaS is referred to here although the two models work in much the same way. Operators typically offer RaaS in one or more of the following four models: (i) a monthly subscription; (ii) a one-time fee; (iii) an

whereby operators sell malicious code to other hackers, known as "affiliates," who then use the code to conduct ransomware attacks on victim organizations.[55] "[M]any of the most infamous and devastating ransomware strains . . . spread through RaaS sales."[56] In addition to providing ransomware, RaaS operators may offer ongoing technical support, access to forums where affiliates exchange tips, support in implementing payment processing tools, and "[t]ools and support for writing custom ransom notes or negotiating ransom demands."[57] Some of these groups have grown particularly powerful, as adversary nation-states, like Russia, turn a blind-eye to cybercriminals as the state shares a mutual interest in seeing the crippling of American companies and economic value.

RaaS poses a significant concern for private industry and law enforcement officials alike. With a few clicks and a little seed money, nearly anyone can effectuate a lucrative ransomware attack. Moreover, with the release of artificial intelligence (AI) tools, such as Anthropic's Claude Code, even individuals with no coding experience can attempt to "vibe code" malicious software.[58] The ubiquity of RaaS makes it much harder to predict both adverse actors and victim targets, further complicating the efforts of organizations and the United States to guard against potential cyberattacks.

affiliate program; and (iv) profit-sharing. Operators often offer other amenity services at additional cost similar to those offered by lawful Software as a Service (SaaS) vendors.

[55] Jim Holdsworth and Matthew Kosinski, *What is ransomware as a service (RaaS)?*, IBM (Sep. 5, 2024), https://www.ibm.com/think/topics/ransomware-as-a-service [https://perma.cc/K7GZ-NQLB].

[56] *Id.*

[57] *Id.*

[58] *See* ANTHROPIC, *supra* note 32. Vibe coding is the practice of using AI "to generate functional code from natural language prompts, accelerating development, and making app building more accessible, especially for those with limited programming experience." *What Is Vibe Coding?*, GOOGLE CLOUD (Dec. 4, 2025), https://cloud.google.com/discover/what-is-vibe-coding [https://perma.cc/PA2D-XJ6C]. It is too early to tell how vibe coding will impact the RaaS business model, although presumably it will introduce more competition in the market.

2. *The Dual Threat to National Security and Economic Stability*

Ransomware has the potential to cripple or even render inoperable critical American industries and infrastructure. Moreover, ransomware attacks destabilize and undermine the U.S. economy, further weakening the country's ability to grapple with subsequent attacks.

For industries, such as water, energy, and other critical infrastructure, ransomware attacks can have catastrophic effects.[59] According to the National Security Agency (NSA), the FBI, and other Federal agencies, adversaries are "silently pre-positioning" themselves to conduct "disruptive or destructive cyberattacks against U.S. critical infrastructure in the event of a major crisis or conflict with the United States."[60] In effect, adversaries are planting "cyber sleeper cells" across the U.S. in both public and private organizations.[61] At any moment, adversaries could "trigger [these sleeper cells] to create confusion and disarray across America by disrupting our power supply, our transportation, our communication networks, and our water and our food supply."[62] This threat is exacerbated by the fact that by some estimates, roughly 65% of U.S. infrastructure is privately owned.[63] As such, companies are largely left to themselves to manage their cybersecurity.[64] In regulated industries, such as energy, companies argue that it is extremely challenging to bolster cybersecurity efforts

---

[59] CISA recognizes sixteen critical infrastructure sectors, including communications, energy, financial services, healthcare and public health, water and wastewater systems, and nuclear. *See Critical Infrastructure Sectors*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors [https://perma.cc/TL2L-QK4R].

[60] *Red Alert: Countering the Cyberthreat From China Hearing Before the Subcomm. on Cybersecurity, Info. Tech., & Gov't Innovation of the H. Comm. On Oversight & Accountability*, 118th Cong. 2 (2024) (statement of Nancy Mace, Chairwoman of Subcomm. on Cybersecurity, Info. Tech., & Gov't Innovation).

[61] *Id.*

[62] *Id.*

[63] *See* Chris Storey, *Crossroads: The Role of Private Companies in Safeguarding U.S. Critical Infrastructure*, CYBER DEF. MAG. (Dec. 18, 2024), https://www.cyberdefensemagazine.com/cybersecurity-at-the-crossroads-the-role-of-private-companies-in-safeguarding-u-s-critical-infrastructure/ [https://perma.cc/RZ9R-RQNP].

[64] *See id.*

when they are required to keep prices low.[65] They argue that as they are constrained from raising rates, they are unable to fund shoring up their defenses.[66] Other critical infrastructure industries, such as healthcare, face similar struggles to raise the necessary funds to harden their networks. Many hospital groups are wary of raising the price of already unprecedentedly high healthcare costs even further.[67] In the meantime, ransomware attacks continue to put millions of American lives at risk and increase the financial strain on companies, with many resorting to paying out ransoms.[68] The American Hospital Association has gone as far as to liken these attacks to 9/11, given the risk of loss of life they pose.[69]

Ransomware attacks undermine the American economy. These attacks are particularly devastating as organizations must not only deal with the cost of paying a ransom, but also with costs resulting from lost revenue, rebuilding, legal fees, and reputational damages. For instance, cloud-technology company Blackbaud stated it expected to incur $50 million in legal fees attributable to a ransomware attack, according to its filings with the Securities and

[65] *See Implementing the Department of Defense Cyber Strategy Hearing Before the H. Comm. Of Armed Services*, 114th Cong. 42–43 (2015) (statement of Admiral Michael Rogers, the Commander of U.S. Cyber Command).

[66] *See id.*

[67] *See*, *e.g.*, *USA Hospitals Face Rising Operational Costs Pressure*, HEALTHMANAGEMENT (May, 8, 2024), https://healthmanagement.org/c/hospital/News/usa-hospitals-face-rising-operational-costs-pressure [https://perma.cc/WQY2-VQ53].

[68] Sean Lyngaas, *'It's putting patients' lives in danger': Nurses say ransomware attack is stressing hospital operations*, CNN (May 29, 2024), https://www.cnn.com/2024/05/29/tech/ransomware-attacks-hospitals-patients-danger/index.html [https://perma.cc/SN4R-3E45]; Rachana Pradhan & Kate Wells, *Cyberattack Led to Harrowing Lapses at Ascension Hospitals, Clinicians Say*, NPR (June 19, 2024), https://www.npr.org/2024/06/19/nx-s1-5010219/ascension-hospital-ransomware-attack-care-lapses [https://perma.cc/J2UN-HYHD] (explaining that hospitals are "the No. 1 target of ransomware" attacks).

[69] John Riggi, *Ransomware Attacks on Hospitals Have Changed*, AM. HOSP. ASS'N, https://www.aha.org/center/cybersecurity-and-risk-advisory-services/ransomware-attacks-hospitals-have-changed [https://perma.cc/YZ3C-FBYD] (lasted visited Jan. 8, 2025) (noting that ransomware has accounted for more than 70% of the successful cyberattacks on healthcare organizations in 2018 and 2019).

Exchange Commission (SEC).[70] Meanwhile, the media and broadcasting giant Sinclair Broadcasting Group stated that it lost roughly $63 million in advertising revenues due to a ransomware attack.[71] At an industry level, the estimated total cost associated with ransomware attacks on the healthcare industry alone was $21 billion in 2020.[72] While these examples illustrate the high costs of reported ransomware attacks, it is worth noting that for every example listed, there are hundreds more that go unreported.[73]

To combat the high costs of ransomware attacks, companies are increasingly turning to cyber insurance. Cyber insurance or cyber liability insurance coverage (CLIC) is a type of insurance policy that helps to cover the costs associated with cyberattacks, which, depending on the policy, may include ransomware.[74] Over the last few years, ransomware payouts have exceeded seventy percent of premiums, leading insurers to raise premiums, impose stricter underwriting requirements, and, in some cases, apply coverage limitations (e.g., when an attack is promulgated by a nation-state or state-backed group).[75] However, since not all CLIC policies cover ransomware attacks, many companies either seek additional ransomware-specific policies or bear the risk of exposure to attack.[76] To compensate for this surge

[70] *See* Cynthia Brumfield, *SEC Filings Show Hidden Ransomware Costs and Losses*, CSO (Mar. 17, 2022), https://www.csoonline.com/article/572321/sec-filings-show-hidden-ransomware-costs-and-losses.html [https://perma.cc/SUT3-CCBV].

[71] *Id.*

[72] Stacy Weiner, *The Growing Threat of Ransomware Attacks on Hospitals*, ASS'N AM. MED. COLLS. (July 20, 2021), https://www.aamc.org/news/growing-threat-ransomware-attacks-hospitals [https://perma.cc/ZSU4-F7EX].

[73] Rebecca Harpur, *2025 Q3 Ransomware Report*, BLACKFOG (Oct. 20, 2025), https://www.blackfog.com/2025-q3-ransomware-report/ [https://perma.cc/W539-DRA6] (estimating that 85% of ransomware attacks go unreported).

[74] *See* Michael Hill et al., *Cyber Insurance Explained: Costs, Terms, How to Know It's Right For Your Business*, CSO (Oct. 10, 2024), https://www.csoonline.com/article/571703/cyber-insurance-explained.html [https://perma.cc/3B2V-F6LY].

[75] *Id.*

[76] *See*, *e.g.*, *What is Ransomware Insurance?*, COALITION, https://www.coalitioninc.com/topics/what-is-ransomware-insurance [https://perma.cc/PH2D-HPVD] (last visited May 12, 2026) (discussing ransomware insurance as "one of the most important elements" of modern cyber insurance).

in ransom payments and the cost of rebuilding organizations, companies are increasingly passing on the cost of ransomware attacks to consumers, and the share of companies planning to do so is increasing.[77]

The practice of shifting costs onto consumers is further exacerbated by the trend toward double and triple extortion. A ransomware attack necessarily produces one form of extortion: the ransom payment demanded to receive the decryption key. However, in a double extortion ransomware attack, hackers steal an organization's data and threaten to release it publicly.[78] Consequently, organizations are tasked with paying two ransom demands: one to receive the decryption key and another to prevent their stolen data from being publicly leaked or sold. In a triple extortion ransomware attack, the threat is even more pernicious.[79] Hackers will not only encrypt a victim's systems and threaten to leak stolen data, as in a double extortion attack, but also introduce a third layer of extortion. For instance, hackers might deploy a Distributed Denial-of-Service (DDoS) attack or even target third-parties, such as the customers or stakeholders of a victim.[80] In what is largely understood as the first triple extortion attack, individual patients of the Finnish mental health provider Vastaamo were sent

[77] *See* IBM CORP., *supra* note 34, at 20 ("The share of organizations that planned to do so increased to 63% this year from 57% last year, representing a 10.5% increase."). This trend is exacerbated by the use of infostealer infections, which have the potential to expose companies across sectors. *See* SPYCLOUD, *supra* note 28, at 9.

[78] Marilyn Wilkinson, *What is Double, Triple and Multi Extortion Ransomware?*, PROLION (July 2025), https://prolion.com/blog/double-extortion-ransomware/ (on file with Columbia Business Law Review).

[79] Triple extortion ransomware is an "advanced cyber attack strategy that builds upon the traditional ransomware model by adding layers of extortion to increase pressure on victims to pay the ransom." *See What is Triple Extortion Ransomware? [2024 Update]*, HEIMDAL SEC. (Mar. 21, 2024), https://heimdalsecurity.com/blog/triple-extortion-ransomware/ [https://perma.cc/G5YK-K3CD].

[80] *See id.* A DDoS attack "attempts to crash an online resource—such as a website or cloud service—by overloading it with traffic" and it can effectively slow or completely shut down access to systems. Gregg Lindemulder & Matthew Kosinski, *What is Cybersecurity?*, IBM CORP. (Aug. 12, 2024), https://www.ibm.com/think/topics/cybersecurity [https://perma.cc/XVD3-NBWC].

ransom demands related to their patient records.[81] Given the rise of double and triple extortion in ransomware attacks, the cost of these attacks is only expected to worsen.

Individual ransomware attacks cause acute harm to organizations while the cumulative effect undermines the American economy and threatens the U.S.'s national security. Yet despite the devastating impact of ransomware attacks, American organizations face severe legal constraints, leaving many to either pay out ransoms or suffer operational paralysis in the wake of an attack.

II. CURRENT LEGAL FRAMEWORKS AND THE FAILED PROMISE OF THE ACTIVE CYBER DEFENSE CERTAINTY ACT (ACDC ACT)

While the threat ransomware attacks pose to the economy and the nation's security grows, the legal framework for combating ransomware remains piece-meal. The primary statute used by prosecutors in ransomware cases is the Computer Fraud and Abuse Act (CFAA). However, this same statute bars organizations from employing self-help measures, like hacking back, when faced with an attack.[82] Recognizing gaps in the nation's response to ransomware, some members of Congress and numerous state and federal agencies have pursued various other reforms, such as mandating reporting requirements and supplying best practices for organizations' cybersecurity strategies. Still, these efforts focus largely on preventing and reporting attacks and do little in offering actionable remedies to organizations in the wake of ransomware attacks. Congress's most ambitious attempt to combat the ransomware problem—the Active Cyber Defense Certainty Act (ACDC Act)—failed in both 2017 and 2019, as concerns over technical feasibility and foreign policy implications were left largely unresolved. This Part examines the current legal and regulatory framework for addressing ransomware and analyzes why proposed

[81] *See* Natalie Paskoski, *What Are Double and Triple Extortion Ransomware Attacks*, RETAIL & HOSP. ISAC (Feb. 16, 2022), https://rhisac.org/special-interest-resilience/ransomware-double-and-triple-extortion/ [https://perma.cc/KS96-8DHJ]; *see also* Zoe Kleinman, *Therapy Patients Blackmailed For Cash After Clinic Data Breach*, BBC (Oct. 26, 2020), https://www.bbc.com/news/technology-54692120 [https://perma.cc/C63G-GKSS].

[82] *See* BERRIS, *supra* note 2.

and existing measures remain inadequate in combating the ransomware threat.

A. *The CFAA Framework and Its Limitations*

There are several laws that prosecutors could employ in ransomware cases.[83] However, the CFAA remains the primary enforcement tool in the Justice Department's arsenal. In conjunction with prosecuting hackers, law enforcement can take remedial measures. The CFAA provides an exception for law enforcement to engage in investigative or protective activities on a malicious hacker's computer systems, such as accessing and disabling infrastructure used to promulgate a ransomware attack.[84]

1. *Traditional Prosecution Under the CFAA*

Enacted in 1986, the Computer Fraud and Abuse Act serves as the cornerstone of internet and computer crime law.[85] The

[83] Prosecutors can indict hackers under the Electronic Communications Privacy Act (ECPA) and the Economic Espionage Act (EEA). *See generally* Electronic Communications Privacy Act, 18 U.S.C. §§ 2510, 2701 (2002, 2018). The ECPA prohibits the interception or access of electronic communications without authorization. Therefore, individuals who use ransomware to hijack communication channels necessarily violate the ECPA. 18 U.S.C. § 2701(a)(1)–(2). The EEA "authorizes criminal penalties for theft of trade secrets, including intangible 'financial, business, scientific, technical, economic, or engineering information' that the owner 'has taken reasonable measures to keep . . . secret' and that 'derives independent economic value' from 'not being generally known.'" PETER G. BERRIS & JONATHAN M. GAFFNEY, CONG. RSCH. SERV., R46932, RANSOMWARE AND FEDERAL LAW: CYBERCRIME AND CYBERSECURITY 4 (Oct. 5, 2021) (citing 18 U.S.C. §§ 1831, 1832, 1839(3)). That said, it does not appear that the DOJ has ever used the EEA to prosecute a ransomware attack. *Id.* No results were found in the Westlaw database for cases citing 18 U.S.C. §§ 1831, 1832 and using the word "ransomware."

[84] 18 U.S.C. § 1030(f) ("This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.").

[85] 18 U.S.C. § 1030(a)(5). The Supreme Court in *Van Buren v. United States*, 593 U.S. 374 (2021), clarified that the CFAA is not aimed at misuse of information obtained from computers but rather it "covers those who obtain information from particular areas in the computer—such as files, folders, or databases—to which their computer access does not extend." Welter v. Medical

CFAA "prohibits fraudulent and unauthorized access of computer systems."[86] The archetypal ransomware attack violates 18 U.S.C. § 1030(a)(7)(C), which prohibits transmitting extortive threats "in relation to damage to a protected computer, where such damage was caused to facilitate the extortion."[87] Hackers who engage in double or triple extortion may be implicated under § 1030(a)(7)(B), which criminalizes threats to (i) "obtain information from a protected computer without authorization" or (ii) "impair the confidentiality of information obtained from a protected computer without authorization."[88] Additionally, developers who create and sell ransomware, such as RaaS providers, may also violate 18 U.S.C. § 1030(a)(5).[89] A violation of either § 1030(a) subsection is a felony, each count punishable by fines or imprisonment up to five years for first offenses and ten years for subsequent offenses.[90]

Despite the DOJ's best efforts, it is extremely difficult to convict a cybercriminal in ransomware attacks. Given that ransomware attacks often originate outside of the United States,[91] defendants are hard to track down.[92] And while extradition treaties

Professional Mutual Insurance Co., No. 22-cv-11047-PBS, 2023 WL 2988627, at *7 (D. Mass. Feb. 23, 2023) (quoting *Van Buren*, 374 U.S. at 378). *See generally* Just. Manual § 9-48.000, U.S. DEP'T OF JUST. (2022), https://www.justice.gov/jm/jm-9-48000-computer-fraud [https://perma.cc/5C8Z-4AN6].

[86] Switzer v. Franklin Investment Corp., No. 22-CV-00201-SPB, 2023 WL 1072987, at *3 (W.D. Pa. Jan. 8, 2023).

[87] *Id.* The term "protected computer" includes computers that are connected to the internet. *See, e.g.*, *Van Buren*, 593 U.S. at 379 (noting that the prohibition to intentionally access a computer without authorization extends to "all computers that connect to the internet" under § 1030(a)(2)); *see also* hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985, 999 (9th Cir. 2019) ("The term 'protected computer' refers to any computer 'used in or affecting interstate or foreign commerce or communication,' . . . effectively any computer connected to the Internet . . . including servers, computers that manage network resources and provide data to other computers." (quoting 18 U.S.C. § 1030(e)(2)(B)) (internal citations omitted)).

[88] 18 U.S.C. § 1030(a)(7)(B).

[89] BERRIS & GAFFNEY, *supra* note 83, at 5.

[90] 18 U.S.C. § 1030(c). *See also* BERRIS & GAFFNEY, *supra* note 83, at 4. If combined with other criminal statutes, such as economic espionage (18 U.S.C. §§ 1831(a)(2), (a)(4), and 2) or trade secret theft (18 U.S.C. §§ 1832(a)(2), (a)(4), and 2), the term of imprisonment could be longer.

[91] *See America Under Cyber Siege Hearing*, supra note 30, at 5 (statement of Vorndran) ("We know our most significant threats come from foreign actors using global infrastructure to compromise U.S. networks.").

[92] *See* BERRIS & GAFFNEY, *supra* note 83, at 6.

may help to obtain some convictions, it does little to curb nation-states—like Russia, China, Iran, and North Korea—who actively conduct, fund, and openly tolerate ransomware attacks against American organizations.

2. *The § 1030(f) Law Enforcement Exception and "Hacking Back" Defined*

While the CFAA prohibits the unauthorized access of computer systems, § 1030(f) provides an exception for law enforcement. It stipulates that the CFAA "does not prohibit any lawfully authorized investigative, protective or intelligence activity *of a law enforcement agency*."[93] Section 1030(f) equally applies to any "law enforcement agency of the United States, a State or a political subdivision of a State, or of any intelligence agency."[94] Therefore, under § 1030(f), government agencies are authorized to take remedial measures in the wake of an attack.

One such remedial measure is known as "hacking back."[95] "Hacking back" broadly refers to "attacked parties . . . detect[ing], trac[ing], and then actively respond[ing] to a threat by, for example, interrupting an attack in progress to mitigate damage to the[ir] system."[96] In short, hacking back enables the victim of an attack to launch "a counterattack designed to proactively engage with, disable, or collect evidence about an attacker."[97] It is a "part of a larger concept of internet self help or remediation encompassing terms such as counterstrikes, active defense, hacking back, retaliatory hacking, or offensive countermeasures."[98] As many scholars have argued, hacking back serves much the same role as

[93] 18 U.S.C. § 1030(f) (emphasis added).

[94] *Id.*

[95] *See* Sara Sun Beale & Peter Berris, *Hacking the Internet of Things: Vulnerabilities, Dangers, and Legal Responses*, 16 DUKE L. & TECH. REV. 161, 189 (2018). Following the terminology set out by Beale and Berris, the term "hacking back" refers to invasive counterattacks, while the term "remedial action" refers to the broader category of self-help measures, which includes hacking back.

[96] *Id.* at 190 (quoting Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 HARV. J. L. & TECH. 429, 475 (2012)).

[97] John P. Carlin, *So You Want to Hack Back*, ASPEN DIGITAL (Oct. 9, 2025), https://www.aspendigital.org/blog/so-you-want-to-hack-back/ [https://perma.cc/XC2X-Z2DG].

[98] Beale & Berris, *supra* note 95, at 190.

self-defense law does in the traditional, physical world.[99] Hacking back is "necessary to establish attribution of an attack, . . . retrieve and destroy stolen files, [and] monitor the behavior of the attacker."[100] By hacking back, a victim can gain information that is necessary to determine "attribution" (i.e., which particular actor is behind the attack). Furthermore, a victim can disrupt certain continued unauthorized activity or monitor the behavior of the attacker to better bolster its cyber defense systems.[101]

But the CFAA, and more specifically § 1030(f), has limited this "hacking back" power to law enforcement. When U.S. organizations fall prey to a ransomware attack, they turn to law enforcement to ascertain which actor(s) lie behind the attack. The agency that predominantly assumes this role is the FBI. The FBI can help victims attribute an attack to a particular actor as well as aid victims in getting their systems back online. But while the federal government is clearly intent on combating ransomware, the efficacy of its efforts is limited. According to the testimony of former FBI Director Christopher Wray, "even if the FBI focused all of its cyber agents and intelligence analysts on the [Peoples Republic of China (PRC)] threat, PRC-backed cyber threat actors would still outnumber FBI Cyber personnel at least 50 to 1, and they are attempting multiple cyber operations each day in domestic internet space, where only the FBI has the authorities to monitor and disrupt."[102] Perhaps even more shocking is that this staggering statistic—that the FBI is outnumbered at least fifty to one—does not account for other nation-state, state-sponsored, or rogue actors.[103] The limitations of law enforcement have put pressure on the private sector, who face a hard legal boundary: it can engage law enforcement but cannot unilaterally deploy countermeasures. Recognizing these limitations, Congress, the White House, and

[99] *Id.*

[100] BERRIS, *supra* note 2, at 30.

[101] H.R. 3270 116th Cong. § 4(3)(B)(i)(II)(aa)–(cc) (2019).

[102] *Statement for the Record Before the H. Select Comm. on Strategic Competition Between the U.S. & the Chinese Communist Party,* 118th Cong. 4 (2024) (statement of Christopher Wray, Director, Fed. Bureau of Investigation).

[103] *Id.* ("But, of course, China's not the only challenge in cyberspace—not even close. We're investigating over 100 different ransomware variants, each with scores of victims, as well as a host of other novel threats posed by both cybercriminals and nation-state actors—in addition to China, countries like Russia, Iran, and North Korea.").

numerous federal agencies have introduced policies to further curb the threat of ransomware.

B. *Recent Reform Efforts: Prevention and Reporting, Not Response*

Recent reform efforts to combat ransomware have largely focused on reporting and prevention measures, rather than methods for actively responding to attacks. In 2015, Congress passed the Cybersecurity Information Sharing Act (CISA Act), which encourages private organizations to voluntarily share cybersecurity threat information with the federal government.[104] The CISA Act aims to curb cybersecurity threats, including ransomware, by enabling the U.S. to identify, share, and thwart threats with other industry actors.[105] Yet critics have argued that the CISA Act is limited in how effective it can be, given that reporting and disclosure is voluntary and some companies may not wish to share information as doing so could carry "legal, competitive, and reputational risks."[106] Recognizing the limitations of voluntary

[104] Keith M. Gerver, *President Obama Signs Cybersecurity Act of 2015 to Encourage Cybersecurity Sharing Information*, NAT'L L. REV. (Jan. 2, 2016), https://natlawreview.com/article/president-obama-signs-cybersecurity-act-2015-to-encourage-cybersecurity-information [https://perma.cc/L873-DTQ5]; *see* 6 U.S.C. §§ 1500–1510. There have been considerable challenges in reauthorizing the 2015 CISA Act, which lapsed on September 30, 2025. As part of the appropriations bill signed on November 12, 2025, Congress extended CISA 2015 through to January 30, 2026. It is unknown whether this reauthorization will be extended again. David Aaron & Ariel B. Glickman, *President Trump Approves Short-Term Renewal of CISA 2015*, PERKINS COIE (Nov. 14, 2025), https://perkinscoie.com/insights/blog/president-trump-approves-short-term-renewal-cisa-2015 [https://perma.cc/4GA5-FR2U].

[105] *See* 6 U.S.C. § 1504 (describing the sharing of cyber threat indicators and defensive measures with the federal government).

[106] Karp, *supra* note 35. Notably, liability protection offered by CISA is limited to private actors sharing information with the Department of Homeland Security (DHS) and thus does not extend to other federal agencies. *Id.* Some critics fear that CISA Act leads to an increased collection of citizen data by the U.S. government, which in turn carries Fourth Amendment privacy concerns. *See* Lange, *supra* note 35, at 78. Critics' privacy concerns are exacerbated by the fact that CISA requires DHS "to automatically and immediately share information in real-time with any federal agency, including the Central Intelligence Agency (CIA), Federal Bureau of Investigation (FBI), Department of Commerce, and the National Security Agency (NSA), and must refrain from doing anything to impede that real-time dissemination of information." *Id.* (internal quotation

reporting, Congress enacted the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) in 2022.[107] CIRCIA requires critical infrastructure operators to report substantial cybersecurity incidents, including ransomware attacks, to the Cybersecurity and Infrastructure Security Agency (CISA)—the federal agency[108] within DHS responsible for civilian cybersecurity and critical infrastructure security—within 72 hours[109] and ransomware payments within 24 hours.[110] CIRCIA also established the Joint Ransomware Task Force (JRTF), which "serves as the central body for coordinating an ongoing nationwide campaign against ransomware attacks in addition to identifying and pursuing opportunities for international cooperation."[111] More recently, the 2025 National Defense Authorization Act (NDAA) required that within 180 days of enactment, the Director of National Intelligence, in consultation with the Director of the FBI, submit a report to Congress on the national security threat that ransomware poses to

marks omitted). Finally, critics contest that while the Act has led to more data collection by the federal government, it has done little to curb attacks. *Id.* at 94–95.

[107] *See Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia [https://perma.cc/TD7H-2CH4] (last visited May 13, 2026).

[108] *See* Cybersecurity and Infrastructure Security Agency Act of 2018, 6 U.S.C. § 652(a)–(i) (2022) (redesignating the National Protection and Programs Directorate, on or after November 16, 2018, the Cybersecurity and Infrastructure Security Agency).

[109] The Cyber Incident Reporting for Critical Infrastructure Act, 6 U.S.C. § 681b(a)(1) (2022).

[110] *Id.* § 681b(a)(2) (2022).

[111] *Id.* (to be codified at 6 U.S.C. § 665j); *Joint Ransomware Task Force*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/joint-ransomware-task-force [https://perma.cc/USW5-T6TW] (last visited May 13, 2026). CIRCIA also created the Ransomware Vulnerability Warning Pilot, which seeks to proactively warn critical infrastructure organizations of vulnerabilities that could enable ransomware attacks. Consolidated Appropriations Act, 2022, Pub. L. No. 117-103, § 105, 136 Stat. 49 (2022) (to be codified at 6 U.S.C. § 652 note); *Ransomware Vulnerability Warning Pilot (RVWP)*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/stopransomware/Ransomware-Vulnerability-Warning-Pilot [https://perma.cc/Q83X-V5BX] (last visited May 13, 2026).

the United States.[112] The Act went as far as to raise ransomware attacks to the level of terrorism by proclaiming actors and nation-states who harbor them as "hostile foreign cyber actors."[113] Outside of these efforts, numerous other bills have been introduced, although not yet passed, further underscoring the significant threat that ransomware poses.[114]

In addition to legislation, several agencies and federal executive departments have taken steps toward combating ransomware. In response to the aforementioned ransomware attack on Colonial Pipeline—the largest pipeline transporting refined petroleum products in the United States—CISA turned its attention to curbing ransomware.[115] CISA developed stopransomware.gov, a

[112] Servicemember Quality of Life Improvement and National Defense Authorization Act for Fiscal Year 2025, Pub. L. No. 118-159, tit. LXV § 6508 (2024).

[113] *Id.* § 6507. Notably, the list of cyber actors includes multiple Russian groups, including DarkSide, Conti, REvil, C10p, Play, and Killnet. The list also includes several RaaS operators, such as BlackCat, LockBit, and Rhysida.

[114] For instance, the State and Local Cybersecurity Improvement Act (part of the Infrastructure Investment and Jobs Act) would establish a grant program to help state, local, Tribal, and territorial (SLTT) governments improve cybersecurity, with ransomware defense being a key focus. State and Local Cybersecurity Improvement Act, H.R. 3138, 117th Cong. (2021). The Ransom Disclosure Act would require any entity (1) engaged in interstate commerce, (2) engaged in an activity affecting interstate commerce, or (3) that receives federal funds to disclose ransom payments to DHS within 48 hours. Ransom Disclosure Act, H.R. 5501, 117th Cong. (2021). This bill was particularly contentious, as it would have, in effect, punished victims who pay to get their organizations back up-and-running as opposed to targeting efforts on combating cybercriminals who launch ransomware attacks. Bill Toulas, *Ransom Disclosure Act would give victims 48 hours to report payments*, BLEEPING COMPUTER (Oct. 6, 2021), https://www.bleepingcomputer.com/news/legal/ransom-disclosure-act-would-give-victims-48-hours-to-report-payments/ [https://perma.cc/G5PQ-27ZN]. In addition, the Ransomware and Financial Stability Act of 2024 would prohibit U.S. financial institutions from paying ransoms before submitting notification to the Director of the Financial Crimes Enforcement Network (FCEN). Under this Act, it would be illegal to make a ransom payment in an amount greater than $100,000 without first notifying and receiving approval. Ransomware and Financial Stability Act of 2024, H.R. 7965, 118th Cong. (2024).

[115] *See* Jen Easterly, *The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (May 7, 2023), https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years [https://perma.cc/RK92-W6D3]. The Colonial Pipeline attack caused havoc.

website that links to various resources about cybersecurity for businesses and individuals. Additionally, in conjunction with the FBI, NSA, and the Multi-State Information Sharing and Analysis Center (MS-ISAC), the JRTF created the #StopRansomware Guide.[116] The Justice Department is also spearheading several initiatives to tackle ransomware. The DOJ created the Ransomware and Digital Extortion Task Force, which is comprised of the FBI, Executive Office for United States Attorneys (EOUSA), and representatives from their Criminal, Civil, and National Security Divisions, to enhance intelligence and information sharing and improve DOJ coordination on ransomware cases.[117] In conjunction with the DOJ's efforts, the FBI has launched the Internet Crime Complaint Center (IC3), where individuals and organizations can report ransomware attacks, learn more about recent attacks,[118] and engage the Recovery Asset Team, which helps victims recover ransomware payments when possible.[119] And, as noted above, the

Americans across the eastern seaboard queued for hours waiting to get gas and local police asked residents to limit non-essential travel, check on neighbors, and refrain from hoarding fuel. *See also* Ron Lee, *GasBuddy reports 71% of gas stations without fuel in Charlotte metro amid Colonial Pipeline shutdown*, WBTV (May 12, 2021), https://www.wbtv.com/2021/05/11/long-lines-charlotte-gas-supply-squeezed/ [https://perma.cc/J2SH-2Z5B]. Four state Governors declared states of emergency. *See* Marisa Iati, *How the Colonial Pipeline hack is affecting gas prices and supply*, WASH. POST (May 17, 2021), https://www.washingtonpost.com/business/2021/05/12/faq-gas-shortages/ [https://perma.cc/LXG3-EVAJ].

[116] *#StopRansomware Guide*, CISA (Oct. 19, 2023), https://www.cisa.gov/sites/default/files/2023-10/StopRansomware-Guide-508C-v3_1.pdf [https://perma.cc/7XSD-S7XK]. However, the guide was last updated in October of 2023 and does not address notable, novel and evolving threats, such as double or triple extortion ransomware attacks. *See id.*

[117] *See* KRISTIN FINKLEA, CONG. RSCH. SERV., IN11698, DEPARTMENT OF JUSTICE EFFORTS TO COUNTER RANSOMWARE 2 (2021).

[118] *See About Us*, INTERNET CRIME COMPLAINT CENTER (IC3), https://www.ic3.gov/Home/About [https://perma.cc/UC78-V6YG] (last visited May 13, 2026).

[119] *See* FBI LAS VEGAS, *FBI Las Vegas Federal Fact Friday: Recovery Asset Team*, FBI (May 13, 2022), https://www.fbi.gov/contact-us/field-offices/lasvegas/news/press-releases/fbi-las-vegas-federal-fact-friday-recovery-asset-team (on file with Columbia Business Law Review). Prior to President Trump's second Administration, the DOJ had a Cryptocurrency Enforcement Team (NCET), created in 2021, that focused on prosecuting criminal misuses of cryptocurrency. Press Release, U.S. Dep't of Justice, Deputy Attorney General

FBI can also utilize hack-back measures to help victims respond to attacks per § 1030(f) of the CFAA.[120] In tandem with the DOJ and FBI's efforts, the Treasury Department has started imposing sanctions on cryptocurrency exchanges and specific wallet addresses linked to ransomware payments.[121] Even agencies with seemingly little expertise in or relation to ransomware, such as the SEC, have started taking action.[122]

Lisa O. Monaco Announces National Cryptocurrency Enforcement Team, (Oct. 6, 2021), https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-national-cryptocurrency-enforcement-team [https://perma.cc/6G4D-FN33]. NCET was disbanded in April 2025. *See* Sarah N. Lynch & Chris Prentice, *US Justice Dept disbands crypto enforcement team, citing Trump order*, REUTERS (Apr. 8, 2025), https://www.reuters.com/world/us/us-justice-dept-disbands-cryptocurrency-enforcement-unit-2025-04-08/ (on file with Columbia Business Law Review).

[120] 18 U.S.C. § 1030(f); *see supra* Part II.A.2.

[121] Press Release, U.S. Dep't of Treasury, Treasury Department Issues Ransomware Advisories to Increase Awareness and Thwart Attacks, (Oct. 1, 2020), https://home.treasury.gov/news/press-releases/sm1142 [https://perma.cc/ZF24-CSYB]. For instance, the Treasury Department imposed sanctions on a Russian hacker for his role in launching ransomware attacks on police and other U.S. key infrastructure. Press Release, U.S. Dep't of Treasury, Treasury Sanctions Russian Ransomware Actor Complicit in Attacks on Police and U.S. Critical Infrastructure, (May 16, 2023), https://home.treasury.gov/news/press-releases/jy1486 [https://perma.cc/AC6E-QHKM]. The Department has warned that ransomware payments to individuals or entities on the Office of Foreign Assets Control's (OFAC) Specially Designated Nationals and Blocked Persons List (SDN List) or those "covered by comprehensive country or region embargoes" could be subject to civil forfeiture and possibly result in criminal penalties. *See* BERRIS & GAFFNEY, *supra* note 83, at 7.

[122] Recognizing that "there is an increased risk of the effect of cybersecurity incidents on the economy and registrants[,]" the SEC issued new cybersecurity disclosure rules in 2023 to limit the amount of market volatility that results from cyber incidents. *See* Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 88 Fed Reg. 51896, 51897–99 (Aug. 4, 2023) (to be codified at 17 CFR Parts 229, 232, 239, 240, and 249). Introduced in July 2023, Item 1.05 of Form 8-K requires registrants to disclose material cybersecurity incidents within four business days after the registrant determines that they have experienced an incident. *See* Erik Gerding, Dir., Div. of Corp. Fin., *Disclosure of Cybersecurity Incidents Determined To Be Material and Other Cybersecurity Incidents*, SEC (May 21, 2024), https://www.sec.gov/newsroom/speeches-statements/gerding-cybersecurity-incidents-05212024 [https://perma.cc/5MXJ-JWET]. However, it is ultimately up to the registrant to determine whether an incident is material, leaving significant gaps in

Still, despite all these reform efforts, ransomware attacks continue to increase in frequency and disrupt American organizations. That is, for all the resources the federal government has thus far devoted to ransomware, none of the strategies above provide a readily actionable remedy for organizations in the wake of an attack.

C. *The ACDC Act: Why Congress's Reform Attempt Failed*

Against the backdrop of an increasing number of attacks and growing private-sector frustration, Congressman Tom Graves (R–GA) sought to provide American organizations with one such actionable remedy—the power to "hack back." In 2017, and then again in 2019, Congressman Graves introduced the Active Cyber Defense Certainty Act, which proposed amending the CFAA to legalize hacking back.[123] The ACDC Act was unsuccessful both times, largely due to concerns over the inclusion of vague terms and difficulties in ascribing attribution to attackers, which could lead to undesirable foreign policy outcomes.

1. *"Hacking Back" Under the ACDC Act*

The ACDC Act would have modified the CFAA to legalize the use of "active cyber defense measures," thereby enabling private organizations to pursue self-help measures in the wake of an attack. The amendment would have reclassified certain forms of unauthorized access to an attacker's system as an authorized "active cyber defense measure" when undertaken by a victim. In short, the amendment would have carved out a narrow safe harbor from CFAA liability for conduct that today plainly violates § 1030. Ideally, the ACDC Act would have provided "legal certainty" to

disclosure. Still, despite these reporting gaps, the adoption of Item 1.05 could lead to more securities class action cases, allowing shareholders to seek damages for cybersecurity breaches. Item 1.05 does not provide any tangible means for a public company to respond to a cyberattack, but it does have the added benefit of incentivizing public companies to invest more heavily in their cybersecurity upfront.

[123] *See* H.R. 4036, *supra* note 4; *see also* H.R. 3270 *supra* note 4.

companies by clarifying which countermeasures could be taken without triggering criminal or civil liability under the CFAA.[124]

The ACDC Act defined an "active cyber defense measure" as "consisting of accessing without authorization the computer of the attacker to the defender's own network to gather information" in order to (i) establish attribution of the attack to inform authorities, (ii) disrupt persistent unauthorized activity, and (iii) monitor the behavior of attackers to improve cyber defense techniques.[125] An attacker was defined as "a person or an entity that is the source of the persistent unauthorized intrusion into the victim's computer,"[126] while a defender was defined as "a person or an entity that is a victim of a persistent unauthorized intrusion of the individual entity's computer."[127]

To avoid escalating a cyber incident, only "qualified defenders" who have "a high degree of confidence" in their assailant's identity would be authorized to use active cyber defense techniques.[128] Additionally, these "qualified defenders" would be required to take "extreme caution . . . to avoid impacting intermediary computers or resulting in an escalating cycle of cyber activity."[129] The ACDC Act would require a defender to notify the FBI National Cyber Investigative Joint Task Force (NCIJTF) and "receive a response from the FBI acknowledging receipt of the notification prior to using the [active cyber defense] measure."[130] A defender would need to specifically include the following in their notification to NCIJTF:

---

[124] H.R. 3270 § 2(11) (providing "legal certainty by clarifying the type of tools and techniques that defenders can use that exceed the boundaries of their own computer network"). The Act would have protected a "defender" against prosecution for using a cyber defense that could violate the CFAA in its current form. Alice M. Porch, *Spoiling for a Fight*, 65 SOUTH DAKOTA L. REV. 467, 477 (2020). That said, the Act would "not apply to civil action, so an entity or defender can be held liable for damages caused to others." *Id.*

[125] H.R. 3270 § 4(3)(B)(i)(II)(aa)–(cc). The ACDC Act would have provided for hacking back as to *any* type of cyberattack. As noted previously, this Note is principally focused on hacking back in the context of ransomware. Therefore, the analysis that follows is limited in scope to ransomware.

[126] *Id.* § 4(3)(C).

[127] *Id.* § 4(3)(A).

[128] *Id.* § 2(10).

[129] *Id.*

[130] H.R. 3270 § 5(1).

> the type of cyber breach that the person or entity was a victim of, the intended target of the active cyber defense measure, the steps the defender plans to take to preserve evidence of the attacker's criminal cyber intrusion, . . . [and] the steps they plan to prevent damage to intermediary computers.[131]

Had the Act passed, a defender could have submitted a proposed active cyber defense measure to NCIJTF and received an "assessment on how the proposed . . . measure may be amended to better conform to Federal law . . . and [how to] improve the technical operation of the measure."[132]

The ACDC Act intended to provide four benefits to American organizations. First, the Act would provide assurance to companies who would no longer need to wait days, weeks, or months for law enforcement to act.[133] Second, legalizing hacking back would enable companies to identify and track persistent threats targeting their specific sector or industry and share this information with other, similarly situated organizations. By sharing information with other organizations, companies can crowdsource solutions to common attack and threat types.[134] Third, by legalizing hacking back, the Act would reduce the economic disruption companies face because of cyberattacks. Rather than paying millions of dollars in ransom, companies could spend comparatively fewer dollars by launching a counterattack, potentially saving the American economy millions, if not billions, every year in ransomware payments. Fourth and finally, legalizing

---

[131] *Id.* § 5(2).

[132] *Id.* § 6(b).

[133] As House Representative Graves, the sponsor of the ACDC has argued, legalizing hacking back would in essence implement a neighborhood watch: "We're only asking for a neighborhood watch—an extra set of eyes and ears, to notify law enforcement so they can do their job a little bit quicker." Nicholas Schmidle, *The Digital Vigilantes Who Hack Back*, NEW YORKER (Apr. 30, 2018), https://www.newyorker.com/magazine/2018/05/07/the-digital-vigilantes-who-hack-back?_sp=2c64657f-a785-467c-b37c-4f39d649c287.1738870323048 (on file with Columbia Business Law Review).

[134] At the technical level, hacking back can provide options for disrupting ongoing attacks by interfering with command-and-control servers, and it may allow for the recovery of stolen data before it can be used or sold.

hacking back could have a deterrent effect as it increases the costs and risks for attackers, making some targets less attractive.

2. *Criticisms of the ACDC Act and Requirements for Active Cyber Defense*

There were three main concerns lawmakers had in considering ACDC as an amendment to the CFAA: (i) the technical ability of companies to attribute attacks and hack back; (ii) foreign policy and diplomatic implications; and (iii) guaranteed immunity considerations.

Firstly, critics argue that the statute's terms are too vague to be operable, raising serious concerns on attribution. As one critic put it: "[t]he most significant problem with the ACDC Act and the most immediately obvious is the broad, bordering on useless, definition[s]."[135] For example, the ACDC Act stipulates that only "qualified defenders" may engage in hacking back, but nowhere does the Act does define the term "qualified defender."[136] This vague definition could allow "all kinds of businesses [to] hack back . . . [and] while, say, a Google [or another technology giant] almost certainly has the know-how to do so effectively, many others won't."[137] Furthermore, as noted above, attribution is technically challenging. While the Act would have provided an "exception" for a defender using "attributional data," attribution can be far more challenging in practice.[138] Experienced hackers are skilled in obfuscating their identity. An experienced hacker can "compromise a series of computers[,]" making it more difficult to trace the hacker

[135] Dylan Hoffman, Highway to Hell: The Shortcomings of the ACDC Act (Spring 2018) (final project, Tufts University Department of Computer Science), available at https://www.cs.tufts.edu/comp/116/archive/ [https://perma.cc/Y2S3-KZCR].

[136] *See* H.R. 3270.

[137] Martin Giles, *Five reasons "hacking back" is a recipe for cybersecurity chaos*, MIT TECH. REV. (June 21, 2019), https://www.technologyreview.com/2019/06/21/134840/cybersecurity-hackers-hacking-back-us-congress/ [https://perma.cc/4SDT-U9GA]; *see also* Porch, *supra* note 124, at 485 ("[M]ost companies do not possess the abilities or resources to take on sophisticated attackers.").

[138] H.R. 3270 § 3(2). The exception includes utilizing "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" in attribution.

from the victim's computer.[139] Additionally, hackers can use other tools, like the Tor browser, that make it challenging to trace their identity through the chain of computers used in a hack.[140] If a victim is not careful in attributing an attack, it risks crippling "innocent organizations that are unaware they were compromised."[141]

Secondly, these technical concerns necessarily give rise to foreign policy and diplomatic concerns. By extending beyond merely attribution and towards retaliation, hacking back under the ACDC Act could lead to a form of vigilantism with potentially devastating consequences. Rob Joyce, President Trump's former top cybersecurity advisor, said he worries that even if hacking back was authorized "in a prescribed way, with finite-edge cases . . . you're still going to have unqualified actors bringing risk to themselves, their targets, and their governments."[142] Critics point out that "companies are not as well-equipped as the government to assess the likelihood of foreign escalation."[143] Without the knowledge and insight of the federal government, victims could actually be trying to hack back a state-sponsored group or, worse, a nation-state. Given that China, North Korea, Russia, and Iran are behind some of the largest attacks, "[i]t certainly would not be advisable for a single company to take them on."[144] And should an American organization proverbially poke the wrong bear, the United States could become enveloped in a quickly escalating diplomatic row, which may be more difficult to wriggle out of than it was to enter into. Some experts, such as General (Ret.) Keith Alexander, the former director of the NSA and commander of USCYBERCOM under President Obama, argue that at its most extreme, hacking back could spark wars.[145] In effect, hacking back

[139] Porch, *supra* note 124, at 486.

[140] *See id.* ("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.") (quoting 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/ [https://perma.cc/DR2W-XHXB]) (internal quotation marks omitted).

[141] Porch, *supra* note 124, at 485.

[142] Schmidle, *supra* note 133.

[143] Beale & Berris, *supra* note 95, at 197.

[144] Giles, *supra* note 137.

[145] *See* Schmidle, *supra* note 133.

would enable companies to take the first shot.[146] Therefore, Joyce, Alexander, and other critics of the ACDC Act argue that the practice of hacking back should remain limited to government cybersecurity experts.

Thirdly, critics argue that ACDC Act's proposed advance authorization from the FBI NCIJTF would not guarantee immunity or eliminate an organization's risk of facing civil liability. The statute stipulates that NCIJTF would have discretion in prioritizing "the issuance of [its] guidance" given "the availability of [the FBI's] resources."[147] Consequently, provided the FBI's finite resources and its prioritization methodology, some organizations may not be able to get advanced sign-off from the FBI, effectively leaving them in the same position they were in prior to the Act.[148] Additionally, critics note that organizations who hack back might not be guaranteed immunity from other acts, like the Electronic Communications Privacy Act, the Stored Communications Act (SCA), the Federal Wiretap Act of 1968, or the Economic Espionage Act.[149] Moreover, "even if the ACDC Act [had] passed, it would [have] still le[ft] businesses liable to costly civil lawsuits at both the federal and state levels if they harmed other [U.S.] businesses' computers or data."[150]

In sum, the ACDC Act was unable to assuage the fears of lawmakers and experts that active cyber defense or hacking back could be carried out by U.S. organizations with the required technical expertise without potentially causing diplomatic conflict or risking immunity.

III. A NEW APPROACH TO LEGALIZING HACKING BACK: THE HACK-BACK CONTRACTOR INDUSTRY

While the ACDC Act has failed to pass twice, the discussion of hacking-back and the underlying need for it have not subsided. One seemingly straightforward way to legalize hacking-back would be to narrow the language of the ACDC Act so that it could pass muster in Congress. For example, Congress could amend the

[146] *Id.*

[147] H.R. 3270 § 6(c).

[148] *Id.*

[149] *See generally* discussion *infra* Part III.C; *see also* Porch, *supra* note 124, at 481–83.

[150] Giles, *supra* note 137.

statute to narrow its application to only certain remedial actions[151] or delegate rulemaking authority to a particular agency to more clearly enumerate the requirements for organizations to obtain immunity.[152] Still, such a solution would require the agreement of lawmakers in Congress—a tall ask for our increasingly polarized Legislature.

This Part argues that neither the ACDC Act nor any other amendment to the CFAA is necessary to authorize limited hacking back. Instead, this authorization is found within the existing statute's law enforcement exception. This Part begins by discussing the legal foundation for this proposal, including a revisit of § 1030(f) and two recent federal district court cases on point. Next, it argues that this proposal is congruent with the U.S.'s existing policy on private military contractors (PMCs) and the granting of facility security clearances (FCLs). Then, this Part proposes that the federal government leverage this Note's reading of § 1030(f) of the CFAA to combat the growing ransomware crisis. It proposes that the federal government should create a regulated industry of private

[151] For example, Congress could limit language to focus only on legalizing select tools, like offensive honeypots or port scanning. A honeypot is a type of defense tool 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." Porch, *supra* note 124, at 481. Port scanning is "a reconnaissance method that involves systematically probing a target system for open ports" on a computer system as well as determining what services might be running. Bon Adamson, *Internet Port Scanning Explained: What is it, and how it works*, SLASHGEAR (Dec. 18, 2023), https://www.slashgear.com/1470406/internet-port-scanning-explained/ [https://perma.cc/K3DP-4NY5]; *see also Combating Ransomware: A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force*, INST. FOR SEC. + TECH. 1, 33 (Sep. 23, 2021), https://securityandtechnology.org/wp-content/uploads/2021/04/IST-Ransomware-Task-Force-Report.pdf [https://perma.cc/P7F4-3GBW] ("If a service provider is tipped to malicious infrastructure, it should be able to take action against the infrastructure without fear of legal liability . . . Congress should ensure private industry can actively block or limit traffic when acting in good faith without fear of legal liability.").

[152] The ACDC Act does not delegate rulemaking authority to one particular agency, meaning no agency is tasked with defining key terms or implementing regulations in association with the statute. As noted in Part II.C.1., under the statute, the FBI would oversee the advanced review of a private organization's "hack back" plan. *See* H.R. 3270 § 6. Additionally, the DOJ would be required to update the "Prosecuting Computer Crimes Manual" to reflect the changes made by the ACDC Act and would be encouraged "to seek additional opportunities to clarify the manual and other guidance to the public to reflect evolving defensive techniques and cyber technology." *Id.* § 8(a)–(b).

"hack back contractors" that may conduct limited active cyber defense operations on behalf of victim organizations while operating under federal tasking orders, approval, and after-action review by agencies like the FBI or DHS. This Part then discusses how this solution would address outstanding concerns over attribution, foreign policy implications, and guaranteed immunity. Finally, this Part delves into additional considerations for policy and lawmakers in the cybersecurity and national security context.

A. *The Legal Foundation and Historical Precedent*

There is both legal and historical support for the proposal outlined below. Section 1030(f) of the CFAA provides an exception for law enforcement, and recently two federal district courts weighed in on the applicability of the exception to private parties. These cases support a reading of § 1030(f) that provides private organizations with the legal authorization to hack back when delegated to do so by U.S. law enforcement. Moreover, the proposal to create an industry of private "hack back contractors" is supported by the federal governments historical practice of delegating authority to private military contractors.

1. *Legal Foundation: Section 1030(f) and Recent Case Law*

Two recent district court cases have opened the door to the exact framework this Note proposes. As noted above, § 1030(f) of the CFAA provides an exception for law enforcement. It stipulates that the CFAA "does not prohibit any lawfully authorized investigative, protective or intelligence activity *of a law enforcement agency*."[153] As early as 2013, some scholars have "posited that under § 1030(f) private companies could reach out to the [DOJ] to 'borrow' their law enforcement authority under the CFAA to authorize a [hack back]."[154] In 2016, Jeremy and Ariel Rabkin concretized this proposal in their article, *Hacking Back Without*

[153] *See* Part II.A.ii; 18 U.S.C. § 1030(f) (emphasis added).

[154] Sam Parker, *Shot in the Dark: Can Private Sector "Hackbacks" Work?*, 13 J. NAT'L SEC. L. & POL'Y 211, 225 (2022). This topic was first explored in a podcast that took place in 2013, featuring law professor Orin Kerr and former NSA official Stewart Baker. See Stewart Baker, The HackBack Debate Revisited, Steptoe Cyber Blog (Mar. 4, 2013) [https://perma.cc/7MTP-YMFP].

Cracking Up.[155] They proposed "reinterpreting § 1030(f) of the CFAA to allow law enforcement or intelligence agencies to designate companies to launch [hack backs] exempted from CFAA liability, by letting the companies in effect 'borrow' their law enforcement authority."[156] However, at the time of publication, such a reading of § 1030(f) was largely speculative, as there had never been a case interpreting the exact meaning nor bounds of § 1030(f).[157] Finally, in 2024, two federal courts—the District of Puerto Rico and the Northern District of California—weighed in.

The first instance of a court interpreting § 1030(f) was the District Court of Puerto Rico in *Naicom Corp. v. Dish Network Corp.*[158] Naicom, a Puerto Rican broadcasting company, alleged that defendants DISH Network, NagraStar, and federal authorities (including FBI agents and U.S. Attorneys) conspired to steal Naicom's proprietary technology and trade secrets by conducting searches of Naicom's facilities under the pretense of a piracy investigation.[159] According to Naicom, the defendants knew that the company was a legitimate business but used search warrants based on false information to gain access to Naicom's intellectual property.[160] Naicom alleged that "by accessing Naicom's computer systems without authorization or in excess of authorization and

[155] Jeremy Rabkin & Ariel Rabkin, *Hacking Back Without Cracking Up*, HOOVER INST. (June 28, 2016), https://www.hoover.org/research/hacking-back-without-cracking [https://perma.cc/YTN7-NXVC].

[156] Parker, *supra* note 154, at 224 (citing Rabkin & Rabkin, *supra* note 155).

[157] *Id.*

[158] *See* Naicom Corp. v. Dish Network Corp., No. 3:21-cv-01405-JAW, 2024 WL 1363781 (D.P.R. Mar. 29, 2024), *aff'd* by Naicom Corp. v. Dish Network Corp., No. 24-1416, 2025 WL 4694553 (1st Cir. Dec. 2, 2025); Naicom Corp. v. Dish Network Corp., No. 3:21-cv-01405-JAW, 2024 WL 1363462 (D.P.R. Mar. 29, 2024), *aff'd* by Naicom Corp. v. Dish Network Corp., No. 24-1416, 2025 WL 4694553 (1st Cir. Dec. 2, 2025). Appellants requested an opinion affirming judgment but were denied. *See* Naicom Corp. v. Dish Network Corp., No. 24-1416 (1st Cir. Dec. 8, 2025) (Order Denying Motion for Opinion Affirming Judgment). Appellants petitioned for rehearing and petitioned for hearing en banc but both petitions were denied. *See* Naicom Corp. v. Dish Network Corp., No. 24-1416 (1st Cir. Feb. 24, 2026) (Order Denying Petition for Rehearing and Rehearing En Banc).

[159] *Naicom Corp.*, 2024 WL 1363781, at *8; *Naicom Corp.*, 2024 WL 1363462, at *8.

[160] *Naicom Corp.*, 2024 WL 1363781, at *8; *Naicom Corp.*, 2024 WL 1363462, at *8.

obtaining and using valuable information from those computers" defendants—federal authorities in conjunction with DISH Network and NagraStar—violated the CFAA.[161] The court dismissed the claim against both federal and private corporate defendants, finding that the conduct of these defendants fell within the § 1030(f) exception in pursuance of a lawful search warrant.[162] It considered the actions of private defendants as "lawfully authorized investigative activity" falling within the § 1030(f) exception.[163] The First Circuit affirmed the dismissal on appeal, providing the first doctrinal precedent for extending the application of § 1030(f) to private corporate defendants, who work with law enforcement on activities otherwise prohibited by the CFAA.[164]

In August of 2024, the Northern District of California similarly left the door open for private companies to utilize the § 1030(f) exception in an order issued in the case *Whatsapp Inc. v. NSO Group Technologies Ltd.*[165] WhatsApp sued the NSO Group, an Israeli technology company that develops and sells spyware, alleging that NSO Group used WhatsApp's infrastructure to deliver its spyware to approximately 1,400 targeted mobile devices in violation of the

[161] *Naicom Corp.*, 2024 WL 1363781, at *8; *Naicom Corp.*, 2024 WL 1363462, at *8.

[162] *Naicom Corp.*, 2024 WL 1363781, at *29; *Naicom Corp.*, 2024 WL 1363462, at *29.

[163] *Naicom Corp.*, 2024 WL 1363462, at *29 ("Because the DISH/NagraStar Defendants' challenged conduct was 'lawfully authorized investigative . . . activity' under the search warrants, Plaintiffs have not pleaded a viable CFAA claim.").

[164] *See* Naicom Corp. v. Dish Network Corp., No. 24-1416, 2025 WL 4694553, at *1 (1st Cir. Dec. 2, 2025).

[165] Whatsapp Inc. v. NSO Group Technologies Ltd., No. 19-cv-07123-PJH, 2024 WL 3639375 (N.D. Cal. Aug. 1, 2024) (noting that it would "be premature to preclude certain affirmative defenses" at such an early stage of litigation). Note, this case is incredibly complex given its international scope and resulting implications. In December of 2024, the court granted summary judgment to Plaintiffs, Whatsapp, Inc. but left the decision of damages for jury trial. WhatsApp Inc. v. NSO Grp. Techs. Ltd., No. 19-CV-07123-PJH, 2024 WL 5190365, at *9 (N.D. Cal. Dec. 20, 2024). In November of 2025, the court entered a final judgment for damages in the amount of $167,698,719. *Whatsapp Inc.,* No. 736 (N.D. Cal. Nov. 12, 2025). The case is currently up for appeal to the Ninth Circuit. Whatsapp Inc. v. NSO Group Technologies Ltd., No. 838 (N.D. Cal. Feb. 11, 2026).

CFAA.[166] NSO Group raised an affirmative defense under § 1030(f), arguing that its activities fell within the category of lawfully authorized investigative activity.[167] Whatsapp argued that "NSO does not and cannot invoke [the § 1030(f)] law-enforcement exception" and moved for the defense to be stricken from the record.[168] The court asserted that "it would be premature to preclude certain affirmative defenses as lacking legal or factual support, as that remedy is more properly suited to a motion in limine."[169] Still, the court ultimately rejected NSO's affirmative defense on the grounds that "NSO ha[d] not made even an initial showing that the [§ 1030(f)] exception applies . . . in this case."[170] That is, while the court rejected NSO's attempt to use the defense under § 1030(f), it did not rule out that a private defendant could bring such an argument. Thus, the court leaves the door open for a private company to invoke § 1030(f) if it could make a sufficient factual showing that it was conducting "lawfully authorized investigative activity" on behalf of a qualifying law enforcement or intelligence agency.[171]

Of course, neither of these cases are controlling precedent across the U.S. Nonetheless, taken collectively, these two cases strengthen the argument that the § 1030(f) exception can be applied to private contractors who work on behalf of law enforcement to engage in activities otherwise prohibited by the CFAA. *Naicom Corp.* and *Whatsapp Inc.*, assuming it too is affirmed on appeal, provide doctrinal precedent for private organizations to invoke § 1030(f) and support an interpretation of the CFAA to allow law enforcement to deputize hacking-back authority to private cyber contractors.

2. *Historical Precedents in Public-Private Defense Partnerships*

The United States has a storied history and tradition of deputizing authority to the private sector to supply military and

---

[166] Complaint, Whatsapp Inc. v. NSO Group Technologies Ltd., Case No. 3:19-cv-07123-JSC, 2019 WL 5571028, at *1 (Oct. 29, 2019) (No. 1).

[167] *Whatsapp Inc.*, 2024 WL 3639375, at *1.

[168] *Id.* at *1.

[169] *Id.* at *2.

[170] *Id.*

[171] 18 U.S.C. § 1030(f).

defense capabilities. This history dates back to the Nation's founding and has continued well into the twenty-first century.

The U.S. Constitution grants Congress the power to issue letters of marque,[172] and these letters historically served as the first means of delegating authority to a private contractor.[173] A letter of marque is a "legal authorization[] enabling private entities—privateers—to use force on behalf of the state to harass or prey on vessels belonging to foreign nations or individuals."[174] A letter of marque functions like a government license authorizing the licensed entity to engage in privateering. Early in the Nation's history, the letters of marque provided an opportunity for Congress to outsource defense capabilities to private industry rather than (i) passing the cost on to the American taxpayer and (ii) possibly landing the United States in adversarial conflicts or war. In effect, the letters of marque provided the U.S. with diplomatic cover and sheltered the U.S. from bearing the cost of war.[175] The U.S. utilized the letters of marque most notably in the War of 1812, where employing privateers proved critical as the U.S. was far

[172] U.S. CONST. art. 1, § 8, cl. 11. The letters of marque can be dated back to 1295, when the English Crown issued a letter of marque after an English merchant ship was captured by the Portuguese. The letters were utilized in the early days of the Colonies and in the French and Indian War fought from 1756 to 1763. Thus, the letters of marque were quite familiar to the founding fathers at the time that they were drafting the U.S. Constitution. *See* Theodore M. Cooperstein, *Letters of Marque and Reprisal: The Constitutional Law and Practice of Privateering*, 40 J. MAR. L. & COM. 221, 223–25 (2009).

[173] Todd Emerson Hutchins, *Structuring Sustainable Letters of Marque Regime: How Commissioning Privateers Can Defeat Somali Pirates*, 99 CAL. L.R. 819, 844 (2011) ("The Framers incorporated letters of marque into the U.S. Constitution to protect America's seagoing interests, and Congress can issue them to encourage private, profit-making military ventures to undertake activities that align with the national security interests of the sovereign.").

[174] *Id.* at 843–44. A privateer is a "vessel owned, equipped, and armed by one or more private individuals, and duly commissioned by a belligerent power to go on cruises and make war upon the enemy, usually by preying on his commerce." *Privateer*, BLACK'S LAW DICTIONARY (6th ed. 1990).

[175] *Id.*; *see also* Theodore T. Richard, *Reconsidering the Letter of Marque: Utilizing private Security Providers Against Piracy*, 39 PUB. CONT. L.J. 411, 427–28 (2010) ("The concept of privateers as private citizens who could be summoned for the defense of the nation fit into the American founders' belief in militias and fears of standing armies.").

outnumbered.[176] The U.S. continued to issue letters of marque after the war,[177] but the practice fell out of vogue in the latter half of the nineteenth century following the Paris Declaration and Civil War with shifts in international relations and technology.[178] While Congress has not issued any letters in two centuries, "the failure of Congress to exercise the authority . . . does not mean [that] the authority no longer resides in Congress."[179] In fact, several lawmakers and public servants have advocated for the use of letters of marque in recent decades,[180] including in the cyber context.[181]

[176] *See* An Act Concerning Letters of Marque, Prizes, and Prize Goods, 2 STAT. 759 (1812); *see also* Hutchins, *supra* note 173, at 853 (arguing that employing privateers through issuing letters of marque was "the only economically viable way to provide meaningful resistance").

[177] *See* Hutchins, *supra* note 173, at 854.

[178] *Id.* at 854–56. The Paris Declaration of 1856 was a treaty that bound signatories to refrain from issuing letters of marque. While the U.S. never signed the treaty, the issuance of letters of marque considerably slowed in the latter half of the century. *See also* Cooperstein, *supra* note 172, at 244–52 for a discussion of why this practice dwindled. "Following the Civil War, and for the remainder of the century, privateering continued its decline into disuse by the United States." *Id.* at 248. This change was also spurred on by technological changes, such as the advent of the submarine, which was costly for private parties to produce. "The modernization of arms and the centralization of modern war economies during the two world wars subsumed the private actor into the public war effort." *Id.* at 251.

[179] Cooperstein, *supra* note 172, at 251.

[180] In response to Somali pirates, for example, scholars suggested that letters of marque should be revived in the piracy context. *See generally* Richard, *supra* note 175; Hutchins, *supra* note 173. After the September 11, 2001 attack, Congressman Ron Paul suggested that Congress issue letters of marque against terrorist assets connected to the attack. September 11 Marque and Reprisal Act of 2001, H.R. 3076, 107th Cong. (1st Sess. 2001); 147 CONG. REC. E1837-38 (2001) (statement of Rep. Ron Paul), available at https://www.congress.gov/107/crec/2001/10/10/147/135/CREC-2001-10-10-pt1-PgE1837-2.pdf ("Although modern America does not face the threat of piracy on the high seas, we do face the threat of international terrorism. . . . Like the pirates who once terrorized the high seas, terrorists today are also difficult to punish using military means."). Congressman Paul again suggested reviving the letters of marque a few years later. Marque and Reprisal Act of 2007, H.R. 3216, 110th Cong. (1st Sess. 2007).

[181] Major General (Ret.) Thomas Ayres, the former Deputy Judge Advocate General of the United States Army and General Counsel of the United States Air Force under President Trump, has advocated for the issuance of cyber letters of marque. Thomas Ayres, *A Maritime Solution for Cyber Privacy: Congress*

In the last two centuries, Congress has pursued an alternative route to harness the capabilities of the private sector for military and defense purposes. The United States utilizes private military contractors (PMCs) to augment its armed forces and support efforts to bolster national security. PMCs are private companies that provide military and security services to governments, corporations, or other organizations. These services may include providing "logistical support, transportation, engineering, construction, skilled and unskilled laborers, maintenance, technical expertise, and other paramilitary operations."[182] The use of contractors in the U.S. military dates as far back as the Revolutionary War.[183] Then, the Continental Army relied on contractors for "transportation and engineering services, construction, clothing, and weapons."[184] By World War II, roughly ten percent of America's armed forces were privately contracted.[185] After the war, the number of contracted PMCs only continued to grow, as engaging PMCs was viewed as a cheaper alternative to

should revive the 'letter of marque' and authorize companies to defend against hackers, WALL ST. J. (May 13, 2021), https://www.wsj.com/articles/a-maritime-solution-for-cyber-piracy-11620922458 (on file with Columbia Business Law Review). The letters of marque historically "provided financial incentives to overcome fear and inaction in the face of dangerous outcomes and national needs. . . . Cyber letters of marque could establish incentives for timely information sharing and ensure that companies have the freedom to defend themselves." *Id.* While constitutionally permissible and legally possible, the issuance of cyber letters of marque is unlikely to prove implementable in practice. For one thing, the letters of marque would raise many of the same questions that led to the rejection of the ACDC Act, such as concerns over foreign policy and the technical capabilities of licensees. For another, seeking the approval of the partisan and highly polarized Congress on short notice seems infeasible today.

[182] DEBORAH C. KIDWELL, PUBLIC WAR, PRIVATE FIGHT? THE UNITED STATES AND PRIVATE MILITARY COMPANIES AND PRIVATE MILITARY INSTITUTIONS 1 (2005).

[183] MOSHE SCHWARTZ & JOYPRADA SWAIN, CONG. RSCH. SERV., R40764, DEPARTMENT OF DEFENSE CONTRACTORS IN AFGHANISTAN AND IRAQ: BACKGROUND AND ANALYSIS 1 (2011).

[184] *Id.*

[185] *See* Alexander Casendino, *Soldiers of Fortune: the Rise of Private Military Companies and their Consequences on America's Wars*, BERKELEY POL. REV. (Oct. 25, 2017), https://bpr.studentorg.berkeley.edu/2017/10/25/soldiers-of-fortune-the-rise-of-private-military-companies-and-their-consequences-on-americas-wars/#:~:text=,private%20military%20companies%2C%20or%20PMCs [https://perma.cc/BW2V-KP6G].

government defense spending.[186] This trend was further exacerbated by the collapse of the Soviet Union, which led to a dramatic reduction in the U.S. defense budget.[187] As a result, the country massively downsized its armed forces.[188] "With thousands of former military personnel out of work, there was a surplus of individuals with military expertise and [PMCs] provided employment for those possessing such skills."[189] When the wars in Iraq and Afghanistan began, contractors comprised of approximately fifty percent of the country's armed forces engaged in active conflict zones.[190] By 2011, the number of private contract employees outnumbered the number of actual U.S. military personnel deployed.[191]

While PMCs have been used multiple times in U.S.'s history, they have been subject to scrutiny following a few high-profile incidents.[192] These incidents led to several reforms to hold PMCs accountable for their actions.[193] For example, the Military Extraterritorial Jurisdiction Act (MEJA) was enacted to allow the

[186] KIDWELL, *supra* note 182, at 28 ("Beginning in 1955, the Eisenhower administration encouraged federal agencies to rely on the private sector to limit government expansion and to manage resources efficiently.").

[187] PETER W. SINGER, CORPORATE WARRIORS: THE RISE OF THE PRIVATIZED MILITARY INDUSTRY 53 (Cornell Univ. Press ed. 2007) (2003).

[188] *Id.*

[189] Natasha Arnpriester, *Combating Impunity: The Private Military Industry, Human Rights, and the "Legal Gap"*, 38 U. PA. J. INT'L L. 1189, 1205 (2017).

[190] SCHWARTZ & SWAIN, *supra* note 183, at 2.

[191] *Costs of War: Other Costs to the U.S. Economy*, WATSON SCH. OF INT'L & PUB. AFFS., BROWN U., https://costsofwar.watson.brown.edu/costs/economic/other-costs-us-economy [https://perma.cc/YH9F-V4R7] (last visited May 13, 2026).

[192] Arnpriester, *supra* note 189, at 1189–1239 (arguing that PMCs operate in a "legal gap" that allows them to commit human rights violations with impunity, necessitating an international legal framework to ensure proper accountability and oversight); *see also* Mitchell McNaylor, *Mind the "Gap": Private Military Companies and the Rule of Law*, 5 YALE J. INT'L AFF. (2010), available at https://www.yalejournal.org/publications/mind-the-gap-private-military-companies-and-the-rule-of-law [https://perma.cc/AY8W-6GG5] (arguing that PMCs "operate outside of any legal framework.").

[193] Perhaps the most notable incident was the 2007 Nisour Square shooting in Baghdad, Iraq involving Blackwater (rebranded Academi, after a brief rename as Xe) contractors. Arnpriester, *supra* note 189, at 1192. For collecting incidents, *see id.* 1192–97.

DOJ to prosecute contractors who commit crimes overseas,[194] and the Uniform Code of Military Justice (UCMJ) was amended to potentially subject contractors in combat zones to court-martial.[195] Furthermore, PMCs are tightly regulated by contract law, federal regulations, and applicable criminal laws.[196] PMCs are required to obtain security clearances at the appropriate level, known as Facility Clearance Levels (FCLs).[197] A FCL is defined as "a determination made by the Government that a contractor is eligible for access to classified information."[198] That is, to work on classified contracts, a PMC must obtain a FCL at the required classification level, which in itself is no easy task.[199]

The regulatory structure governing security clearances serves as a critical instrument through which the U.S. incorporates commercial entities into defense activities while protecting classified information. PMCs that satisfy these security standards effectively become reliable government allies and are permitted to access sensitive details regarding military strategy, intelligence gathering, and digital security operations. The potential consequences of non-compliance—including clearance termination and contract cancellation—create a compelling motivation for PMCs to adhere to federal security protocols.

B. *The Proposal: Facility Clearances for Designated Hack-Back Contractors*

This Note proposes designating select cybersecurity firms as PMC-style cyber contractors to address the growing ransomware crisis.[200] Designating select cybersecurity firms as contractors with

[194] *See* Katherin J. Chapman, *The Untouchables: Private Military Contractors' Criminal Accountability under the UCMJ*, 63 VAND. L. REV. 1047, 1064 (2010).

[195] *Id.* at 1052–53.

[196] *See generally* Federal Acquisition Regulation, 48 C.F.R. pts. 1–53 (2024); Defense Federal Acquisition Regulation Supplement, 48 C.F.R. pts. 201–53 (2024).

[197] *Facility Security Clearance (FCL) FAQ*, U.S. DEP'T OF STATE, https://www.state.gov/facility-security-clearance-fcl-faq [https://perma.cc/SB6U-QW54] (last visited May 13, 2026).

[198] *Id.*

[199] *See* discussion *infra* Part III.B.

[200] This Note uses modern PMCs and the FCL regime primarily as an institutional analogy for delegating security functions to private contractors while

appropriate clearances pursuant to § 1030(f) offers numerous advantages and would address concerns that stalled the ACDC Act in Congress—namely, technical complexity, foreign policy, and uncertainty in immunity. Granting FCLs to designated hack-back contractors could provide a viable solution to the current impasse in active cyber defense. In effect, the federal government would create a regulated industry of private "hack back contractors" to conduct active cyber defense operations on behalf of victim organizations and remain under the oversight of federal agencies like the FBI or DHS.

By contracting with select cybersecurity firms, the U.S. can ensure that the companies engaging in hacking back cases have the deep experience and expertise required to deal with complex technical issues, such as attribution. Examples of such U.S. firms include CrowdStrike, Trellix (formerly FireEye and McAfee Enterprise) and Mandiant. Attribution poses technical difficulties regardless of who conducts the investigation. However, by concentrating these technical challenges among a small group of vetted contractors with specialized expertise, experts can leverage one another's and the government's insights to correctly attribute attacks. In short, these contractors would operate with superior technical capabilities, access to classified threat intelligence unavailable to most private companies, and established protocols for attribution verification before taking action.

These proposed "hack-back contractors" could operate under the close eye of the FBI or DHS, ensuring that there is proper consideration of potential diplomatic implications before any actions are taken. Federal oversight could include tasking orders, approval, and after-action review by agencies like the FBI or DHS. Moreover, this structure would facilitate critical information and knowledge sharing about threat actors and attack methodologies, making it easier to combat the growing RaaS model while limiting this capability to a carefully vetted group of actors.[201] As such, this

maintaining federal oversight. There are important differences between the traditional kinetic context and presently considered cyber context. A full analysis and discussion of MEJA, the UCMJ, international law, and related accountability mechanisms warrants separate consideration in a future work. Discussion of some of these considerations in part can be found *infra* Part III.C.

[201] This information sharing model is especially appealing in light of recent challenges in renewing CISA 2015. *See* discussion *supra* Part II.B.

proposal could directly address lawmakers' primary concerns regarding potential escalation of cyber incidents into broader diplomatic conflicts. By establishing clear chains of command, operational boundaries, and government oversight, risks of unintended consequences or misattribution would be significantly reduced compared to allowing individual companies to conduct independent hack-back operations.

The federal government already has bodies that could assume this oversight role, and these entities should step in when an attacker is identified as either a nation-state or state-funded group. Both the FBI and DHS are already well-placed to oversee this industry of private "hack back contractors." For one thing, the FBI has worked in coordination with some of these contractors in previous engagements. For another, the FBI has institutional knowledge of malicious actors as well as their patterns, targets, and practices, and it already works in close company with the DOJ on ultimately prosecuting ransomware cases. Alternatively, it might make more sense for DHS or even CISA (which sits within DHS) to oversee this industry. As these private "hack-back contractors" serve a defensive role for U.S. organizations and their efforts carry significant domestic policy considerations, it follows that DHS would play an advisory role in their operations. Irrespective of which entity is designated to oversee these PMC-style cyber contractors, there would almost assuredly still be inter-governmental coordination on challenging cases. Indeed, when complex cases arise—namely, when a contractor identifies that a nation-state or state-sponsored group is the actor behind an attack—the contractor should relinquish its duties to the federal government. For example, assuming CrowdStrike discovers that the North Koreans are behind an attack against an American organization, CrowdStrike should immediately stop all operations and hand over active control, monitoring, and activity to the FBI or DHS. This would better ensure that relevant governmental agents or military personnel assume responsibility in cases that may implicate foreign relations or that are more likely to escalate to inter-state conflict. Consequently, these measures, coupled with existing oversight mechanisms,[202] would address concerns over the foreign

[202] *See* discussion *supra* Part III.A.2 on federal laws that government contractors are required to comply with. Additionally, as briefly noted previously,

policy implications any unintended rows with foreign nation-states might have.

In specifically working with a select number of cyber contractors and under the guidance of a government entity, this proposal would better address concerns over guaranteed immunity for entities that engage in hacking-back. The FBI and DHS could provide clear guidance for hack-back contractors on which actions contractors are authorized to take and which they are not. For instance, should a contractor, who discovers that an attacker is a nation-state or state-funded group, not relinquish control to the federal government, it would not be afforded the privilege of immunity. Concerns over immunity should be primarily directed at the contractors conducting active cyber defense activities and not at the client who is paying for such services.[203] This policy choice would put more onus on contractors to ensure that they are complying with federal law enforcement and pressure them to maintain high operating standards. Regardless, FCL clearance termination and contract cancellation provide a strong incentive for contractors to proceed with caution.

Finally, in addition to addressing the primary concerns outlined above, this proposal would enable the U.S. to address the cyber talent shortage in government and shift the cost of this

PMCs would need to comply with the rigorous requirements for obtaining an FCL. In brief, these are: a company must be sponsored by either a government agency or an existing cleared contractor; it must submit documentation detailing its ownership, membership, practices, and work authorization; it is subject to evaluation by the Defense Counterintelligence and Security Agency (DCSA), which assesses whether a company is under significant foreign ownership, control, or influence (FOCI). *See Why Should They Have All the Fun? DoD Instruction Expands DCSA's FOCI Reach Beyond Cleared Contractors*, CROWELL & MORING LLP (June 6, 2024), https://www.crowell.com/en/insights/client-alerts/why-should-they-have-all-the-fun-dod-instruction-expands-dcsas-foci-reach-beyond-cleared-contractors [https://perma.cc/ZSA4-T85K]. A company granted a FCL, it must abide by strict rules for protecting classified information or risk having their clearance and contract terminated. *See* National Industrial Security Program Operating Manual, 32 C.F.R. pt. 117 (2024). For example, the company must ensure all employees with access to classified information have personal security clearances, maintain secure information systems, and submit to periodic government inspections. *See id.*

[203] For instance, the FBI or DHS could require liability provisions for any third-party damage in the contracts of these PMC-style cyber contractors. Such liability provisions would further incentivize contractors to exercise caution in conducting limited active cyber defense measures.

defense onto private industry. By offering competitive compensation packages that government positions often cannot match, hack-back contractors could increase both job availability and attract more Americans to the cybersecurity field. While the federal government would oversee these PMC-style cyber contractors who engage in active cyber defense on behalf of companies, it would not be responsible for the bill. Instead, private companies employing these contractors would be responsible for picking up the tab. That is, the U.S. could leave the bill—in whole or in part—to the private companies that solicit their help in the wake of ransomware attacks. Beyond these cost savings, legalizing and regulating this novel industry would generate a new tax revenue stream for the federal government.

By operating under the § 1030(f) law enforcement exception rather than creating a new statutory carve-out as the ACDC Act attempted, this approach builds on established legal principles instead of introducing novel and potentially problematic exceptions to the CFAA. Ultimately, while critical challenges still remain in concretizing the details of such a hack-back regime, § 1030(f) and recent case law provide a supportive pathway for deputizing active cyber defense to hack-back contractors.

C. *Addressing Remaining Concerns*

Of course, while designated hack-back contractors could alleviate concerns over technical complexity, foreign policy and guaranteed immunity, this proposal would first need to be reconciled with other legal and policy considerations.

Firstly, implementation would require careful consideration of existing legal frameworks. As scholars have pointed out, applying § 1030(f) to private corporations on behalf of the government could raise federalism concerns.[204] Namely, as § 1030(f) applies equally to any "law enforcement agency of the United States, a State or political subdivision of a State, or of any intelligence agency," a hack-back contractor could, in theory, work pursuant to the

[204] Parker, *supra* note 154, at 225 ("Baker acknowledged that under their interpretation 'this is not something where you would have to go to the Justice Department. You could . . . go to the Alameda County Sheriff . . . you don't have to wander into Washington to get the protection of [§ 1030(f)].'").

authorization of a local law enforcement department.[205] This outline would not be ideal, given the comparative few resources at the disposal or state or local law enforcement or intelligence agencies. Furthermore, should a contractor at the delegation of a state authority engage with a nation-state or state-funded group, there could be drastic consequences for the nation as a whole. Still, this potential problem could be alleviated if the DOJ issued a policy guidance stipulating that it will more rigorously enforce any misapplications or violations of related law when contractors operate outside of the oversight of a federal body.[206]

Secondly, deputizing active cyber defense to hack-back contractors could raise and trigger other state and federal laws, echoing the guaranteed immunity concerns raised in the ACDC Act.[207] Namely, contractors may face liability under some applicable state laws.[208] That said, a federal agency, such as the FBI, could clarify that the federal government's program preempts state regulation in this area. Additionally, contractors might still be liable under the Electronic Communications Privacy Act, as the statute reads today.[209] Still, the DOJ could issue guidance that it would not seek to prosecute violations if conducted in pursuance of active cyber defense activities as a designated hack-back contractor; or, if necessary, Congress could amend the ECPA to extinguish this concern.

Thirdly, designating hack-back contractors could raise conflicts with U.S. obligations under international law. While "[h]ack backs may not be *per se* contrary to standing international law," international legal hurdles certainly exist. [210] Some scholars contend that international law concerns pose a grave challenge to

[205] *Id.*

[206] Similarly, other agencies, such as the Treasury Department, could stipulate that they will more rigorously enforce potential violations of OFAC payments for contractors operating outside of the oversight of a federal body.

[207] Parker, *supra* note 154, at 225.

[208] *See, e.g.*, the California Comprehensive Computer Data Access and Fraud Act (CDAFA), Cal. Penal Code § 502.

[209] *See generally* 18 U.S.C. §§ 2510, 2701.

[210] Henning Lahmann, *Hacking Back and International Law: An Irreconcilable Pair?*, ZEITSCHRIFT FÜR AUSLÄNDISCHES ÖFFENTLICHES RECHT UND VÖLKERRECHT 80 (2020).

such a program.[211] However, others argue that even if all activities of hack-back contractors were attributable "to the U.S. government, a vast majority are unlikely to violate international law as it is currently understood."[212] As noted previously, to mitigate the number of potential incidents, contractors could be bound to strict guidelines to ensure compliance with international obligations.

While it is nearly impossible to predict every potential form of liability an entity might face, it does not appear that any of the challenges outlined above are fatal on their face.

CONCLUSION

Ransomware attacks represent an escalating threat to American economic and national security interests, yet the current legal framework leaves private organizations without effective remedies when targeted. This Note has demonstrated that despite the federal government's expanding cybersecurity initiatives, law enforcement agencies remain dramatically outmatched by the volume and sophistication of attacks from nation-states, state-sponsored groups, and rogue actors. The proposal to create a regulated industry of hack-back contractors—operating under facility clearances and with government oversight—offers a pragmatic solution that addresses the key shortcomings of previous legislative attempts. By drawing from recent case law supporting private contractor involvement in government cybersecurity operations under CFAA § 1030(f) and the country's historical precedents of PMCs, this proposal would enable rapid response capabilities while mitigating concerns about technical competence, diplomatic complications, and immunity. Rather than allowing the status quo to continue, where organizations face a stark choice between paying ransoms or suffering extended downtime, the federal government should consider this measured approach to deputizing active cyber defense through cleared contractors. This approach would allow the United States to leverage private sector

[211] Parker, *supra* note 154, at 226 ("Even if the FBI is not actively directing or controlling the private sector [hack backs], it would require tortured logic to suggest that they are legal under domestic law because they are an authorized law enforcement activity, but simultaneously to claim for the purposes of international law that the FBI has no control or direction over deputized law enforcement activity under the color of its authority.").

[212] *Id.*

expertise and resources to effectively counter ransomware threats while maintaining necessary governance and accountability.