Shot in the Dark: Can Private Sector "Hackbacks" Work?

Sam Parker*

Introduction

Former FBI Director Robert Mueller once said that "[t]here are only two types of companies: those that have been hacked and those that will be."[1] In a cyber domain where offense has generally dominated defense and the U.S. government is often unwilling or unable to help defend private company networks from cyberattacks, some of those companies would like to go on the offensive to deter and defend against such attacks. They are precluded from engaging in these "hackback" responses, however, by the Computer Fraud and Abuse Act (CFAA), which prohibits accessing computer networks without authorization.

Critics of this legal restriction claim the government is tying the hands of companies trying to effectively defend themselves; proponents warn that legalizing hackbacks would create a cyber Wild West where private companies firing back blindly would lead to chaos with potential foreign policy ramifications. One recent legislative proposal, the most prominent on this issue, is the Active Cyber Defense Certainty (ACDC) Act, which would establish an affirmative defense to CFAA liability for "active cyber defense measures," allowing private hackbacks in limited circumstances.[2]

This paper will proceed as follows. Part I provides policy background on private sector active cyber defense and the relevant domestic and international legal frameworks. Part II outlines three recent proposals for enabling active cyber defense. Part III illustrates what a potential model hackback attack could look like under these proposals. Part IV evaluates the strengths and weaknesses of each proposal. Part V assesses what a model proposal might look like, and whether it would be an improvement over the status quo. Part VI concludes that ACDC and other proposed solutions are too open-ended because any hackback legislation should retain approval authority with federal law enforcement agencies to be granted on a case-by-case basis.

I. Background

This section briefly describes recent developments in cyber policy and prominent attacks on private sector companies, explaining why some want to hack

* J.D., Georgetown University Law Center, 2022; MPP, Harvard Kennedy School, 2018; B.A., Colby College, 2015. The author would like to thank Professor Mary B. DeRosa for her invaluable assistance and mentorship.

1. Nicholas Schmidle, *The Digital Vigilantes Who Hack Back*, New Yorker (Apr. 30, 2018), https://perma.cc/ZLK2-B7FT.

2. Active Cyber Defense Certainty (ACDC) Act, H.R. 3270, 116th Cong. (2019).

back and why the government has prohibited it. It also outlines how the CFAA restricts active cyber defense and discusses the international legal implications if the government were to permit or endorse private sector hackbacks.

A. A Rising Tide of Costly Attacks

In the cyber domain, a general consensus exists that offense has a sizeable advantage over defense.[3] Cyberattacks are relatively low-cost to launch and often difficult to attribute to their source. Defensively, government and private sector companies alike have struggled to modernize and shore up their networks, leaving a plethora of soft targets for malicious actors. The federal government spends over $18 billion per year specifically on cybersecurity,[4] with uneven success disrupting or deterring malicious actors. The SolarWinds attack, for example, a Russian government-backed breach discovered in late 2020, infected networks in at least nine federal agencies—including the State Department, the Department of Homeland Security, and parts of the Pentagon[5]—and may have caused upwards of $100 billion in damage.[6]

Private companies regularly face similar attacks, with only a fraction of the government's resources to defend themselves. Global cybercrime is expected to cost $6 trillion this year, double the total from 2015.[7] By one estimate, there are 2,444 attempted cyberattacks per day,[8] one every 39 seconds. According to IBM the average business cost of a cyberattack is $3.86 million.[9] Former NSA Director Keith Alexander has estimated cumulative U.S. company losses to cyberattacks to be "the greatest transfer of wealth in history."[10] And cybercrime is on the rise—since the start of the global COVID-19 pandemic, the FBI has reported a 300% increase in the number of cybersecurity complaints it receives daily, now up to around 4,000 per day.[11]

Several prominent examples illustrate the havoc a malicious cyberattack can wreak on a company. In 2014, North Korean hackers attacked Sony Pictures in

3. *See* Rebecca Slayton, *What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment*, 41 INT'L SECURITY 72, 72 (2017).

4. Jason Miller, *VA, HHS, SBA Among Biggest Winners in $92B IT Budget Request for 2021*, FED. NEWS NETWORK (Feb. 11, 2020, 8:37 AM), https://perma.cc/HNU7-64ZF ("[T]he White House requested $18.78 billion for governmentwide cybersecurity funding [in Fiscal Year 2021], down slightly from $18.79 billion in 2020."). Information technology funding is classified separately and amounts to over $90 billion per year. *Id.*

5. David Sanger, Nicole Perlroth & Eric Schmitt, *Scope of Russian Hacking Becomes Clear: Multiple U.S. Agencies Were Hit*, N.Y. TIMES (Dec. 14, 2020), https://perma.cc/8CW4-WYB9.

6. Gopal Ratnam, *Cleaning up SolarWinds Hack May Cost as Much as $100 Billion*, ROLL CALL (Jan. 11, 2021, 6:00 AM), https://perma.cc/8AQX-D4C6.

7. Steve Morgan, *Global Cybercrime Damages Predicted to Reach $6 Trillion Annually By 2021*, CYBERSECURITY VENTURES (Oct. 26, 2020), https://perma.cc/2GJM-KTYB.

8. *Hackers Attack Every 39 Seconds*, SEC. MAG. (Feb. 10, 2017), https://perma.cc/A55J-D7CD.

9. IBM SECURITY, COST OF A DATA BREACH REPORT 40 (2020), https://perma.cc/ENV6-R7V4.

10. Josh Rogin, *NSA Chief: Cybercrime Constitutes the "Greatest Transfer of Wealth in History"*, FOREIGN POL'Y (July 9, 2012, 6:54 PM), https://perma.cc/6DHZ-MDZ4.

11. Maggie Miller, *FBI Sees Spike in Cyber Crime Reports During Coronavirus Pandemic*, HILL (Apr. 16, 2020, 3:27 PM), https://perma.cc/2USE-YUR9.

response to the planned release of a movie parodying Kim Jong Un. The attack paralyzed the company for weeks, destroying servers and filching terabytes of confidential data, including Social Security numbers, unreleased movies, and embarrassing emails (the release of which would soon cause the company's co-chair to resign).[12] Then-Director of National Intelligence James Clapper called the Sony breach the "most serious" cyberattack yet against U.S. interests,[13] but its costs paled in comparison to attacks that would soon follow. The 2017 NotPetya ransomware attack cost an estimated $10 billion,[14] including $400 million alone to FedEx and $670 million to Merck.[15] Also in 2017, the WannaCry ransomware attack disabled 200,000 computers in 150 countries, causing an estimated $4-8 billion in damage.[16]

B. The CFAA and the Criminalization of Hacking Back

Facing a rising tide of costly attacks in a domain dominated by offense, some companies want to be able to fight back. The U.S. government can strike back at attacker networks to disrupt attacks and deter adversaries as it did by disabling a Russian troll farm's network to prevent interference with the 2018 election.[17] But a private company launching a similar counterattack into a hacker's network would likely be committing a federal crime by violating the CFAA.[18]

The CFAA is a computer trespass statute that makes it a federal offense to "intentionally access[] a computer without authorization" and cause damage or otherwise obtain "information from any protected computer."[19] The Act defines "protected computer" broadly as a computer "which is used in or affecting interstate or foreign commerce or communication . . ."[20] but because "[a]ny computer that is connected to the internet is . . . part of a system that is inexorably intertwined with interstate commerce,"[21] courts have held that this definition effectively includes "all computers with Internet access."[22] The statute defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information."[23] It does not define "authorization" or "obtain

12. Michael Cieply & Brooks Barnes, *Sony Cyberattack, First a Nuisance, Swiftly Grew Into a Firestorm*, N.Y. TIMES (Dec. 30, 2014), https://perma.cc/M6BM-5T6E.

13. *Sony Hack Most Serious Cyberattack Yet on U.S. Interests: Clapper*, NBC NEWS (Jan. 7, 2015, 11:07 AM), https://perma.cc/2XZQ-HAQL.

14. Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, WIRED (Aug. 22, 2018, 5:00 AM), https://perma.cc/KJQ9-H98V.

15. Kim Nash, Sara Castellanos & Adam Janofsky, *One Year After NotPetya Cyberattack, Firms Wrestle with Recovery Costs*, WALL ST. J. (June 27, 2018, 12:03 PM), https://perma.cc/FR8T-R4GX.

16. John Snow, *Top 5 Most Notorious Cyberattacks*, KASPERSKY DAILY (Nov. 6, 2018), https://perma.cc/HVF9-82VU.

17. *See* Julian Barnes, *Cyber Command Operation Took Down Russian Troll Farm for Midterm Elections*, N.Y. TIMES (Feb. 26, 2019), https://perma.cc/8SAW-8Z26.

18. *See* 18 U.S.C. § 1030.

19. *Id.* § 1030(a)(1)–(2), (5).

20. *Id.* § 1030(e)(2)(B).

21. United States v. Yucel, 97 F. Supp. 3d 413, 419 (S.D.N.Y. 2015).

22. United States v. Nosal, 676 F.3d 854, 859 (9th Cir. 2012).

23. 18 U.S.C. § 1030(e)(8).

information," so courts have generally applied the plain meaning of these terms.[24] It also notably does not include any type of self-defense provision that would exempt unauthorized access to a network by persons or companies under attack from that network.

Thus, while hackback responses could take on a variety of forms, most—if not all—would at least seriously risk violating the CFAA. Several examples of hackback countermeasures could include accessing the attacker's network to disrupt the attack, to destroy stolen data, to establish attribution, or to monitor the hacker to prevent future attacks.[25] By definition, each of these options would require the counterattacker to "intentionally access" an adversary's protected computer "without authorization."[26] Disrupting the attacker's network or destroying stolen information would qualify as causing "damage" as an "impairment to the integrity or availability of data," while monitoring or attribution could only be accomplished by "obtain[ing] information" likely in violation of the CFAA. The Department of Justice's Computer Crime and Intellectual Property Section (CCIPS), which prosecutes cybercrime, adopts this view in its manual advising companies on responding to cyberattacks, stating clearly: "Do Not Hack into or Damage the Source Computer."[27] It goes on to add:

> Although it may be tempting to do so (especially if the attack is ongoing), the company should not take any offensive measures on its own, such as "hacking back" into the attacker's computer—even if such measures could in theory be characterized as "defensive." Doing so may be illegal, regardless of the motive. Further, as most attacks are launched from compromised systems of unwitting third parties, "hacking back" can damage the system of another innocent party.[28]

The CFAA also includes provisions creating civil liability for violations.[29] While it would require serious chutzpah for a malicious hacker to sue a company for striking back, a third-party owner could easily do so, and the potential to violate the CFAA with respect to innocent intermediaries or through misattribution raises the cost for companies considering even narrowly-tailored hackbacks.

II. HACKBACK PROPOSALS

There have been several proposals to modify or reinterpret the CFAA to permit limited hackbacks, and this paper will analyze three of the most prominent. The

24. Shane Huang, *Proposing a Self-Help Privilege for Victims of Cyber Attacks*, 82 GEO. WASH. L. REV. 1229, 1238 (2014).

25. *See* Robert Chesney, *Hackback Is Back: Assessing the Active Cyber Defense Certainty Act*, LAWFARE (June 14, 2019, 5:31 PM), https://perma.cc/9EZA-MP7V.

26. 18 U.S.C. § 1030(a)(1).

27. U.S. DEP'T OF JUST., PROSECUTING COMPUTER CRIMES MANUAL 180 (2010), https://perma.cc/HL95-WWGF.

28. *Id.*

29. 18 U.S.C. § 1030(g).

best-known proposal was the Active Cyber Defense Certainty (ACDC) Act, introduced by Representative Tom Graves in 2017 and again in 2019.[30] ACDC would establish an affirmative defense to CFAA charges for responses that qualify as "active cyber defense measures" (ACDMs).[31] This would allow victims of cyberattacks to access the attacker's computer without authorization, in order to establish attribution, disrupt attacks, and monitor the attacker.[32] A company must first notify the FBI's National Cyber Investigative Joint Task Force and can request voluntary FBI review of a planned hackback, but no government approval or oversight is required.[33] The 2019 bill garnered bipartisan support from 18 cosponsors.[34] A companion bill was not introduced in the Senate, but Senator Sheldon Whitehouse floated the idea, stating that "[w]e ought to think hard about how and when to license hack-back authority so capable, responsible private-sector actors can deter foreign aggression."[35] To become law, the Act would first need to be reintroduced in the current session of Congress. Last summer, members of the Senate Finance Committee introduced legislation entitled the Study on Cyber-Attack Response Options Act, which would instruct the Department of Homeland Security to study potential costs and benefits of legalizing some private hackbacks.[36]

Another, somewhat similar, hackback proposal would also amend the CFAA to create a self-help provision for companies under attack.[37] This idea, proposed in 2014 by Shane Huang in *The George Washington Law Review*, would also codify an affirmative defense exemption to CFAA liability, but suggests slightly different restrictions than ACDC, requiring:

> (1) the counterattack must be necessary and proportional to the threat being mitigated or prevented; (2) the counterattack must be in response to an ongoing or repeated attack; (3) the counterattacker must submit a good-faith justification and notification to the government; and (4) the counterattacker must assume strict liability for all damage to third parties, and liability for all negligently caused unnecessary damage to the original attacker.[38]

ACDC is more specific about the *types* of counterattacks that may be used (disruption, attribution, etc.), while the self-help proposal elides technical details to focus

30. *See* H.R. 3270, 116th Cong. (2019).
31. *Id.* § 4.
32. *Id.*
33. *Id.*
34. Overview of H.R. 3270, C-SPAN, https://perma.cc/DJL4-T792 (last visited Aug. 3, 2022).
35. Derek Hawkins, *The Cybersecurity 202: Sen. Whitehouse says Congress should consider letting companies 'hack back' after cyberattacks*, WASH. POST (Aug. 21, 2018, 7:31 AM), https://perma.cc/B49S-JSLR.
36. Corey Nachreiner, *The Pros and Cons of the Proposed Hack Back Bill*, SC MEDIA (Jan. 28, 2022), https://perma.cc/R86Z-MGBZ.
37. *See generally* Huang, *supra* note 24.
38. Huang, *supra* note 24, at 1259.

on the *principles* that should guide the attacks (necessity and proportionality).[39] Additionally, while each requires government *notification*, neither requires government *approval* or *oversight*.

The third proposal, originating in a Hoover Institution paper written by Jeremy and Ariel Rabkin, would reinterpret the CFAA instead of amending it, finding a "way around the seemingly all-encompassing language of the CFAA."[40] Section 1030(f) of the CFAA notes that the statute "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 any intelligence agency of the United States."[41] The Rabkin proposal posits that "[i]t is entirely plausible for federal agencies to read this language as allowing particular cyber security firms to be 'lawfully authorized' to engage in 'investigative, protective or intelligence activity' on behalf of relevant federal agencies."[42] Under this proposal, the federal government could effectively deputize private firms to help respond to cyberattacks, shielding them from CFAA liability in a way that "would retain government control but harness the resources of the private sector and accommodate the security priorities of private corporations prepared to invest in added security."[43] The report is somewhat circumspect about what types of hackbacks could be authorized, stating that the most promising "simply involve information gathering" but "[w]e suspect that there are a range of viable tactics that such companies could employ."[44] Because this paper focuses on the authorization of a broad range of hackback techniques (beyond mere information gathering), it will analyze an aggressive construction of the Rabkin reinterpretation that could include a broader scope of deputized company hackbacks, including counterstrikes to disrupt attacker networks.[45]

III. WHAT COULD A MODEL HACKBACK LOOK LIKE?

Before analyzing the merits of these proposals, it is helpful to illustrate what a successful real-world hackback could look like. Because hacking back remains illegal, there are few good examples, but a quirk of trademark law recently enabled Microsoft—in coordination with U.S. Cyber Command—to temporarily disable a malicious botnet without running afoul of the CFAA.[46]

---

39. Huang, *supra* note 24, at 1259.

40. Jeremy Rabkin & Ariel Rabkin, *Hacking Back Without Cracking Up*, HOOVER INST. (June 28, 2016), https://perma.cc/4PT2-9479.

41. 18 U.S.C. § 1030(f).

42. Rabkin & Rabkin, *supra* note 40, at 15.

43. Rabkin & Rabkin, *supra* note 40, at 15.

44. Rabkin & Rabkin, *supra* note 40, at 16.

45. To be clear, the Rabkin plan did not yet endorse using this CFAA exemption for aggressive hackbacks – instead reserving that issue for further study. Rabkin & Rabkin, *supra* note 40, at 16. Their "lawfully authorized" reinterpretation of the CFAA, however, does not make this distinction, and by its plain language could legalize any method of hackback. Rabkin & Rabkin, *supra* note 40, at 15. This paper will assess the use of this loophole to authorize disruptive hackbacks as well.

46. *See* Brian Krebs, *Microsoft Uses Trademark Law to Disrupt Trickbot Botnet*, KREBS ON SEC. (Oct. 12, 2020), https://perma.cc/8YLN-2N74.

"TrickBot" is a botnet that has infected more than a million computers since 2016, with Russian-speaking attackers taking control of these "zombie" computers to operate a "malware-as-a-service" business—selling access for malicious purposes, including implanting ransomware.[47] Ahead of the 2020 election, when it was feared that TrickBot could be used to attack voting systems, U.S. Cyber Command and Microsoft both acted to disable it.[48] Microsoft unleashed a cyber "Death Star" against TrickBot, taking defensive measures to purge the malware but also "sinkholing" some of its command and control (C&C) servers.[49] Sinkholing is "a coordinated legal sneak attack"[50] that involves gaining legal control of an attacker's domain and then "sever[ing] the attacker's control over the malware and the systems the malware controls."[51] These domains can "be used to help identify compromised systems: when the malware reaches out to the sinkholed domain for instructions, the new owners can identify those systems and attempt to locate and warn the owners."[52] Eventually, Microsoft "basically changed its phasers from 'stun' to 'kill' . . . a drastic action that could cause systems to crash but will effectively kill the malware when it finds it."[53]

The counterattack was at least temporarily effective, reportedly disabling 94% of TrickBot servers within a week.[54] It demonstrated that Microsoft has the *technical* capability to effectively combat sophisticated hacker networks. But Microsoft was only *legally* able to take this action under the CFAA because the compromised systems "still [bore] the Microsoft and Windows trademarks."[55] Thus Microsoft was able to argue that malicious use "causes extreme damage to Microsoft's brands and trademarks" and obtain a court order from the U.S. District Court for the Eastern District of Virginia that granted it legal control of the servers.[56] Its access and destruction were therefore not "unauthorized" under the CFAA. The TrickBot operation illustrated the will and technical capability of some U.S. companies to hack back effectively, but this legal authority—absent rare trademark exceptions—only applies in narrow circumstances, as most hacked companies obviously do not own the trademark to their attacker's systems. Broader use of these tactics by private companies would require first amending or reinterpreting the CFAA.

47. Shannon Vavra, *Cyber Command, Microsoft Take Action Against TrickBot Botnet Before Election Day*, CYBERSCOOP (Oct. 12, 2020), https://perma.cc/ZBT9-GDJH.

48. *Id.*

49. Krebs, *supra* note 46.

50. Krebs, *supra* note 46.

51. Christopher Budd, *Microsoft Unleashes 'Death Star' on SolarWinds Hackers in Extraordinary Response to Breach*, GEEKWIRE (Dec. 16, 2020), https://perma.cc/CF7C-QUGC.

52. *Id.*

53. *Id.*

54. Tom Burt, *An Update on Disruption of Trickbot*, MICROSOFT (Oct. 20, 2020), https://perma.cc/C4SD-MNL5.

55. Krebs, *supra* note 46.

56. Krebs, *supra* note 46.

IV. EVALUATION OF HACKBACK PROPOSALS

None of the three proposals described broadly authorizes private sector hackbacks without creating unjustifiable risks—to the companies themselves, to innocent intermediaries, and to U.S. foreign policy. The ACDC and Huang proposals contain insufficient oversight provisions and could cause cyber mayhem by allowing unqualified companies to fire back wildly at perceived attackers, potentially drawing innocent parties or the U.S. government into the fray. By exempting only specifically-designated firms from the CFAA, the Rabkin plan mostly avoids the "loose cannon" problem of unqualified companies launching misguided attacks, but deputizing private companies in this manner could implicate U.S. obligations under international law. The Rabkin plan may overall carry the lowest risks, but allowing only a handful of companies to engage in a single, modest form of hackbacks is unlikely to truly move the needle on private sector active cyber defense.

A. The ACDC Act: A Shot in the Dark

"Ain't got no gun, Ain't got no knife, Don't you start no fight" – AC/DC.[57] It is a very dangerous proposition for any private person or company to strike back at a sophisticated, malicious cyber actor, especially if that hacker turns out to be affiliated with a hostile nation state.[58] ACDC may somewhat limit *how* companies can respond in cyberspace, but it fails to sufficiently limit *who* can take action, and *when* it is appropriate to do so. This lack of real oversight almost certainly ensures that the U.S. government would be insulated from responsibility for private hackbacks under international law,[59] but it also creates the potential for cyber mayhem with potential foreign policy implications.

Former NSA Director Mike Rogers once warned that a hackback bill would be "putting more gunfighters out on the street in the Wild West."[60] Under ACDC, many of those gunfighters could be insufficiently trained, inadequately armed, and firing blindly at the wrong targets. Very few American companies have the technical capabilities or resources to go toe-to-toe with a sophisticated hacker group, and in a gray zone where attribution is murky, they could find themselves accidently hacking back at innocent third parties. Even if they hit the right target, they could quickly become outmatched—especially if they find they have engaged a nation state-backed actor—increasing the damage and potentially drawing the U.S. Government into the conflict. Former White House cybersecurity advisor Rob Joyce warned that ACDC could lead to "vigilantism," where even if hackbacks were limited "in a prescribed way, with finite-edge cases . . .

57. AC/DC, T.N.T. Lyrics, https://perma.cc/6Y7R-FHV7.

58. To mix AC/DC song titles, a single Dirty Deed by a company Shooting to Thrill could quickly launch it down the Highway to Hell.

59. *See* Rabkin & Rabkin, *supra* note 40, at 23 (discussing this international law issue in depth).

60. Tim Starks, *Scoop: 'Hack Back' Bill Gets Version 2.0,* POLITICO, (May 25, 2017), https://perma.cc/GG8M-K2GV.

you're still going to have unqualified actors bringing risk to themselves, their targets, and their governments."[61]

The risks of ACDC are best illustrated by several variations on a hypothetical scenario showing how a hackback could go wrong and what it might cost. The year is 2025 and ACDC has been passed into law. Seth Rogen has convinced Sony to make a sequel of "The Interview" (ignoring the protests of movie critics across the nation). Sony recognizes that this may again provoke a North Korean cyberattack, but it has upgraded its cyber capabilities and is willing to take the risk. Several weeks before the movie's release, however, Sony IT discovers that a malicious actor has breached its servers and is in the process of implanting ransomware that could destroy the company's servers or force it to pay a fortune to regain control. Based on some technical signatures and prior history, they suspect the attack is coming from North Korea, but—as in 2014—the hackers claim to be part of an unaffiliated group.

Fortunately, Sony's new-and-improved IT Department has acquired a reverse-engineered version of the Remote Access Tool (RAT) the attackers are using, giving it the capability "to decrypt stolen documents and even to break into the attacker's command and control link—while the attacker is still on line."[62] Sony thus has the technical ability to shut down the attacker's C&C server before it can implant more ransomware. Sony's general counsel, who has read the newly-passed ACDC Act, advises that "disrupt[ing] continued unauthorized activity against the defender's own network" is explicitly permissible as an "active cyber defense measure" as long as it doesn't *intentionally* destroy the adversary's data or *recklessly* cause financial loss.[63] Sony must quickly notify the FBI in advance and wait for it to confirm receipt, but it does not need approval.[64] Armed with this technical and legal advice, Sony's CEO gives the green light.

1. First Outcome: The Best-Case Scenario

This hackback could play out in several different ways. In the best-case scenario, the company has accurately isolated the attacking server and responded with a narrowly tailored and technically sophisticated counterattack. The hackback is successful. The attacker's C&C server is taken offline before the malware can be widely implanted, giving Sony time to contain the damage, quarantine the breach, and patch up any vulnerabilities that have been exposed. The attacker lacks either the motive or the immediate capability for follow-up or escalating attacks. Sony has saved tens of millions of dollars and free speech wins the day as the movie's release continues as planned.

Even in this best-case scenario, however, textual ambiguities within the ACDC pose potential problems. The Act allows a company that is "a victim of a

61. Schmidle, *supra* note 1.
62. *The Hack Back Debate*, STEPTOE CYBER BLOG (Nov. 2, 2012), https://perma.cc/ANU9-L4MR.
63. H.R. 3270, 116th Cong. § 4 (2019).
64. *See id.* § 5.

persistent unauthorized intrusion" to "disrupt" an attack, but does not protect conduct that "intentionally destroys or renders inoperable" information that does not belong to the victim or intentionally causes a persistent internet disruption resulting in damages.[65] Disabling a malicious ransomware attack by a sophisticated attacker is clearly at the core of ACDC's self-defense purpose. But can Sony claim this is a "persistent" intrusion if it was only just discovered? If not, this seems to create a catch-22 where companies cannot quickly hack back to repel an adversary breaking into their systems; instead, they may have to wait until the attacker gains a foothold—and is thus harder to dislodge.

The ambiguity surrounding acceptable "disruptions" is also problematic. Reading the intent provisions strictly, almost any disruptive response that disables an attacker's server—even temporarily—would seem to "intentionally . . . render[] inoperable" information belonging to the server's owner, thus implying the hackback is *not* covered by ACDC.[66] Reading intent loosely, however, a company could cause fairly broad, persistent, and destructive disruptions as long as they do not "recklessly" lead to financial loss.[67] These issues arise even in the best-case scenario, but the problems are magnified when things begin to go wrong.

2. Second Outcome: Mistaken Attribution

Former NSA Deputy Director Rick Ledgett has warned that companies are foolishly optimistic about their ability to accurately attribute cyberattacks, cautioning that "[a]ttribution is really hard. Companies have come to me with what they *thought* was solid attribution, and they were wrong."[68] The attribution process is difficult enough for the NSA and FBI, which deal with countless cyberthreats on a daily basis, learning over time to recognize patterns and technical signatures with the support of other intelligence sources. Private companies do not have a fraction of the experience, expertise, or technical capabilities of the U.S. Intelligence community, and a company making a snap decision to go after what it *thinks* is its attacker may find itself firing back blindly.

In the Sony hypothetical, Sony may believe its attacker is the North Korean government or an affiliate, based on past experience and the type of attack utilized. But without the resources of a U.S. intelligence agency, the company would likely be, at best, making an educated guess. What it *thinks* is a North Korean state-sponsored attack may actually be an unaffiliated Russian hacker group looking to use ransomware to make a quick buck—perhaps having mimicked the known technical signatures of North Korean hackers or pirated a North Korean server to disguise its efforts.

65. *Id.* § 4.
66. *Id.*
67. *Id.*
68. Schmidle, *supra* note 1.

If Sony retaliates against any North Korean-based server, all bets are off. North Korea is likely to respond with an attack against Sony's networks, but Pyongyang may not necessarily draw much of a distinction between an attack coming from an American company versus the American government. In recent years, North Korean hackers have attempted to infiltrate networks at U.S. banks, energy firms, healthcare companies, and other critical infrastructure.[69] North Korea could strike back at Sony, or aim at one of these other targets where it may already have malware implanted. The U.S. Government could feel compelled to intervene to stop a devastating North Korean cyberattack, possibly creating a cycle of escalation. This hypothetical may represent the outer bound of negative consequences for hackback attacks, but the concern is not purely speculative—the month after Congressman Graves first introduced ACDC, former NSA Director Keith Alexander warned journalists that "[y]ou can't have companies starting a war."[70]

3. Third Outcome: Good Attribution, Bad Aim

In a related problem, even if Sony miraculously establishes 100% accurate attribution and aims at the right target, it may not hit it. Sony could somehow have obtained gold-plated intelligence that identifies the specific North Korean hacker group, its physical address, and even the name of the person sitting at the keyboard, but even then it may still hit the wrong target. This is because hackers often launch their attack through numerous "hop points," or intermediary servers between them and the target. "If hackers in Bucharest want to steal from a bank in Omaha, they might first penetrate a server in Kalamazoo, and from there one in Liverpool, and from there one in Perth, and so on, until their trail is thoroughly obscured."[71] Some sophisticated actors may hop as many as 30 times before launching an attack.[72]

North Korean hackers have at times operated "well over a hundred" front businesses in countries such as China, Russia, and Malaysia.[73] North Korean operators in an office building in Pyongyang may "hop" the Sony attack through several dozen unwitting servers along the way. Even if Sony has the technical sophistication to track them through most of these disguises, it may fall short, disabling what it thinks is their Malaysian C&C server, but is actually the network for a hospital in Kuala Lumpur—which the hackers have "hopped" to from their office in Pyongyang. Sony would thus have counterattacked against a Malaysian hospital. ACDC may shield Sony from criminal liability in the United States, but companies hacking back would be regularly violating the domestic law of foreign countries in which the servers are located. By accessing foreign-based servers

69. *See* Troy Stangarone, *North Korea Is Still Trying to Hack US Critical Infrastructure,* DIPLOMAT (Mar. 14, 2019), https://perma.cc/587G-T2M9.

70. Schmidle, *supra* note 1.

71. *Id.*

72. *Id.*

73. Sam Kim, *Inside North Korea's Hacker Army*, BLOOMBERG (Feb. 7, 2018, 4:00 PM), https://perma.cc/9BNM-MGZE.

without authorization, Sony, whether its aim is accurate or not, could be putting its employees at risk of prosecution around the globe.

This problem is often intertwined with attribution issues, and together they illustrate why cyber is a gray zone where it is easier to attack than defend.

4. Fourth Outcome: Escalation Dominance

Ledgett, the former NSA Deputy Director, has "also raised concerns about what military strategists call 'escalation dominance.' Don't pick a fight, the theory goes, unless you know you can win it,"[74] because one of the main challenges of hackbacks "is the difficulty of seeing what a company is up against."[75]

In this scenario, Sony may find that by engaging North Korea's intelligence services, it has bitten off more than it can chew. There are numerous possible permutations—maybe the immediate counterattack fails, maybe it succeeds—but the hackback provokes North Korea into escalating the conflict. What was intended as a limited, low-resourced ransomware campaign morphs into a scorched earth cyberattack, stealing emails, Social Security numbers, and unreleased movies, and frying servers companywide. It is 2014 again but on a larger, more damaging scale.

In this hypothetical scenario, Sony at least knew in advance that this was probably a North Korean attack—so the company should have known what it was getting into. But Sony is a rare example, and most companies launching hackbacks may not actually have any idea who is at an adversary's keyboard, whether it's a lone wolf, a criminal gang, or a sophisticated nation state. This is a "tip of the iceberg" problem, where a company would often have to decide whether or not to counterattack before having any idea what is actually below the waterline. Most U.S. companies are not particularly sophisticated cyber actors, and switching from defense to offense could draw them into a conflict that they do not have the capability to win.

This series of Sony hypotheticals is not intended to suggest that this is a representative example of what an average company would face, nor is it designed to fabricate a parade of horribles exaggerating the risks of enacting ACDC. It is instead an attempt to illuminate some of the challenges—attribution, targeting, escalation dominance—inherent to a landscape where *any* company can decide to strike back at an attacker without effective government oversight. Some companies are technically highly sophisticated and will act responsibly; others are not and will not. ACDC might enable Microsoft to conduct a broad array of effective sinkhole-type attacks against malicious cyber actors, but it could also be responsible for gung-ho twenty-something IT staffers at a small business accidentally crashing a hospital's network when they miss their target—and America has far more gung-ho small business IT staffers than it does Microsofts.

---

74. Schmidle, *supra* note 1.
75. *Id.*

ACDC's core flaw is not that all hackbacks are inherently bad; it is instead a near-complete lack of oversight to allow "good" hackbacks while preventing "bad" ones. ACDC only requires that a company first notify the FBI and wait for the FBI to acknowledge receipt.[76] Presumably, in acknowledging, the FBI could offer some informal advice along the lines of "hey, this planned hackback looks like a disastrous idea," but nothing in the bill requires any entity of the U.S. Government to actually review, approve, or oversee a hackback. This may insulate the U.S. from responsibility under international law,[77] but it also creates the potential for chaos. As multiple former NSA directors and deputy directors have suggested, giving every company a gun is unlikely to make the Wild West any safer.[78]

B. The Huang Self-Help Proposal

Much of this ACDC analysis—including the Sony scenarios—applies to Huang's proposal as well. Overall, the proposals are similar, but ACDC sets out technical guidelines for which hackbacks would qualify as an affirmative defense while Huang focuses more on guiding legal principles.

As a result, Huang's proposal would likely be both more permissive and more uncertain in what it allows. The ACDC is relatively specific: certain hackback purposes are permitted, including attribution, monitoring, and disruption; other actions are explicitly forbidden, including intentionally destroying an adversary's data and intentionally intruding into an intermediary's network.[79] A company that paints between those lines is likely legally protected from criminal liability as long as it does not *recklessly* cause loss or *intentionally* cause damage or impact an intermediary.[80] The Huang proposal, by contrast, includes fewer restrictions but instead imposes strict liability to keep companies from abusing the exemption.[81] There are no permitted or forbidden categories of hackbacks—a company could presumably employ *any* technical methods it assesses to be necessary and proportional, as long as it is willing to assume the financial risk of unintended damage. But this freedom could be constraining, as companies would be forced to make a snap judgement about what is a necessary and proportional response to a rapidly developing cyber intrusion, and then—no matter how cautious or conservative it is in planning or execution—assume strict liability for any damages the hackback causes. An exception exists for "necessary" damage to the attacker, but "necessary" is yet another legal term difficult to assess in the heat of an attack.[82]

---

76. *See* H.R. 3270, 116 116th Cong. § 5 (2019).

77. *See* Rabkin & Rabkin, *supra* note 40, at 23 (discussing the international law implications of these proposals in depth).

78. *See e.g.,* Schmidle, *supra* note 1 ("Ledgett, the former N.S.A. deputy director, told me that legalizing hacking back in the private sector would be 'an epically stupid idea.'").

79. *See* H.R. 3270, 116th Cong. § 4 (2019).

80. *Id.*

81. *See* Huang, *supra* note 24, at 1259.

82. *See* Huang, *supra* note 24, at 1259.

The relative ambiguity regarding what exactly is permitted under Huang's proposal could lead to some very dangerous outcomes, but on the whole the necessary and proportionate requirement—combined with the Damocles' Sword of strict liability—could motivate companies to proceed with caution. ACDC in effect tells companies that as long as they stick to the permitted types of attack and are not completely reckless, they may fire at will without significant risk of criminal liability. Under Huang's proposal, however, a counterattacking company can seemingly respond however it wants, as long as it believes the hackback to be necessary and proportional. Leaving the interpretation of what is "necessary and proportional" to each individual company is dangerous. Most companies would approach this analysis responsibly; others would not. Without technical restrictions on the types of permissible hackbacks, less responsible companies may overestimate the scale of the threat and respond with more force than is permitted under ACDC, increasing the potential for collateral damage and escalation.

On balance, however, companies may behave more cautiously under Huang's proposal, as its strict liability forces companies to pay for any damages to third parties and any "unnecessary damage" to the attacker.[83] Companies are profit-driven, and may often find that under strict liability the potential costs of a hackback do not justify the benefits. And given that hackbacks found not to be necessary and proportionate would also expose the company to criminal liability under the CFAA, many might tread lightly until courts begin to develop what "necessary" and "proportionate" mean when it comes to active cyber defense.

While Huang's proposal may discourage some reckless attacks that ACDC does not, it suffers from the same fatal flaw in only requiring that "the counterattacker must submit a good-faith justification and notification to the government," but not that the government must *approve* or *oversee* the attack. As with ACDC, this lack of oversight poses the risk of the feared "Wild West" scenario, where government has little control over *who* is attacking and *how* until the damage is already done.

C. The Rabkin Proposal

The Rabkin proposal is the most creative but least developed of the three analyzed in this paper. It centers around reinterpreting § 1030(f) of the CFAA to allow law enforcement or intelligence agencies to designate companies to launch hackbacks exempted from CFAA liability, by letting the companies in effect "borrow" their law enforcement authority.[84] This legal theory is untested, but could enable the FBI or U.S. Cyber Command to deputize trusted, sophisticated companies to assist with cyber operations without creating a "Wild West" — instead of freely passing out guns at the saloon, the sheriff would be deputizing

83. *See* Huang, *supra* note 24, at 1259.

84. Stewart Baker, *The HackBack Debate Revisited*, STEPTOE CYBER BLOG (Mar. 4, 2013), https://perma.cc/7MTP-YMFP.

only John Wayne and a few other trusted associates. The government approval requirement is essential to a workable hackback regime, but this application of the Rabkin proposal[85] would devolve "deputizing" authority to too low a level, would fail to specify technical and proportionality limits for acceptable hackbacks, and would likely make the U.S. Government responsible under international law for private company hackbacks.

Rabkin's reinterpretation argument derives from a 2013 podcast discussion between law professor Orin Kerr and former NSA official Stewart Baker.[86] Kerr and Baker posited that under § 1030(f) private companies could reach out to the Department of Justice to "borrow" their law enforcement authority under the CFAA to authorize a hackback.[87] This theory receives lukewarm support at best from the plain language of the statute, which clarifies that the CFAA "does not prohibit any lawfully authorized investigative, protective or intelligence activity *of a law enforcement agency*" (emphasis added).[88] Section 1030(f) has existed in its current form since 1986, and in the 35 years since, this author has been unable to find any instances of a law enforcement agency invoking this authority to authorize a private company hackback. As Kerr and Baker note, "there's no cases interpreting [1030(f)], so exactly what it means really is kind of a mystery."[89]

If Kerr and Baker are wrong about § 1030(f) interpretation, the Rabkin proposal is dead in the water—unless, of course, it is proposed as a clarifying amendment to the CFAA. Either way, this new interpretation poses new problems. While the ACDC Act requires notification specifically to the FBI's national cybersecurity task force, § 1030(f) applies equally to any "law enforcement agency of the United States, a State or a political subdivision of a State, or of any intelligence agency."[90] 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)]."[91] This interpretation thus raises significant policy and federalism concerns since it would presumably enable the Alameda County Sheriff to authorize a private company to launch a destructive hackback against a North Korean state actor. Most sheriffs would not be this reckless, but as with "necessary and proportionate" this interpretation creates a lowest common denominator problem: allowing the least responsible of America's

85. Again, in fairness to the Rabkins, their proposal was commendably cautious. This version has pushed their CFAA loophole idea toward its logical limit, but further than they were willing to endorse without further study.

86. *See* Baker, *supra* note 84.

87. *See* Baker, *supra* note 84.

88. 18 U.S.C. § 1030(f).

89. *Cybersecurity and Hacking Back*, STEPTOE CYBER BLOG, at 50:37 (Feb. 20, 2013) (podcast link available at https://perma.cc/7MTP-YMFP).

90. 18 U.S.C. § 1030(f).

91. *Cybersecurity and Hacking Back*, *supra* note 89, at 49:40.

18,000[92] federal, state, and local law enforcement agencies to authorize international cyberattacks could largely defeat the purpose of requiring government authorization in the first place.

Deputizing private companies to conduct hackbacks could in some circumstances trigger U.S. obligations under international law. The companies themselves would not be liable under international law, although they could find themselves liable under the domestic law of foreign countries targeted by their hackbacks. This is because, according to the Tallin Manual (which does not have the force of law), under international law "cyber operations conducted by non-State actors that are not attributable to States (Rules 15 and 17) do not violate the sovereignty of the State into which they are launched (Rule 4), constitute intervention (Rule 66), or amount to a use of force (Rule 68) because these breaches can be committed only by States."[93] But if hackbacks are deemed "attributable" to the U.S., it could be held responsible under international law.

According to the International Law Commission's Articles on the Responsibility of States for Internationally Wrongful Acts, the actions of non-State actors "shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct."[94] In 2016, State Department Legal Adviser Brian Egan expressed the U.S. view that "cyber operations conducted by non-State actors are attributable to a State under the law of state responsibility when such actors engage in operations pursuant to the State's instructions or under the State's direction or control."[95] By requiring only government *notice* in advance, ACDC and Huang's proposal likely steer clear of this "instructions, direction, or control" test. But Rabkin's plan to have law enforcement agencies designate or deputize companies, explicitly justifying it as "lawfully authorized . . . activity of a law enforcement agency,"[96] is likely to constitute state control under this standard. Even if the FBI is not actively directing or controlling the private sector hackbacks, 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.

Fortunately, even if all Rabkin hackbacks were attributed to the U.S. government, a vast majority are unlikely to violate international law as it is currently understood. Cyberattacks can violate international law in three primary ways:

92. U.S. DEP'T OF JUST., NATIONAL SOURCES OF LAW ENFORCEMENT EMPLOYMENT DATA 1 (2016), https://perma.cc/9GKZ-XKFC.

93. TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 175 (Michael N. Schmitt ed., 2013).

94. Kristen Eichensehr, *Would the United States Be Responsible for Private Hacking?* JUST SEC., (Oct. 17, 2017), https://perma.cc/NQJ3-NYEK.

95. *Id.*

96. 18 U.S.C. § 1030(f).

(1) by causing physical damage or injury sufficient to qualify as a use of force or armed attack under Articles 2(4) or 51 of the U.N. Charter; (2) by violating the prohibition against coercive intervention in the internal or external affairs of other states; and (3) by breaching a foreign state's sovereignty by severely disrupting its cyber infrastructure or interfering with its inherently governmental functions.[97] While it is not entirely impossible, it is nearly unimaginable to envision a private sector hackback—approved in advance by the U.S. government—that would be devastating or nefarious enough to violate one of these three principles of international law.

Rabkin's plan leaves that door ajar only slightly by declining to impose any limits on the permissible technical methods or scale of a hackback—presumably leaving these guidelines to be set by the deputizing law enforcement agency.[98] By contrast, ACDC closes the door entirely by only decriminalizing hackbacks that monitor an adversary or *temporarily* disrupt an attack,[99] explicitly proscribing counterattacks that could cause physical damage or persistent network disruptions.[100] But unless the FBI becomes grossly negligent in managing its deputies under the Rabkin plan, hackbacks are highly unlikely to implicate the U.S. in violations of international law.

While the Rabkin option proposes no technical restrictions or guiding legal principles for hackbacks, in practice it would be by far the most modest of the three proposals—assuming it can first overcome the legal hurdle of reinterpreting the CFAA in a way no one has done before. ACDC and the Huang proposal endow private companies with broad authority to conduct hackbacks without significant government oversight. But the Rabkin plan maintains hackback authority in government hands, only to be doled out to trusted companies in limited circumstances. Proponents of a broad hackback authority would argue correctly that only a tiny fraction of companies would benefit under Rabkin, but this proposal would also dramatically reduce the potential costs inherent to the broader plans. Of the three options, the Rabkin proposal carries the lowest reward but also the lowest risk.

V. ANALYSIS: DEVELOPING A HYBRID OPTION

None of these proposals is perfect, nor should they be adopted as currently written. ACDC and the Huang proposal grant overly broad authority, while the Rabkin plan is too vague and rests on shaky legal ground. This author is not convinced—nor are numerous national security and technical experts[101]—that any

97. *See generally* TALLINN MANUAL, *supra* note 93.

98. Rabkin & Rabkin, *supra* note 40, at 15–16.

99. As mentioned previously, the Act is relatively ambiguous regarding acceptable disruptions, but forbids responses that "intentionally result[] in the persistent disruption to . . . internet connectivity resulting in damages." H.R. 3270, 116th Cong. § 4 (2019).

100. *Id.*

101. S*ee, e.g.*, Rob Lemos, *Why the Hack-Back is Still the Worst Idea in Cybersecurity,* TECH. BEACON, https://perma.cc/6ES8-M6RV.

hackback bill carving out a broad CFAA exemption for companies would solve more problems than it causes. Any hackback legislation should be significantly narrowed to retain private hackback authority with federal law enforcement, rather than devolving it to the companies themselves. This paper recommends a hybrid approach that combines ACDC's detailed technical guidelines with Rabkin's government approval restriction. In practice, it would lead to dramatically fewer hackbacks than ACDC proponents envision, but that is a feature, not a bug, of the hybrid plan.

This hybrid proposal would take the legislative text of ACDC and significantly upgrade its notice (Section 5) and voluntary preemptive review (Section 6) provisions. In the current version, Section 5 requires only that "[a] defender who uses an active cyber defense measure under the preceding section must notify the FBI National Cyber Investigative Joint Task Force and receive a response from the FBI acknowledging receipt of the notification prior to using the measure."[102] The statute provides some guidance about information that a notification should include, including the intended target, planned response, and precautions to prevent unintentional damage, but does not require government approval.[103] Section 6 creates a pilot program for voluntary preemptive review, providing in § 6(b) that:

> A defender who intends to prepare an active defense measure under section 4 may submit their notification to the FBI National Cyber Investigative Joint Task Force in advance of its use so that the FBI and other agencies can review the notification and provide its assessment on how the proposed active defense measure may be amended to better conform to Federal law, the terms of section 4, and improve the technical operation of the measure.[104]

This hybrid proposal would combine Section 5's notice provision with Section 6's preemptive review provision and significantly upgrade the review requirement. Section 6(b) would be amended to require that a defender *must* "submit their notification … in advance" (rather than *may*). The company *must* also receive approval from the FBI before commencing its response, *must* update the FBI regularly on its progress, and *must* at any point be willing to immediately cease or modify its counterattack at the direction of the FBI.[105] The FBI would in turn be required to regularly report to Congress on how often it has granted this authority.[106]

Instead of passing the hackback ball directly from Congress to thousands of American companies, this proposal instead places it in the FBI's court. Whether

---

102. H.R. 3270, 116th Cong. § 5 (2019).

103. *Id.*

104. *Id.* § 6.

105. This would presumably preempt Section 5's notice requirement, but the § 5(b) "Required Information" for a notification should also be required for a § 6(b) advance review. *See id.* § 5.

106. This would require only a slight modification of § 7(8).

the FBI will actually put it into play is an open question. It is entirely possible that the FBI distrusts company hackback abilities and never actually approves a request, in which case the bill would be a waste of ink, but would at least not change the status quo for the worse.

Alternatively, the FBI might use this authority to partner with tech giants—the Microsofts and Googles—to harness private sector know-how and resources as force multipliers to deter and defend against malicious cyberattacks. If it decides to go one step further, it could also work with advanced private cybersecurity companies—the FireEyes and Mandiants—as trusted partners. When a Sony (or another non-cybersecurity company) is breached, it could (as many often do) hire one of these cybersecurity companies to assess and contain the damage. Under this new authority, the cybersecurity company could, as part of its mission, request FBI approval to trace the attacker back to its own network and then attribute or disrupt the attack. The FBI is far more likely to trust FireEye to carry out this type of hackback than it is to trust Sony. In any event, it is highly unlikely that the FBI will on more than rare occasions approve disruptive hackback requests not made by sophisticated cybersecurity or technology companies, avoiding the feared "Wild West" scenario.

Critics would likely argue this proposal is a half-measure that would not help a majority of companies seeking a right to cyber self-defense. Those critics would be correct. But that is by design—a majority of companies do not have the technical competence to respond effectively against sophisticated hackers, and should not be allowed to just give it a try at their own discretion, unless they can first demonstrate to the FBI that they have a workable plan. It is certainly possible that under this plan the FBI would be overly cautious and reject even the most prudent and effective hackback requests. In that case, the bill would be worthless, but it would not negatively affect the status quo. But if Congress is considering legalizing some hackbacks, it is far more responsible to bestow that decision-making authority on a centralized group of FBI cybersecurity experts, who may approach it too conservatively, than on *every American company*, some of which would undoubtably approach it too aggressively. If the FBI's annual reports show that it has only approved a fraction of requests, but with overwhelming success, Congress could then consider scaling the hackback program up—a far better potential option than (under ACDC) reports of companies gone wild forcing Congress to scale down or cancel hackback authority.

Some critics on the other side might argue that the FBI review provisions *still* provide insufficient checks on companies—perhaps the FBI could be overly aggressive or too lax in exercising oversight. But this ACDC hybrid requires annual reports to Congress and the bill expires in two years if not reauthorized.[107] With FBI oversight comes public responsibility for the Bureau for botched attacks, and it seems far more likely that it will err on the side of caution rather than aggression.

107. *Id.* §§ 7(8), 9.

In the end, this restrained hybrid proposal is unlikely to be a game-changer, but it also probably would not hurt. It is indeed a half-measure, but with so many dangers and unknowns, a half-measure is more prudent than opening up a massive legal loophole in the CFAA and hoping that companies do not misuse or abuse it. Far better to have each hackback pre-reviewed by experts on a case-by-case basis than to live in fear of the lowest common denominator of private sector IT departments doing something reckless or foolish. Under this proposal, any company can request hackback authorization, but only those with feasible and responsible plans are likely to receive it.

CONCLUSION

Overall, both sides have a point, but this paper errs on the side of hackback skeptics such as former NSA Directors Rogers and Alexander. Proponents of hackbacks are correct that at least some companies are highly sophisticated and technically capable, and that authorizing them to hack back could serve as a force multiplier to protect American businesses. But hackback critics are right to point out the potentially disastrous consequences of broadly authorizing companies to fire back blindly at mysterious attackers. For the current legislative proposal, ACDC, the risk is not worth the reward. But it is also possible to significantly scale back the bill to keep authority in government hands, only to be shared in specific circumstances and with strict oversight. Under this hybrid proposal, the FBI would have the opportunity to test out limited hackback operations in coordination with America's most technically sophisticated companies before considering whether to grant this authority more broadly to the American business community.