Marquette Intellectual Property Law Review

Volume 24 | Issue 1 Article 3

Winter 2020

If the Law Can Allow Takebacks, Shouldn't it Also Allow Hackbacks?

Adam Rodrigues

Follow this and additional works at: https://scholarship.law.marquette.edu/iplr

 Part of the Intellectual Property Law Commons, Internet Law Commons, Privacy Law Commons, and the Science and Technology Law Commons

Recommended Citation

Adam Rodrigues, *If the Law Can Allow Takebacks, Shouldn't it Also Allow Hackbacks?*, 24 Marq. Intellectual Property L. Rev. 1 (2020).

This Article is brought to you for free and open access by the Journals at Marquette Law Scholarly Commons. It has been accepted for inclusion in Marquette Intellectual Property Law Review by an authorized editor of Marquette Law Scholarly Commons. For more information, please contact megan.obrien@marquette.edu.

IF THE LAW CAN ALLOW TAKEBACKS, SHOULDN'T IT ALSO ALLOW HACKBACKS?

ADAM RODRIGUES

I. INTRODUCTION

In 2004, the Computer Emergency Response Team Coordination Center gave up tracking cyberattacks after tracking several hundred thousand successful attacks a year for several years.[1] In that same year, the Department of Defense (DoD) reported that it recorded several million scans of its computers every day by potential attackers.[2] In the years since, hacking efforts have only grown in scale and sophistication.[3]

This unprecedented level of espionage helps provide some context for the United States' current intellectual property crisis. In 2008, the U.S. government estimated the loss in economic value from cyberespionage to be upwards of $1

1. CLAY WILSON, CONG. RESEARCH SERV., RL32114, BOTNETS, CYBERCRIME, AND CYBERTERRORISM: VULNERABILITIES AND POLICY ISSUES FOR CONGRESS 7–8, 28 (2008).

2. JOHN ROLLINS & CLAY WILSON, CONG. RESEARCH SERV., RL33123, TERRORIST CAPABILITIES FOR CYBERATTACK: OVERVIEW AND POLICY ISSUES 17 (2007).

3. Devon Milkovich, *15 Alarming Cyber Security Facts and Stats*, CYBINT (Sept. 23, 2019), https://www.cybintsolutions.com/cyber-security-facts-stats/ [https://perma.cc/G8A9-7F57] ("The cybersecurity industry is rapidly growing every day."). "As more specialists join the ranks, more malware is being launched than ever before, with approximately 230,000 new malware samples/day." *Devon Milkovich*, CYBINT, https://www.cybintsolutions.com/author/devon-milkovichbarbri-com/page/2/ [https://perma.cc/8G6L-3QDJ] (last accessed Feb. 23, 2020).

trillion.[4] In March of 2018, the United States Trade Representative, who led a seven-month investigation into China's intellectual property theft, found that Chinese theft of American IP currently costs between $225 billion and $600 billion annually.[5] Just twenty years ago, such looting could only have happened through military occupation.[6] Today, China does not need to storm our borders and steal our files. They only need computers and a connection to the Internet.

In response to this growing problem, the purpose of this note is to advocate that the legalization of privatized active defense is a better approach for deterring this growing cybercriminal enterprise. Current deterrence efforts are not working. Maintaining a conservative reading of the Computer Fraud and Abuse Act (CFAA) and telling companies they are only allowed to either bolster their defenses[7] or turn their concerns over to the government is no longer sustainable.[8] Companies need more freedom to respond at the point of cyberattack to better deter cybercriminals.

II. DEFINING AND DISTINGUISHING PRIVATIZED AND PUBLIC ACTIVE DEFENSE

As a first point, it is important to note that the government engages in active defense.[9] The Pentagon has already come to the conclusion that solely passive defense does not provide sufficient protection for military secrets.[10] In its 2011 report entitled *The Department of Defense Strategy for Operating in Cyberspace*, the DoD openly used the term "active defense" and defined it as "synchronized, real-time capability to discover, detect, analyze, and mitigate

4. Alexander Melnitzky, *Defending America Against Chinese Cyber Espionage Through the Use of Active Defenses*, 20 CARDOZO J. INT'L & COMP. L. 537, 566 (2012).

5. Sherisse Pham, *How Much Has the U.S. Lost from China's IP Theft?*, CNN BUS. (Mar. 23, 2018), https://money.cnn.com/2018/03/23/technology/china-us-trump-tariffs-ip-theft/index.html [https://perma.cc/27HW-JTE2].

6. Melnitzky, *supra* note 4, at 566.

7. Steptoe, *The Hackback Debate*, CYBERBLOG (Nov. 2, 2012), https://www.steptoecyberblog.com/2012/11/02/the-hackback-debate/ [https://perma.cc/76K6-YTYS] (arguing that the CFAA's intended meaning of exceeding authorized access is to prohibit hacking back).

8. *Episode 240: If Paris Calls, Should We Hang Up?*, THE CYBERLAW PODCAST (Nov. 18, 2018), https://podcasts.apple.com/us/podcast/episode-240-if-paris-calls-should-we-hang-up/id830593115?i=1000424171542 [https://perma.cc/AB7G-WM3U]. Mieke Eoyang notes that through her research in the *To Catch a Hacker Report*, only about 15% of cyber incidents are reported, and of those, only 0.3% result in a conviction. *Id*.

9. Lyu Jinghua, *A Chinese Perspective on the Pentagon's Cyber Strategy: From 'Active Cyber Defense' to 'Defending Forward'*, CARNEGIE ENDOWMENT FOR INT'L PEACE: LAWFARE BLOG (Oct. 19, 2018), https://carnegieendowment.org/2018/10/19/chinese-perspective-on-pentagon-s-cyber-strategy-from-active-cyber-defense-to-defending-forward-pub-77540 [https://perma.cc/Y4M8-3AMK].

10. *See id*.

threats and vulnerabilities,"[11] so as "to prevent intrusions onto DoD networks and systems."[12] It has been used widely since and was even broadened in the most recent report published in 2018.[13] Active defense, then, is not as new or extreme as some might think it to be.[14] The government has already decided it is in the nation's best interests to employ active defense, and that it can do so in a way that does not escalate into an international catastrophe. Accordingly, the point of this note is to argue the same could be said for allowing the use of active defense in the private sector.

III. PRIVATIZED ACTIVE DEFENSE AS EQUITABLE REMEDY

A primary reason for allowing private companies to "hackback"[15] is that it is an equitable response. The American legal system has always provided room for people to be able to take action in defending their personal property and possessions.[16] This is a justification defense—a category of legal defense in which something that would usually be considered unlawful is considered lawfully *justified* for moral and/or utilitarian purposes.[17] In this case, it feels morally wrong to not allow someone to defend their possessions. It is recognized that people have a right to their property, and therefore allowing someone to defend their property against theft is the right thing to do. Additionally, a great deal of social harm would come if criminals knew people were not allowed to resist thieves. Most importantly, though, for the defense

11. *Department of Defense Strategy for Operating in Cyberspace*, NIST: COMPUTER SECURITY RESOURCE CTR. 7 (July 2011), https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf [https://perma.cc/8RU7-SGJM].

12. *Id*. at 6.

13. Jinghua, *supra* note 9.

14. *Episode 19: HackBack*, MALICIOUS LIFE (Mar. 7, 2018), https://podcasts.apple.com/us/podcast/hack-back/id1252417787?i=1000409163160 [https://perma.cc/P6BB-662J]. Sam Curry, Cybereason's Chief Product Officer stated that "there's a cold war online in a very cyber turbulent space and its multipolar. . . . So I don't want to see a world where everyone feels like . . . it's a Mexican standoff . . . and someone pulls the trigger." *Episode Transcript: HackBack*, MALICIOUS LIFE, https://malicious.life/episode/episode-19/ [https://perma.cc/668J-RAM5] (last visited Jan. 14, 2020).

15. Here, a "hackback" considers any action by the cyber victim that goes beyond purely defensive measures. *See Active Defense: It Ain't 'Hacking the Hackers',* BRAKEING DOWN SECURITY PODCAST (Nov. 18, 2014), https://brakeingsecurity.com/size/5/?search=adhd [https://perma.cc/R9LK-XVY5]. However, it is important to mention that in considering offensive measures, some consider a "hackback" to be inherently more offensive than "active defense." *See id*. For more discussion on what type of offensive measure is intended in this note, see *infra* Part V.

16. *Justification*, BLACK'S LAW DICTIONARY (11th ed. 2019), Westlaw (defining defensive-force justification as "[a] justification defense available when an aggressor has threatened harm to the particular interest that is the subject of the defense—usu. to the actor (self-defense), to other persons (defense of others), or to property (defense of property).").

17. *Id*.

of property, is that much of the deterrent value for this defense hinges on the capacity for *instant response, as that is not something law enforcement can offer*. As the National Rifle Association (NRA) puts it, "when seconds count, the police are only minutes away."[18]

An important underlying point to a justification defense is whether or not the defensive action in question actually falls within the established parameters for that defense and *is* in fact justified. That is ultimately the question here. If privatized active defense were perfectly analogous to defense of property, there would be no reason to debate whether or not it can be lawfully justified. As it is, there is extensive debate on this point. In fact, this is arguably *the* point of disagreement on whether the U.S. should legalize privatized hackbacks. With that in mind, the remainder of this note will argue privatized active defense is analogous enough to the equitable rationales for defense of property to merit its legalization.

IV. THE ATTRIBUTION PROBLEM ISN'T WHAT IT USED TO BE

Proper attribution is a core component to satisfying a defense of property claim.[19] This includes not harming or causing an unreasonable risk of harm to innocent third parties.[20] Consequently, a victim cannot justify tackling someone running down the street if *she thinks* that person is the person who just stole her purse. She needs to *in fact* tackle the right person to justify her actions, and even then, it could be up to her lawyer and the jury to determine if she subjected any other parties to an unreasonable risk of harm (such as if she pushed other people out of the way during the chase).[21]

Opponents of hackbacking invariably point out that identifying a cybercriminal is not nearly so straightforward. Unlike the physical world, a cyber victim cannot simply look and see the person who breaks into her server, "runs off" with her data, and then chase down and "tackle" that person. In reality, a cyber victim usually does not even know anything has been stolen for weeks or months after the incident.[22] Consequently, this can often lead to the

---

18. *Episode 155: Debate with Greg Nojeim and Jamil Jaffer*, THE CYBERLAW PODCAST (Mar. 19, 2017), https://podcasts.apple.com/us/podcast/debate-with-greg-nojeim-and-jamil-jaffer/id830593115?i=1000437540885 [https://perma.cc/5W62-9MS8].

19. A person may also act in defense of property unless the act creates an unreasonable risk of causing harm to innocent third parties. JOHN KIMPFLEN & KARL OAKES, 86 CORPUS JURIS SECUNDUM TORTS § 30 (2019).

20. *Id.*

21. *Id*.

22. Jeremy Rabkin & Ariel Rabkin, *Hacking Back Without Cracking Up* 11 (Hoover Institution, Aegis Paper Series No. 1606), https://www.hoover.org/sites/default/files/research/docs/rabkin_webreadypdf.pdf [https://perma.cc/LS7D-FYSY].

wrongful attribution of a cybercrime to an innocent third party. Because of this heightened risk of subjecting innocent third parties to harm, detractors argue hackbacking should not be legalized.

However, the concern of proper attribution has been dissipating in recent years. In a recent interview, the general counsel for the Government Communications Headquarters (GCHQ), the British equivalent to the National Security Agency (NSA), had this to say about attribution: "I think the idea that attribution in cyberspace is somehow this impossible task that we shouldn't even try to get past . . . something that people involved in this area have moved away from some time ago."[23] He went on to mention the "recent attributions of the GRU generally, the NotPetya attacks, [and] WannaCry [attacks]" are evidence that "we've demonstrated this can be done."[24] To give another government example, in 2016, attribution was "reliable enough for the US government to accuse named individuals of a particular attack in the recent indictment of Iranian government employees for cyber attacks against US banks and an attempted attack on a dam."[25]

Granted, attribution is still not as reliable in cybercrime as it is in the physical world. But given how much it has improved in recent years, permitting the vast resources of the American private sector to freely contribute to addressing this problem could accelerate the process even more. For one, companies are more motivated to find their attacker because they have more of a vested interest in protecting their data than the government does. They are the ones facing the brunt of this harm.[26] Additionally, there are simply too many attacks for the government to handle. Permitting the private sector to begin actively defending its own intellectual property could provide an immense amount of manpower to help attribute these attacks to more and more offenders.

Moreover, it is not as if private security firms are not already doing this. In 2014, the cybersecurity firm CrowdStrike published a report that included "not only external pictures of the Shanghai office building where a [hacking] unit

---

23. *Episode 235: It's a Bird, It's a Plane, It's . . . Doug?*, THE CYBERLAW PODCAST (Oct. 14, 2018), https://podcasts.apple.com/us/podcast/episode-235-its-a-bird-its-a-plane-its-doug/id830593115?i=1000421889072 [https://perma.cc/S6VA-WC7Y] (noting that the interviewee went by codename "Doug" for security purposes).

24. *Id*. The GRU is the "intelligence arm of the Russia's armed forces." S.J., *What is the GRU?*, THE ECONOMIST (Sept. 11, 2018), https://www.economist.com/the-economist-explains/2018/09/11/what-is-the-gru [https://perma.cc/9VXA-TXZD].

25. Rabkin & Rabkin, *supra* note 22, at 11.

26. Zach West, *Young Fella, If You're Looking for Trouble I'll Accommodate You: Deputizing Private Companies for the Use of Hackback*, 63 SYRACUSE L. REV. 119, 134 (2012) ("In many cases, this intellectual property represents the future of the company; at least one British firm went bankrupt after a foreign nation stole their signature technology.").

operated but also photographs and names of individual hackers involved in its operations."[27] Mandiant, another firm, published a more detailed report on another hacking unit in Shanghai.[28] Freely supporting companies in hiring such firms would multiply the chances of producing similar results.

A. What is the harm, really?

Despite past or future improvements in attribution, opponents to hackbacking would likely still argue that harming an innocent third party is not allowable regardless of how unlikely it becomes.[29] It is therefore appropriate to consider just what exactly *is* the potential harm an innocent third party faces via hackback.

In a 2017 debate hosted by the Center for Strategic and International Studies (CSIS), Greg Nojeim points out to his opponent, Stewart Baker, that a third party has no way to tell the difference between a hackback and a standard hack or how to tell a "good guy" from a "bad guy."[30] Because of this, a third party—Nojeim uses the example of a hospital—may feel attacked and trigger its extensive defensive response protocols in response to someone who may have good intentions.[31]

But Baker points out this argument creates a hypothetical unlike anything that would occur in the real world.[32] If a system has been compromised enough for a hacker to store data on that server, there would be multiple people accessing the server on any given day.[33] The idea, then, that the person hacking back would singularly cause the innocent party to freak out is simply untrue.[34] The bigger problem the hospital should recognize is that their system is compromised and therefore being utilized as a pathway for cyber espionage, likely by numerous bad actors.[35] Baker then points out, that in trying to determine the most equitable solution, it seems odd to be more concerned about a party whose system is so poorly defended it has become a hub of cyber espionage, than for a victim accessing that system attempting to retrieve stolen data.[36]

---

27. Rabkin & Rabkin, *supra* note 22, at 10.
28. *Id*.
29. *Episode 155: Debate with Greg Nojeim and Jamil Jaffer*, *supra* note 18. In his final rebuttal, Greg Nojeim uses this sentiment to sum up his concerns with Stewart Baker's position. *Id*.
30. *Id*.
31. *Id*.
32. *Id*.
33. *Id*.
34. *Id*.
35. *Id*.
36. *Id*.

Moreover, there are two important underlying problems with Nojeim's example. Firstly, there is an over-weighing of the privacy concern caused by the breach itself. Secondly, there is the underlying fear that further, direct harm to the hospital is inevitably going to be caused because of the breach. These two concerns will be dealt with in turn.

B. Internet privacy and hackbacking as justified exigent response

There is a broader Fourth Amendment privacy issue with many anti-hackbackers' concerns. Most importantly, the protection against illegal searches and seizures of the Fourth Amendment do not extend to private actors,[37] and most states have not passed laws providing further protection.[38] Thirty-seven states allow the recording or "interception" of private communications at the consent of one party to an exchange; only twelve states require the consent of both parties.[39] There is, then, no inherent Fourth Amendment bar to a private investigator searching the property of a third party in hopes of tracking down his primary suspect. Of course, this does not mean this behavior could not run afoul of other laws (such as breaking and entering) but serves to show that the third party's interest, if breached by a private party, is not as protected as one may expect.

Further, even if the search was being conducted by government actors, they are allowed to search a third party's property if there are "exigent circumstances."[40] The typical example of this is if officers are in "hot pursuit" of a suspect who then retreats into someone's home.[41] The three things courts consider to make this determination are (1) if there is a concern of the imminent destruction of evidence, (2) the need to prevent a suspect's escape, and (3) safety for both the pursuing officer and the general public.[42] Hackbacking arguably meets these first two criteria. Unless private citizens are able to respond close to the moment of detecting intrusion, the suspect is likely to escape and the evidence of their crime—the stolen data—will disappear with it.

It could be difficult, however, to convince a court that the third criterion applies to a hackback. The type of safety this criterion typically considers is physical in nature, and the gap between cyber harms and kinetic harms is, to some, too wide to merit emergency action. There is reason, though, to believe

37. Burdeau v. Mcdowell, 256 U.S. 465, 476 (1921).

38. *See* Corey A. Ciocchetti, *The Privacy Bailout: State Government Involvement in the Privacy Arena*, 5 ENTREPRENEURIAL BUS. L.J. 597, 607, 609, 610 (2010).

39. Ciocchetti, *supra* note 38, at 609–10.

40. Warden v. Hayden, 387 U.S. 294, 298 (1967).

41. *Id*. at 310.

42. Minnesota v. Olson, 495 U.S. 91, 92 (1990).

the current pillaging of American intellectual property amounts to a kinetic harm meriting the more proactive approach of a hackback. As noted earlier, in the past, it would require military occupation to steal the amount of material currently being stolen through cyber espionage.[43]

Consider the following hypothetical: if bombs were dropped on a city's stock exchange at night, so that casualties were minimized, this would be considered a use of force by most observers meriting an equally forceful response, even if physical backup facilities were promptly available so that actual trading was only briefly disrupted.[44] But while a cyberattack will not result in the destruction of a building, when it occurs repeatedly and continually, so that trading is disrupted for months or years, the resultant economic harm is arguably far worse than the destruction of a building.[45] A forceful response, then, to intensive, chronic cyberespionage, may be warranted.

Or even if a judge is unwilling to equate a primarily economic harm with a physical harm, the Stuxnet incident has already shown that a cyberattack can be used to inflict physical harm.[46] Moreover, the booming industry of the Internet of Things (IoT) is heightening concern that physical harms inflicted by cyberattacks will soon have grave consequences for the American public.[47] Bruce Schneier focuses on this in his book, *Click Here to Kill Everybody,* arguing that as the IoT becomes more and more pervasive, it is only a matter of time before regulatory agencies have to crack down on innovation in response to a wrongful death suit.[48]

Finally, there is no precedent for whether or not the exigent circumstances doctrine applies to a hackback because *no court decisions* have been made regarding the legality of a hackback.[49] But considering the points just made, there is reason to think a plaintiff-friendly court may believe a third party's

---

43. Melnitzky, *supra* note 4, at 566.

44. *Id*. at 566–67.

45. *Id*. at 567.

46. Josh Fruhlinger, *What is Stuxnet, Who Created It and How Does It Work?*, CSO (Aug. 22, 2017), https://www.csoonline.com/article/3218104/malware/what-is-stuxnet-who-created-it-and-how-does-it-work.html [https://perma.cc/86R5-M926] (providing that Stuxnet was a malicious software designed to cause centrifuges in Iran's nuclear facilities to explode).

47. BRUCE SCHNEIER, CLICK HERE TO KILL EVERYBODY: SECURITY AND SURVIVAL IN A HYPER-CONNECTED WORLD 5–8 (2018).

48. *Episode 230: Click Here to Kill Everybody*, THE CYBERLAW PODCAST (Sept. 9, 2018), https://podcasts.apple.com/us/podcast/episode-230-click-here-to-kill-everybody/id830593115?i=1000419482170 [https://perma.cc/HH4A-FWT5]. Bruce Schneier makes note of the fact that currently the brakes on some cars can be cut off by remote. *Id*. He further argues that it only seems like a matter of time before someone hacks this technology and loss of life occurs. *Id*.

49. Rabkin & Rabkin, *supra* note 22, at 14–15.

privacy interest is outweighed by the public safety interest of deterring growing cyber harms. But, either way, the freedom granted to private actors in conducting third party searches bodes well for the legality of allowing private security firms to procure identifying information from third-party servers.

C. Licensing private professionals to limit collateral damage

Beyond the privacy issue, the other problem with arguments like Nojeim's is that they assume those who hackback are not going to be able to retrieve their data or cease the spreading of that data to other parties, *without inflicting further harm on intermediaries*. This is a valid concern, and why this note would argue that the safest way to implement hackbacks in the private sector is to confine private companies to a set list of qualified security firms to do the job.[50] These professionals would be at least as qualified, if not more so, than a company's internal staff and certainly more qualified than the law enforcement officials to whom they are currently told to turn over their cybersecurity issues.[51]

It is not as if this is anything new. As Stewart Baker puts it in a 2012 hackbacking debate, "allowing private counterhacking does not mean reverting to a Hobbesian war of all against all. Government sets rules and disciplines violators, just as it does with other privatized forms of law enforcement, from the securities industry's FINRA [Financial Industry Regulatory Authority] to private investigators"[52]

This is an important clarification. Without the oversight of licensing agencies, the comparison between hackbacking and defense of property would break down. Justification defenses only work when there are regulatory bodies in place who can prosecute those who go beyond the boundaries of sanctioned, justified behavior. In regards to the defense of property, this keeps people from going to extreme and immoral lengths when taking defensive action. Regarding hackbacks, licensing agencies are necessary to ensure that companies do not use excessive measures and potentially start a war.

An additional reason to allow companies to hire private security firms to hackback is that multiple Fortune 500 companies have already installed active defense software on their systems, out of frustration with the current legal landscape's inability to offer them sufficient protection.[53] Baker mentions that

---

50. *Id*.

51. *Episode 240: If Paris Calls, Should We Hang Up?*, *supra* note 8. Aside from the woeful conviction rates, Mieke Eoyang also notes that she has spoken with companies who properly attributed an attack, handed it to the authorities, and nothing was done about it. *Id*.

52. Steptoe, *supra* note 7.

53. Ruperto P. Majuca & Jay P. Kesan, *Hacking Back: Optimal Use of Self-Defense in Cyberspace* 5–6 (Ill. Pub. Law & Legal Theory Papers Series, Research Paper No. 08-20, 2009), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1363932 [https://perma.cc/7AUD-AH33] ("[A]

this sort of widespread unregulated use of active defense software is concerning and could lead to the "Hobbesian war."[54] The U.S. would be wise to quickly take steps to channel these privatized defensive efforts into the hands of qualified professionals.

As a final point on attribution, there comes a point in considering an equitable remedy where the potential harm caused needs to be weighed against the harm it deters. In this case, with the current improvements in attribution, bolstered by the resources of the private sector, and considering that licensed professionals will inflict minimal collateral harm in searching through a third party's system, the harm of hackbacking is sufficiently minor in comparison to the immense harm it deters. Even obvious physical crimes are subject to error and wrongful convictions, but a certain amount of error is allowed for the greater good of society.[55]

V. POTENTIAL FOR ESCALATING INTERNATIONAL CONFLICT

Perhaps the most pointed objection to privatized hackbacking is allowing private actors to involve themselves in conflicts with other nation-states.[56] There is concern that once provoked, these nations "may assume that any attack of any kind can be blamed on the US government and impose retribution on a larger segment of American society . . . ."[57] If anything, hackbacking opponents would argue provoking entire nation-states heightens the risk of harm to innocent third parties to an unjustifiable level.[58] This is no longer only putting the few people at risk who happen to be in the way of apprehending a thief; this is putting the entire country at risk.

The issue with this concern is that it either assumes an unregulated version of hackbacking in which unqualified citizens are the ones prying into other nation's systems—something which no serious proponents are advocating[59]—or it assumes private security firms are not as qualified as government officials to hackback without starting a war. Again, the government is already employing active defense,[60] so there is already a belief that its deterrent value

survey of 320 Fortune 500 corporations revealed that around 30% of the companies have installed software capable of launching counterattack measures.").

54. *Id*. at 7.

55. Rabkin & Rabkin, *supra* note 22, at 11.

56. *Episode 155: Debate with Greg Nojeim and Jamil Jaffer*, *supra* at note 18. Jamil Jaffer makes the point that allowing private security to conflict with international actors is like allowing the stereotypically incompetent mall cop to engage in international diplomacy. *Id*.

57. Rabkin & Rabkin, *supra* note 22, at 12.

58. *Episode 155: Debate with Greg Nojeim and Jamil Jaffer*, *supra* note 18.

59. Steptoe, *supra* note 7; *see also* Rabkin & Rabkin, *supra* note 22, at 10.

60. *See generally* Jinghua, *supra* note 9.

is worth the risk of international provocation. The concern is if private actors are capable of toeing the line between deterrence and provocation.

The problem, though, is that there are already examples of private security firms hacking into opposing international systems without starting a global conflict.[61] Moreover, it is hard to see how a private firm could be more provocative than the NSA is.[62]

However, an important distinction comes up at this point, between retrieving data and halting its proliferation. While the NSA is confined to data retrieval, the idea behind hacking back is to take steps to ensure that the data is not only retrieved but that the bad actors are prevented from distributing it further. This is where concern arises that hackbackers would employ disproportionately harmful tactics in attempts to teach the enemy a lesson. Earlier it was mentioned that privatized active defense is preferable because these companies have more of a vested interest in protecting their data. This same benefit could be a detriment, as more invested security firms could want to inflict punishment on the perpetrators beyond that of an impartial government official.

The answer to this lies in the fact that arguably the best deterrent for hackers is not extreme physical force, such as implanting malicious malware capable of frying their computer or the entire network of which it is a part, but in *exploiting their anonymity*.[63] For one, destroying a hackers' computer or software is readily replaceable.[64] This is like trying to deter terrorists by destroying readily replaceable vehicles instead of going after the terrorists themselves.[65] The more effective deterrent is focusing on the cyber attackers by undermining their anonymity.[66] This is especially the case for the U.S.' primary opponents, China and Russia, for whom much weight is given to maintaining secrecy around how their governments operate and how their senior officials live.[67] Moreover, this creates a helpful asymmetry for the U.S., as the highly public nature of our government and business operations means disclosure is generally a much bigger threat to our opponents than to U.S. firms.[68]

---

61. Rabkin & Rabkin, *supra* note 22, at 10.

62. David E. Sanger & Nicole Perlroth, *N.S.A Breached Chinese Servers Seen as Security Threat*, N.Y. TIMES (Mar. 22, 2014), https://www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html [https://perma.cc/P3GE-KK5U].

63. Rabkin & Rabkin, *supra* note 22, at 7.

64. *Id*.

65. *Id*.

66. *Id*.

67. *Id*.

68. *Id*.

Regarding the execution of this, it could be sending a message to the opposing hacker saying: "We have learned a lot about you by probing your email and your computerized records, your finances, personal whereabouts, typical tactics and past victims. If you do not immediately return the stolen data and delete it from your servers, we will post some of this information on public websites in retaliation for your attacks on American corporations."[69] Coupling this sort of action with the vast resources the private sector could bring to the attribution problem could rapidly shrink the pervasive anonymity within which cybercriminals currently operate. This, in turn, could lead to a marked decrease in cybercriminal activity, as countries like China or Russia would likely reach a point at which their discomfort with the disclosure of their internal operations would force them to cut back on their hacking initiatives. Admittedly, this may not do much to halt the proliferation of the data for the first few companies who try it. Currently, foreign nations do not have much confidence that America will actually take retaliatory action for hacking.[70] This sentiment would fade, however, once nations realize these are not empty threats.

These sorts of threats are, of course, provocational. Perhaps more limited language would be what the licensing agencies agree upon. Again, it would be up to the regulators and not the private actors to decide what kind of offensive action is appropriate. The broader point is that firms would not need to engage in overtly kinetic harm to shift from purely data retrieval to the halting of data proliferation. Exposing hackers' anonymity could itself be a sufficient deterrent to slow the growing cybercriminal threat.

VI. LEGALIZING HACKING BACK WITHIN THE CFAA

A final point to consider is whether or not hacking back is clearly illegal under the CFAA. While there have not been any prosecutions on this topic, even those in favor of hacking back have granted it is a risky proposition to encourage private actors to hackback under the current legal regime.[71] There is, however, a clear way within the CFAA to legalize hacking back without having to draft new legislation.

Subsection (f) says the CFAA "does not prohibit any *lawfully authorized* investigative,

---

69. *Id*. at 3.

70. West, *supra* note 26, at 134. "Some believe that the U.S. government's cyber-deterrence strategy does not work because foreign hackers know that the U.S. will not respond to cyber-espionage. However, if U.S. companies openly exercise their ability to hackback, foreign hackers might think twice about attacking U.S. systems." *Id*.

71. *Episode 155: Debate with Greg Nojeim and Jamil Jaffer*, *supra* note 18; *see also* Rabkin & Rabkin, *supra* note 22 at 15.

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."[72] It is entirely plausible for federal agencies to read this as allowing private security firms to be "lawfully authorized" to engage in "investigative, protective or intelligence activity."[73] This was the case in 2004 when the Department of Justice (DOJ) "authorized a U.S. Air Force cybersecurity team to hackback when two hackers infiltrated the computer networks of Rome Labs in Upstate New York. The military does not necessarily fall under section 1030(f), so the DOJ had to expand section 1030(f)'s protections to a new entity."[74] Moreover, since the 9/11 attacks, there "is a growing comfort with private actors handling sensitive national security tasks."[75] Ultimately, then, the collaboration between the public and private sector discussed to this point could, if desired, fit squarely within the CFAA.

VII. CONCLUSION

People are breaking into American computer systems literally thousands of times per day and running off with billions of dollars' worth of property. While comparing hackbacking to defense of property has its limitations, the equitable considerations it highlights provides a helpful backdrop for why, in view of the scope of the current harm caused by cyberespionage, hackbacking is a viable option. The law has long recognized the need to allow the private sector to defend itself against harms for which either law enforcement or the courts cannot offer protection. Sometimes, justice lies primarily in the hands of the American public.

72. 18 U.S.C. §1030(f) (2018) (emphasis added).
73. Rabkin & Rabkin, *supra* note 22, at 15.
74. West, *supra* note 26, at 142.
75. *Id*.