HACKING THE INTERNET OF THINGS: VULNERABILITIES, DANGERS, AND LEGAL RESPONSES*

SARA SUN BEALE† AND PETER BERRIS††

ABSTRACT

The Internet of Things (IoT) is here and growing rapidly as consumers eagerly adopt internet-enabled devices for their utility, features, and convenience. But this dramatic expansion also exacerbates two underlying dangers in the IoT. First, hackers in the IoT may attempt to gain control of internet-enabled devices, causing negative consequences in the physical world. Given that objects with internet connectivity range from household appliances and automobiles to major infrastructure components, this danger is potentially severe. Indeed, in the last few years, hackers have gained control of cars, trains, and dams, and some experts think that even commercial airplanes could be at risk. Second, IoT devices pose an enormous risk to the stability of the internet itself, as they are vulnerable to being hacked and recruited into botnets used for attacks on the digital world. Recent attacks on major websites including Netflix and Twitter exemplify this danger. This article surveys these dangers, summarizes some of their main causes, and then analyzes the extent to which current laws like the Computer Fraud and Abuse Act punish hacking in the IoT. The article finds that although hacking in the IoT is likely illegal, the current legal regime punishes hacking after the fact and therefore lacks the prospective force needed to fully temper the risks posed by the IoT. Therefore, other solutions are needed to address the perilousness of the IoT in its current form. After a discussion of the practical and legal barriers to investigating and prosecuting hacking, we turn to the merits and pitfalls of hacking back from legal, practical, and ethical perspectives. We then discuss the advantages and disadvantages of two possible solutions—regulation and the standards approach.

---

* An earlier version of this project was presented at a conference on Technology and the Law at University of Würzburg, and it will be published by with other conference papers in DIGITALIZATION AND THE LAW (Eric Hilgendorf & Jochen Feldle, eds., forthcoming 2018).

† Charles L.B. Lowndes Professor, Duke Law School.
†† J.D., Duke Law School, 2017.

INTRODUCTION

This is the age of the Internet of Things (IoT), where "everyday objects . . . connect to the Internet and . . . send and receive data."[1] The lines between computers and humans have blurred as "[t]he Internet now affects the world in a direct physical manner."[2] The Federal Trade Commission predicts that more than fifty billion devices will be part of the IoT by 2020,[3] including items ranging from kitchen appliances to Fitbits and heart monitors.[4] As Bruce Schneier explained to Congress, "everything is now a computer."[5] The reach of the IoT extends beyond consumer goods to major items and infrastructure components, including cars, airplanes,[6] hospitals, telecommunications networks, and power grids.[7] As a result, "insecurity" in the IoT "puts human safety at risk."[8] Moreover, in the age of the IoT, the actions of "hackers" may carry physical consequences.[9]

This article proceeds as follows. Section I describes episodes in which the IoT has already been hacked as well as the potential for other

---

[1] FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127IOTrpt.pdf.

[2] *Understanding the Role of Connected Devices in Recent Cyber Attacks: Hearing Before H. Comm. on Energy and Commerce*, 114th Cong. 3 (2016) (statement of Bruce Schneier), [hereinafter "Schneier"].

[3] Christina Scelsi, *Care and Feeding of Privacy Policies and Keeping the Big Data Monster at Bay: Legal Concerns in Healthcare in the Age of the Internet of Things*, 39 NOVA L. REV. 391, 396 (2015).

[4] Andrew Meola, *What is the Internet of Things (IoT)?*, BUSINESS INSIDER, Dec. 19, 2016, http://www.businessinsider.com/what-is-the-internet-of-things-definition-2016-8.

[5] *Understanding the Role of Connected Devices in Recent Cyber Attacks* (preliminary transcript): *Hearing Before H. Comm. on Energy and Commerce*, 114th Cong. 27 (2016) (testimony of Bruce Schneier), http://docs.house.gov/meetings/IF/IF17/20161116/105418/HHRG-114-IF17-Transcript-20161116.pdf [hereinafter "Schneier Testimony"]. At the time of his testimony, Schneier was identified as special advisor to IBM Security and CTO of Resilient: an IBM Company, a fellow of the Berkman-Klein Center at Harvard University, and a lecturer and fellow at Harvard's Kennedy School of Government.

[6] *Id.* at 29.

[7] *Id.* at 57.

[8] *Understanding the Role of Connected Devices in Recent Cyber Attacks: Hearing Before H. Comm. on Energy and Commerce*, 114th Cong. 3 (2016) (statement of Kevin Fu), http://docs.house.gov/meetings/IF/IF17/20161116/105418/HHRG-114-IF17-Wstate-FuK-20161116.pdf [hereinafter "Fu"] (warning the HECC that "the Dyn attack is a sign of worse pains to come").

[9] *See* section I, *infra*.

attacks, and Section II examines the reasons for the vulnerabilities that facilitate hacking. Section III explores how criminal law now responds to attacks on the IoT, focusing on the applicability of the federal Computer Fraud and Abuse Act (CFAA)[10] to common forms of hacking IoT devices, and Section IV discusses the practical and legal barriers to investigation and prosecution of hacking. Section V evaluates the merits and pitfalls of hacking back against botnets, from legal, practical, and ethical standpoints. Section VI briefly summarizes two other possibilities for securing the IoT, before the article provides a general summary in Section VII. We conclude that solutions are urgently needed, despite the difficulty in crafting a fully satisfactory response.

I. THREATS AND VULNERABILITIES

A. How the IoT Has Been Hacked

On October 21, 2016, major websites, including Netflix, Twitter, Reddit, and the New York Times, were inaccessible for as long as several hours.[11] The interruption was the result of a Distributed Denial of Service attack ("DDoS")[12] against the company Dyn, which "is one of many outfits that host the Domain Name System, or DNS, which functions as a switchboard for the internet."[13] The perpetrators of the Dyn attack exploited "a vulnerability in large numbers—possibly millions—of . . . devices like webcams and digital video recorders" and used them as a botnet[14] to flood Dyn with traffic.[15] This "attack traffic" combined with

---

[10] 18 U.S.C. § 1030 (2012).

[11] Nicole Perlroth, *Hackers Used New Weapons to Disrupt Major Websites Across U.S.*, N.Y. TIMES, Oct. 21, 2016, https://www.nytimes.com/2016/10/22/business/internet-problems-attack.html?_r=0.

[12] A DDoS is when "an attacker attempts to prevent legitimate users from accessing information or services. . . . [such as] when an attacker 'floods' a network with information. . . . The server can only process a certain number of requests at once, so if an attacker overloads the server with requests, it can't process [legitimate requests]. This is a 'denial of service' because you can't access that site." Mindi McDowell, *Security Tip (ST04-015) Understanding Denial-of Service Attacks*, US-CERT, Feb. 6, 2013, https://www.us-cert.gov/ncas/tips/ST04-015.

[13] Perlroth, *supra* note 11.

[14] A botnet is a "collection of computers compromised by malicious code and controlled across a network." *Glossary*, US-CERT, Jan. 11, 2017, https://niccs.us-cert.gov/glossary#B. Although they can be used for collaboration, "botnet" is a pejorative term. Zach Lerner, *Microsoft the Botnet Hunter: The Role of Public-Private Partnerships in Mitigating Botnets*, 28 HARV. J.L. & TECH. 237, 237–38. (2014).

[15] Schneier, *supra* note 2, at 2.

"legitimate traffic" to overwhelm Dyn,[16] taking down "dozens of websites" with it.[17]

Despite the large scale of the interruption, the Dyn attack has been characterized as "benign" since it did not result in physical injury or property damage.[18] Nevertheless, it demonstrated the risk that the next attack may be devastating.[19]

In response to the Dyn attack, the House Energy and Commerce Committee (HECC) held a hearing to address the threats posed by hacking in the IoT.[20] Expert testimony was grave. Bruce Schneier warned that "the internet is now dangerous . . . ."[21] Dr. Kevin Fu told the HECC that he "fear[s] for the day where every hospital system is down, for instance, because an [IoT] attack brings down the entire healthcare system."[22] Dale Drew cautioned that the culprits of the Dyn attack relied on "just a fraction of the total available compromised [IoT devices] . . . demonstrating the potential for significantly greater havoc . . . ."[23]

Illustrations of the dangers abound. Many prominent examples of hacking in the IoT pertain to automobiles.[24] In 2015, Fiat Chrysler recalled

---

[16] Scott Hilton, *Dyn Analysis Summary of Friday October 21 Attack*, VANTAGE POINT, Oct. 26, 2016, http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/.

[17] Schneier, *supra* note 2, at 2.

[18] Schneier, *supra* note 2, at 3.

[19] *See* Fu, *supra* note 8, at 2.

[20] *Understanding the Role of Connected Devices in Recent Cyber Attacks* (preliminary transcript)*: Hearing Before the H. Comm. on Energy and Commerce*, 114th Cong. 4–5 (2016) (statements of Greg P. Walden, Chairman, Subcomm. on Commc'n & Tech.), http://docs.house.gov/meetings/IF/IF17/20161116/105418/HHRG-114-IF17-Transcript-20161116.pdf .

[21] Schneier Testimony, *supra* note 5, at 59.

[22] *Understanding the Role of Connected Devices in Recent Cyber Attacks* (preliminary transcript)*: Hearing Before the H. Comm. on Energy and Commerce*, 114th Cong. 43. (2016) (testimony of Kevin Fu), http://docs.house.gov/meetings/IF/IF17/20161116/105418/HHRG-114-IF17-Transcript-20161116.pdf [hereinafter "Fu Testimony"].

[23] *Understanding the Role of Connected Devices in Recent Cyber Attacks: Hearing Before the H. Comm. on Energy and Commerce*, 114th Cong. 3 (2016) (statements of Dale Drew), http://docs.house.gov/meetings/IF/IF17/20161116/105418/HHRG-114-IF17-Wstate-DrewD-20161116.pdf [hereinafter "Drew"]. At the hearing, Drew was identified as senior vice president and chief security officer for Level 3 Communications.

[24] Automobiles are an obvious target for hackers because they can cause physical damage, *and* because they are vulnerable. *See* Cheryl Dancey Balough & Richard C. Balough, *Cyberterrorism on Wheels: Are Today's Cars Vulnerable to Attack?*, BUS. L. TODAY, Nov. 2013, at 1 ("The potential exists that a car's computers, like

1.4 million cars in response to a widely publicized demonstration where hackers took control of a Jeep Cherokee through its infotainment system.[25] They were able to "turn the steering wheel, briefly disable the brakes and shut down the engine."[26] Additionally, in 2010, the disgruntled former employee of a used-car dealership remotely accessed the company's computers and wreaked havoc by setting off car alarms and shutting down engines.[27]

The danger is not limited to cars. For example, in 2008, a fourteen-year-old boy hacked into the system controlling the trains of Lodz, Poland as a prank.[28] He made several trains change tracks, causing multiple derailments and injuries.[29] In 2013, the Federal Bureau of Investigation and the Department of Homeland Security "issued a warning" about "several . . . attacks against the 911 system."[30] The attacks were an attempt to extort money, and when the perpetrators received nothing they "launched [a] high volume of calls against the target network, tying up the system from receiving legitimate calls."[31] In 2016, Iranian hackers breached "the computer-guided controls" of the small Bowman Dam in suburban Rye

---

any computer system, can be hacked, leaving the car vulnerable to infection by malware. These vulnerabilities pose serious safety hazards should they be exploited nefariously. Legal implications of this technological vulnerability have yet to be adequately addressed."). Cars contain dozens of Electronic Control Units (ECUs) "embedded in the body, doors, dash, roof, trunk, seats, wheels, navigation equipment, and entertainment centers," many of which connect to the internet and provide access points for hackers. *Id.* Disturbingly, "[t]he potential vulnerability of cars to hacking will increase as vehicle-to-vehicle (V2V) and self-driving cars become available" and "the average auto maker is about 20 years behind software companies in understanding how to prevent cyber attacks." *Id.* at 3.

[25] Kelly Pleskot, *FCA Recalls 1.4 Million Vehicles over Hacking Concern*, MOTORTREND, Jul. 24, 2015, http://www.motortrend.com/news/fca-recalls-1-4-million-vehicles-over-hacking-concern/.

[26] Craig Timberg, *Hacks on the Highway*, WASHINGTON POST, Jul. 22, 2015, at 3, http://www.washingtonpost.com/sf/business/2015/07/22/hacks-on-the-highway/?utm_term=.f074b322c45a.

[27] *Id.* at 7; Matthew Shaer, *Disgruntled Hacker Remotely Disables 100 Cars*, CHRISTIAN SCIENCE MONITOR, Mar. 18, 2010, at 1, http://www.csmonitor.com/Technology/Horizons/2010/0318/ Disgruntled-hacker-remotely-disables-100-cars.

[28] Graeme Baker, *Schoolboy Hacks into City's Tram System*, THE TELEGRAPH, Jan. 11, 2008, http://www.telegraph.co.uk/news/worldnews/1575293/Schoolboy-hacks-into-citys-tram-system.html.

[29] *Id.*

[30] Kim Zetter, *How America's 911 Emergency Response System Can Be Hacked*, WASHINGTON POST: THE SWITCH, Sept. 9, 2016, at 1, https://www.washingtonpost.com/news/the-switch/wp/2016/09/09/how-americas-911-emergency-response-system-can-be-hacked/?utm_term=.9cfcc5fc5a3d.

[31] *Id.* (internal citation omitted).

Brook, New York.[32] The dam was offline for repair and immune to remote access, but the implications are disturbing because the hackers may have been trying to access an identically named dam in Oregon, which is a formidable "245 feet tall and 800 feet long . . . ."[33]

B. Other Ways the IoT Could Be Hacked

Machine Security researchers have identified a range of other frightening vulnerabilities. Researchers have "demonstrated ransomware against home thermostats and exposed vulnerabilities in implanted medical devices. They've hacked voting machines and power plants."[34] Indeed, many computer security experts fear that the USB port at an airline seat could potentially be used to control the plane's avionics.[35]

Clearly, the IoT offers a broad array of dangerous tools hackers can employ for a wide range of motives, including: terrorism,[36] "national aggression,"[37] pranking,[38] election tampering,[39] and monetary extortion.[40] Whatever the impetus for hacking in the IoT, the threats moving forward are considerable.

---

[32] Joseph Berger, *A Dam, Small and Unsung, Is Caught Up in an Iranian Hacking Case*, N.Y. TIMES, Mar. 25, 2016, https://www.nytimes.com/2016/03/26/nyregion/rye-brook-dam-caught-in-computer-hacking-case.html?_r=0.

[33] *Id.*

[34] Schneier, *supra* note 2, at 5. Although there is evidence of Russian hacking intended to affect the U.S. presidential election in 2016, these efforts seem to have been focused on the computers themselves and information contained on them (e.g., emails and donor databases), rather than on things connected to the computers, such as voting machines. *But see* David Smith & John Swain, *Russian Agents Hacked US Voting System Manufacturer Before U.S. Election*, THE GUARDIAN, June 5, 2017, at 1 (noting that although hacking and release of Democratic emails had been traced to Russia vote counting "was thought to be unaffected" before leaked report that Russian intelligence hacked into U.S. manufacturer of voting systems weeks before election).

[35] Schneier Testimony, *supra* note 5, at 102.

[36] *See generally* Balough, *supra* note 24, at 1 (theorizing about the possibility that cars might be exploited for terrorism through the internet).

[37] Schneier Testimony, *supra* note 5, at 57.

[38] *See* Baker, *supra* note 28 & 29, and accompanying text (chronicling a hacking attack executed as a prank).

[39] *See generally* Bruce Schneier, *American Elections Will Be Hacked*, N.Y. TIMES, Nov. 9, 2016, https://www.nytimes.com/2016/11/09/opinion/american-elections-will-be-hacked.html (summarizing the vulnerabilities of voting machines and infrastructure and the danger of election fraud).

[40] *See* Drew, *supra* note 23, at 3 ("The primary motivation for [DDoS] attacks appears to be financial").

II. WHY IS THE IOT SO INSECURE AND VULNERABLE TO HACKING?

Security researchers have attributed the scale and ease of attack to "the quantity of insecure IoT devices operated by a highly distributed set of unwitting consumers,"[41] and to a "fundamental market failure."[42] Because electronics consumers care most about affordability, "the market has prioritized features and cost over security."[43] Thus, the teams that make many IoT devices have less "security expertise" than major companies like Apple, because "the market won't stand for the additional costs that [similar training] would require."[44] Further complicating matters, many IoT devices are part of a complex global supply chain where they are "designed and built offshore, then rebranded and resold."[45] The resulting devices are the product of differing international standards of security.[46]

As a result, IoT devices in the U.S. exhibit a wide range of serious vulnerabilities. Many come with "default and easily-identifiable passwords that hackers can exploit."[47] Some of these passwords cannot be changed.[48] Similarly, many "devices also lack the capability of updating their firmware, forcing consumers to monitor for and install updates themselves."[49] Additionally, in many cases consumers have little or no way to know when their IoT devices have been compromised.[50] The relationship between hardware and software further exacerbates the problem. When the underlying software has been corrupted, the object itself often continues to function as intended, leaving little reason to replace it.[51] Even devices used as part of a botnet in an attack will "still work fine."[52] Many objects

---

[41] *See* Fu, *supra* note 8, at 4 ("What's new is the scale and ease of attack because of the quantity of insecure IoT devices operated by a highly distributed set of unwitting consumers.").
[42] Schneier, *supra* note 2, at 3.
[43] *Id.*
[44] *Id.*
[45] *Id.*
[46] Dale Drew Committee on Energy and Commerce, *Understanding the Role of Connected Devices in Recent Cyber Attacks* (preliminary transcript), Hearing, pp 37–38 Nov 16, 2016. Available at: http://docs.house.gov/meetings/IF/IF17/20161116/105418/HHRG-114-IF17-Transcript-20161116.pdf; Accessed: 2/26/17 [hereinafter "Drew Testimony"] (explaining the need for international standards).
[47] Drew, *supra* note 23, at 2.
[48] *Id.*
[49] *Id.*
[50] *Id.*
[51] *See* Fu Testimony, *supra* note 22, at 88 (using the example of an MRI machine to explain that consumers do not want to replace functioning hardware to fix a problem with vulnerable software, especially where the machine is expensive).
[52] Schneier, *supra* note 2, at 4.

connected to the internet continue to serve the function for which consumers purchased them long after their software becomes insecure.[53]

III. WHEN IS HACKING THE IOT A CRIME?

This section explores the interaction between the IoT and the current legal regime. Subsection A discusses whether current laws prohibit hacking with an intent to control an object. Subsection B explores the problem of botnets. This section concludes that hacking in the IoT will often be illegal, though the existing laws punish conduct after the fact without addressing the vulnerabilities that facilitate hacking.

A. Scenario One: Hacking with the Intention of Controlling an Object

Consider the following hypothetical. Bill has a grudge against his neighbor Jeremy. Bill discovers a security vulnerability in one of the many electronic control units (ECUs) of Jeremy's late model sedan,[54] and he hacks in through the internet and enters commands that enable him to take control of Jeremy's car.[55]

Bill's actions are increasingly plausible as cars become ever more connected and automakers struggle to update outmoded software.[56] The hypothetical identifies a fundamental aspect of the IoT: the hackers' target is not the computer, but the object connected to the computer. This is true of many of the examples outlined above, though the motives varied: the fourteen-year-old hacked a train system for a prank; the Iranians hacked a dam apparently as an act of terrorism; the extortionists attacked the 911 system for money; and the disgruntled employee hacked into cars sold by his former employer for revenge. All sought to achieve their goals by controlling a remotely accessible object in the IoT.[57] In the IoT, a major objective of remote access will be to control the "things." Thus, a key question is whether the current legal regime covers this relatively new threat, governing scenarios like the one involving Bill and Jeremy. It does.

---

[53] *Id.* at 3–4 (identifying the problem of longevity in internet enabled devices including cars, refrigerators, and thermostats).

[54] Such vulnerabilities are apparently not hard to track down. *See* Timberg, *supra* note 26.

("[S]ecurity researchers" discovered "readily accessible Internet links to thousands of other privately owned Jeeps, Dodges and Chryslers . . . .").

[55] The exact form of hacking varies based on the specific ECU: "[s]ome entry points to a car's ECUs require a direct hard-wired connection, while others can be accessed wirelessly, including Wi-Fi or [Radio-frequency identification]." Balough *supra* note 24, at 1. Researchers demonstrated that once a vehicle has been started normally, key functions including the engine, brakes, and transmission can be controlled remotely by "typing on a MacBook Pro." Timberg, *supra* note 26.

[56] Timberg, *supra* note 26.

[57] *See supra* text accompanying notes 27–33.

1. The Computer Fraud and Abuse Act

The most obvious law that can be employed to combat hacking with the intent to control an object is the Computer Fraud and Abuse Act ("CFAA"). The CFAA was "[o]riginally designed as a criminal statute aimed at deterring and punishing hackers, particularly those who attack computers used for compelling federal interests,"[58] but it also includes "a trespass-like civil remedy under federal law" for various forms of hacking.[59] It is logical that the law would cover hacking with an intent to control an object, as there is some evidence that Congress passed the CFAA in response to the movie WarGames,[60] where the protagonist accidentally hacks into the computer controlling America's nuclear weaponry and nearly starts a third world war.[61]

The provisions of the CFAA cover a range of conduct. The Act prohibits:

> (1) unauthorized obtaining of national security information; (2) unauthorized obtaining of information from a financial institution, United States department or agency, or from any protected computer; (3) unauthorized access to government computers; (4) computer fraud; (5) computer damage; (6) passwords trafficking; and (7) computer extortion.[62]

Section 1030(a)(5) is the subsection most likely to cover hacking with an intent to control an object. It criminalizes:

> knowingly caus[ing] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally caus[ing] damage without authorization, to a protected computer; intentionally access[ing] a protected computer without authorization, and as a result of such conduct, recklessly caus[ing] damage; or intentionally

---

[58] COMPUTER FRAUD AND ABUSE ACT, SS032 ALI-ABA 993, 995.

[59] 5.06. Computer Fraud and Abuse Act, 1 E-Commerce and Internet Law 5.06 (2016 update).

[60] *See* Fred Kaplan, *'WarGames' and Cybersecurity's Debt to a Hollywood Hack*, N.Y. TIMES, Mar. 25, 2016, at https://www.nytimes.com/2016/02/21/movies/wargames-and-cybersecuritys-debt-to-a-hollywood-hack.html?_r=0 (chronicling the emergence of early federal cybersecurity laws in response to President Ronald Reagan's concern over the movie "WarGames"); Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 HARV. J.L. & TECH. 429, 492 (2012).

[61] For a synopsis of the movie WarGames, *see WarGames*, IMDB, http://www.imdb.com/title/tt0086567/plotsummary?ref_=tt_stry_pl#synopsis (last visited August 31, 2017).

[62] Ioana Vasiu & Lucian Vasiu, *Break on Through: An Analysis of Computer Damage Cases*, 14 U. PITT. J. TECH. L. POL'Y 158, 163 (2014).

> access[ing] a protected computer without authorization, and as a result of such conduct, caus[ing] damage and loss.[63]

Whether §1030(a)(5) prohibits hacking with an intent to control hinges on four key definitions: (1) "transmission," (2) "computer," (3) "protected computer," and (4) "damage."

"Transmission" encompasses a range of hacking activities, such as "[t]he transfer of operation or confidential information," "malicious software updates," "code injection attacks," DDoS, and the "embedding of malicious code" or malware.[64] Under the CFAA, transmission "can be accomplished either over the Internet or through a physical medium such as a compact disc."[65] This would cover many forms of hacking aimed at controlling an object. To return to the example of Bill and Jeremy, Bill's conduct qualifies, as he transmitted commands via the internet to take control of Jeremy's car.

Within the CFAA, "computer" is an expansive term. It is defined as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device . . . ."[66] As Judge Easterbrook explained, the definition of "computer" in the CFAA is an example where the exclusions from the definition "show just *how* general" that definition is.[67] Indeed, CFAA subsection (e)(1) "carves out automatic typewriters, typesetters, and handheld calculators; this shows that other devices with embedded processors and software are covered."[68] Thus, most IoT devices are computers for purposes of the CFAA. The ECUs that Bill hacked in Jeremy's car certainly would qualify, as they "are high speed data processing devices performing logical, arithmetic, or storage functions."[69]

Many IoT devices are also *protected* computers. The CFAA defines protected computers as not only those "exclusively for the use of a financial institution or the United States Government" but also computers that are "used in or affecting interstate or foreign commerce or communication . . . ."[70] Courts have interpreted this definition broadly. Indeed, in *U.S. v. Mitra*, Judge Easterbrook explained:

---

[63] 18 U.S.C. § 1030(a)(5) (2012).
[64] Vasiu, *supra* note 62, at 167–169.
[65] 174 A.L.R. Fed. 101 (Originally published in 2001).
[66] 18 U.S.C. § 1030 (e)(1) (2012).
[67] *United States v. Mitra*, 405 F.3d 492, 495 (7th Cir. 2005) (emphasis in original).
[68] *Id.*
[69] Balough *supra* note 24, at 3.
[70] 18 U.S.C. § 1030 (e)(2)(b) (2012).

> [T]he statute . . . protects computers (and computerized communication systems) used in such commerce, no matter how the harm is inflicted. Once the *computer* is used in interstate commerce, Congress has the power to protect it from a local hammer blow, or from a local data packet that sends it haywire.[71]

This standard included the afflicted computer in *Mitra*—Madison, Wisconsin's "computer-based radio system for police, fire, ambulance, and other emergency communications"[72]—even though the hacker's "interference did not affect any radio system on the other side of a state line."[73] What mattered was that Madison's computerized radio system "operated on spectrum licensed by the FCC" and therefore implicated interstate commerce.[74]

Mitra is not an exception. Particularly relevant for devices that are part of the IoT, "[c]ourts generally hold that because the Internet and interstate commerce are inexorably intertwined, any computer connected to the Internet should be considered a computer affecting interstate commerce and therefore protected."[75] Thus, if Jeremy's ECU is internet-enabled, it is a protected computer under the CFAA. This seems a safe bet in an era where cars are increasingly connected and can "talk to the outside world through remote key systems, satellite radios, telematic control units, Bluetooth connections, dashboard internet links and even wireless tire-pressure monitors."[76]

"Damage" is "defined as 'any impairment to the integrity or availability of data, a program, a system, or information,'"[77] and almost certainly encompasses hacking with the intent of controlling an object.[78] To begin with, a hacker damages a computer under the statute by forcing it to behave in a manner not intended by its owner.[79] Additionally, "[a]dverse

---

[71] *Mitra*, 405 F.3d at 496.
[72] *Id.* at 493.
[73] *Id.* at 496.
[74] *Id.*
[75] Vasiu, *supra* note 62, at 164.
[76] Timberg, *supra* note 26.
[77] Jeffrey K. Gurney, *Driving into the Unknown: Examining the Crossroads of Criminal Law and Autonomous Vehicles*, 5 WAKE FOREST J.L. & POL'Y 393, 439 (2015) (quoting 18 U.S.C. § 1030(e)(8) (2012))."
[78] As one commentator has summarized it, "nearly any instance of unauthorized hacking could be said to impair the integrity of a computer system." Ric Simmons, *The Failure of the Computer Fraud and Abuse Act: Time to Take an Administrative Approach to Regulating Computer Crime*, 84 GEO. WASH. L. REV. 1703, 1712 (2016).
[79] *See* Vasiu, *supra* note 62, at 160 ("Integrity generally refers to maintaining computer data in a protected state, unaltered by improper, unauthorized or

actions . . . that alter, encrypt, encipher, encode, transmit or delete data or exhaust system resources" all are damage under the CFAA because they impair the availability of the computer by making it unusable and inaccessible.[80] Transmission is damage under the CFAA because it frequently "involves the deletion of computer data or files."[81] Clearly, Bill damaged Jeremy's car under the CFAA, since he caused it to behave contrary to the wishes of its owner.

Finally, CFAA penalties are structured in a manner that enhances punishment depending on the outcome of the hacking. The Act provides harsher penalties for those whose hacking causes "physical injury," "a threat to public health or safety," "damage affecting a computer used by or for an entity of the United States government in furtherance of justice, national defense, or national security," damage to at least ten computers within a year, or "modification or impairment . . . of the medical examination, diagnosis, treatment, or care of 1 or more individuals . . . ."[82] Unsurprisingly, the stiffest retribution is reserved for those who "knowingly or recklessly caus[e] death from conduct in violation of" subsection (a)(5)(a).[83] Depending on the nature and results of Bill's hacking, he may be subject to some of these increased CFAA penalties. For example, if he took control of Jeremy's car while it was hurtling down a busy highway, it is easy to imagine how Bill might have threatened public safety. If Jeremy's car crashed as a result of the hacking, Bill would face steeper sentencing under the CFAA if Jeremy were injured or killed.

There are many other laws that could govern hacking with an intent to control an object. These include state laws similar to the CFAA.[84]

---

subversive conduct or acts contrary to what the system owner or privilege grantor intended.").

[80] *Id.*

[81] *Id*. at 192.

[82] 18 U.S.C. § 1030(c)(4) (2012).

[83] 18 U.S.C. § 1030(c)(4)(F) (2012).

[84] Computer Crime Law, 29 (noting all "fifty states . . . enact[ed] statutes specifically prohibiting computer misuse"). Like the CFAA, all of these laws employ the "common building block of unauthorized access to a computer," which is "usually supplemented by other elements to create additional criminal prohibitions, such as statutes preventing . . . computer damage." *Id*. at 29–30. Many of these laws could be construed as anti-hacking statutes. Gurney, *supra* note 77, at 434. And some state computer crime laws prohibit damaging the object for which control is sought, or other property. *See*, *e.g.*, CONN. GEN. STAT. § 53-451(b) (criminalizing "use [of] a computer or computer network without authority and with the intent to: … (5) Cause physical injury to the property of another . . . .").

B. Scenario Two: Botnets

As discussed in Section I, a botnet is a network of compromised computers, "often programmed to complete a set of repetitive tasks" without "the owner's knowledge or permission."[85] Botnets "are the instrumentality through which substantial amounts of cybercrime takes place."[86] Botnet-based cybercrime includes spam, fraud, and—of particular relevance for the IoT—DDoS and the installation of malware.[87] Hackers used a botnet in the Dyn attack, which prompted the HECC hearing (discussed in Section I) about the dangers of hacking in the IoT.[88]

By their nature, botnets are illegal under the CFAA.[89] For example, CFAA section 1030(a)(5) criminalizes "knowingly caus[ing] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally caus[ing] damage without authorization, to a protected computer . . . ."[90] Botnets are often created through malicious software that behaves in this manner.[91] Although combating botnets with laws like the CFAA poses many practical problems,[92] there have been some successful prosecutions.[93]

IV. PRACTICAL AND PROCEDURAL ISSUES IN BRINGING CFAA PROSECUTIONS

Although the CFAA is broad enough to reach the hacking in scenarios one and two, any investigation and prosecution would confront significant practical and procedural issues—issues that are common to nearly all computer hacking prosecutions, and not limited to those involving

---

[85] Lerner, *supra* note 14, at 237–38.
[86] Zachary K. Goldman & Damon McCoy, *Deterring Financially Motivated Cybercrime*, 8 J. NAT'L SECURITY L. & POL'Y 595, 608 (2016).
[87] Lerner, *supra* note 14, at 237–38.
[88] *See* text accompanying notes 11-23 *supra*; Bruce Schneier, *Lessons From the Dyn DDoS Attack*, SCHNEIER ON SECURITY (November 8, 2016, 6:25 AM), https://www.schneier.com/blog/archives/2016/11/lessons_from_th_5.html.
[89] *See* Kesan *supra* note 60 at 493 ("The CFAA's language is very broad and can be read to prohibit the creation of botnets.").
[90] 18 U.S.C. § 1030(a)(5) (2012).
[91] *See* Kesan, *supra* note 60 at 442–444 (explaining how botnets are created).
[92] *See* Lerner, *supra* note 14, at 244 ("CFAA enforcement requires precise knowledge of the defendant's identity, which is often impossible to obtain in DDoS attacks . . . [In addition] CFAA prosecution of DDoS masters in foreign countries is impeded by a number of jurisdictional obstacles.").
[93] *See*, *e.g*, Department of Justice Office of Public Affairs, *Arizona Man Sentenced to 30 Months in Prison for Selling Access to Botnets*, JUSTICE NEWS (Sept. 15, 2014), https://www.justice.gov/opa/pr/arizona-man-sentenced-30-months-prison-selling-access-botnets (describing successful prosecution of a man who had sold "access to and use of thousands of malware-infected computers").

the IoT. First, attribution is very difficult. It poses technical problems and often requires remote electronic searches. The Federal Rules of Criminal Procedure were amended in 2016 to remove some procedural barriers to remote electronic searches. But the amendments—and remote searches in general—have been controversial. As we discuss in more detail below in subsection B, Critics have voiced a variety of concerns, including Fourth Amendment and privacy objections. These issues will likely be raised in prosecutions that rely on evidence secured by means of remote electronic searches, and there are ongoing efforts to repeal the amendments. Moreover, when IoT hacking originates outside the United States, those prosecutions will raise the question whether the CFAA provides for extraterritorial jurisdiction. Despite all of these difficulties, there have been some successful investigations, allowing the government to prosecute hackers and neutralize their botnets.[94]

A. Attribution

Reliable attribution of most forms of computer hacking is extremely difficult.[95] As Professor Orin Kerr explained, investigating computer crimes is necessarily different than investigating traditional physical offenses:

> With the physical crime, the chances were good that the crime scene would yield substantial leads. Even if no one could identify [the perpetrator] in a lineup, his physical presence at the crime scene greatly narrowed the number of suspects. The electronic crime scene looks very different. In most cases, evidence gathered at the victim site will tell the investigator only that someone, located somewhere in the world, hacked into the [victim's computer]. In most cases, the biggest investigative lead comes in the form of an originating Internet Protocol (IP) address recorded by the [victim's] servers. An IP address is the internet equivalent of a telephone number . . . .[96]

---

[94] One such success is described in the text accompanying nn.179–88, *infra*. The indictment and extradition of Fabio Gasperini, an Italian citizen changed with creating and running a global botnet, is another. Press Release, U.S. Attorney's Office, E.D.N.Y., Cybercriminal Who Created Global Botnet Infected with Malicious Software Extradited to Face Click Fraud Charges (Apr. 21, 2017), https://www.justice.gov/usao-edny/pr/cybercriminal-who-created-global-botnet-infected-malicious-software-extradited-face.

[95] *See* Paul N. Stockton & Michele Golabek-Goldman, *Prosecuting Cyberterrorists: Applying Traditional Jurisdictional Frameworks to a Modern Threat*, 25 STAN. L. & POL'Y REV. 211, 214–15 (2014) (noting the technical difficulty of attribution).

[96] Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 279, 284 (2005). *See also* Susan W. Brenner, *Law, Dissonance, and Remote Computer Searches*, 14 N.C. J.L. & TECH. 43, 46 (2012) (comparing the cybercrime

Because hackers typically route their attacks through a series of intermediaries, investigators must "try to follow the trail of electronic bread crumbs" back to the perpetrator's computer, a cumbersome process.[97] Moreover, hackers intentionally target intermediary computers with lax security and poor record keeping, meaning that the trail is likely to break down.[98] When that occurs, investigators must use other techniques, such as prospective surveillance.[99]

These difficulties are compounded in cases involving multiple computers. Attribution is especially difficult in the case of cross-jurisdictional botnet cases, which may involve one million or more computers from many nations.[100] The perpetrator may be an individual, but it may also be a business entity or a foreign government agency.[101] The Federal Bureau of Investigation, other U.S. government agencies, and private organizations are attempting to improve their capacity to meet these challenges.[102] In some cases, the government has collaborated with the private sector.[103]

Anonymizing technology adds another layer to this already complicated attribution problem. For example, Tor is a private global computer network that allows users to conduct anonymous transactions without revealing their location.[104] As one commentator explained:

> Computers on the Tor Network use an encrypted communications protocol that cannot be accessed using normal web browsers. Instead, they require the use of special software, like the Tor Browser. Proper use of the Tor Network makes it practically impossible for

---

investigations with traditional investigations and noting that a computer hacker may be hundreds or even thousands of miles away from the victim, unseen by and unknown to him or her).

[97] Kerr, *supra* note 96, at 285.

[98] *Id*. at 286.

[99] *Id*.

[100] *E.g.*, Stockton & Golabek-Goldman, *supra* note 95, at 214 (describing DDOS attack on Estonia involving one million slave computers in countries from Vietnam to the United States).

[101] *See*, *e.g.*, Orin S. Kerr & Sean D. Murphy, *Government Hacking to Light the Dark Web: What Risks to International Relations and International Law*, 70 STAN. L. REV. ONLINE 58, 58 (describing hacking by Russian, Chinese, and North Korean governments).

[102] *Id*. at 214–15.

[103] *See* Garrett M. Graff, *How the FBI Took Down Russia's Spam King—and His Massive Botnet*, WIRED, April 11, 2017, https://www.wired.com/2017/04/fbi-took-russias-spam-king-massive-botnet/ (last visited Oct. 26, 2017) (describing outside security researchers and FBI agents).

[104] Ahmed Ghappour, *Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web*, 69 STAN. L. REV. 1075, 1087 (2017).

> governments to trace the location of computers hosting "hidden" websites on the network, the location of computers accessing those hidden websites, or the location of computers that tunnel through the network to "anonymously" visit public websites on the World Wide Web.[105]

Tor bounces message packets through a series of intermediate computers (proxies) scattered around the globe, making it impossible for government investigators to determine the location of the original sender.[106]

B. Remote Electronic Searches

When a physical search is not possible because anonymizing technology has hidden the location of electronic storage media, the government may be able to conduct a remote electronic search of the media to seize or copy electronically stored information. Although searches of this nature are a common feature of hacking investigations, they raise a variety of ethical and legal issues. Some of the issues were addressed in 2016 by amendments to the Federal Rules of Criminal Procedure. These amendments generated substantial controversy, and the constitutional issues raised by critics of remote searches will need to be resolved on a case-by-case basis when warrant applications are presented for judicial approval or evidence obtained by the use of such warrants is introduced at trial. And some commentators have urged Congress to limit remote electronic searches.

Remote electronic searches employ network investigative techniques (NITs) that allow investigators to reach a computer without knowledge of its physical location.[107] A remote search requires only a means of communicating with the target computer, such as an active email address.[108] For example, an NIT may be an email containing software that can extract from the target computer and relay back information such as the target computer's IP address, its host name, media access control (MAC) address, time zone, and registered computer name, registered company name, and current logged-in user name.[109] The government has employed

---

[105] *Id*. (footnote omitted).
[106] *Id*. at 1088.
[107] *Id.* at 1096. For a description of the NIT, see United States v. Croghan, 209 F.Supp.3d 1080, 1084 (S.D. Iowa 2016). For a general description of NITs, see Devin M. Adams, *The 2016 Amendments to Criminal Rule 41: National Search Warrants to Seize Cyberspace, "Particularly" Speaking*, 51 U. RICH. L. REV. 727, 737–41 (2017).
[108] *Id*.
[109] *See*, *e.g.*, Memorandum from Jonathan J. Wroblewski to Judge John F. Keenan, Chair, Subcommittee on Rule 41, Jan. 17, 2014, Attachment B, April 2014 Agenda Book Advisory Comm. Crim. Rules 179, 187, available at

other NITs as well.[110] Although the lower courts have been divided on this issue, several courts have concluded that NITs constitute searches for the purpose of the Fourth Amendment when the government obtains information (such as the defendant's IP address) not from a third party provider, but rather from an intrusion into the defendant's computer.[111]

In 2014, the Department of Justice recommended that the Judicial Conference Advisory Committee on Criminal Rules amend the Federal Rules of Criminal Procedure to "update the provisions relating to the territorial limits for searches of electronic storage media."[112] The Department sought amendments to deal with "two increasingly common situations (1) where the warrant sufficiently describes the computer to be searched but the district within which that computer is located is unknown, and (2) where the investigation requires law enforcement to coordinate searches of numerous computers in numerous districts."[113] Additionally, the Department noted that the provisions for notice following a search had not been adapted to address remote searches.[114]

The Department explained that when persons committing criminal offenses have used anonymizing technology, like Tor, the territorial limits of Federal Rule of Criminal Procedure 41 could prevent the issuance of warrants for remote searches although the government had met all of the

---

http://www.uscourts.gov/rules-policies/archives/agenda-books/advisory-committee-rules-criminal-procedure-november-2014.

[110] For example, after the government seized the server for the "Playpen" child pornography website, it obtained a warrant to install an NIT on the server consisting of software to be deployed when any user logged into the site with a username and password, regardless of the user's physical location. The NIT would then force the "activating" computer to transmit information back to the FBI, including: the IP address of the activating computer; the date and time the NIT determined the IP address; a unique identifier generated by the NIT to distinguish data from different activating computers; the type of operating system running on the activating computer, including type, version, and architecture; information on whether the NIT had already been delivered to the activating computer; the "host name" of the activating computer; the operating system used by the activating computer; and the Media Access Control ("MAC") address of the activating computer.

[111] *E.g.*, United States v. Horton, 863 F.3d 1041, 1047 (8th Cir. 2017); Adams, *supra* note 107, at 755–57 (collecting cases).

[112] Letter from Mythili Raman, Acting Assistant Attorney General, to The Honorable Reena Raggi, Chair, Advisory Committee on the Criminal Rules 1 (Sept. 18, 2013), http://www.uscourts.gov/rules-policies/archives/suggestions/hon-mythili-raman-13-cr-b [hereinafter Raman letter].

[113] *Id*.

[114] *Id*. at 4.

other constitutional and statutory requirements. With certain exceptions,[115] prior to the 2016 amendment Rule 41 authorized "a magistrate judge with authority in a district" to issue warrants to search for and seize "property located within the district."[116] But anonymizing technology like Tor disguises the location of the storage media or information to be searched. Thus under a strict reading of the rule, disguising the district in which the computer was located precluded any court from issuing a warrant, even if the government had presented probable cause and met all of the other statutory and constitutional requirements for the issuance of a warrant.[117] The government would be unable to obtain venue in any district, regardless of the seriousness of the offense.[118]

The venue or territorial limitation for the issuance of warrants also imposed a particularly heavy burden in botnet investigations, where the affected computers (and other IoT devices that would be classed as computers under the CFAA) are often located in all ninety-four federal districts. Although the information establishing probable cause would be virtually identical in each district, presenting this information in each

---

[115] Before amendment, Rule 41(b) authorized search warrants for property located outside the judge's district in only four situations: (1) for property in the district that might be removed before execution of the warrant; (2) for tracking devices installed in the district, which may be monitored outside the district; (3) for investigations of domestic or international terrorism; and (4) for property located in a U.S. territory or a U.S. diplomatic or consular mission. FED. R. CRIM. P. 41(b)(2)-(5).

[116] FED. R. CRIM. P. 41(b)(1).

[117] Raman letter at 2, citing In re Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753, 761 (S.D. Tex. 2013).

[118] For example, in describing the need for the Rule 41 amendments, Assistant Attorney General Leslie Caldwell wrote of the dismissal of prosecutions of users of the Playpen site, which allowed pedophiles to trade images and videos of child sex exploitation:

> Despite being prepared to comply fully with the Fourth Amendment's warrant requirements, including persuading a federal judge that a lawful basis for a warrant exists, investigators are being told that, because criminals have successfully used technology to hide their location, there is no court available to hear their warrant application. Unless that nonsensical outcome is addressed, cases such as Playpen fail, meaning that pedophiles – including hands-on abusers – will be free to continue their crimes.

Leslie R. Caldwell, Ensuring Tech-Savy Criminals Do Not Have Immunity from Investigation, U.S. Dept't Justice (Nov. 21, 2016), https://www.justice.gov/archives/opa/blog/ensuring-tech-savvy-criminals-do-not-have-immunity-investigation.

district would impose a heavy burden both on the investigators seeking the warrants and on the courts reviewing those warrants in each district.[119]

Finally, before amendment, the notice provisions of Rule 41 were ill-adapted to remote electronic searches.[120] The rule required the officer executing the warrant to give a copy of the warrant and receipt for any property seized "to the person from whom, or from whose premises, the property was taken or leave a copy of the warrant or receipt at the place where the officer took the property."[121] This language seemed to contemplate leaving the warrant and receipt at a physical place, which would not be feasible for remote electronic searches.

After a period of notice and comment on proposed revisions,[122] and a public hearing[123] on draft amendments, the Advisory Committee proposed amendments to Rule 41 that addressed the problems with venue and made explicit provision for the notice to be provided after remote electronic searches.[124] When "technological means," such as Tor, had been used to conceal the location of the media or information, the proposed amendment authorized the issuance of a warrant by "a magistrate judge with authority in any district where activities related to the crime may have occurred."[125] Additionally, in CFAA investigations under 18 U.S.C. § 1030(a)(5), such as botnet investigations, the amendment authorized the government to seek a single warrant when protected computers had been damaged in five or more districts.[126] Finally, the amendment added a new provision regarding notice for remote electronic searches, which required the officer conducting the search to "make reasonable efforts to serve a copy of the warrant and receipt on the person whose property was searched or who possessed the information that was seized or copied."[127] It also allowed service to be

---

[119] Raman letter at 2–3.
[120] *Id*. at 3.
[121] FED. R. CRIM. P. 41(f)(1)(C).
[122] *See* Proposed Amendments to the Federal Rules of Criminal Procedure (posted Aug. 14, 2015) (providing proposed amendments and seeking comments between August 15, 2014 and February 17, 2015) https://www.regulations.gov/docket?D=USC-RULES-CR-2014-0004.
[123] *See* Transcript of Proceedings, Judicial Conf. Advisory Comm. on Crim. Rules, Public Hearing on Proposed Amendments to the Fed. Rules of Crim. Proc., Wash., D.C., Nov. 5, 2014, available at http://www.uscourts.gov/rules-policies/records-and-archives-rules-committees/transcripts-and-testimony.
[124] Comm. on the Rules of Practice and Procedure, Report of the Advisory Comm. on Criminal Rules, (May 6, 2015), in Final Materials for Congress 23, 24 [hereinafter Final Materials for Congress], http://www.uscourts.gov/file/document/2016-04-28-final-package-congress.
[125] FED. R. CRIM. P. 41(b)(6)(A).
[126] FED. R. CRIM. P. 41(b)(6)(B).
[127] FED. R. CRIM. P. 41(f)(1)(C).

"accomplished by any means, including electronic means, reasonably calculated to reach that person."[128]

After review by the Standing Committee on Practice and Procedure, the Judicial Conference, and the Supreme Court, the proposed amendments were submitted to Congress,[129] which took no action and allowed them to go into effect December 1, 2016.[130]

The amendments have generated substantial opposition. Although a variety of other concerns were also raised during the public notice and comment period,[131] "[t]he most common theme in the comments opposing the amendments was a concern that they relaxed or undercut the protections for personal privacy guaranteed by the Fourth Amendment."[132] Critics expressed concern that warrants issued pursuant to the proposed rules would not meet the particularity and notice requirements, would be exceptionally intrusive, destructive, and dangerous, and yet largely insulated from judicial review.[133] Several commentators urged that changes of this nature were not appropriate for rulemaking because they raised policy issues that should be resolved by Congress.[134] Finally, some commentators also urged that the amendments would improperly allow extraterritorial searches in violation of

---

[128] *Id*.

[129] *See* Final Materials for Congress at 201-249 (providing Chief Justice John Roberts' transmittals of proposed amendments to Rule 41 to Congress, Judicial Conference's transmittal of amendments to the Supreme Court, and excerpts from the Report of the Advisory Committee on Criminal Rules to the Standing Committee on Practice and Procedure).

[130] *See* STAFF OF S. COMM. ON THE JUDICIARY, 114TH CONG., 2D SESSION, FEDERAL RULES OF CRIMINAL PROCEDURE: RULE 41 (Comm. Print 2016).

[131] For summaries of the comments, see Adams, *supra* note 107, at 746–48 (noting opponents portrayed amendment as "a substantive expansion on the government's investigative authority, which raised a number of emphatic constitutional, legal, and geopolitical concerns"); Sara Sun Beale & Nancy King, Reporters, Memo to the Members, Advisory Committee on Criminal Rules, Feb. 25, 2015, at 4–18, in Agenda Book, Advisory Comm. on Crim. Rules, March 16-17, 2015, at 87, 90-104, available at http://www.uscourts.gov/rules-policies/archives/agenda-books/advisory-committee-rules-criminal-procedure-may-2015 (describing concerns about (1) the Fourth Amendment, (2) the effect on the use of virtual private networks (VPNs) and anonymizing technology, (3) forum shopping, (4) tension or conflict with the Wiretap Act, 18 U.S.C. § 2518 (Title III), (5) extraterritorial searches, (6) the potential for collateral damage, (7) searches of victim computers, and (8) intrusions into the constitutional and statutory rights of the media).

[132] *Id*. at 4.

[133] *Id*. at 4–10.

[134] *Id*. at 15.

international law.[135] Similar concerns were later raised by Senator Ron Wyden and several other members of Congress.[136]

The Advisory Committee concluded that these constitutional and policy arguments raised substantive issues that were not germane to its task under the Rules Enabling Act,[137] and should be resolved by the courts on a case-by-case basis, or by Congress. The Department of Justice had brought to the Committee's attention a procedural problem that was impairing its ability to investigate serious computer crimes. In the Committee's view, its task was to remove a barrier created by the Rules (not the Constitution), and to allow the courts to rule on constitutional issues if (and when) they were raised by particular warrant applications.[138] The amendment would facilitate judicial review and the development of applicable constitutional standards by allowing the government to seek warrants, rather than conducting exigent warrantless searches.[139] Broad policy questions—such as whether additional non-constitutional limitations should be imposed on

---

[135] *Id*. at 13–15.

[136] *See* Markus Rauschecker, *Rule 41 Amendments Provide for a Drastic Expansion of Government Authority to Conduct Computer Searches and Should Not Have Been Adopted by the Supreme Court*, 76 MD. L. REV. 1085, 1091–92 (2017) (describing congressional opposition).

[137] 28 U.S.C. § 2072 (2012).

[138] *See* HONORABLE REENA RAGGI, ADVISORY COMM. ON CRIMINAL RULES, 13–14 (2015) [hereinafter Committee Report] (explaining Committee's view that "Venue is not substance. Venue is process, and the Rules Enabling Act tells the judiciary to promulgate rules of practice and procedure, not to wait for Congress to act," and expressing the Committee's confidence "judges will address Fourth Amendment requirements on a case-by-case basis both in issuing warrants under these amendments and in reviewing them when challenges are made thereafter."); ADVISORY COMM. ON CRIMINAL RULES, Minutes from Meeting on March 16-17, 2015 in Orlando, Florida, 3–8 (2015) [hereinafter Minutes] (statements by Rule 41 Subcommittee chair and members characterizing many of the objections to the amendments as substantive, not procedural, noting Committee's responsibility under the Rules Enabling Act to address new procedural problem (such as the venue gap), and observing that providing venue for warrant applications would allow caselaw on the constitutional issues to develop in an orderly fashion, shedding light on the issues should Congress wish to legislate). The Advisory Committee addressed this point in the Committee Note, which provides:

> The amendment does not address constitutional questions, such as the specificity of description that the Fourth Amendment may require in a warrant for remotely searching electronic storage media or seizing or copying electronically stored information, leaving the application of this and other constitutional standards to ongoing case law development.

FED. R. CRIM. P. 41(b)(6), 2016 Committee Note.

[139] Minutes at 5 (comments of Judge Raggi and Judge Kethledge), 6 (comments of Judge Sutton).

remote searches to protect privacy—are substantive, not procedural, and accordingly they would fall outside the rulemaking authority conferred by the Rules Enabling Act. Congress would be the appropriate body to weigh the competing policy concerns and consider whether legislation should be enacted.[140] Finally, the Committee was not persuaded by the argument that the amendment would authorize the courts to issue extraterritorial searches in violation of international law.[141]

Post-amendment scholarship has renewed and developed more fully the Fourth Amendment issues,[142] and produced a debate about whether Rule 41 authorizes searches that raise foreign relations and international law concerns. One recent article argued that searches authorized by the amendments to Rule 41 violate other nations' sovereignty, which offends customary international law and disrupts foreign relations.[143] But other

---

[140] *See* Committee Report at 13–14 (noting that many of the objections to the proposed amendments "were about substantive limits on government searches, which are not affected by the proposed amendment"); Minutes at 3, 5 (comments of Judge Kethledge) (subcommittee chair's characterization of many objections to the amendments as substantive, not procedural), 6 (comments of Judge Sutton) (noting that approving venue for searches was not approving remote electronic searches; rather, it permits litigation "that will shed light on the process and the issues," and noting that under the Rules Enabling Act the judiciary's role is to promulgate rules, to which Congress reacts).

[141] *See* Raman letter at 4–5 (citations omitted), stating:

> In light of the presumption against international extraterritorial application, and consistent with the existing language of Rule 41(b)(3), this amendment does not purport to authorize courts to issue warrants that authorize the search of electronic storage media located in a foreign country or countries. The Fourth Amendment does not apply to searches of the property of non-United States persons outside the United States, and the Fourth Amendment's warrant requirement does not apply to searches of United States persons outside the United States. Instead, extraterritorial searches of United States persons are subject to the Fourth Amendment's "basic requirement of reasonableness." Under this proposed amendment, law enforcement could seek a warrant either where the electronic media to be searched are within the United States or where the location of the electronic media is unknown. In the latter case, should the media searched prove to be outside the United States, the warrant would have no extraterritorial effect, but the existence of the warrant would support the reasonableness of the search.

[142] *See* Rauschecker, *supra* note 136, at 1095–1100 (arguing that the amendment allows searches that will violate the Fourth Amendment and greatly expand the government's investigative authority); Adams, *supra* note 107, at 753–72 (proposing a Fourth Amendment framework for courts considering remote access warrants).

[143] *See* Ghappour, *supra* note 104.

scholars disagreed, noting "the pervasive nature of transnational law enforcement cooperation generally and the existing practice of government cooperation and coordination in dark web investigations specifically," and challenging the claim that the use of NITs in this context would violate international law.[144]

The law governing remote electronic searches is still in its infancy. Because Rule 41(b)(6) now provides venue for remote electronic searches, it has opened the courthouse door not only to applications seeking these warrants, but also to litigation challenging particular searches on constitutional grounds. This litigation will allow the development of precedents that will clarify—and may limit—remote electronic searches. There may also be legislative developments. Bills have been introduced in both houses to repeal the amendments to Rule 41,[145] and Congress may eventually develop a framework to regulate remote electronic searches, as it did with wiretaps.[146] The imposition of additional limits on remote searches could have a significant impact on the government's ability to prosecute hacking, given the practical necessity to use remote searches to identify hackers.

C. Jurisdiction to Prosecute Extraterritorial Conduct

If hacking originates outside the United States, it raises the question of whether the CFAA has extraterritorial reach. Unlike some other federal statutes,[147] the CFAA does not expressly confer jurisdiction over conduct that occurred outside the United States. It is well established that the United States exercises jurisdiction to prescribe with respect to conduct that occurs within its territory,[148] and U.S. statutes are presumed to apply in United

---

[144] *See* Kerr & Murphy, *supra* note 101, at 61.

[145] Stop Mass Hacking Act, S. 406, 115th Cong., 1st Sess. (2017); Stop Mass Hacking Act, H.R. 1110, 115th Cong., 1st Sess. (2017).

[146] *Cf.* Minutes at 6 (comments of Prof. Beale) (noting that as in the case of Title II, Congress enacted limitations on wire taps after case law shed light on the policy issues).

[147] *See*, *e.g.*, 18 U.S.C. § 1956(f) (providing extraterritorial jurisdiction over money laundering if the transactions involve more than $10,000 and the conduct is by a U.S. citizen or by a non-U.S. citizen in the United States); 18 U.S.C. § 1596(a) (providing extraterritorial jurisdiction over several trafficking offenses if the alleged offender is a national of the United States or a permanent resident alien, or "the alleged offender is present in the United States, irrespective of the nationality of the alleged offender.")

[148] RESTATEMENT (FOURTH) THE FOREIGN RELATIONS LAW OF THE UNITED STATES: JURISDICTION § 201(1)(a), comment E (AM. LAW INST. Tentative Draft No. 2, 2017) (approved May 22, 2017). *See also* Diane Marie Amann, *Jurisdictional, Preliminary, and Procedural Concerns*, AM SOC'Y INT'L L, www.asil.org/bench book/jurisdiction.pdf (last visited Mar. 12, 2017).

States territory.[149] Although the U.S. also recognizes prescriptive extraterritorial jurisdiction based upon nationality, active and passive personality, the protective principle, and universal jurisdiction,[150] the question whether a particular crime will have extraterritorial application must be determined by the courts. This determination is subject to a presumption in favor of domestic application of U.S. laws and against extraterritoriality. In a series of recent decisions, the Supreme Court has reemphasized and strengthened the presumption against extraterritoriality, raising the question whether the CFAA will be construed to have extraterritorial effect.

1. Statutory Construction and Extraterritoriality

In *United States v. Bowman*, a decision from 1922, the Supreme Court indicated that some offenses are not subject to the presumption against extraterritorial application. The Court recognized that crimes "affect[ing] the peace and good order of the community," such as murder, robbery, and arson, are presumed to be territorial.[151] Other crimes, however, are "not logically dependent on their locality for the government's jurisdiction, but are enacted because of the right of the government to defend itself against obstruction, or fraud wherever perpetrated," and they are not presumed to be territorial.[152] In the intervening decades, that lower courts understood *Bowman* to mean "a substantial number of . . . crimes operate overseas by virtue of the implicit intent of Congress."[153]

Recent decisions in the Supreme Court have tightened the rules of statutory interpretation, restricting access to the federal courts in civil cases involving extraterritorial conduct and casting doubt on the continuing vitality of *Bowman*. In two major civil cases, *Kiobel*[154] and *Morrison*[155] the Court instructed the federal courts to apply a strong presumption against

---

[149] *Id*.
[150] *See* RESTATEMENT (THIRD) OF THE LAW OF FOREIGN RELATIONS § 401 (AM. LAW INST. 1987); RESTATEMENT (FOURTH) THE LAW OF FOREIGN RELATIONS OF THE UNITED STATES: JURISDICTION § 101 (AM. LAW INST., Tentative Draft No. 3, 2017) (approved May 22, 2017).
[151] United States v. Bowman, 260 U.S. 94, 98 (1922).
[152] *Id.*
[153] Charles Doyle, Cong. Research Serv., No. 94-166, *Extraterritorial Application of American Criminal Law* 19–20 (2016). *See also* S. Nathan Williams, Note, *The Sometimes "Craven Watchdog": The Disparate Criminal-Civil Application of the Presumption Against Extraterritoriality*, 63 DUKE L.J. 1381, 1395 (2014) (stating "courts have found that some crimes are so inherently transnational as to deserve the blessing of the *Bowman* exception. Typical crimes in this . . . category include trafficking (human or drug) and racketeering.").
[154] Kiobel v. Royal Dutch Petroleum Co., 569 U.S. 108, 124 (2013).
[155] Morrison v. Nat'l Austl. Bank Ltd., 561 U.S. 247, 265 (2010).

extraterritoriality: absent a clearly expressed congressional intent to the contrary, federal laws will be construed to have only domestic application.[156] In justifying this presumption, the Court emphasized the need to avoid international discord[157] or friction, as well as the "common sense" view that Congress ordinarily focuses on domestic matters.[158]

Although the Supreme Court has not expressly overruled *Bowman*, it is doubtful whether that case is still good law. Initially, many courts and commentators concluded that *Bowman* had not been overruled or limited.[159] But the Court's decision in a *RJR Nabisco v. European Community*,[160] a civil suit brought under the Racketeering and Corrupt Organization (RICO) Act,[161] cast serious doubt on the Supreme Court's continued adherence to *Bowman*. The Court first considered the question whether the criminal provisions of RICO itself (and various federal crimes that are RICO predicate offenses) have extraterritorial effect.[162] The Court drew no distinction between civil and criminal statutes. In determining the reach of these offenses, the Court applied the presumption against exterritorial effect, citing its prior decisions in civil cases.[163] It stated:

> The question is not whether we think "Congress would have wanted" a statute to apply to foreign conduct "if it had thought of the situation before the court," but whether Congress has affirmatively and unmistakably instructed that the statute will do so. When a statute gives no clear indication of an extraterritorial application, it has none."[164]

The Court did not discuss or even cite the *Bowman* decision, but this passage can be read as repudiating the *Bowman* approach. As one commentator stated, "the Court seemed to take direct aim at *Bowman* without naming it,"[165] and the American Law Institute's *Restatement of Foreign Relations (Fourth)* treats the presumption against extraterritoriality as fully applicable to criminal statutes.[166]

---

[156] *Kiobel*, 569 U.S. at 117; *Morrison*, 561 U.S. at 261.
[157] *Kiobel*, 569 U.S. at 117.
[158] RJR Nabisco v. European Cmty., 136 S. Ct. 2090, 2100 (2016).
[159] Doyle, *supra* note 153, at 10, n.45 (collecting cases).
[160] *Nabisco*, 136 S. Ct. at 2093.
[161] 18 U.S.C. § 1962 (1970).
[162] *Nabisco*, 136 S. Ct. at 2099–2106.
[163] *Id.* at 2100–01.
[164] *Id*. at 2100 (citations omitted).
[165] Doyle, *supra* note 153, at 10.
[166] *See* RESTATEMENT (FOURTH) THE LAW OF FOREIGN RELATIONS OF THE UNITED STATES: JURISDICTION § 203 reps. notes 1, 4 (AM. LAW INST., Tentative Draft No. 3) (approved May 22, 2017) (describing evolution of presumption, drawing no

2. Construing the CFAA

The CFAA would be severely hamstrung if it were not applicable to foreign-based hacking, and there is some evidence that Congress intended the CFAA to have extraterritorial application. But it is not clear whether the evidence is sufficient to demonstrate that Congress "clearly and unmistakably" directed that result. Thus, the CFAA could provide the test case to determine whether the strong presumption developed in civil cases will be applied with the same rigor in construing criminal statutes, particularly those involving crimes that inherently cross borders. The balance of interests may be calculated differently in civil and criminal cases, since the Executive Branch, which controls foreign relations, is also responsible for the discretionary determination whether to prosecute cases that may have foreign relations implications.

Only one district court has considered whether the CFAA provides for extraterritorial jurisdiction, and that decision predated the Supreme Court's decision in *RJR Nabisco*. In *United States v. Ivanov*[167] the defendant, who was physically in Russia, hacked into the computer system of a financial-transaction clearinghouse using an internet service provider located in the state of Washington. Noting the detrimental effect of the conduct occurred in the United States,[168] the court concluded it had subject matter jurisdiction and turned to the question whether the CFAA provided for extraterritorial jurisdiction. It recognized the presumption against extraterritoriality, but found that Congress "clearly manifested its intention" to give the CFAA extraterritorial effect.[169]

The *Ivanov* court focused on several changes made by Congress in 1996. Although the changes to the text focused on defining which computers were protected and what conduct was prohibited, the legislative history indicates the Senate was concerned about foreign-based hackers. As the *Ivanov* court noted, the 1996 amendments revised the definition of "protected computer" to include a computer used in "foreign commerce or communication," added subsections dealing with "interstate or foreign commerce," and defined the term "government entity" to include foreign governments.[170] Foreign commerce, in this context, "must mean international" commerce.[171] The legislative history, moreover, suggests that Congress intended the CFAA to apply to foreign-based hackers. As the court noted, the Senate Judiciary Committee "specifically noted its concern

---

distinction between civil and criminal or private and public enforcement, and concluding *Bowman* can be read to be consistent with more recent cases).

[167] United States v. Ivanov, 175 F. Supp. 2d 367, 368–69 (D. Conn. 2001).

[168] *Id*. at 370–73.

[169] *Id*. at 373, 375.

[170] *Id*. at 374.

[171] *Id*.

that . . . hackers are often foreign-based," and cited two specific instances of foreign-based hackers as examples of the kind of cases that the amendments were intended to address.[172]

Under the Supreme Court's recent decisions on extraterritorial jurisdiction, it is not clear whether other courts will follow *Ivanov*. On the one hand, courts construing the CFAA will be well aware that construing it to apply only to conduct that occurs in the United States would severely limit its effectiveness. However, it is doubtful whether a brief passage from a committee report constitutes an affirmative and unmistakable instruction that the CFAA should be applied to extraterritorial conduct, as well as to computers engaged in foreign commerce or and communication, including protected computers located outside the United States.[173] Thus a challenge to the CFAA's jurisdiction could provide a test for the criminal applicability of the most restrictive language in *RJR Nabisco*.[174]

Some scholars of international law have expressed concern that extraterritorial hacking prosecutions may violate international law,[175] and those concerns might trigger the application of two other rules of statutory construction in CFAA prosecutions. First, the federal courts apply the so-called *Charming Betsy* principle that "an act of Congress ought never to be construed to violate the law of nations if any other possible construction remains."[176] This principle is applied, however, only when a construction avoiding such a conflict is "fairly possible."[177] But when such a

---

[172] *Id*., citing S. Rep. No. 357, 104th Cong. (2d Sess. 1996).

[173] *See also* Doyle, *supra* note 153, at 6–7, 33–35 (noting the question whether 18 U.S.C. 1030(a)(3), which criminalizes access to government computers, is applicable to extraterritorial conduct).

[174] One factor that might affect the courts' response, at least at the margins, is a perception that concerns about interference with U.S. foreign relations should be less important in criminal than in civil cases. Private civil claimants may neither know, nor care about, the possible diplomatic and foreign relations problems their case may generate. In contrast, the Executive Branch has responsibility for both foreign affairs and the enforcement of criminal laws. In cases involving the interests of other nations—such as the prosecution of foreign-based hackers—the Executive can weigh any foreign relations or foreign policy concerns in exercising prosecutorial discretion. However, because the CFAA does create a private right of action for civil damages, any extraterritorial interpretation would apply to civil cases as well. *See* 18 U.S.C. § 1030(g) (2012) (authorizing civil actions for "compensatory damages and injunctive relief or other equitable relief).

[175] *See*, *e.g.*, Stockton & Golabek-Goldman, *supra* note 95 (analyzing international law grounds for extraterritorial jurisdiction applied to cyberterrorism).

[176] Murray v. The Schooner Charming Betsy, 6 U.S. 64, 118 (1804).

[177] *See* RESTATEMENT (FOURTH) THE LAW OF FOREIGN RELATIONS OF THE UNITED STATES: JURISDICTION § 205 reps. notes 1, 4 (AM. LAW INST., Tentative Draft No.

construction is not fairly possible, the intent of Congress—rather than international law—governs, and "the federal statute is controlling as a matter of law."[178] The Supreme Court has also twice invoked the canon of "construi[ing] ambiguous statutes to avoid unreasonable interference with the sovereign authority of other nations."[179]

D. Success Against the Odds

Despite the practical and legal difficulties, there have been some successful efforts to prosecute and disrupt hacking, the most recent of which involved the use of the Rule 41 amendments.

In April 2017, the Department of Justice announced "an extensive effort to disrupt and dismantle the Kelihos botnet," which it described as "a global network of tens of thousands of infected computers under the control of a cybercriminal that was used to facilitate malicious activities including harvesting login credentials, distributing hundreds of millions of spam e-mails, and installing ransomware and other malicious software."[180] Pursuant to amended Rule 41, the Department of Justice had obtained a single warrant authorizing it to "redirect Kelihos-infected computers to a substitute server and to record the Internet Protocol addresses of those computers as they connect to the server."[181] This allowed "the government to provide the IP addresses of Kelihos victims to those who can assist with removing the Kelihos malware including internet service providers."[182] Some critics of the Rule 41 amendments were impressed that the government had been protective of individual privacy: it collected only the victims' IP addresses and "non-content" routing and signaling information so Internet Service Providers could notify the victims.[183] Moreover, the court order "limited the government's interactions with victimized computers to commands that block an infected computer from performing malicious activities and communicating with other devices on the botnets," which prohibits the government from seizing any of the contents of victim

---

3) (approved, May 22, 2017); *Accord* RESTATEMENT (THIRD) OF THE LAW OF FOREIGN RELATIONS § 114 (AM. LAW INST. 1987).

[178] *Id.*

[179] F. Hoffmann-La Roche Ltd. v. Empagran S.A., 542 U.S. 155, 164 (2004). This canon has not, however, been invoked by the Court since its 2007 holding in Microsoft Corp. v. AT&T Corp., 550 U.S. 437, 455 (2007).

[180] Dep't of Justice, *Justice Department Announces Actions to Dismantle Kelihos Botnet*, DEPARTMENT OF JUSTICE (Apr. 10, 2017), https://www.justice.gov/opa/pr/justice-department-announces-actions-dismantle-kelihos-botnet-0.

[181] *Id*.

[182] *Id.*

[183] Aliya Sternstein, *FBI Allays Some Critics with First Use of New Mass-Hacking Warrant*, ARSTECHNICA (Apr. 24, 2017), https://arstechnica.com/tech-policy/2017/04/fbi-allays-some-critics-with-first-use-of-new-mass-hacking-warrant/.

computers.[184] But other commentators were critical of the government's efforts because they involved invading the victim computers to take corrective actions.[185] To permanently disable the Kelihos botnet, the government had to prevent the victim computers from communicating with other hacker-controlled devices.[186]

The government also collected sufficient information to attribute the Kelihos botnet to Russian hacker Peter Yuryevish Levashov, who was indicted for CFAA violations and other related charges.[187] In an ironic twist of fate, government investigators finally linked Levashov to the botnet because he had committed the same security lapse that allows cybercriminals to victimize innocent consumers: using the same IP and login credentials on various consumer sites, including Apple and Google.[188] With the cooperation of Spanish authorities, Levashov was arrested in Spain while on holiday, the National Court of Spain ruled that he could be extradited, and he was brought to the United States in February 2018.[189]

V. LEGALIZING HACKING BACK AGAINST BOTNETS

Although the CFAA provides a tool to prosecute hacking in the IoT, given the difficulties implicit in bringing prosecutions under it, other solutions are needed to address the dangers posed by the IoT. This section discusses one such possible solution: remedial action.190 Although

---

[184] *Id*.

[185] *See, e.g.*, Tim Cushing, *FBI Tries New Rule 41 Changes on Size in Fight Against Long-Running Botnet for Size*, TECHDIRT (Apr. 12, 2017), https://www.techdirt.com/articles/20170411/09411837126/fbi-tries-new-rule-41-changes-size-fight-against-long-running-botnet.shtml.

[186] *See* Sternstein, *supra* note 183 (quoting security expert involved in Kelihos cleanup who explained that because of the peer-to-peer nature of this botnet, "the FBI 'had to infect machines,' convert them into so-called supernodes that distribute connection lists to other victimized computers, and then 'poison' all the computers so they would never again try to communicate with hacker-controlled devices").

[187] Garrett M. Graff, *How the FBI Took Down Russia's Spam King*, WIRED (Apr. 11, 2017), https://www.wired.com/2017/04/fbi-took-russias-spam-king-massive-botnet/.

[188] *Id*.

[189] *See* Andrew Blake, *Foreign Courts OK Extradition of Russians Charged in U.S. Cybercrime Probes*, WASH. TIMES (Oct. 4, 2017), https://www.washingtontimes.com/news/2017/oct/4/peter-levashov-and-alexander-vinnik-russians-charg/ (describing Spanish court's approval of extradition to the United States); U.S. Department of Justice, *Alleged Operator of Kelihos Botnet Extradited From Spain*, Feb. 2, 2018, https://www.justice.gov/opa/pr/alleged-operator-kelihos-botnet-extradited-spain.

[190] We use the term "hacking back" to refer to invasive counterattacks. We use the term "remedial action" to denote the broader category of self-help measures which hacking back is a part of.

remedial actions might sometimes be useful when hackers seek to control an object as discussed in Section III.A., we will focus here on their potential to reduce the threat posed by botnets, where such efforts would have the greatest utility. It is a controversial route, mired in legal, ethical, and practical dilemmas. This section begins by discussing the danger of botnets, the potential benefit of hacking back, and the legal barriers to doing so. It then assesses how hacking back may be legalized, before summarizing some of its primary critiques.

A. The Danger of Botnets and the Allure of Hacking Back

The Botnets have a different relationship to the IoT than many of the other dangers discussed in this article. Much of this article focuses on how the internet may be used to corrupt devices connected to it.[191] In contrast, botnets present the reverse issue: devices connected to the internet may be used to disrupt the internet itself.[192] Compounding the problem, botnets are not only an existential threat to the internet but a persistent one as well. Without curative solutions, botnets can be used in multiple crimes.[193] Once a device is recruited into a botnet, it becomes part of a "commodity" that can be rented out "by the hour" or purchased.[194]

Thus, to eliminate the threat of botnets, a solution with retroactive and curative force is needed. Enter hacking back, part of a larger concept of internet self help or remediation encompassing terms such as counterstrikes, "'active defense,' 'back hacking,' 'retaliatory hacking,' or 'offensive countermeasures'"[195] As the assorted terms suggest, remedial action encompasses a range of different self-help measures to prevent and counter botnets and hacking. Remedial actions might "enable attacked parties to detect, trace, and then actively respond to a threat by, for example, interrupting an attack in progress to mitigate damage to the system."[196] Specific strategies could include implementing a "DoS attack at the botnet controller or hacking the botnet controller and thereby taking control of the botnet."[197] However, not all remedial efforts are so forceful: "Hacking back

---

[191] See discussion *supra* Section I.A.

[192] *See supra* notes 11–19 and accompanying text (describing the role of botnets in the Dyn attack which disrupted several leading websites).

[193] One illustration of the resilience of botnets can be found in Microsoft and Europol's attempt to dismantle the ZeroAccess botnet: despite taking down portions of the botnet it was revived within months. Goldman, *supra* note 86, at 610.

[194] Janine S. Hiller, *Civil Cyberconflict: Microsoft, Cybercrime, and Botnets*, 31 SANTA CLARA HIGH TECH. L.J. 163, 168–69 (2015).

[195] Sean L. Harrington, *Cyber Security Active Defense: Playing with Fire or Sound Risk Management?*, 20 RICH. J.L. & TECH. 12, at *4 (2014). *See* Kesan, *supra* note 60, at 434 (using the terms "hack back" and "counterstrike").

[196] *Id.* at 475.

[197] *Id.*

against a botnet can be as simple and nonaggressive as pushing security patches onto infected computers, just as patients with a deadly virus could be forcibly treated or quarantined to prevent a contagion's spread."[198] Unlike enforcement and litigation which do little to prevent future attacks, and are "inherently *ex post facto*,"[199] hacking back has the crucial ability to prevent future attacks by combatting existing botnets.

Despite these potential benefits, there is also a potential problem. At least if undertaken by private parties,[200] such behaviors may be illegal.[201] Ironically, "[t]he same laws that make it illegal to hack in the first place—for instance, to access someone else's system without authorization—presumably make it illegal to hack back."[202] The CFAA both criminalizes botnets and limits recourse against them.[203] The Department of Justice, the FBI, and "White House officials" have all suggested that such remedial efforts may be illegal.[204] Scholarship echoes this conclusion.[205] As a result, the legal regime that is intended to protect the public from hacking also limits the manner in which such dangers may be fought. A logical question then, is how hacking back might be legalized.[206]

B. Possible Theories for the Legalization of Hacking Back

There are a variety of ways in which hacking back might be legalized. This subsection focuses primarily on one possibility: creating exceptions for strikebacks through a legal framework modeled on the laws governing recapture of property. It then briefly summarizes other possibilities.

Recapture laws provide a promising framework for remedial action. They balance two conflicting considerations implicated by hacking back: the right to protect personal property, and the understanding that that right cannot be absolute. On the one hand, "[t]he law has always recognized that a person is justified in using some degree of force to protect his property

---

[198] Patrick Lin, *Ethics of Hacking Back*, U.S. NAT'L SCI. FOUND. (Sept. 26, 2016), http://ethics.calpoly.edu/hackingback.pdf.
[199] *See* Kesan, *supra* note 60, at 474.
[200] For a discussion of the government's use of remedial measures to neutralize the Kelihos botnet, *see* supra notes 174–80 and accompanying text.
[201] *See* Kesan, *supra* note 60, at 475 ("Even though counterstrikes are currently of questionable legality . . . .").
[202] Lin, *supra* note 198, at 6.
[203] *Id.* (identifying CFAA as a law contributing to this paradox).
[204] *Id.*
[205] *See* Harrington, *supra* note 195, at *17 ("[T]here is little debate that affirmative retaliatory hacking is unlawful . . .").
[206] Some less aggressive remedial actions may be legal. Although a full review is beyond the scope of this paper, for a summary, *see id.* at *9–*16.

from wrongful invasion or appropriation by another."[207] On the other, the law has been wary of the dangers surrounding self-help measures to regain property.[208]

The Model Penal Code (MPC) provides an important compromise of these conflicting interests in the context of recaption of property. Under MPC 3.06(1)(b), "use of force upon or toward the person of another" when protecting property is justifiable if:

> [T]he actor believes that such force is immediately necessary . . . to effect an entry or re-entry upon land or to retake tangible movable property provided that the actor believes that he or the person by whose authority he acts or a person from whom he or such other person derives title was unlawfully dispossessed of such land or movable property and is entitled to possession, and provided, further, that:
>
> > (i) the force is used immediately or on fresh pursuit after such dispossession; or
> >
> > (ii) the actor believes that the person against whom he uses force has no claim of right to the possession of the property and, in the case of land, the circumstances, as the actor believes them to be, are of such urgency that it would be an exceptional hardship to postpone the entry or re-entry until a court order is obtained.[209]

Although closely related to the use of force to protect property, recaption is separate in the Model Penal Code.[210]

This separate right of recaption provides a useful template for laws governing hacking back, although further analogy is necessary. Returning to the example of Bill and Jeremy, imagine that Jeremy steals some of Bill's

---

[207] *The Use of Deadly Force in the Protection of Property Under the Model Penal Code*, 59 COLUM. L. REV. 1212 (1959).

[208] *See* MODEL PENAL CODE: ANALYSIS AND RECOMMENDATIONS § 3.06 comment 5(c) (AM. LAW INST. 1985) ("To allow recaption in [the circumstance of retaking chattel after time has elapsed] would create a grave risk of a breach of the peace, for the aggressor acting under the claim of right is likely to defend his newly won possession, and to permit recaption would therefore to be to permit fighting. . . . [The purpose of the traditional Statute of Forcible Entry governing recapture of land was to] "require parties to submit disputes to the courts, and thus to prevent breaches of the peace."

[209] MODEL PENAL CODE: ANALYSIS AND RECOMMENDATIONS § 3.06(1)(b) (AM. LAW INST. 1985).

[210] *See* MODEL PENAL CODE: ANALYSIS AND RECOMMENDATIONS § 3.06 comment 5(e) (AM. LAW INST. 1985) (explaining that the Model Penal Code distinguishes between "rules for the use of protective force and the rules for re-entry and recaption . . . .").

personal possessions. Applying the test of MPC 3.06, it could be justifiable for Bill to take back his personal property if he believed it "immediately necessary." Jeremy's initial interference with Bill's property rights justifies some resulting intrusion by Bill into Jeremy's rights.

To illustrate how the framework of MPC 3.06 could shape laws governing hacking back, imagine the digital equivalent. Assume that Bill operates a thriving retail and manufacturing business out of his home comprised of a computer, a website, and an internet enabled 3D printer. Jeremy hacks into Bill's computer and steals consumer credit card information stored on it, saving it to his hard drive. Jeremy also controls a sizeable botnet through his personal computer and directs it to launch a DDoS attack on Bill's website, bringing it down. Finally, Jeremy exploits the botnet to gain control of Bill's 3D printer and causes it to malfunction. The basic scenario is the same as in the hypothetical above: Jeremy has interfered with Bill's property. Only the nature of the intrusion is different. Bill still has physical possession of his computer and printer, but Jeremy has wrongfully copied some files, and taken control of the printer. If MPC 3.06 were the framework for hacking back laws, Bill might be able to hack back to erase the stolen files, end the DDoS attack, and regain control of his printer. It is analogous to Bill taking back his physical property above. The basic premise is the same: Jeremy's meddling with Bill's property merits some form of response to restore Bill's property interests.

Of course, there is a fundamental threshold difference between recaption as envisioned by MPC 3.06, and hacking back of the sort contemplated in the Bill and Jeremy example. The MPC right of recaption is not directly relevant to hacking back. It provides a justification for the use of non-deadly force against the person of another, rather than for interference with property, such as a computer within the meaning of the CFAA. Except for the general defense of "choice of evils," the MPC does not address the justification for interference with property.[211] However, the law generally regards any use of force against a person as a more serious wrong than interference with personal property. Therefore, the framework for recaption in MPC 3.06 should be sufficient, as a policy matter, to justify the lesser wrong of interference with personal property.

Such interference already has a close analogy in the context of torts. Although tort law does not permit the use of force for recapture of chattels "once possession is clearly lost," it "permits a defendant who is entitled to immediate possession to recover the goods from another's land (a) if the defendant did not cause the intrusion of the goods in the first place and (b)

---

[211] *See* MODEL PENAL CODE: ANALYSIS AND RECOMMENDATIONS § 3.02 (AM. LAW INST. 1985).

if entry is reasonable as to both time and manner."[212] For example, "[i]t is not disputed that if . . . [chattels belonging to another] have come upon the land through the wrongful conduct of the landowner, a privilege to enter and recover them exists."[213] In exercising that privilege, "[r]easonable amounts of damage may be done, even to the extent of breaking down a fence or a door . . . The privilege is complete, and, so long as only reasonable force is used, the defendant is not liable for any damage he may do."[214] In some circumstances a person may use force against the physical property of someone who has taken his own property, in the attempt to recapture it. This is particularly instructive in the context of hacking back, because breaking down a thief's door to regain stolen property is similar to hacking back against a digital aggressor to restore a compromised computer.

Allowing for some leeway regarding where force may be directed in recapturing property, the conceptual underpinning of MPC 3.06 fits well with the basic nature of remedial action in the IoT. Reworking is necessary to accommodate the differences between the physical and digital arenas, because they result in somewhat distinct property interests and methods of recaption. A rudimentary sketch of a law governing counterstrikes may be imagined by modifying MPC 3.06(1)(b) to rectify these disparities and to clarify that force may be used against the *property* of another:

> Damage to, intrusion into, or interference with, the computer of another . . . is justifiable when protecting property . . . if the actor believes that such action is immediately necessary . . . to regain control of a computer, website, digital information, or computer enabled device, provided that the actor [reasonably][215] believes that he or the person by whose authority he acts . . . was unlawfully deprived of control of such computer, website, digital information, or computer enabled device . . . and is entitled to regain control, and provided, further, that:
>
> > (i) the action is used immediately after such interference with control; or

---

[212] Dan B. Dobbs et al., THE LAW OF TORTS § 91, at 275, 278 (2d ed. 2011).
[213] W. Page Keeton et al., PROSSER AND KEETON ON THE LAW OF TORTS § 22, at 139 (5th ed. 1984).
[214] *Id.* at 140.
[215] It would be important to consider whether to qualify a defense based on 3.06 with the requirement that the defendant's beliefs be reasonable. M.P.C. Section 3.06 focuses solely on the defendant's subjective belief. But it is qualified by Section 3.09(2), which makes the defense unavailable for certain offenses if the defendant was reckless or negligent in having a belief required for 3.06 or other justification defenses. *See* MODEL PENAL CODE AND COMMENTARIES, §3.09 comment 2 (AM. LAW INST. 1985).

> (ii) the actor believes that the person against whom he takes this action has no claim of right to the interference with control of the computer, website, digital information, or computer enabled device . . . ."

This formulation is intended as merely a rough illustration of how the template of recaption law might apply to hacking back, and to further paint the analogy between recapture of physical property and remedial action in the IoT. A comprehensive statute is well beyond the scope of this paper. Nevertheless, an additional consideration demands attention.

MPC 3.06 contains temporal limitations that could greatly hinder an analogous right to hack back. MPC 3.06(1)(b) demands immediacy, requiring a belief of "immediate" necessity, and actions that are "used immediately or on fresh pursuit after such dispossession."[216] These requirements may be impractical in the context of an attack in the IoT because it may be impossible to quickly assess the harm and identify the perpetrator.[217] State laws modifying MPC 3.06 provide models for a more flexible timing requirement. For example, Connecticut allows force for the recapture of personal property "when and to the extent that [the recapturer] reasonably believes such to be necessary . . . to regain property which he reasonably believes to have been acquired by larceny within a reasonable time prior to the use of such force."[218] Extending the window in which the victim of a botnet attack may respond from immediacy to reasonableness, as Connecticut does for recaption, could better accommodate a range of remedial actions.

With these modifications to recapture law framework, more aggressive forms of hacking back might be legally permissible. Of course, creating a right of reentry or recapture based on the MPC is just one way that hacking back might be legalized. Other routes have been suggested. For example, one proposal would amend the CFAA to allow a limited self-help privilege narrowly cabined by four requirements:

> (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

---

[216] *Id.* We omitted the MPC language about "fresh pursuit" from our model statute because we are unaware of a digital equivalent for the concept.

[217] *See* Lin, *supra* note 198, at 15 (observing that quick attribution is inaccurate, and accurate attribution is slow).

[218] CONN. GEN. STAT. § 53a-21 (1969).

> parties, and liability for all negligently caused unnecessary damage to the original attacker. [219]

Amending the CFAA has some proponents in Congress. Indeed,

> Georgia representative Tom Graves proposed the Active Cyber Defense Certainty Act (ACDC), which would change the CFAA so that it would not apply to victims of cyberattacks who accessed attackers' networks to "gather information in order to establish attribution of criminal activity to share with law enforcement" or to "disrupt continued unauthorized activity against the victim's own network."[220]

Others propose a path for legalizing remedial action through analogy to retail security guards,[221] bounty hunters, or private investigators.[222] Under these theories, remedial actions like planting malware in botnets or searching the networks of invaders could be "considered seizure of an offensive weapon" or security patrols, respectively. Other theories have looked to tort law exceptions such as private nuisance, trespass to chattels,[223] "the recapture of chattels privilege, entry upon land to remove chattels, private necessity, or even the castle doctrine."[224] But even if legalizing hacking back under any of these theories would be possible, it is not necessarily a good idea. The next subsection explores the pitfalls.

C. The Ethical and Logistical Problems with Hacking Back

Hacking back has garnered considerable attention in the wake of prominent hacks,[225] but the attention has not all been positive.[226] Critics have highlighted a range of logistical and ethical issues. Logistically, it is

---

[219] Shane Huang, *Proposing a Self-Help Privilege for Victims of Cyber Attacks*, 82 GEO. WASH. L. REV. 1229, 1259 (2014).

[220] Josephine Wolff, *When Companies Get Hacked, Should They Be Allowed to Hack Back?.*, ATLANTIC (Sept. 27, 2017), https://www.theatlantic.com/business/archive/2017/07/hacking-back-active-defense/533679/.

[221] Harrington, *supra* note 195, at 24–25.

[222] *See* Wolff, *supra* note 220 (interviewing Stewart Baker).

[223] Huang, *supra* note 219, at 1241–49.

[224] Harrington, *supra* note 195, at 23–24. Indeed, the Restatement Second of Torts has many provisions which could be applicable to hacking back, but are beyond the scope of this criminal law-focused article. *See, e.g.*, RESTATEMENT (SECOND) OF TORTS §§ 100–110 (AM. LAW INST., Tentative Draft No. 17, 1974); RESTATEMENT (SECOND) OF TORTS §§ 197–201, 213–215 (AM. LAW INST., 1965).

[225] *See* Lin, *supra* note 198, at 2 (noting that in light of "any number of high-profile incidents" it is "no wonder that self-help by way of 'hacking back' has been gaining attention").

[226] *See* Wolff, *supra* note 220 ("Legalizing proactive responses to cybercrime is a wildly unpopular idea.").

unclear that hacking back would be an effective solution even if legalized. One major logistical concern is the danger of escalation. Hacking back may create new attacks rather than end ongoing ones.[227] Two considerations magnify this danger. First, not all hackers will be deterred by remedial action.[228] Some, such as hacktivists, may welcome the challenge and ramp up their attacks.[229] Alternatively, where the initial aggressor is a foreign government or criminal organization, escalated retaliation is likely.[230] American companies engaged in hack backs against such actors will not be able to out-violate the law.[231] Second, companies are not as well-equipped as the government to assess the likelihood of foreign escalation.[232] Disturbingly, a company's remedial action could be perceived by a foreign country as "a military response from our state."[233] Remedial action from an American company could become "the opening volleys of a cyberwar, which could escalate into a physical or kinetic war."[234]

Another major logistical concern focuses on the danger that remedial actions could create chaos in the wake of hacks. Some in law enforcement warn that remedial action could "lead to confusion in investigating cyberattacks."[235] Remedial action looks similar to the tools used by the initial aggressors, and makes it "much harder to distinguish between the good guys and the bad guys online."[236] And remedial action could also muddle the judicial recourse for cyberattacks because evidence gained through hacking back may be inadmissible for those bringing suit under the CFAA.[237]

One last logistical criticism of remedial action is rooted in the relationship between companies and the cybersecurity firms they may contract with to provide remedial action. Cybersecurity firms are given access to corporate networks and are in the ideal position to steal information from the companies that hired them.[238] Even if outright theft by cybersecurity firms is unlikely, there is a perverse incentive. As one article phrased the relationship: "Would there not be a conflict of interest . . .

---

[227] *Id.* (Security experts are concerned that hacking back could become a "vehicle for more attacks.").
[228] Harrington, *supra* note 195, at 28.
[229] *Id.*
[230] *Id.*
[231] *Id.*
[232] Lin, *supra* note 198, at 14.
[233] *Id.* at 15.
[234] *Id.*
[235] Wolff, *supra* note 220.
[236] *Id.*
[237] Harrington, *supra* note 195, at 26.
[238] Wolff, *supra* note 220.

between treating a problem (ongoing revenue for your security firm) and curing it (which ends their engagement)?"[239]

The ethical critiques of remedial action are similarly varied. One focuses on the relationship between private and public that hacking back might fuel. For example, remedial action intrudes on the domain of force against foreign actors that generally belongs to the state.[240] Alternatively, remedial action by private companies presents a danger of government ratification of illegal behavior as in Russia, which is said to rely on "intelligence gathered by criminals, allowing it to benefit from crimes without accepting responsibility for them."[241]

Other ethical concerns abound. For example, information security professionals that engage in remedial actions may actually violate the professional code of their licensing agency.[242] Additionally, even if hacking back were to be legalized under U.S. law, it might still "violate foreign laws."[243] Finally, some distinguish hacking back from self-defense because unlike self-defense, the justifying threat is not existential.[244]

One last major criticism involves both logistical and ethical dilemmas. For hacking back to work, the entity doing it must be able to identify the perpetrator of the hack. As discussed more fully in Section IV.A., identifying hackers is difficult because they "'like to cover their tracks by routing attacks through other people's computers, without the owners' knowledge."[245] As a result, remedial action is hampered by time and certainty.[246] Quick remedial actions are likely to be uncertain and could be against the wrong party, while accurate attribution is likely to be too slow to be to allow for effective remediation.[247] Ethically, this presents two major problems. First, remedial actions risk collateral damage to innocent parties. Second, the limitations on attribution temper the justification of remedial action as self-defense. Using force against a cyber aggressor is one thing, using it against a victim is another.

---

[239] Lin, *supra* note 198, at 22.
[240] *Id*. at 8.
[241] Wolff, *supra* note 220 (quoting Michael Chertoff).
[242] Harrington, *supra* note 195, at 30–32.
[243] Wolff, *supra* note 220.
[244] *See* Lin, *supra* note 198, at 11 (observing that unlike "fistfights or home invasions," cyberattacks "do not usually pose existential threats . . . .").
[245] Harrington, *supra* note 195, at 27 (quoting *A Byte for a Byte*, ECONOMIST (Aug. 10, 2013), https://www.economist.com/news/leaders/21583268-letting-companies-strike-back-computer-hackers-bad-idea-byte-byte.
[246] Lin, *supra* note 198, at 13.
[247] *See id*. at 13 (discussing the inverse relationship between time and accuracy in attributing hacking attacks to their aggressor).

When applied to a hypothetical, many of these logistical and ethical critiques are damning. Return one last time to the example of Jeremy's hack. In using Bill and Jeremy to illustrate how recapture of property law might provide a framework for the legalization of hacking back, it was necessary to analogize between the physical world and the digital world as so many accounts of hacking do.[248] But many of the ethical and logistical critiques of remedial action illustrate that such analogies are imperfect, even if plausible. For example, in the Jeremy and Bill example, Bill was able to attribute the attack to Jeremy. That degree of certainty is unlikely in reality, and especially within a short period of time. Second, the hypothetical presented Jeremy and Bill as sharing physical proximity. In the digital age a hacker may be far away, often in another country. The hacker may even be the agent of a foreign government. By hacking back against Jeremy, Bill may have waded into the waters of international aggression and escalation. Alternatively, Jeremy could be an innocent party whose network has been compromised by someone else. He might then mistake Bill's defensive hack back for an initial aggression, and respond with a new attack. Of course, it is unlikely that both parties would be individuals. They could be corporations, governments, criminal organizations, or teams. Perhaps that is most indicative of the core problem: the uncertainty inherent in cyberattacks and the IoT makes solutions simultaneously essential but difficult.

VI. OTHER OPTIONS FOR IMPROVING THE SECURITY OF THE IOT

If remedial actions like hacking back cannot remedy the numerous and grave threats that permeate the era of the IoT, and the CFAA is insufficient, then it is essential to find another way to reduce vulnerabilities and prevent attacks. Although there are many possibilities,[249] this section briefly explores two possible prospective solutions: (1) a standards approach; and (2) agency regulation.

Both solutions differ from remedial actions such as hacking back by focusing more on securing new IoT devices rather than combatting existing ones that have already been corrupted. Both solutions are grounded in the same understanding of the problems with the IoT. Proponents of a standards approach and agency regulation often view the IoT as a victim of a market failure, as Section II illustrates.[250] Consumers want IoT devices to be as

---

[248] *See, e.g.*, Huang, *supra* note 219, at 1241–45 (describing attempts to superimpose real property and torts doctrines regarding physical property onto hacking back).

[249] *See, e.g.*, *Iot Is Vast and Has Many Security Related Issues*, IOT SECURITY FOUNDATION, https://iotsecurityfoundation.org/working-groups/ (last visited Nov. 14, 2017) (listing and summarizing different practice groups, each focused on a different aspect of IoT security).

[250] *See* text accompanying note 41– 42, *supra*.

cheap as possible.[251] Manufacturers and retailers oblige, prioritizing cost over security because they have no incentive not to.[252] International supply chains and the limited security expertise of many IoT design teams further complicate matters.[253] The widespread weaknesses in IoT devices offer an enticing tool and opportunity for nefarious activity. This section evaluates the potential of a standards approach or agency regulation to break this cycle.

A. The Standards Approach

Vulnerabilities like default passwords and static firmware threaten IoT security. Although they are suboptimal, because there is no uniform set of standards that IoT manufacturers or retailers must meet they are not technically substandard.[254] The standards approach would attempt to remedy this by imposing such a system on key players.

A standards system would combat the market failure by incentivizing better security practices in the proliferation of IoT devices.[255] According to one expert, adopting "defined standards" will "change buying and investment patterns" that are responsible for the current state of vulnerability in the IoT.[256] Imposing stronger security measures through standards for IoT developers is important because "[s]ecurity needs to be built into IoT devices, not bolted on. If cybersecurity is not part of the early design of an IoT device, it's too late for effective risk control."[257] Establishing standards that require better security measures from the start implicates "domestic and international" standards setting entities like the International Standards Organization (ISO) or the National Institute of Standards and Technology (NIST),[258] and may require government intervention.[259]

---

[251] *See* text accompanying note 43, *supra*.
[252] *Id.*
[253] *See* text accompanying note 44–45, *supra*.
[254] *See* Drew, *supra* note 23, at 4 ("The current lack of any security standards for IOT devices is certainly part of the problem that ought to be addressed.").
[255] *See id.* ("IoT manufacturers and vendors should embrace and abide by additional security practices to prevent harm to users and the internet.").
[256] *See* Drew Testimony, *supra* note 46, at 97.
[257] Fu, *supra* note 8, at 3.
[258] *See* Drew Testimony, *supra* note 46, at 97–98. Indeed, the Institute of Electrical and Electronics Engineers is currently working on "P2413," which is "an architectural framework for the [IoT]" addressing security among other considerations. IEEE Standards Association, *Standard for an Architectural Framework for the Internet of Things (IoT)* IEEE (2017), http://grouper.ieee.org/groups/2413/.
[259] *See* Drew, *supra* note 23, at 4 (Noting that in the context of standards setting, "there may be a role for the government to provide appropriate guidance.").

Generally, organizations advocating for the use of a standards-based approach emphasize the importance of a consistent and uniform standard,[260] but the priorities of an IoT security standard might vary. For example, Dale Drew—a proponent of a standards approach—is preoccupied with remedying vulnerabilities like default passwords, "hard-coded credentials," and the "lack of capability of updating [IoT device] firmware."[261]

One bipartisan legislative attempt at employing a standards approach, titled "The Internet of Things Cybersecurity Act of 2017," is currently pending before Congress.[262] The Bill would apply to IoT devices sold to the federal government, and "requires that manufacturers that sell smart devices to government agencies regularly patch their products for vulnerabilities and steer clear from using hard-coded passwords to access the devices via a backdoor."[263]

Assuming arguendo that agreement could be reached on the correct standards, this approach would still have a serious limitation: it would not affect the millions of existing devices.

B. Agency Regulation

Some experts have concluded that the pervasive threats to the IoT, and the related market failure, require increased government involvement.[264] They argue that "[c]ybersecurity ought to be a public good much like automobile safety."[265]

One possibility is to expand the capabilities of existing government agencies to test IoT security. To promote automobile safety, there are federally funded research and development centers, testing facilities run by the National Transportation Safety Board (post market), automotive crash safety testing (premarket), and the Nevada National Security Site

---

[260] *See Standard for an Architectural Framework for the Internet of Things*, IEEE STANDARDS ASSOCIATION (2017), https://standards.ieee.org/develop/project/2413.html ("The adoption of a unified approach to the development of IoT systems will reduce industry fragmentation and create a critical mass of multi-stakeholder activities around the world.").

[261] Drew, *supra* note 23, at 2.

[262] Harold Stark, *A Bipartisan Bill to Strengthen Cybersecurity for the Internet of Things*, FORBES (Aug. 20, 2017), https://www.forbes.com/sites/haroldstark/2017/08/20/a-bipartisan-bill-to-strengthen-cybersecurity-for-the-internet-of-things/#7eb1d0675a5f.

[263] *Id.*

[264] *See* Schneier Testimony, *supra* note 5, at 43 ("The choice is not between government involvement and no government involvement, but between smart government involvement and stupid government involvement.").

[265] Fu, *supra* note 8, at 8

(destruction and survivability testing).[266] But no analogous regulatory entities or research facilities currently exist to provide a proving ground for embedded cybersecurity defenses needed by IoT.[267] Such facilities would remedy the government's lack of a means to "conduct thorough security testing and assessment on IoT devices" and would reduce the inefficiencies of having diffuse entities conducting independent research.[268] This expansion could potentially fall under the control of the National Science Foundation or the NIST.[269]

Another possibility is the creation of a new regulatory agency. Bruce Schneier advocates for this position and analogizes the IoT to the once-new technologies of the past that gave rise to new agencies: "trains, cars, airplanes, radio, and nuclear power."[270] He argues that "[i]n the world of dangerous things, we constrain innovation,"[271] and that the IoT presents new dangers just as those earlier technologies did during their development. As a result, even if regulation would stifle some creativity, Schneier suggests that this is a necessary sacrifice for security.[272] Furthermore, the IoT presents problems that the market cannot or will not solve on its own. The most prominent is the market failure and the lack of consumer and manufacturer incentives to resolve technological vulnerabilities in the IoT.[273] Schneier argues that—as with environmental pollution—regulation is essential because the dangers and ill effects are felt only downstream.[274]

In the current political environment, which favors smaller government and reducing regulation, it seems doubtful that this approach could get traction in Congress. And if it did so, recruiting the necessary expertise and resources could be a daunting task.

CONCLUSION

The dangers in the IoT are complex, multifaceted, and numerous; and none of the possible solutions discussed in this article is wholly satisfying. For example, the current legal regime under the CFAA governs many of the threats in the IoT, and there have been some successful prosecutions under it. However, the CFAA's utility is severely limited by

---

[266] *Id.* at 3.
[267] *Id.*
[268] *Id.* at 8–9.
[269] *See* Fu Testimony, supra note 22, at 35 (advocating for increased support for these agencies).
[270] *See* Schneier Testimony, *supra* note 5, at 31.
[271] *Id.* at 59.
[272] *See id.* ("So, yes, this is going to constrain innovation . . . but this is what we do when innovation can cause catastrophic risk.").
[273] *Id.* at 58.
[274] *Id.*

practical and jurisdictional concerns, and it also prohibits some remedial actions against hacking. Similar contradictions are apparent with the alternative solutions evaluated in this article. Remedial actions like hacking back could ameliorate the perils of botnets, but they suffer from legal, ethical, and practical drawbacks. A standards approach might help secure the IoT prospectively, but it does nothing to eliminate the threat posed by preexisting botnets and compromised IoT devices. Agency regulation might provide similar relief, but seems unlikely in the current political climate.

Given these obstacles, it is tempting to do nothing, despite the overwhelming and quickly accelerating dangers posed by the IoT. That would be the worst option of all. First, an absence of official action should not be mistaken for an absence of action. If the government does not act to secure the IoT, others will, and the results could be chaotic and perilous. This inevitability may already be occurring: self-appointed vigilante "white hat" hackers are suspected in the proliferation of three botnets. One, known as Hajime, "has infected at least 10,000 home routers, network-connected cameras, and other so-called Internet of Things devices" with the apparent goal of "disrupt[ing] Mirai and similar IoT botnets."[275] Even assuming that the vigilante hackers have good intentions, their solution is fleeting, the methodology is illegal, and it interferes with "tens of thousands of devices" without the permission of their owners.[276] The other botnets, known as "BrickerBot.1" and "BrickerBot.2" may have a similar goal, but are particularly destructive: they are "designed to damage routers and other Internet-connected appliances so badly that they become effectively inoperable."[277] If these developments are any indication, without official intervention, the fight to secure the IoT could become a war of attrition with many innocent victims.

Second, the extraordinary growth of the IoT and its extreme vulnerability threaten individuals, businesses, and the broader society. Insecure IoT devices may be corrupted and exploited to attack the internet itself, threatening our reliance on the internet for things such as finance, news, healthcare, education, communication, information storage, and more.[278] Alternatively, IoT devices present new and unique opportunities

---

[275] Dan Goodin, *Vigilante Botnet Infects IoT Devices*, ARSTECHNICA (Apr. 18, 2017), https://arstechnica.com/information-technology/2017/04/vigilante-botnet-infects-iot-devices-before-blackhats-can-hijack-them/.

[276] *Id.*

[277] Dan Goodin, *Rash of in-the-Wild Attacks Permanently Destroys Poorly Secured IoT Devices*, ARSTECHNICA (Apr. 6, 2017), https://arstechnica.com/information-technology/2017/04/rash-of-in-the-wild-attacks-permanently-destroys-poorly-secured-iot-devices/.

[278] *See supra* Section I.A.

for malicious actors to turn digital hacking into physical consequences.[279] Hackers can already jeopardize a frightening array of internet-enabled objects including cars, trains, voting machines, power plants, dams, home thermostats, implanted medical devices, and possibly airplanes.[280] With ever-increasing internet connectivity, the perils could implicate any device that is connected to the internet. In the face of these potentially crippling threats, action is essential. If we wait passively for the full array of dangers of the IoT to become a reality, the wait will not be long, and the crisis could be severe.

---

[279] *Id.*
[280] *Id.*