ARTICLE

Detect, Disrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats

John P. Carlin*

* Assistant Attorney General for National Security, United States Department of Justice. I would like to thank David Forscey, Chloe Goodwin, Megan Henry, Sarah Howard, Allison Kempf, Alan Rozenshtein, Paul Schied, Yishai Schwartz, and Joshua Silverstein for their help in preparing this Article. I would also like to thank Josh Goldfoot, Chris Hardee, Adam Hickey, Alex Iftimie, James Melendres, Anita Singh, Brad Wiegmann, and several other individuals both inside and outside the government for their comments and assistance. This material has been reviewed by the Department of Justice to prevent the disclosure of classified information.

Table of Contents

Introduction

The United States faces an inflection point when it comes to the Internet's effect on daily life. What has enriched our economy and quality of life for the past several decades may start to hurt us more than help us, unless we confront its cybersecurity challenges.[1] Waves of network intrusions—increasing in number, sophistication, and severity—have hit American companies and the U.S. government. In 2012, former CIA Director and Defense Secretary Leon Panetta described the nation's cybersecurity weaknesses as presenting a "pre-9/11 moment."[2] And in July 2014, the 9/11 Commission itself warned: "We are at September 10th levels in terms of cyber preparedness."[3] Following that ominous prediction, in a span of less than two years, the United States was besieged by intrusions originating from around the globe. There was no single target, and no common perpetrator. Our adversaries stated or demonstrated that they hacked on behalf of China, North Korea, Syria, Iran, and many others. They stole sensitive information from government databases, damaged and destroyed private companies' computer systems, and—in a new twist—even targeted individuals' personally identifiable information to benefit terrorist organizations. The list of victims is broad and varied—the private sector, the government, and individual citizens. The past two years have publicly demonstrated the extent of the threat.

Former Federal Bureau of Investigation (FBI) Director Robert Mueller once offered the following analogy to describe our growing cyber vulnerabilities:

> In the days of the Roman Empire, roads radiated out from the capital city, spanning more than 52,000 miles. The Romans built these roads to access the vast areas they had conquered. But, in the

---

[1] For the purposes of this Article, "cybersecurity" means the protection of "computers, networks, programs and data from unintended or unauthorized access, change or destruction." "Cyberspace" refers to the "interdependent network of information technology infrastructures[] that includes the Internet, telecommunications networks, computer systems and embedded processors and controllers." *What is Cyber Security?*, UNIV. OF MD. UNIV. COLL., http://www.umuc.edu/cybersecurity/about/cybersecurity-basics.cfm. Importantly, cybersecurity extends to the protection of devices that are connected to the Internet—whether large-scale critical infrastructure or consumer devices (e.g., the emerging "Internet of Things"). More generally, the word or prefix "cyber" broadly refers to the domain of activity that arises from the close integration of computers, and in particular the Internet, into our society. The term has its detractors, who prefer more specific terms like "online" or "network." Nevertheless, the term is used here to capture, in one word, otherwise disperse subjects that are the greatest concern in governance.

[2] Leon E. Panetta, U.S. Sec'y of Def., Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City (Oct. 11, 2012), http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136.

[3] BIPARTISAN POLICY CTR., REFLECTIONS ON THE TENTH ANNIVERSARY OF THE 9/11 COMMISSION REPORT (July 2014), http://bipartisanpolicy.org/wp-content/uploads/sites/default/files/files/%20BPC%209-11%20Commission.pdf.

> end, these same roads led to Rome's downfall, for they allowed the invaders to march right up to the city gates.[4]

Like the Roman roads, the Internet connects us to the world. Empowered by advances in technology like cheap storage, increased bandwidth, miniaturized processors, and cloud architecture, we've extended Internet connectivity throughout our lives. But this expansion carries a risk not fully accounted for. Increased connectivity makes our critical infrastructure—water, electricity, communications, banking—and our most private information more vulnerable. We invested an enormous amount over the past few decades to digitize our lives. But we made these investments while systematically underestimating risks to our digital security. If we don't secure our Internet connectivity, what has been an important driver of prosperity and strength for the past twenty years could have disastrous effects in the next twenty.

To meet this challenge, the U.S. government has changed its approach to disrupting national security cyber threats. One element of its new strategy involves implementing and institutionalizing a "whole-of-government" approach. No one agency can beat the threat. Instead, success requires drawing upon each agency's unique expertise, resources, and legal authorities, and using whichever tool or combination of tools will be most effective in disrupting a particular threat. At times, that may mean economic sanctions from the Treasury Department, proceedings initiated by the Office of the U.S. Trade Representative, and cyber defense operations from the Defense Department. At other times, it might mean information sharing coordinated by the Department of Homeland Security, diplomatic pressure from the State Department, intelligence operations from the U.S. Intelligence Community (IC),[5] and prosecution and other legal action from the Justice Department. And in many instances, it will mean a coordinated application of several capabilities from the U.S. government's menu of options.

The United States' approach to combating Chinese theft of sensitive U.S.-company business information and trade secrets—activity that former National Security Agency Director Keith Alexander described as the "greatest transfer of

---

[4] Robert S. Mueller, Dir., Fed. Bureau of Investigation, Speech at Penn State Forum Speaker Series State College, Pennsylvania, The FBI: Stopping Real Enemies at the Virtual Gates (Nov 6, 2007), https://www.fbi.gov/news/speeches/the-fbi-stopping-real-enemies-at-the-virtual-gates.

[5] The IC is "a coalition of 17 agencies and organizations . . . within the Executive Branch that work both independently and collaboratively to gather and analyze the intelligence necessary to conduct foreign relations and national security activities." OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, http://www.dni.gov/index.php. It consists of: Air Force Intelligence, Army Intelligence, Central Intelligence Agency, Coast Guard Intelligence, Defense Intelligence Agency, Department of Energy, Department of Homeland Security, Department of State, Department of the Treasury, Drug Enforcement Administration, Federal Bureau of Investigation, Marine Corps Intelligence, National Geospatial-Intelligence Agency, National Reconnaissance Office, National Security Agency, Navy Intelligence, and the Office of the Director of National Intelligence. *Id.*

wealth in history"[6]—illustrates the power of this coordinated approach. In May 2014, after an unprecedented investigation spanning several years, a federal grand jury indicted[7] five uniformed members of the Chinese military on charges of hacking and conducting economic espionage against large U.S. nuclear-power, metal, and solar-energy companies. The 48-page indictment describes numerous, specific instances where officers of the People's Liberation Army (PLA) hacked into the computer systems of American companies to steal trade secrets and sensitive, internal communications that could be used for economic gain by Chinese companies. The recipient companies could use the stolen information against the victims in competition, negotiation, and litigation.[8]

This landmark case was the first prosecution of official state actors for hacking.[9] But the indictment was not pursued in isolation; nor was it seen as an end in and of itself. Rather, the investigation and prosecution of the PLA members were pieces of a larger deterrence strategy. In spring 2015, the President issued an executive order authorizing sanctions against companies engaging in malicious cyber activity.[10] At the same time, the government was advocating diplomatically for basic international norms in cyberspace.

It appears that these coordinated efforts are starting to establish new norms in cyberspace. In September 2015, President Obama and Chinese President Xi Jinping affirmed that neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors.[11] Although we don't know the extent to which China will honor this commitment, the fact that the commitment was made is itself significant, as is the fact that at the November 2015 G20 Summit in Turkey, leaders representing the twenty largest economies in the world

---

[6] Josh Rogin, *NSA Chief: Cybercrime Constitutes the "Greatest Transfer of Wealth in History,"* FOREIGN POLICY (July 9, 2012), http://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/.

[7] Throughout this Article, I refer to indictments and other criminal complaints. It is important to note that an indictment contains allegations that a defendant has committed a crime, and every defendant is presumed to be innocent until proven guilty in court.

[8] Press Release, U.S. Dep't of Justice, U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage (May 19, 2014), http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor [hereinafter PLA Indictment Summary]. Federal prosecutors in the Western District of Pennsylvania, where the indictment was returned, deserve special mention. The U.S. Attorney's Office for the Western District of Pennsylvania, led by U.S. Attorney David Hickton, has been at the forefront of pursuing cyber-related federal prosecutions, despite the challenges that such cases pose due to their novelty, length, and cost.

[9] *Id.*

[10] Exec. Order No. 13,694, 80 Fed. Reg. 18,077 (Apr. 2, 2015)

[11] *See* Press Release, White House, FACT SHEET: President Xi Jinping's State Visit to the United States (Sept. 25, 2015), https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

agreed to norms related to acceptable behavior in cyberspace.[12] As President Obama has noted, the Internet can sometimes seem like the "Wild Wild West."[13] But we are beginning to bring law and order to the Internet through concrete actions designed to ensure there are consequences for impermissible or unlawful behavior in cyberspace.

A whole-of-government approach is critical to success in disrupting national security cyber threats. But given the complexity of the threats we face, no strategy, regardless of the number of agencies involved or the breadth of tools available, would be complete without coordination with the private sector. In an increasingly flattened and connected world, the threat can easily move and change—but one constant is that private entities remain on the front lines of this fight. Thus, a second element of the United States' new approach involves deeper partnerships with the private sector.

This Article explains how national security investigators and lawyers in the Department of Justice (DOJ) play a crucial role in this new approach. As practiced at DOJ, national security law goes beyond the use of one set of tools or body of law. It is cross-disciplinary—encompassing a practical, problem-solving approach that uses all available tools, and draws upon all available partners, in a strategic, intelligence-driven, and threat-based way to keep America safe. As former Acting Assistant Attorney General (AAG) for National Security Todd Hinnen has noted, "[n]ational security investigations seek to harness and coordinate the authorities and capabilities of all members of the national security community, state and local law enforcement, and foreign law enforcement and intelligence partners,"[14] and "may result in a wide variety of national security activity, including . . . arrest and prosecution of perpetrators, imposition of economic sanctions, diplomatic overtures to foreign governments, and actions undertaken by U.S. intelligence services or armed forces overseas."[15]

Key to almost any of these responses is attribution. Attribution is the ability to confidently say who did it: which country, government agency, group, or even individual is responsible for a cyber intrusion or attack. To respond to cyber activity, you must know who is responsible, and what makes them tick. Defense, deterrence, and disruption all require an understanding of the adversary.[16] Government lawyers, agents, analysts, computer scientists, and other

---

[12] G20 LEADERS' COMMUNIQUÉ, ANTALYA SUMMIT 6 (2015), http://www.consilium.europa.eu/en/meetings/international-summit/2015/11/G20-Antalya-Leaders-Summit-Communique-_pdf/.

[13] Nicole Perlroth & David E. Sanger, *Obama Calls for New Cooperation to Wrangle the "Wild West" Internet*, N.Y. TIMES (Feb. 13, 2015), http://www.nytimes.com/2015/02/14/business/obama-urges-tech-companies-to-cooperate-on-internet-security.html.

[14] Todd Hinnen, *National Security Investigations*, *in* NATIONAL SECURITY LAW IN THE NEWS 215, 225 (Paul Rosenzweig et al. eds., 2012).

[15] *Id.* at 215–16.

[16] *See, e.g.*, David D. Clark & Susan Landau, *Untangling Attribution*, *in* COMM. ON DETERRING CYBERATTACKS, PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS 25 (2010).

national security investigators are particularly good at developing the building blocks of attribution—they have expertise honed in criminal investigations and carry a host of legal authorities that allow them to investigate and gather information.

Although attribution is a simple idea, doing so on the Internet is very complex. The Internet's architecture allows hackers to route their activities through a global network of computers, almost all of which are owned and operated by a variety of private actors. In addition, knowing which specific computer or network caused the malicious activity doesn't necessarily tell you which person or organization ordered, carried out, or supported the hack.

But attribution is still possible. DOJ, including the Federal Bureau of Investigation (FBI) and other law enforcement agencies, and with support from the IC, has unique expertise and legal authorities it can use to attribute cyber activities to their source. We can then take steps based on that attribution—including but not limited to prosecuting those responsible—to help us fight cyber threats. Each of these steps may seem small, but incrementally they can help us turn the tide.

This Article proceeds in three parts. Part I describes the cyber threats we face and emphasizes that any long-term solution must include deterrence and disruption. Part II explains why DOJ is well-placed to attribute network intrusions, and how it goes about doing so. Part III lays out the tools—within DOJ, across the federal government, and in the private sector—that rely on attribution to defend against, disrupt, and deter cyber threats. Throughout, this Article attempts to give concrete details and examples. But the need to protect sensitive sources and methods—in particular the means by which the government attributes cyber activity—limits what can be publicly described.

Before proceeding, it's important to emphasize that we are at the very beginning of the effort to confront national security cyber threats. All of the organizational and legal innovations discussed below—for example, increased intelligence coordination and the use of prosecutions, sanctions, and other legal tools to counter cyber threats—are evolving. The number of successful operations is still modest, especially given the size of the problem. And although we're moving in the right direction, we need to move faster.

We might need to modify or abandon some of the approaches if they prove unworkable, unscalable, or ineffective. Tools and techniques we haven't even thought of may ultimately take center stage. We welcome criticism and suggestions—indeed, encouraging this conversation is one of the main purposes behind this Article.

I. The Cyber Threat and the Need for Deterrence

The United States is under constant attack online. Every day, a wide range of actors try to hack government agencies, non-government organizations (NGOs), non-profits, and private companies. Some seek proprietary information and trade secrets. Others hunt for classified military documents and intelligence files, or information concerning NGOs or dissident activities. And still others want control over our infrastructure for disruptive, destructive, or even deadly ends. The culprits range from lone hackers in the United States, to organized criminal syndicates, to foreign military or intelligence officers and their proxies, to terrorists acting from terminals around the world. The vast majority fail, but too many still succeed.

Many of these activities—because of their motive, origin, or objective—threaten national security or public safety. For example, in addition to data loss, litigation risk, and reputational damage from cyber incidents, private sector companies now also confront the possibility of attacks that could destroy entire networks, threaten the viability of businesses, and even cause physical damage or loss of life.

To understand how we arrived at this troubling state of affairs, it is helpful to consider *how* cyber hacks operate, *who* perpetrates them, and *why* they're targeted at us.

A. *Means of Intrusion and Attack*

Hacking often begins with software vulnerabilities. Every time we access the Internet—whether it is to visit websites, check email, or use smartphone apps—we unwittingly expose ourselves to cyber threats. That's because software design prioritizes functionality. Developers often pay insufficient attention to security concerns, so most programs suffer from vulnerabilities that an intruder can exploit to get the software to crash or act in unexpected ways. That in turn can give intruders access to information or other programs, which they can use, for example, to install malware (software that is malicious by design). With full or even partial control over the system, malware can steal or delete information and target other computers.[17] Of course, when developers discover vulnerabilities for software, they usually distribute free patches. But users often fail to install patches, either because they're not aware of them or because installation is a resource-intensive hassle. According to one bulletin from the Department of Homeland Security, "[c]yber threat actors continue to exploit unpatched software to conduct attacks against critical infrastructure organizations. As many as 85

[17] NAT'L SEC. AGENCY/CENT. SEC. SERV., DEFENSIVE BEST PRACTICES FOR DESTRUCTIVE MALWARE (2015), https://www.nsa.gov/ia/_files/factsheets/Defending_Against_Destructive_Malware.pdf.

percent of targeted attacks are preventable."[18] The bulletin goes on to list "the 30 most commonly exploited vulnerabilities used in these attacks."[19] Patches exist for all of those vulnerabilities; for some, patches have existed for nearly eight years.[20]

Widespread software vulnerabilities enable industrial-scale hacking. For example, we face a proliferation of "botnets"—networks of thousands or even millions of malware-infected computers controlled by botnet "herders" for illicit uses, including attacking other systems.[21] Botnets are often responsible for distributed denial-of-service (DDoS) attacks, in which massive groups of computers simultaneously try accessing a website to overwhelm its servers and cause them to crash. One security research firm reported that, in the fourth quarter of 2014, such attacks increased by an annual 57% compared to the previous year.[22] Although DDoS attacks typically neither destroy computer systems nor degrade stored data, they can disrupt government services or make it impossible for companies to interact with their customers. DDoS attacks can have devastating economic effects,[23] and botnet herders have tried to extort large sums from companies by threatening DDoS attacks.[24]

Botnets are good for more than just DDoS attacks. They also distribute malware. For example, an increasing number of organizations and individuals are targets of "ransomware"—malware through which hackers take control of and then threaten to delete or disseminate valuable files unless the victim pays a ransom (often in Bitcoin).[25] 2013 saw the spread of a new version of ransomware

---

[18] *Alert (TA15-119A): Top 30 Targeted High Risk Vulnerabilities*, U.S. COMPUT. EMERGENCY READINESS TEAM (Apr. 29, 2015), http://www.us-cert.gov/ncas/alerts/TA15-119A.

[19] *Id.*

[20] *See Microsoft Security Bulletin MS08-042—Important: Vulnerability in Microsoft Word Could Allow Remote Code Execution (955048)*, MICROSOFT (Aug. 12, 2008), https://technet.microsoft.com/library/security/ms08-042.

[21] "Security researchers estimate that between 500,000 and one million computers worldwide are infected with GOZ, and that roughly 250,000 of those infected computers are active 'bots' in the GOZ network at any given time." Decl. of Special Agent Elliot Peterson in Supp. of Appl. for an Emergency TRO and Order to Show Cause re Preliminary Inj. at 3, United States v. Bogachev, No. 2:14-cv-00685 (W.D. Pa. June 2, 2014).

[22] Bill Brenner, *Q4 2014 State of the Internet—Security Report: Numbers*, AKAMAI (Jan. 29, 2015), https://blogs.akamai.com/2015/01/q4-2014-state-of-the-internet---security-report-some-numbers.html.

[23] *See, e.g.*, TIM MATTHEWS, INCAPSULA, INCAPSULA SURVEY: WHAT DDOS ATTACKS REALLY COST BUSINESSES 8 (2014), http://lp.incapsula.com/rs/incapsulainc/images/eBook%20%20DDoS%20Impact%20Survey.pdf (estimating that DDoS attacks can cost companies $40,000 every hour).

[24] *See* Liam Tung, *Giant DDoS Attacks Are Now Hitting 500Gbps as Criminals Flex Their Muscle*, ZDNET (Jan. 27, 2016), www.zdnet.com/article/giant-ddos-attacks-are-now-hitting-500gbps-as-criminals-flex-their-muscles/.

[25] *See* Lucian Constantin, *Ransomware that Demands Bitcoins Is Distributed by Malware that Steals Bitcoins*, PC WORLD (Mar. 25, 2014), http://www.pcworld.com/article/2111520/new-bitcrypt-ransomware-variant-distributed-by-bitcoin-stealing-malware.html; Brian Krebs, *"Operation Tovar" Targets "Gameover" ZeuS Botnet, CryptoLocker Scourge*, KREBS ON

called CryptoLocker, which encrypts a user's files and demands a ransom of anywhere from $200 to $5,000.[26] In 2014, crypto-ransomware attacks increased by an astonishing 4,000%, and the total number of known ransomware attacks more than doubled.[27] More recently, we've seen a disturbing trend across the country of ransomware attacks aimed at hospitals.[28] By disrupting hospital operations, such attacks not only cut into hospitals' bottom line, but also put patient health at serious risk.

Hackers can also gain control over systems by preying on the human weaknesses of their users. Spearphishing schemes send customized, legitimate-looking emails to extract sensitive information or install malware.[29] Spear phishing is enabled by the expanding universe of personally identifiable information on the Internet. Skilled hackers can access public and private data—from tweets to medical records and everything in between. This information lets them craft messages that convince even the most cyber-savvy among us to transfer money and divulge passwords and credit card numbers. Even military-grade encryption is worthless if you are tricked into giving your credentials to an overseas hacker pretending to be your employer's IT department. According to one industry security report, over 80% of companies with more than 2,500 employees were targets of spear-phishing attempts in 2014—a 40% increase over the prior year.[30] Spear phishing will only get more sophisticated as hackers

---

SECURITY (June 2, 2014), http://krebsonsecurity.com/2014/06/operation-tovar-targets-gameover-zeus-botnet-cryptolocker-scourge/ (reporting that the curators of the GameOver ZeuS botnet "loaned out sections of their botnet . . . for a variety of purposes," including infecting systems with CryptoLocker); *see generally Ransomware*, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/about-us/investigate/cyber/ransomware-brochure.

[26] James B. Comey, Dir., Fed. Bureau of Investigation, Statement Before the House Judiciary Committee (Oct. 22, 2015), https://www.fbi.gov/news/testimony/oversight-of-the-federal-bureau-of-investigation-7. In a perverse twist, CryptoLocker set up a "customer service" site to make paying the ransom easier. *See* Brian Krebs, *CryptoLocker Crew Ratchets Up the Ransom*, KREBS ON SECURITY (Nov. 6, 2013), http://krebsonsecurity.com/tag/cryptolocker-decryption-service/.

[27] SYMANTEC, INTERNET SECURITY THREAT REPORT 7 (2015), https://www.symantec.com/content/en/us/enterprise/other_resources/21347933_GA_RPT-internet-security-threat-report-volume-20-2015.pdf.

[28] *See, e.g.*, Alex Dobuzinskis & Jim Finkle, *California Hospital Makes Rare Admission of Hack, Ransom Payment,* REUTERS (Feb. 19, 2016), http://www.reuters.com/article/us-california-hospital-cyberattack-idUSKCN0VS05M; Brian Krebs, *Hospital Declares 'Internal State of Emergency' After Ransomware Infection*, KREBS ON SECURITY (Mar. 22, 2016), https://krebsonsecurity.com/2016/03/hospital-declares-internet-state-of-emergency-after-ransomware-infection/; Jim Finkle & Dustin Volz, *Washington's MedStar Computers Down for Second Day After Virus*, REUTERS (Mar. 29, 2016), http://www.reuters.com/article/us-usa-cyber-medstar-idUSKCN0WV1J7.

[29] *See Spear Phishing: Scam, Not Sport,* NORTON BY SYMANTEC, http://us.norton.com/spear-phishing-scam-not-sport/article; *Spear Phishers Angling to Steal Your Financial Information*, FED. BUREAU OF INVESTIGATION (Apr. 1, 2009), https://www.fbi.gov/news/stories/2009/april/spearphishing_040109.

[30] *See* SYMANTEC, *supra* note 27, at 7.

improve their social-engineering techniques and steal even more of our personal data.[31]

B. *Threat Actors*

Although hacking is a skill that requires knowledge and experience, hackers don't need (and often don't have) formal training. Computer skills can be honed anywhere, using materials publicly available on the Internet, and the equipment needed to engage in malicious activity and evade detection is inexpensive and widely available. As a result, we face cyber threats driven by an array of groups—from Russian criminal syndicates, to Al-Qaeda and the so-called Islamic State of Iraq and the Levant (ISIL), to foreign intelligence services and their proxies. As scholars Benjamin Wittes and Gabriella Blum have noted, cyberspace is a world of distributed threats, easily available weapons, and universal vulnerability.[32] Reviewing the different actors we confront in cyberspace—especially terrorist groups and foreign powers—and the disturbing and dangerous ways in which these threats are blending with one another, illustrates the troubling breadth of the cyber threat.

Today, many of the same terrorist organizations that have threatened our national security for years actively seek to attack America over the Internet. For example, in 2012 Al-Qaeda released a video comparing the vulnerabilities in computer network security to weak points in aviation security before 9/11.[33] The film called for "electronic jihad" against the United States.[34] James Clapper, the Director of National Intelligence (DNI), noted in his 2014 Worldwide Threat Assessment that "terrorist organizations have expressed interest in developing offensive cyber capabilities," in addition to their established expertise in using the

---

[31] *See* Phil Muncaster, *Spear Phishing to Get More Personal in 2015*, INFOSECURITY (Dec. 22, 2014), http://www.infosecurity-magazine.com/news/spear-phishing-to-get-more. Social engineering attacks "typically involve some form of psychological manipulation, fooling otherwise unsuspecting users or employees into handing over confidential or sensitive data. Commonly, social engineering involves email or other communication that invokes urgency, fear, or similar emotions in the victim, leading the victim to promptly reveal sensitive information, click a malicious link, or open a malicious file." Nate Lord, *Social Engineering Attacks: Common Techniques and How to Prevent an Attack*, DIG. GUARDIAN (May 18, 2016), https://digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent-attack.

[32] *See generally* BENJAMIN WITTES & GABRIELLA BLUM, THE FUTURE OF VIOLENCE (2015).

[33] *Senators Say Video Urging Electronic Jihad Underscores Need for Cybersecurity Standards*, U.S. SENATE COMM. ON HOMELAND SEC. AND GOVERNMENTAL AFF. (May 22, 2012), http://www.hsgac.senate.gov/media/majority-media/senators-say-video-urging-electronic-jihad-underscores-need-for-cybersecurity-standards.

[34] Jack Cloherty, *Virtual Terrorism: Al Qaeda Video Calls for "Electronic Jihad,"* ABC NEWS (May 22, 2012), http://abcnews.go.com/Politics/cyber-terrorism-al-qaeda-video-calls-electronic-jihad/story?id=16407875.

Internet to recruit personnel, finance activities, and disseminate propaganda.[35] In 2015, he predicted that many of these groups would likely "continue to experiment with hacking, which could serve as the foundation for developing more advanced capabilities."[36] This danger is exacerbated by the empowerment of terrorist sympathizers through social media messaging campaigns on behalf of groups such as ISIL. DNI Clapper suggested that such supporters could conduct small-scale online attacks on behalf of terrorist organizations, thereby enhancing the threat these groups pose to the United States.[37] While these groups might not possess powerful cyber capabilities today, there should be no doubt that they are actively working to acquire them.

Even absent terrorist attacks conducted *through* cyberspace, we have already seen how cyber and terror threats can blend in dangerous ways. As just one example demonstrating how cyber attacks can be used to facilitate real-world terrorist attacks in unexpected ways, in August 2015, ISIL-affiliated hackers publicly released the names, locations, phone numbers, and e-mail addresses of over 1,000 U.S. military and other government personnel for the purpose of encouraging terrorist attacks against them. In a first-of-its-kind case, DOJ charged Ardit Ferizi, who ultimately pled guilty,[38] with material support for providing this stolen information to ISIL.[39]

The other major category of national security cyber threat actors consists of states and their proxies. The IC has characterized China's history of economic espionage against the American private sector as an "advanced persistent threat."[40] China's military and intelligence services possess the sophistication and

---

[35] OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, WORLD WIDE THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY 2 (2014), http://www.dni.gov/files/documents/Intelligence%20Reports/2014%20WWTA%20%20SFR_SSCI_29_Jan.pdf.

[36] OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, WORLD WIDE THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY 3 (2015), http://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf [hereinafter ODNI WWTA 2015].

[37] *Id.*

[38] *See* Press Release, U.S. Dep't of Justice, ISIL-Linked Hacker Pleads Guilty to Providing Material Support (June 15, 2016), https://www.justice.gov/opa/pr/isil-linked-hacker-pleads-guilty-providing-material-support.

[39] *See* Press Release, U.S. Dep't of Justice, ISIL-Linked Hacker Arrested in Malaysia on U.S. Charges (Oct. 15, 2015), http://www.justice.gov/opa/pr/isil-linked-hacker-arrested-malaysia-us-charges; Complaint, United States v. Ferizi, No. 1:15-MJ-00515, 2015 WL 6126125, (E.D. Va. Oct. 6, 2015).

[40] *See* ODNI WWTA 2015, *supra* note 36, at 3 (naming Chinese economic espionage an "advanced persistent threat" and specifically describing a believed Chinese hack that resulted in stolen personally identifiable information on 4.5 million individuals from U.S. company Community Health Systems); OFF. OF THE NAT'L COUNTERINTELLIGENCE EXEC., FOREIGN SPIES STEALING US ECONOMIC SECRETS IN CYBERSPACE: REPORT TO CONGRESS ON FOREIGN ECONOMIC COLLECTION AND INDUSTRIAL ESPIONAGE 5 (2011), http://www.ncsc.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf (private sector specialists describe the "onslaught of computer network intrusions originating from Internet Protocol (IP) addresses in China" as "advanced persistent threats"); *see also* NAT'L INST. OF STANDARDS & TECH.,

resources to hack systems using multiple vectors, surreptitiously establish footholds behind perimeter defenses, exfiltrate valuable information, and undermine critical network functions.[41] These are not merely theoretical capabilities—China has routinely used such tactics against the United States over an extended period of time, adapted to our responses, and progressively escalated its intrusions.[42]

Beyond China, the United States has also publicly identified other foreign nations that pose a cyber threat to American national security. Iranian hackers who worked for computer security companies affiliated with the Iranian government, including the Islamic Revolutionary Guard Corps,[43] were publicly charged in March 2016 with perpetrating DDoS attacks on the U.S. financial sector in which 46 financial institutions were flooded with traffic over the course of 176 days. The attacks disrupted online services and prevented hundreds of thousands of Americans from accessing their bank accounts online. In all, these attacks cost victims tens of millions of dollars. One of these defendants was also charged with obtaining unauthorized access to the computer systems controlling the Bowman Dam in Rye, New York.[44] At the time of his alleged intrusion, the dam was undergoing maintenance and had been disconnected from the system. But under ordinary circumstances, the access would have enabled him to control water levels and flow rates. DNI Clapper also implicated Iranian actors in the February 2014 cyber attack on the Las Vegas Sands Casino.[45]

In late 2014, North Korea was also publicly named as a nation engaged in cyber intrusions. After a rigorous FBI investigation into the November 2014 attack against Sony Pictures Entertainment, described more fully below, the U.S. government announced that North Korea was responsible.[46] Only months later, President Barack Obama signed an executive order authorizing additional actions against the North Korean government in response to the cyberattack.

MANAGING INFORMATION SECURITY RISK: ORGANIZATION, MISSION, AND INFORMATION SYSTEM VIEW 8 (2011), http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf (defining "advanced persistent threat" as "a long-term pattern of targeted, sophisticated attacks").

[41] *See* ODNI WWTA 2015, *supra* note 36, at 2 (describing China as a nation with a "highly sophisticated" cyber program).

[42] *Id.* at 3.

[43] The Islamic Revolutionary Guard Corps is one of several entities within the Iranian government responsible for Iranian intelligence.

[44] Press Release, U.S. Dep't of Justice, U.S. Atty's Office, S.D.N.Y., Manhattan U.S. Attorney Announces Charges Against Seven Iranians For Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector On Behalf Of Islamic Revolutionary Guard Corps-Sponsored Entities (Mar. 24, 2016), https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-charges-against-seven-iranians-conducting-coordinated.

[45] ODNI WWTA 2015, *supra* note 36, at 3.

[46] *See* Press Release, Fed. Bureau of Investigation, Update on Sony Investigation (Dec. 19, 2014), http://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation.

Finally, in early 2015, DNI Clapper testified before the Senate that Russia, among other states, has a "highly sophisticated cyber program" that could harm the United States through economic espionage and "reconnoitering and developing access to U.S. critical infrastructure systems."[47]

The list goes on. These are only the countries we have publicly called out for this behavior. There are many more.

C. *Motivations*

Economic espionage is a key driver of many of the data breaches and exfiltrations that have received front-page attention over the past several years.[48] While it is hard to accurately determine losses, the FBI has estimated that in fiscal year 2012 economic espionage and the theft of trade secrets cost the American economy over $19 billion.[49] The Office of the National Counterintelligence Executive[50] has estimated that losses from economic espionage could be orders of magnitude higher.[51] When foreign states steal intellectual property and business strategies from U.S. companies, those firms not only lose valuable proprietary information, they also face regulatory costs, litigation risk, reputational damage, customer or investor flight, and greater competition from companies that unfairly benefit from receiving the stolen information. The consequences of economic espionage are measured not only in terms of the substantial cumulative cost to U.S. companies, but also in the diminution of the competitive advantages of the American economy as a whole.[52]

---

[47] ODNI WWTA 2015, *supra* note 36, at 2.

[48] In 2011, the Office of the National Counterintelligence Executive issued a landmark report in which the IC directly identified China, Russia, and other countries as engaged in widespread economic espionage and theft of trade secrets against the United States. OFFICE OF THE NAT'L COUNTERINTELLIGENCE EXEC., FOREIGN SPIES STEALING U.S. ECONOMIC SECRETS IN CYBERSPACE (2011), https://www.ncsc.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf.

[49] *See* Christopher Munsey, *Economic Espionage: Competing For Trade By Stealing Industrial Secrets*, FBI LAW ENFORCEMENT BULLETIN (Nov. 6, 2013), http://leb.fbi.gov/2013/october-november/economic-espionage-competing-for-trade-by-stealing-industrial-secrets.

[50] The Office of the National Counterintelligence Executive leads the government's counterintelligence efforts. The National Counterintelligence Executive is appointed by the Director of National Intelligence and currently also serves in a dual role as the Director of the National Counterintelligence and Security Center. NAT'L COUNTERINTELLIGENCE & SEC. CTR., http://ncsc.gov/about/director.html.

[51] *See* Randall C. Coleman, Assistant Dir., Counterintelligence Div., Fed. Bureau of Investigation, Statement Before the Senate Judiciary Committee on Crime and Terrorism (May 13, 2014), http://www.fbi.gov/news/testimony/combating-economic-espionage-and-trade-secret-theft; *see also* MCAFEE & CTR. FOR STRATEGIC AND INT'L STUDIES, THE ECONOMIC IMPACT OF CYBERCRIME AND CYBER ESPIONAGE 4 (2013), http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf.

[52] Kenneth L. Wainstein, Assistant Att'y Gen. for Nat'l Sec., U.S. Dep't of Justice, Press Conference Announcing Espionage Charges (Feb. 11, 2008), https://www.justice.gov/archive/nsd/2008/aag-nsd-080211.html (noting that foreign governments "want to steal our secrets and piggy-back on our technological innovation").

Foreign adversaries also hack computer networks for counterintelligence purposes. This is a particular threat for federal employees and contractors, who by necessity must disclose personal information to their government. Malicious actors might use this information to blackmail, extort, and even recruit Americans to serve their ends. The hacks on personnel databases maintained by the Office of Personnel and Management crystalized this threat. Attackers stole dossiers of professional, financial, medical, and personal details for 21.5 million people, some of whom were working at the highest levels of our government. Almost two million people included in this dragnet were the partners and family members of those undergoing background investigations. Many private sector companies have also been targeted for the large volumes of personally identifiable information they maintain, the value of which extends beyond that of identity theft for criminal profit.[53]

Cyber hacking can also be used to retaliate, intimidate, or coerce others. For example, the IC has concluded that both North Korea and Iran view their cyber programs as vital to advancing political objectives.[54] The most notorious such example to date may be the attack on Sony Pictures Entertainment. This attack destroyed Sony's computer systems, compromised private information, released valuable corporate data and intellectual property, and threatened employees, customers, and film distributers with violence. The attackers stole over 38 million files, totaling more than 100 terabytes of data. They released much of it to the public, attempting to tarnish the company's reputation and imposing significant financial and legal consequences. The data included private correspondence, unreleased films, salary records, and over 47,000 social security numbers.[55] The attack forced Sony to take its company-wide computer network offline and left thousands of its computers inoperable.[56] The hackers, originally styling themselves the "Guardians of Peace," threatened violence against theaters and filmgoers, referencing the 9/11 attacks. Their apparent motive was to retaliate against Sony for the planned Christmas Day release of *The Interview*, a comedy satirizing North Korean leader Kim Jong Un. Under immense pressure, Sony and

---

[53] *See* Fred Barbash & Abby Phillip, *Massive Data Hack of Health Insurer Anthem Potentially Exposes Millions,* WASH. POST (Feb. 5, 2015), http://www.washingtonpost.com/news/morning-mix/wp/2015/02/05/massive-data-hack-of-health-insurer-anthem-exposes-millions/; Zachary Tracer*, Premera Blue Cross Says Data on 11 Million Exposed by Hackers*, BLOOMBERG (Mar. 17, 2015), http://www.bloomberg.com/news/articles/2015-03-17/premera-blue-cross-says-data-on-11-million-exposed-by-hackers; Nicole Perlroth, *Hack of Community Health Systems Affects 4.5 Million Patients*, N.Y. TIMES (Aug. 18, 2014), http://bits.blogs.nytimes.com/2014/08/18/hack-of-community-health-systems-affects-4-5-million-patients/; Ellen Nakashima, *DHS Contractor Suffers Major Computer Breach, Officials Say*, WASH. POST (Aug. 6, 2014), https://www.washingtonpost.com/world/national-security/dhs-contractor-suffers-major-computer-breach-officials-say/2014/08/06/8ed131b4-1d89-11e4-ae54-0cfe1f974f8a_story.html.

[54] ODNI WWTA 2015, *supra* note 36, at 3.

[55] *See* Keith Wagstaff, *Sony Hack Exposed 47,000 Social Security Numbers, Security Firm Says*, NBC NEWS (Dec. 5, 2014), http://www.nbcnews.com/storyline/sony-hack/sony-hack-exposed-47-000-social-security-numbers-security-firm-n262711.

[56] *See* Fed. Bureau of Investigation, *supra* note 46.

leading movie theaters initially canceled the film's nationwide release (although it was later distributed).[57] Without firing a single shot, hackers derailed a major motion picture release that they found objectionable.

Political coercion through cyber means is not limited to state actors. Terrorist organizations also wield these tools to intimidate, disrupt, or degrade the performance of military and private sector systems. The conflict in Iraq and Syria is inspiring cyber attacks that have defaced websites and social media accounts used by the U.S. government. For example, on June 8, 2015, a hacker group called the Syrian Electronic Army (SEA) took credit for disabling an Army.mil website and defacing it with the statement: "Your commanders admit they are training the people they have sent you to die fighting."[58] The members of this group, too, were recently charged for their conduct,[59] and one of the named defendants has already been successfully extradited to the United States to stand trial in federal court.[60]

Of note, many of these attacks are not driven by a single motivation. The SEA in particular has allegedly engaged in intrusions aimed not only at causing harm to the economic and national security interests of the United States, but also at lining SEA members' own pockets by extorting victims. We continue to see the threats and motivations blending. We see individual hackers supporting terrorist

---

[57] *See "The Interview" to Screen in Select Theaters on Christmas*, CHI. TRIB. (Dec. 23, 2014), http://www.chicagotribune.com/entertainment/chi-interview-sony-release-20141223-story.html. The film had been scheduled to debut on over 3,000 screens across the country but ultimately opened in fewer than 300 independent theaters. Krishnadev Calamur, *"The Interview" Gets Nationwide Theatrical Release*, NAT'L PUB. RADIO (Dec. 25, 2014), http://www.npr.org/sections/thetwo-way/2014/12/25/373062179/the-interview-gets-nationwide-theatrical-release. To their great credit, both Google and Microsoft quickly agreed to distribute the movie through their online services. *See* Michael Cieply & Brooks Barnes, *Sony Streams "The Interview" on YouTube, Google Play and Xbox*, N.Y. TIMES (Dec. 24, 2014), http://www.nytimes.com/2014/12/25/business/sony-the-interview-online-streaming.html.

[58] Michael Hoffman, *Syrian Electronic Army Takes Down U.S. Army Website*, DEFENSE TECH (June 8, 2015), http://defensetech.org/2015/06/08/syrian-electronic-army-takes-down-us-army-website/. The SEA is a group of hackers who support Syrian President Bashar al-Assad. *See* Kate Vinton, *Syrian Electronic Army Claims Responsibility for Hacking U.S. Army Website*, FORBES (June 8, 2015), http://www.forbes.com/sites/katevinton/2015/06/08/syrian-electronic-army-claims-responsibility-for-hacking-army-website/#4b467a46704d. U.S. Central Command (CENTCOM) suffered a similar attack in January 2015, when hackers purportedly affiliated with ISIL compromised CENTCOM's Twitter and YouTube accounts. As a result, its Twitter account read: "American Soldiers. We are coming. Watch your back. ISIS." Richard Sisk, *Central Command's Twitter, YouTube Hacked to Post Threats to Troops*, MILITARY.COM (Jan. 12, 2015), http://www.military.com/daily-news/2015/01/12/hackers-hit-centcom-sites-reveal-contact-info-and-issue-threats.html.

[59] *See* Press Release, U.S. Dep't of Justice, Computer Hacking Conspiracy Charges Unsealed Against Members of Syrian Electronic Army (Mar. 22, 2016), https://www.justice.gov/opa/pr/computer-hacking-conspiracy-charges-unsealed-against-members-syrian-electronic-army..

[60] Press Release, U.S. Dep't of Justice, Syrian Electronic Army Member Extradited to the United States (May 10, 2016), https://www.justice.gov/usao-edva/pr/syrian-electronic-army-member-extradited-united-states.

aims (Ferizi), groups defacing websites and simultaneously profiting from their criminal activities (SEA), and increasingly the lines between state actor, criminal group, and terrorist are blurring.

A final category of motivation is illustrated by network vulnerabilities that provide opportunities for our adversaries to engage in more strategic levels of harm. For example, consider a nation-state intent on changing the global landscape or disrupting the American way of life: connectivity provides it with ample opportunity to threaten our critical infrastructure. One example is our electric grid. Engineered in an analog age, the grid has been retooled for the digital age in a piecemeal fashion, creating major security flaws along the way. Modernization has been a double-edged sword: while it has unlocked new potential for efficiency and performance, it has also resulted in numerous connections to the Internet and new devices that increase the electric grid's susceptibility to cyber attack. Air-gaps—which once separated the grid and other vital systems like water treatment and industrial plants from the public Internet—are vanishing.[61] As a result, the industrial-control systems that manage and monitor many of our most important industrial facilities are exposed to hackers intent on wreaking havoc.[62] This is no longer merely a hypothetical concern. The Department of Homeland Security reported that a blackout in Ukraine in December 2015 that impacted more than 200,000 customers was caused by a cyber attack.[63]

While industrial-control systems are essential to cost-efficient and reliable power delivery, many of these systems were developed without a focus on security. Encryption and authentication are often non-existent,[64] and automated, networked systems that allow a single supervisor to control multiple networks over a wide geographic area create significant risk.[65] As Senator Sheldon Whitehouse warned in 2012, "[o]ur Nation will be vulnerable if critical infrastructure companies fail to meet basic security standards, as they do right now."[66]

---

[61] *See* RICHARD J. CAMPBELL, CONG. RESEARCH SERV., R43989: CYBERSECURITY ISSUES FOR THE BULK POWER SYSTEM 9 (2015) ("Over time, modification of SCADA [Supervisory Control and Data Acquisition] systems has resulted in connection of many of these older, legacy systems to the Internet."), https://www.fas.org/sgp/crs/misc/R43989.pdf.

[62] *See id.*

[63] *Alert (16-056-01): Cyber-Attack Against Ukrainian Critical Infrastructure*, ICS-CERT (Feb. 25, 2016), https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.

[64] *See* NAT'L INST. OF STANDARDS & TECH., GUIDE TO INDUS. CONTROL SYS. (ICS) SEC. 3-2, 3-14 (2011), http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf (noting that "[m]any [ICS] systems may not have desired features including encryption capabilities" and that "[m]any ICS protocols have no authentication at any level").

[65] BIPARTISAN POLICY CTR., CYBERSECURITY AND THE NORTH AMERICAN ELECTRIC GRID: NEW POLICY APPROACHES TO ADDRESS AN EVOLVING THREAT 56–57 (2014), http://bipartisanpolicy.org/wp-content/uploads/sites/default/files/Cybersecurity%20Electric%20Grid%20BPC.pdf.

[66] 158 CONG. REC. S4846–48 (daily ed. July 11, 2012) (statement of Sen. Sheldon Whitehouse).

These vulnerabilities have not gone unnoticed by our adversaries. As far back as November 2014, NSA Director Admiral Mike Rogers testified before Congress that his organization had already identified foreign intrusions into industrial-control systems in the United States, and that vulnerabilities in those systems were among his most pressing concerns. He described "reconnaissance by many . . . actors in an attempt to [e]nsure they understand our systems so that they can then, if they choose to, exploit the vulnerabilities within those control systems."[67] He went on to say that some state and non-state actors already possess the capability to access, impede, or shut down our basic infrastructure.[68] Just over a year later, we saw that statement proven true by the Bowman Dam intrusion. DNI Clapper likewise told Congress that "unspecified" Russian cyber actors are developing the skills to access those systems responsible for managing "critical infrastructures such as electric power grids, urban mass-transit systems, air-traffic control, and oil and gas distribution networks."[69]

* * *

Obviously, the government and the private sector need to (and will)[70] improve their defensive capabilities to anticipate these and future threats. But merely improving cybersecurity practices and building more resilient systems will not be enough. The difficult truth about cybersecurity is that the attacker always has the advantage. The defender must defend against all vulnerabilities at all times, whereas the attacker only has to succeed in one place at one time.[71] This difficulty is compounded by the incredible complexity of modern information technology systems.

When we first began confronting the full magnitude of the cyber threat, the focus was on defense and hardening our own systems. But defense is not enough. Because we lacked a more proactive strategy of deterrence and disruption, the rate of cyber intrusions and attacks continuously outpaced our ability to defend against them.[72]

Our strategy must be more proactive, and it must include deterrence. Our strategy must and will make clear that being shielded or sponsored by a foreign power will not offer protection. There can be no free passes. Homeland Security

---

[67] *Cybersecurity Threats: The Way Forward*: *Hearing Before the H. (Select) Intelligence Comm.*, 113th Cong. (2014) (statement of Adm. Michael Rogers, Commander of U.S. Cyber Command & Dir. of Nat'l Sec. Agency), https://www.nsa.gov/news-features/speeches-testimonies/testimonies/adm-rogers-testimony-20nov2014.shtml.

[68] *Id.*

[69] ODNI WWTA 2015, *supra* note 36, at 3; *see also Alert (14-281-01C): Ongoing Sophisticated Malware Campaign Compromising ICS (Update C)*, ICS-CERT (Dec. 10, 2014; last revised Jan. 26, 2016), https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B.

[70] *See infra* Part III.C.

[71] *See* AT THE NEXUS OF CYBERSECURITY AND PUBLIC POLICY 36 (David Clark et al. eds., 2014).

[72] In particular, because cyber defenses are frequently insufficient, substantial effort has gone towards making networked systems more resilient to malicious activity.

Advisor Lisa Monaco described our strategy for defending the United States from malicious cyber activity thus: "We will take steps . . . to protect our companies, to protect U.S. persons and to protect our interests in the time and place of our choosing."[73]

Of course, not all adversaries can be deterred. A nation-state stealing industrial secrets does so for economic reasons, and thus is sensitive to the costs—economic, diplomatic, and other—of getting caught. A terrorist group, on the other hand, may have pure destruction and intimidation as its aims, and won't care about the costs of getting caught. Thus, for some threats, disruption will remain the main strategy.

Part III lays out some of the ways the government can both deter and disrupt. Deterrence requires that we fundamentally change an attacker's cost-benefit calculation by dramatically increasing the costs of bad behavior. Disruption requires that we stop the threat before an attack happens or achieves the desired effects. But to do either, we must first strip hackers of their real or perceived cloak of anonymity through public attribution, because if a hacker is invisible, his actions are cost-free. Attribution is the lynchpin of our success, and the topic to which this Article now turns.

II. Attribution and the Role of Investigations

There's no way around it: attributing activity on the Internet is challenging. Hackers often route their malicious traffic through third-party proxies they either rent or compromise. An attacker in Eastern Europe that uses a botnet of compromised computers in the Middle East to conduct a DDoS attack against a U.S. target creates a false narrative that actors located in the Middle East were responsible for that act. Even attributing an attack to the actual originating computer may be insufficient; we may know the machine used to execute a hack, but not the person or group that controlled it.[74] Thus, technical investigation must often be supplemented by credible human intelligence.[75] And all of this must be done quickly and consistently; attribution is of little use if it takes years and only identifies a small fraction of attackers.

Although attribution is difficult, it is far from impossible. Nor is the fundamental challenge new. For example, following 9/11, many were skeptical that the government could detect decentralized terrorist networks, let alone attribute specific attacks or conspiracies to individuals. Although the government tragically cannot stop every attack, since 9/11 the government has succeeded the

---

[73] *Meet the Press Daily* (MSNBC television broadcast Sept. 29, 2015).
[74] *See* Taylor Armerding, *Whodunit? In Cybercrime, Attribution Is Not Easy*, CSO ONLINE (Feb. 5, 2015), http://www.csoonline.com/article/2881469/malware-cybercrime/whodunit-in-cybercrime-attribution-is-not-easy.html.
[75] *Id.*

vast majority of the time, in large part because of the contributions of national security investigators. And more generally, attributing bad acts is at the heart of law enforcement and intelligence gathering, both areas in which, along with the IC, DOJ plays a critical role.

This Part describes key components of our government's investigative toolkit, how they evolved to fight terrorism, and how the lessons from that evolution have shaped how we now confront the cyber threat.

A. *The Post-9/11 National Security Evolution of the Department of Justice*

Before 2006, the national security activities of DOJ were divided among various and largely siloed components and offices. The attorneys prosecuting spies and terrorists and the attorneys who facilitated intelligence collection against those same actors had little interaction.[76] This was by design; separating law enforcement and intelligence collection was thought to enhance the integrity of both, by preventing intelligence tools from improper use, preserving the independence of law enforcement, and protecting the sources and methods of intelligence collection. But this "wall" that separated foreign-intelligence investigations from criminal ones worked to the detriment of both.[77] It hampered our efforts to bring terrorists and spies to justice, and impeded our ability to counter national security threats through comprehensive and effective intelligence collection.

The 9/11 Commission concluded that one factor hindering America's ability to prevent the deadly attacks of September 11, 2001 was this lack of coordination across the government, which led us to underestimate and respond slowly to threats.[78] The Commission specifically identified the wall that blocked information sharing between FBI investigators and DOJ prosecutors as a significant impediment to successful counterterrorism activities.[79] Two key

---

[76] Historically, the primary national security entities of the Department were the Counterterrorism and Counterespionage Sections of the Criminal Division (CTS and CES respectively,) and the Counsel for Intelligence Policy in the Office of Intelligence Policy and Review (OIPR). *See* David Kris, *Law Enforcement as a Counterterrorism Tool*, 5 J. NAT'L SEC. L. & POL'Y 1, 4 (2011) (describing the pre-9/11 "FISA wall" under which "law enforcement and intelligence were largely separate enterprises"); U.S. DEP'T OF JUSTICE, A.G. ORDER 2212-1999 (on file with author). The Executive Office for National Security, established in 1994 within the Office of the Deputy Attorney General, provided basic coordination of national security activities within DOJ. Press Release, U.S. Dep't of Justice, New Executive Office for National Security Announced (Oct. 3, 1994), http://www.justice.gov/archive/opa/pr/Pre_96/October94/564.txt.html.

[77] *See* Kris, *supra* note 76, at 4–5; NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., 9/11 COMMISSION REPORT 78–79, 270–72 (2004) [hereinafter 9/11 COMMISSION REPORT].

[78] *See* 9/11 COMMISSION REPORT, *supra* note 77, at 348–49, 351–53.

[79] *Id.* at 79, 270–71. In 2004, Attorney General John Ashcroft attempted to bridge the divide by establishing the Justice Intelligence Coordination Council to coordinate intelligence practices

developments—the passage of the USA PATRIOT Act[80] and a decision of the United States Foreign Intelligence Surveillance Court of Review[81]—dismantled this wall as a legal matter.[82]

But our work was not done. In 2005, with intelligence failure in Iraq making headlines, the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction—established to explore deficiencies in U.S. intelligence gathering and analysis on weapons of mass destruction (WMDs)[83]—recommended the creation of a new AAG for National Security to oversee the national security activities of DOJ.[84] Acting on these recommendations,[85] in 2005, Congress passed the USA PATRIOT Reauthorization and Improvement Act and created the National Security Division (NSD) of DOJ.[86] It was the first new litigating division to be established in almost 50 years.[87] Its mission was and remains straightforward: to combat terrorism and other threats to national security.

NSD's creation, along with other legislative and internal policy shifts,[88] helped eliminate organizational barriers that previously separated law enforcement from intelligence, both legally and culturally, within DOJ. Functions that were once overseen by different leaders and pursued for different ends are now linked and coordinated. This facilitates greater collaboration and joint efforts among prosecutors, investigators, intelligence attorneys, and the IC. Integrating the efforts of intelligence and law enforcement personnel gives prosecutors and law enforcement agents access to intelligence, allowing them to focus their resources and develop better criminal cases against the most significant targets.

---

across various agencies within the Department. *See* U.S. DEP'T OF JUSTICE, A.G. ORDER 2708-2004 (on file with author) (listing agencies involved).

[80] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (codified as amended in scattered sections of the U.S. Code).

[81] In re Sealed Case, 310 F.3d 717 (Foreign Int. Surv. Ct. Rev. 2002).

[82] *See generally* 1 DAVID S. KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS AND PROSECUTIONS (2d ed. 2012).

[83] President Bush created the Commission by Executive Order. Exec. Order No. 13,328, 69 Fed. Reg. 6901 (Feb. 11, 2004).

[84] COMM'N ON THE INTELLIGENCE CAPABILITIES OF THE U.S. REGARDING WEAPONS OF MASS DESTRUCTION, THE WMD COMMISSION REPORT 472–73 (2005), https://www.gpo.gov/fdsys/pkg/GPO-WMD/pdf/GPO-WMD.pdf.

[85] *See* H.R. REP. NO. 109-333, § 506, at 109 (2005).

[86] USA PATRIOT Reauthorization and Improvement Act, Pub. L. No. 109-77, § 509A, 120 Stat. 192, 249 (2006).

[87] NAT'L SEC. DIV., U.S. DEP'T OF JUSTICE, PROGRESS REPORT (2008), http://www.justice.gov/sites/default/files/nsd/legacy/2014/07/23/nsd-progress-rpt-2008.pdf.

[88] *See* Kris, *supra* note 76, at 5 (citing USA PATRIOT Act); Memorandum from Att'y Gen. John Ashcroft to Various Dep't of Just. & FBI Officials, Intelligence Sharing Procedures for Foreign Intelligence and Foreign Counterintelligence Investigations Conducted by the FBI (Mar. 6, 2002), www.fas.org/irp/agency/doj/fisa/ag030602.html; In re Sealed Case, 310 F.3d 717 (Foreign Int. Surv. Ct. Rev. 2002).

The record of NSD's success testifies to the power of this coordinated approach. We have disrupted countless terrorism plots and convicted hundreds of defendants in terrorism-related cases since the 9/11 attacks.[89] And we have collected a substantial amount of intelligence through these same investigations and prosecutions.

But notwithstanding the importance of the criminal justice system as part of our strategy, we also know that arrests and prosecutions are not always the best way to keep Americans safe. Counterterrorism prosecutors and agents recognize that the end goal is the disruption of the threat and protecting the safety of the public, regardless of the particular legal tool employed. That may mean sharing intelligence with a foreign partner to take action (including but not limited to local prosecution), preventing travel, freezing or seizing assets, warning the public, applying diplomatic pressure, imposing UN and domestic sanctions, supporting designations of groups as terrorist organizations, deploying intelligence operations, or executing military action. Criminal law and its enforcement may not always be central to, or even a component of, using those tools. And of course, our investigations often begin on the classified side. For this reason, in NSD, we have taken to referring to "investigations" generally, without regard to whether they are "criminal" or not. Of course, "national security investigations" do typically involve criminal activity, and prosecution is a potential outcome that we work to preserve as often as we can—but it is a means to an end rather than our principal goal.

In recent years, we have taken a similar approach to addressing cyber threats—for example, through NSD's partnership with the Criminal Division. Computer crimes increasingly resist neat division into criminal and national security categories. Because the identity and goals of the hacker are often unknown at the outset of a cyber intrusion, it is not always possible to segment investigations into clear criminal or national security categories. Many of the same technical, legal, and policy questions arise regardless of which Division handles a matter. And so, although both the Criminal Division and NSD conduct their own respective prosecutions (in partnership with U.S. Attorney's Offices), we increasingly find ourselves working cases jointly (or at least more actively supporting each other's cases). We also work together in the interagency policy process, where cybersecurity issues bear on both of our missions. As in our counterterrorism investigations, prosecution is one way to help protect our country from cyber threats, but it is not the only way.

Another example of collaboration among DOJ offices is the National Security Cyber Specialist (NSCS) network, a nationwide network of headquarters and field personnel trained and equipped to handle national security-related cyber

[89] Kris, *supra* note 76, at 14.

issues.[90] We established the NSCS network in 2012 to empower the field—to ensure that every jurisdiction has at least one specially trained national security prosecutor who not only is fluent with computers and networks, national security threats, and related investigative techniques and case law, but also is cleared to know the most sensitive threat information and is mindful of issues related to sensitive sources and methods that arise in national security investigations. It includes prosecutors from every U.S. Attorney's Office, along with experts from the Computer Crime and Intellectual Property Section of the Criminal Division and attorneys from all parts of NSD. It provides a simple means for two-way communication between the field and headquarters. This allows us to share information quickly and benefit from our respective areas of expertise in a breaking investigation. NSCS network attorneys receive specialized training on issues at the intersection of cyber and national security, and the NSCS network leads outreach to private sector partners to raise awareness of the dangers posed by cyber threats and encourage closer relationships between the private sector and the government (before and after an intrusion).

Of course, the lawyers in DOJ could not do their jobs without the tireless work of the investigators and analysts of the FBI. At the heart of this effort is the FBI's Cyber Division, which has shifted since its inception in 2002 from targeting computer-enabled traditional crimes to addressing sophisticated cyber threats. The Cyber Division is a vital partner in our collective work and has evolved with the changing nature of the challenge.

One of the most significant threats we face is the increase in cyber espionage activity. Many of the most sophisticated threats we investigate are associated with nation-state actors or their proxies. In those matters, the FBI Cyber Division leads the investigation while coordinating closely with the FBI's Counterintelligence Division, which has historical expertise in the unique threats posed by nation-states. These divisions increasingly work together—for example, embedding Counterintelligence Division special agents and intelligence analysts within cyber operations and intelligence units. The Counterintelligence Division provided significant support to the Cyber Division during the economic espionage investigation that resulted in the indictment of five PLA actors in May 2014.[91]

In many ways, DOJ's increasingly close collaboration with the FBI on cyber matters is an example of how intelligence sharing within the U.S. government should operate. Soon after the NSCS network was formed, the FBI directed that new Cyber Task Forces—interagency teams based out of the FBI's

---

[90] *See generally* Press Release, U.S. Dep't of Justice, New Network Takes Aim at Cyber Threats to National Security (Nov. 14, 2012), http://www.justice.gov/opa/blog/new-network-takes-aim-cyber-threats-national-security.

[91] Robert Anderson, Exec. Assistant Dir., Fed. Bureau of Investigation, Press Conference Announcing Charges Against Five Chinese Military Hackers (May 19, 2014), https://www.fbi.gov/news/speeches/combating-state-sponsored-cyber-espionage.

56 field offices that are focused on cyber threats—engage in consistent communication with the NSCS representatives at the U.S. Attorney's Offices and share as much intelligence as possible, just as FBI and DOJ do in counterterrorism investigations. No longer are national security cyber threats deemed a matter solely for intelligence gathering and operations as opposed to investigations. Similar cyber intelligence sharing exists between DOJ and other agencies in the U.S. government, although we must continue to improve and deepen those ties.

Although we are applying the lessons we learned in the wake of 9/11 to our efforts to disrupt national security cyber threats, we have seen that there are new challenges that call for a new approach. After 9/11, the challenge was, as described above, tearing down the wall between law enforcement and intelligence. In cybersecurity, there is a third party involved—private entities. In cybersecurity, this goes far beyond a generalized call to the public that "if you see something, say something." The private sector is now on the front lines, and often possesses the information we need to collectively respond to national security cyber threats. Information sharing is now a three-way affair, and successful collaboration on this front requires proactive outreach. This Article describes our outreach approach in more detail below.[92]

In sum, just as DOJ reorganized in the wake of 9/11 to more effectively counter the threat of international terrorism, DOJ is beginning to adapt to the threat that malicious cyber actors pose to national security. And as the next section describes, one of the immediate benefits of this transformation has been the government's improved ability to attribute malicious cyber activity to the individuals, organizations, and nations responsible for it.

B. *Tools for Attribution*

We cannot effectively respond to a hack if we do not know who perpetrated it. Accordingly, the government must be able to gather and analyze information about cyber incidents quickly. "Online" investigations are in fact conducted mostly offline, which means that investigating a hack requires physically examining servers, talking to network users, and requesting or compelling providers to turn over copies of records. These are all classic techniques of law enforcement agencies.[93]

The Stored Communications Act[94] (SCA) is one of the government's most important authorities for gathering electronic evidence. The SCA sets out the

---

[92] *See infra* Part III.C.

[93] None of this is to downplay the important (and sensitive) tools that the IC, beyond just the FBI, brings to the effort to attribute, disrupt, and deter malicious cyber activity.

[94] 18 U.S.C. § 2701–2712. The SCA was included as Title II of the Electronic Communications Privacy Act of 1986 (ECPA), Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.). ECPA also amended the Wiretap Act and created the Pen

procedures for federal and state law enforcement to obtain voluntary or compelled disclosure of stored communications from communications-service providers.[95] The SCA sets the procedural requirements based on the nature of the information sought. For instance, the government must obtain a search warrant to compel disclosure of content in many circumstances, while a subpoena is sufficient to compel disclosure of basic subscriber information.[96]

The Foreign Intelligence Surveillance Act of 1978[97] (FISA) is a critical authority for national security or foreign intelligence investigations.[98] As a general matter, to obtain a FISA order for electronic surveillance conducted in the United States, the government must demonstrate, among other things, that the "target of the electronic surveillance is a foreign power or an agent of a foreign power;"[99] that "each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;"[100] and that "a significant purpose of the surveillance is to obtain foreign intelligence information."[101]

In addition, the government must frequently search and seize physical devices—for example, phones, computers, or servers—to effectively investigate and attribute malicious cyber activity. It can get the necessary authority to do so either through traditional search warrants[102] or, in the case of national security and foreign intelligence investigations, FISA orders.[103]

For the purposes of this Article, the intricacies of the legal authorities available to DOJ are less important than the following features they share in common. First, they are powerful tools that the government can use to investigate, and ultimately attribute, cyber intrusions and attacks. Second, they safeguard privacy by setting out a detailed and rigorous process by which the government must justify surveillance and manage the acquired information. And of course, the

---

Register and Trap and Trace Statute. Although practitioners often refer interchangeably to the SCA and ECPA, this Article refers to the SCA throughout.

[95] 18 U.S.C. § 2703. For an overview of the SCA, *see* COMPUT. CRIME & INTELLECTUAL PROP. SEC., CRIMINAL DIV., U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 115–49 (3d ed. 2009), https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf.

[96] *Compare* 18 U.S.C. § 2703(a) (requiring search warrant to compel disclosure of "the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less"), *with* 18 U.S.C. § 2703(c)(2) (permitting the use of a subpoena for basic subscriber and session information).

[97] Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended in scattered sections of 50 U.S.C.).

[98] *See generally* 1 KRIS & WILSON, *supra* note 82.

[99] 50 U.S.C. § 1804(a)(3)(A).

[100] *Id.* § 1804(a)(3)(B).

[101] *Id.* § 1804(a)(6)(B).

[102] *See* FED. R. CRIM. P. 41.

[103] *See* 50 U.S.C. § 1822.

government is bound in all its activities to comply with the Constitution, including the Fourth Amendment.

In addition to its legal authorities, DOJ can draw on its institutional expertise to attribute hacks. The FBI has invested heavily in malware technical analysis capabilities. The FBI also hosts the National Cyber Investigative Joint Task Force, through which nineteen federal agencies coordinate cyber threat investigations. According to former National Security Agency General Counsel Stewart Baker, the view that hackers can operate with complete anonymity is antiquated: "[W]e *can* know who our attackers are . . . . The massive amount of data available online makes the job of attackers easier, but it can also help the defenders if we use it to find and punish our attackers."[104] These attribution efforts ensure that we have as complete a picture as possible of who cyber threat actors are and how particular actors conduct malicious cyber activity. For example, a key way the FBI attributed the Sony hack to North Korea was by comparing the malware used in that hack to malware used in other North Korea–sponsored cyber intrusions.[105]

Attribution requires tools beyond the technical analysis of malware. The FBI's National Center for the Analysis of Violent Crime contains several Behavioral Analysis Units that assist law enforcement with criminal investigative analysis for a wide range of offenses—from counterterrorism to bombings to white collar crime.[106] In 2012, the FBI created the Cyber Behavioral Analysis Center (CBAC), which expanded the work of the Behavior Analysis Units to cyber threats. By analyzing the behavioral patterns of malicious cyber actors—from the kind of malware they use, to the way they communicate with victims—the CBAC "profilers" use the traditional skills of law enforcement to help attribute malicious activity on the Internet.

The FBI used these traditional techniques, in addition to technical malware analysis, to attribute the Sony hacks to North Korea. In addition to the data-deletion malware, the Sony hackers left a "splash screen" on infected Sony computers with the name "Guardians of Peace" and various logos. The hackers used these images in ways similar to the behavior of criminals like serial killers who "stage" the crime scene, arranging it to send a message or conceal involvement. Such stagings go beyond what is necessary to commit the crime, and

---

[104] *The Department of Homeland Security at 10 Years: Examining Challenges and Achievements and Addressing Emerging Threats: Hearing Before the S. Comm. on Homeland Security and Governmental Affairs*, 113th Cong. 1 (2013) (statement of Stewart A. Baker, Partner, Steptoe & Johnson LLP).

[105] *See* James B. Comey, Dir., Fed. Bureau of Investigation, Remarks at the International Conference on Cyber Security, Fordham University (Jan. 7, 2015), https://www.fbi.gov/news/speeches/addressing-the-cyber-security-threat.

[106] *See Investigative & Operations Support*, CRITICAL INCIDENT RESPONSE GRP., FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/about-us/cirg/investigations-and-operations-support.

the extra information they disclose—as in the Sony case—can be helpful in attributing the activity.

More generally, prosecutors and agents are motivated and uniquely suited to investigate with the ultimate goal of using the uncovered information *publicly*. Working in law enforcement trains agents and prosecutors to pursue responsible individuals doggedly and to hold them accountable under the heavy burden of proof beyond a reasonable doubt in an open trial. That standard may be unattainable and unnecessary in the vast majority of cases where the government's response is something other than a criminal prosecution, but we benefit enormously from having a cadre of investigators that are trained to aim to meet a rigorous burden of proof with evidence that can be displayed publicly.

In addition to investigative expertise, prosecutors at DOJ and agents, investigators, and analysts at the FBI have a long history of working with private sector victims of criminal activity. Just as importantly, private sector entities are accustomed to working with the FBI and DOJ. This mutual trust and cooperation is critical, since the first step towards a successful attribution is to investigate the crime scene, which in the cyber context is frequently the victim's network—for example, a computer in the server room of a private company. Victims can provide valuable context, including why the bad actors wanted to do what they did when they did it.

This mix of authorities, institutional competence, and cooperative relationships has led to several high-profile public attributions of malicious cyber activity. In addition to the Sony case, for example, DOJ indicted five Chinese military officers for computer hacking, as described above.[107]

DOJ's decades of experience prosecuting espionage and export-control violations—violations that increasingly occur through cyber-enabled means—have proven particularly valuable in facilitating attribution in cyber cases. For example, in August 2014, a federal grand jury indicted Su Bin, a 49-year-old Chinese businessman, on charges of unauthorized computer access, conspiracy to illegally export defense articles, and conspiracy to steal trade secrets. The indictment alleges that Su worked to "infiltrate computer systems and obtain confidential information about military programs, including the C-17 transport aircraft, the F-22 fighter jet, and the F-35 fighter jet."[108] Su pled guilty in March of this year.[109] In May 2015, six individuals, including three professors at Tianjin

---

[107] *See supra* notes 8–9 and accompanying text.

[108] Press Release, U.S. Atty's Office, C.D. Cal., Los Angeles Grand Jury Indicts Chinese National in Computer Hacking Scheme Allegedly Involving Theft of Trade Secrets (Aug. 15, 2014), https://www.fbi.gov/losangeles/press-releases/2014/los-angeles-grand-jury-indicts-chinese-nati onal-in-computer-hacking-scheme-allegedly-involving-theft-of-trade-secrets; *see also* Indictment, United States v. Su Bin, No. 8:14-cr-00131-UA (C.D. Cal. Aug. 14, 2014).

[109] Press Release, U.S. Dep't of Justice, Chinese National Pleads Guilty to Conspiring to Hack into U.S. Defense Contractors' Systems to Steal Sensitive Military Information (Mar. 23, 2016),

University in China, were charged with economic espionage, theft of trade secrets, and conspiracy. The indictment alleged that, over several years, the defendants "stole recipes, source code, specifications, presentations, design layouts and other documents marked as confidential and proprietary from the victim companies and shared the information with one another and with individuals working for Tianjin University."[110]

* * *

This Article began with a description of the cyber threat and why a good defense requires a strong offense—specifically, deterring bad actors from attempting their malicious activity. If actors believe they can attack in cyberspace anonymously, and at no cost to them, they have no incentive to stop. As deterrence is impossible without attribution, DOJ plays an important role in attributing malicious Internet activity to individuals, groups, and governments. The next Part catalogues the specific ways in which attribution enables DOJ, other federal agencies, and the private sector to take action.

III. An All-Tools Approach to National Security Cyber Threats

Sometimes the best response to malicious cyber activity will be a traditional criminal investigation or prosecution. Sometimes it won't. The right path is to adopt an "all-tools" posture by which decisions about how to respond are made in a threat-specific way, using, and if need be creating, the best and most appropriate tool or tools for the job, whatever they may be. And as this Part demonstrates, the most effective tools almost always require knowing whose fingers are at the keyboard on the other side of the screen.

A. *DOJ-Led Activity*

1. Prosecution

Federal prosecutors have at their disposal a wide array of statutes that address the full life cycle of a national security cyber threat—from inchoate planning to completed offenses. The most important such statute is the Computer Fraud and Abuse Act (CFAA),[111] a cornerstone statute that criminalizes computer crime generally, including most of what qualifies as national security computer crime. One common violation is "intentionally access[ing] a computer without

---

https://www.justice.gov/opa/pr/chinese-national-pleads-guilty-conspiring-hack-us-defense-contractors-systems-steal-sensitive.

[110] Press Release, U.S. Dep't of Justice, Chinese Professors Among Six Defendants Charged with Economic Espionage and Theft of Trade Secrets for Benefit of People's Republic of China (May 19, 2015), http://www.justice.gov/opa/pr/chinese-professors-among-six-defendants-charged-economic-espionage-and-theft-trade-secrets; *see also* Superseding Indictment, United States v. Wei Pang, No. CR-15-00106-EJD (N.D. Cal. Apr. 1, 2015).

[111] 18 U.S.C. § 1030.

authorization," thereby obtaining "information from any protected computer."[112] Another is intentionally accessing a protected computer without authorization and, as a result of such conduct, "caus[ing] damage and loss."[113] By way of example, the five PLA officers alleged to have stolen information for purposes of commercial advantage and private financial gain were charged with stealing information (a violation of 18 U.S.C. § 1030(a)(2)(C)), as well as the use of malware to control their victims' systems (a violation of § 1030(a)(5)).[114] Similarly, destructive malware used in the Saudi Aramco and Sony attacks and the typical DDoS attack would also violate § 1030(a)(5) (as would even less destructive website defacements commonly undertaken by terrorist or similar groups like the SEA).

Additional applicable statutes include the Wire Fraud statute, which criminalizes schemes to defraud "by means of false or fraudulent pretenses, representations, or promises . . . transmitted by means of wire,"[115] and the Wiretap Act, which criminalizes the unlawful interception of wire communications, and the intentional disclosure and use of unlawfully intercepted communications.[116]

Prosecutors can also use statutes specifically focused on national security. For example, the theft of trade secrets constitutes economic espionage under 18 U.S.C. § 1831 when the offense is committed with intent to benefit a foreign government, instrumentality, or agent—for example, a state-owned enterprise or the military of a foreign country. Section 1831 violations carry a higher statutory maximum than those under 18 U.S.C. § 1832, which prohibits trade-secrets theft generally.[117] This difference reflects the greater seriousness of a crime committed for a foreign power than for mere financial gain. In addition, the Arms Export Control Act[118] (AECA), the International Emergency Economic Powers Act[119] (IEEPA), and associated Executive Orders and regulations prohibit the export of controlled technology without a license, including through the theft of information and its transfer abroad over the Internet. The case against Su Bin was charged under the AECA and IEEPA.

Of course, it will be difficult to hale some charged individuals into a U.S. court, especially if they are located in—not to mention agents of—unfriendly

---

[112] *Id.* § 1030(a)(2); *see also id.* § 1030(e)(2) (defining "protected computer").
[113] *Id.* § 1030(a)(5)(C).
[114] *See* PLA Indictment Summary, *supra* note 8.
[115] 18 U.S.C § 1343.
[116] *Id.* §§ 2510–2522.
[117] Individuals convicted under § 1832 may be fined or imprisoned up to 10 years, while individuals convicted under § 1831 may be fined up to $5 million or imprisoned up to 15 years. Organizations convicted under § 1832 may be fined up to $5 million, while organizations convicted under § 1831 may be fined the greater of $10 million or 3 times the value of what was stolen. 18 U.S.C. §§ 1831–1832.
[118] 22 U.S.C. § 2778.
[119] 50 U.S.C. §§ 1701–1708.

foreign powers. But history demonstrates that extradition works. The government will wait for as long as it may take to get custody over a defendant, as illustrated by our experience with international narcotics kingpins. For example, in 2012, Benjamin Arellano-Felix, the leader of the Tijuana Cartel, was convicted on federal racketeering and drug trafficking charges and, today, the 63-year-old drug lord is incarcerated in a U.S. prison.[120] He was originally indicted in 1997, at a time when extradition of a cartel leader was unprecedented.[121] He was arrested in 2002 and ultimately extradited for prosecution in 2011, proving that extradition can have tremendous success. And we are already seeing defendants in national security cyber cases being arrested on foreign soil and facing their charges in U.S. court, like the above-mentioned Su Bin and Ardit Ferizi.

But even if some fugitive hackers end up escaping justice before a federal judge, our general practice should nevertheless still be to publicly charge them as we do other defendants and with other crimes. First, publicly identifying perpetrators, as we did with the five PLA officers, reveals methods and signatures, thereby making it more difficult for them to continue hacking. This, along with worries about getting caught, can increase the cost—and thus decrease the frequency—of future intrusions against our systems. Second, indictments create consequences for the charged defendants themselves. Although our goal is to bring defendants before a court, naming them as wanted criminals also imposes costs. Hackers, like other thieves, are typically valued for their ability to get in and out of systems without getting caught. Their livelihood depends on anonymity. Hackers who are identified publicly by the authorities may find it more difficult to work. Potential "business" partners may be less likely to risk working with them (to avoid their own exposure), and employers may think twice before promoting them. They may be forced underground and face difficulty continuing their crimes, to the benefit of potential victims. Especially if public charges are combined with financial tools prohibiting transactions with indicted hackers, it will be more difficult for them to use the proceeds of their crimes. Finally, denying them the ability to travel, study, or work abroad (for fear of being arrested) imposes a high cost. To be forever cut off from most of the world is itself a restriction of liberty, especially for young hackers who are electronically well-connected to the outside world. These consequences deter not only the charged individuals, but others in their line of work.

Public charges also serve important expressive functions. Charging state-sponsored hackers signals that their behavior is a crime distinct from traditional espionage.[122] Imagine what would happen if we never stood up for the rights of

---

[120] *See* Richard Marosi, *Former Drug Kingpin Arellano Felix Gets 25-Year Prison Term*, L.A. TIMES (Apr. 3, 2012), http://articles.latimes.com/2012/apr/03/local/la-me-arellano-felix-20120403.

[121] *See Under New Law, Mexico Extradites Suspect to U.S.*, N.Y. TIMES (May 5, 2001), http://www.nytimes.com/2001/05/05/world/under-new-law-mexico-extradites-suspect-to-us.html.

[122] Charging a criminal case also signals that the government has proof of its allegations and is prepared to back them up, publicly, and beyond a reasonable doubt. That was particularly important in 2014, when in the face of multiple public and private allegations of malicious activity

U.S. companies whose secrets were stolen by foreign governments. Foreign actors would commit economic espionage with impunity. An understanding might develop that such behavior is, at least tacitly, acceptable. And if later we ever tried to challenge it, precedent would be against us. We would have granted our adversaries an easement of sorts—not over our territory, but over our intellectual and economic capital. Bringing public charges is akin to installing a giant "no trespass sign" on our front yard: Get off our lawn. International law is a law of custom, and our response in such a regime is critically important.

Thus, public charges can be particularly important where the United States seeks to persuade its allies of a norm of behavior. Charging PLA officers with hacking into U.S. entities to steal trade secrets for the economic benefit of Chinese companies clarified our position for the world. It likely helped lead Chinese President Xi to publicly agree to a proposed norm that China had been previously unwilling to accept. That norm provides that states should not "conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors."[123] This is a key development, since as Tom Donilon, former National Security Advisor to President Obama and the recently appointed head of the President's Commission on Enhancing Cybersecurity,[124] said in a 2013 speech, "the United States and China, the world's two largest economies, both dependent on the Internet, must lead the way in addressing [the] problem" of cyber-enabled economic espionage and trade-secrets theft.[125] This agreement, as noted above, was followed immediately by the G20's statement adopting norms of acceptable behavior in cyberspace.

---

by PRC officials, *see, e.g.*, MANDIANT, APT1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS (2013), http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf; David E. Sanger et al., *Chinese Army Unit Is Seen as Tied to Hacking Against U.S.*, N.Y. TIMES (Feb. 18, 2013), http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html; Chris Strohm, *Chinese Hackers Seen Exploiting Cloud to Spy on U.S.*, BLOOMBERG (Nov. 20, 2013), http://www.bloomberg.com/news/articles/2013-11-20/chinese-hackers-seen-exploiting-cloud-to-spy-on-u-s-. Chinese officials continued to deny their government engaged in any computer intrusions and challenged the United States to provide proof, *see, e.g.*, *Beijing's Brand Ambassador: A Conversation with Cui Tiankai*, FOREIGN AFF. (July/Aug. 2013), https://www.foreignaffairs.com/interviews/2013-05-15/beijings-brand-ambassador) ("I don't think anybody has so far presented any hard evidence, evidence that could stand up in court, to prove that there is really somebody in China, Chinese nationals, that are doing these [cyberattacks].").

[123] White House, *supra* note 11.

[124] Press Release, O'Melveny & Myers LLP, Donilon to Lead White House Commission on National Cybersecurity (Feb. 18, 2016), https://www.omm.com/our-firm/media-center/press-releases/donilon-to-lead-white-house-commission-on-national-cybersecurity/.

[125] Press Release, White House, Remarks by Tom Donilon, Nat'l Sec. Advisor to the President: "The United States and the Asia-Pacific in 2013" (Mar. 11, 2013), https://www.whitehouse.gov/the-press-office/2013/03/11/remarks-tom-donilon-national-security-advisor-president-united-states-an.

Some commentators have expressed skepticism that the costs imposed by indictments of Chinese actors are sufficient to change Chinese behavior.[126] This argument against indictments oversimplifies the government strategy. Indictments of state-sponsored hackers will not prevent all malicious cyber activity. We need an all-tools, whole-of-government approach. The only way we can succeed is by changing how our adversaries analyze the costs and benefits of their actions. That is how we can help deter cyberattacks. And the effectiveness of this deterrence is dependent on attribution: knowing who our adversaries are and what makes them tick, whether at the level of country, government agency, organization, or individual hacker.

Again, this is no easy feat. That attribution may be difficult, however, is no reason to remove the criminal justice system from our toolkit. In fact, quite the opposite. DOJ and our law enforcement partners are uniquely well-suited to conduct these kinds of investigations. Through a mix of formal authority, cyber expertise, and cooperative relationships with private sector victims and international partners, we can track down cyber attackers and attribute their actions in a manner that can be used publicly. This public attribution is the bedrock of our approach because it facilitates the use of so many other tools—including sanctions, designations, and diplomatic options—that promote deterrence.

Further, we are at the very beginning of aggressively deterring state-sponsored cyber actors that engage in economic espionage and the theft of trade secrets. The goal is a world in which not only the United States but also other like-minded countries, aided by improved attribution techniques, use a variety of tools, including the criminal justice system, against malicious cyber actors as a matter of course. That is the relevant end state for analysis, and to those who are frustrated that we're not there yet, we agree; we should and must move faster. As to those who would abandon the use of indictments and prosecutions altogether, and prefer to do nothing, why give this conduct a free pass? As we have seen in the past, silence merely rewards bad behavior, and letting this behavior go on quietly unpunished is simply unacceptable.

We need to exert pressure on bad actors from every possible angle. Although prosecutions are just one tool in a broader approach[127] by which the U.S. can pressure actors like China, one should not underestimate the impact of public charges, especially with countries like China that are acutely sensitive to their international relationships.[128] Jim Lewis, Director and Senior Fellow at the

---

[126] *See, e.g.*, Jack Goldsmith, *China and Cybertheft: Did Action Follow Words?*, LAWFARE (Mar. 18, 2016), https://lawfareblog.com/china-and-cybertheft-did-action-follow-words.

[127] *See infra* Parts III.A.2 & 3.

[128] *Cybersecurity 2015: China, China, China*, WASH. POST (Oct. 1, 2015), http://www.washingtonpost.com/video/postlive/cybersecurity-2015-china-china-china/2015/10/01/43919c26-6878-11e5-bdb6-6861f4521205_video.html. As former National Security Council Senior Director for Asian Affairs Evan Medeiros has explained, "[t]he big picture is that from 2014 on, the

Strategic Technologies Program at the Center for Strategic and International Studies, noted that "[t]he Chinese hated the indictments," and that the indictments played a "crucial role" in convincing China to change both its public and private stances on cyber-enabled IP theft.[129]

The ultimate success of this approach will depend on the ability of U.S. agencies and departments to strengthen and support one another's actions.[130] That President Xi's commitments to the United States were followed by the adoption of this norm at the November 2015 G20 summit is very promising. Now, it is imperative that the U.S. take every possible action to see that these commitments come to fruition.

Finally, public charges can also have a positive effect on victims of cyber crimes. Charges recognize victims' injuries and reassure them that the U.S. government is dedicated to punishing the criminals who broke into their systems and stole their information. Victims want results, and charges let victims know that the perpetrators are not being given free passes. Public charges also strengthen public-private intelligence sharing relationships by providing concrete evidence to private entities that sharing information with the government gets results.

To be clear, legal culpability is always the key driver of the decision to prosecute. As explained in the United States Attorney's Manual, which provides internal guidance for DOJ attorneys prosecuting violations of federal law, the decision to bring charges requires that the prosecutor "believe[] that the person's conduct constitutes a Federal offense and that the admissible evidence will probably be sufficient to obtain and sustain a conviction."[131] Thus, although the non-prosecutorial benefits described above are important, they must always be secondary considerations in any charging decision.

---

administration pursued a much more direct and coercive approach with China, and it has produced results over time." Ellen Nakashima, *Following U.S. Indictments, China Shifts Commercial Hacking Away from Military to Civilian Agency*, WASH. POST (Nov. 30, 2015), https://www.washingtonpost.com/world/national-security/following-us-indictments-chinese-military-scaled-back-hacks-on-american-industry/2015/11/30/fcdb097a-9450-11e5-b5e4-279b4501e8a6_story.html. Former National Security Council Director for Cybersecurity Policy Robert Knake called the indictments a "strong move" and noted that the subsequent decrease in PLA cyber activity demonstrated that "China is not this implacable, immovable object" and that "[w]e can in fact alter the behavior of at least portions of the Chinese government." *Id*; *see also* Ellen Nakashima, *U.S. Developing Sanctions Against China over Cyberthefts*, WASH. POST (Aug. 30, 2015), https://www.washingtonpost.com/world/national-security/administration-developing-sanctions-against-china-over-cyberespionage/2015/08/30/9b2910aa-480b-11e5-8ab4-c73967a143d3_story.html.

[129] *Cybersecurity 2015: China, China, China*, *supra* note 128, at 8:05 minutes.

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

[131] U.S. DEP'T OF JUSTICE, UNITED STATES ATTORNEYS' MANUAL § 9-27.220, https://www.justice.gov/usam/usam-9-27000-principles-federal-prosecution#9-27.220.

Criminal prosecutions are an effective legal action that can be taken after we have attributed a hack, but they are far from the only one. In those situations where we have not brought formal charges, we may still gain some of the benefits described above—norm-building, damage to hackers' reputations, etc.—merely through public attribution itself. This gives the government great flexibility as to when to bring public charges, knowing that, even in those situations in which charges are not brought, public attribution can have profound deterrent and disruptive effects on our cyber adversaries.

2. Other Civil and Criminal Actions

In addition to indictments and prosecutions, the U.S. government can use other civil and criminal authorities—including injunctions and temporary restraining orders against fraud and illegal interception of communications, as well as seizure warrants—to fight hackers. Although most of the examples I cite below involve activity designed to advance traditional criminal objectives, they show what's possible in the national security context, given the increasing convergence in the cyber tools used by sophisticated criminal, terrorist, and nation-state actors.

In 2011, the Justice Department's Criminal Division, the U.S. Attorney's Office for the District of Connecticut, and the FBI disrupted the Coreflood botnet—which had seized control of over 2.3 million infected computers, including 1.8 million in the United States—using a combination of civil injunctive authorities and criminal search warrants.[132] The Coreflood malware was a virus that allowed criminal operators to steal online banking credentials and other information from unsuspecting users by tracking their every keystroke.[133] The program forced infected computers to repeatedly check in with command-and-control servers, and then receive and execute commands. The criminals behind this scheme used Coreflood to steal hundreds of thousands of dollars through fraudulent wire transfers from victims, most of whom were small- or medium-sized businesses and local governments.[134]

---

[132] Copies of the related court documents are available at Press Release, U.S. Dep't of Justice, Department of Justice Takes Action to Disable International Botnet (Apr. 13, 2011), https://www.fbi.gov/newhaven/press-releases/2011/nh041311.htm. For additional coverage, see also Jason Ryan, *Feds Take "Coreflood Botnet": "Zombie" Army May Have Infected 2 Million Computers, Stolen Hundreds of Millions of Dollars*, ABC NEWS (Apr. 13, 2011), http://abcnews.go.com/technology/feds-crush-coreflood-botnet-infected-million-computers-stole/story?id=13369529.

[133] Coreflood is an example of what is referred to as a "keylogger": a program that records and transmits what users enter through their keyboards.

[134] *See Botnet Operation Disabled: FBI Seizes Servers to Stop Cyber Fraud*, FED. BUREAU OF INVESTIGATION (Apr. 14, 2011), https://www.fbi.gov/news/stories/2011/april/botnet_041411; David B. Fein, *Major Achievements in the Courtroom: Coreflood Botnet Takedown & Civil Action*, U.S. DEP'T OF JUSTICE (July 9, 2015) http://www.justice.gov/usao/priority-areas/cyber-crime/major-achievements-courtroom-coreflood-botnet-takedown-civil-action.

The government obtained seizure warrants to take down the command-and-control servers and confiscate the domain names used to transmit communications between those servers and infected computers.[135] After seizing the illegal hardware, the government obtained a federal injunction as authorized by fraud[136] and wiretapping[137] statutes. The injunction gave the government the authority to redirect infected computers to secure substitute servers that could command the virus to stop running on infected computers.[138] More importantly, the injunctive remedies prevented Coreflood from updating itself.[139] Antivirus companies, in partnership with the government, then developed updated virus signatures that could detect and delete Coreflood from innocent computers. The FBI also worked closely with Internet service providers (ISPs) to identify and notify individuals whose computers had been infected. As of today, using these law enforcement authorities, we have successfully erased Coreflood from 95% of infected computers.[140]

This unprecedented law enforcement operation employed a combination of criminal and civil authorities against an international hacking ring. Notably, these authorities predate the modern Internet, and in some cases, predate computers. For example, the concept of an injunction to prevent ongoing illegal activity dates back to pre-Revolutionary law, and the specific statutes invoked for injunctive authority date to the 1980s. But all of these authorities were used in 2011 to take down a very modern cyber threat.

More recently, the FBI neutralized the GameOver Zeus botnet, which was responsible for an estimated $100 million in losses from businesses and consumers worldwide whose banking credentials were compromised.[141] One senior FBI official described this "peer-to-peer" network as the most sophisticated botnet the FBI had ever attempted to disrupt.[142] To bring down this criminal network, the U.S. Attorney's Office for the Western District of Pennsylvania,

---

[135] *See* Seizure Warrant, In re Seizure of the Premises Known and Described as Twenty-Four Certain Internet Domain Names (Apr. 12, 2011), https://www.fbi.gov/newhaven/press-releases/2011/pdf/nh041311_2.pdf.
[136] *See* 18 U.S.C. § 1345.
[137] *See id.* § 2521.
[138] For copies of the related court documents, see Press Release, Fed. Bureau of Investigation, Department of Justice Takes Action to Disable International Botnet (Apr. 13, 2011), https://www.fbi.gov/newhaven/press-releases/2011/nh041311.htm.
[139] *See* Seizure Warrant, *supra* note 135.
[140] Fein, *supra* note 134.
[141] *See* Press Release, Fed. Bureau of Investigation, GameOver Zeus Botnet Disrupted: Collaborative Effort Among International Partners (June 2, 2014), https://www.fbi.gov/news/stories/2014/june/gameover-zeus-botnet-disrupted; Tony Bradley, *How to Protect Yourself Against Gameover Zeus and Other Botnets*, PCWORLD (June 2, 2014), http://www.pcworld.com/article/2357528/protect-yourself-against-gameover-zeus-and-other-botnets.html.
[142] Press Release, U.S. Dep't of Justice, U.S. Leads Multi-National Action Against "Gameover Zeus" Botnet and "Cryptolocker" Ransomware, Charges Botnet Administrator (June 2, 2014), http://www.justice.gov/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware.

along with DOJ's Criminal Division and the FBI, obtained injunctive relief authorizing them to sever communications between infected botnet computers and the criminal command-and-control servers.[143] That intercession allowed law enforcement to redirect innocent computers to substitute servers under government control. In other words, the government stepped in between the hackers and the victims, and redirected the victims toward a safer place. As of July 2014, all or nearly all of the computers infected with the GameOver Zeus virus had been "liberated from the criminals' control."[144] The same authorities that facilitated this intervention in the criminal context could be used to address national security cyber threats.

At the same time that law enforcement agencies were pursuing civil orders to mitigate the botnet's substantial damage, a parallel and complementary law enforcement investigation was also working to identify and prosecute the particular individuals behind this global scheme. One of those individuals, Evgeniy Bogachev, now ranks as one of the FBI's most wanted criminals. In May 2014, a grand jury in Pittsburgh unsealed an indictment identifying Bogachev as the mastermind behind GameOver Zeus and charging him with over a dozen crimes, including conspiracy, computer hacking, bank fraud, wire fraud, and money laundering.[145]

The same operation that brought down GameOver Zeus was used to target the malware CryptoLocker, which the botnet had implanted on hundreds of thousands of computers around the world. As described above, CryptoLocker is a "ransomware" program that infects computers, encrypts files, and demands a ransom of hundreds of dollars in order to decrypt the files.[146] The GameOver Zeus botnet contains features that allow users to install additional malware on infected computers, and CryptoLocker was one of the most popular choices. At the time the United States sought to bring it down, CryptoLocker had already infected more than 230,000 computers, including more than 120,000 in the United States.[147] One report estimated that victims of this scheme paid $27 million in ransom payments in the final months of 2013.[148]

---

[143] *See* Memorandum of Law in Support of Motion for TRO and Order to Show Cause at 20, United States v. Bogachev, No. 2:14-cv-00685 (W.D. Pa. June 2, 2014), https://www.justice.gov/opa/file/783651/download.

[144] Press Release, U.S. Dep't of Justice, Department of Justice Provides Update on GameOver Zeus and Cryptolocker Disruption (July 11, 2014), https://www.justice.gov/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware.

[145] *See* Indictment at 11–22, United States v. Bogachev, No. 2:14-cv-00685 (W.D. Pa. May 19, 2014), http://www.justice.gov/sites/default/files/opa/legacy/2014/06/02/pittsburgh-indictment.pdf.

[146] *See supra* note 26 and accompanying text.

[147] *Id.* at 9.

[148] Violet Blue, *CryptoLocker's Crimewave: A Trail of Millions in Laundered Bitcoin,* ZDNET (Dec. 22, 2013) http://www.zdnet.com/article/cryptolockers-crimewave-a-trail-of-millions-in-laundered-bitcoin/.

The FBI and DOJ used similarly innovative legal tools to take apart the botnet used in the Iranian DDoS attack against the U.S. financial sector. Through its FBI Liaison Alert System (more commonly known as FLASH), the FBI regularly updated the private sector with information on the botnet. The FBI has also directly contacted ISPs that host victim computers, providing information and assistance on removing the malware. This has led to a near-complete dismantling of the botnet.[149]

3. New Proposals

As the above suggests, law enforcement authorities have more at their disposal than criminal charges. Our tools include search warrants, subpoenas, injunctions, temporary restraining orders, asset forfeiture, and voluntary private sector cooperation—all of which can have operational benefits. A variety of investigative activities also help us understand the threat and how we can assist private citizens to guard against it.

Yet these legal authorities are not enough. We must update our laws to confront the modern threat. The Obama Administration has made a number of proposals to refine and expand the government's authority to conduct these types of operations. The statutes used in the Coreflood and GameOver Zeus operations give federal courts the authority to issue injunctions to stop the ongoing commission of specified fraud crimes or illegal wiretapping.[150] Because the criminals behind Coreflood and GameOver Zeus used them to commit fraud against banks and bank customers, existing laws allowed DOJ to obtain court orders to disrupt the botnets. But the authority to shut down botnets that are not engaged in fraud or wiretapping is unclear.[151] That is why, as part of a larger legislative package, the President proposed to Congress in January 2015 that activities like the operation of a botnet be added to the list of offenses eligible for injunctive relief. Specifically, the amendment would permit the department to seek an injunction to prevent ongoing hacking violations in cases where 100 or more victim computers have been hacked.[152]

DOJ also submitted a proposal to amend Rule 41 of the Federal Rules of Criminal Procedure to modernize those provisions governing the territorial

---

[149] Press Release, U.S. Dep't of Justice, Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector (Mar. 24, 2016), https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged.

[150] 18 U.S.C. §§ 1345, 2521.

[151] *See* Leslie R. Caldwell, *Assuring Authority for Courts to Shut Down Botnets*, U.S. DEP'T OF JUSTICE (Mar. 11, 2015), http://www.justice.gov/opa/blog/assuring-authority-courts-shut-down-botnets.

[152] *See* WHITE HOUSE, UPDATED ADMINISTRATION PROPOSAL: LAW ENFORCEMENT PROVISIONS, https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/updated-law-enforcement-tools-section-by-section.pdf.

boundaries for searches of stored electronic media. Under the current Rule 41(b), magistrate judges are empowered to issue search warrants for physical items within the confines of their districts, with a few limited exceptions for out-of-district warrants. While this framework historically facilitated law enforcement investigations, the proliferation of network-based criminal activity is evading these once-rational restrictions. As the then-Acting AAG for the Criminal Division explained, the current rule does not "directly address the special circumstances that arise when officers execute search warrants, via remote access, over modern communications networks."[153] Specifically, it makes no provision for situations where the computer to be searched via remote access cannot be physically located or where numerous computers spread across multiple districts must be searched or seized at once, as in a botnet takedown. A revision to the rules recommended by DOJ would close these loopholes and arm investigators with the tools they need to address a range of criminal conduct that is currently evading our efforts. The Supreme Court transmitted the revision to Congress in April 2016.[154]

B. *DOJ's Role in a Whole-of-Government Approach*

DOJ's investigations also enable a variety of responses that make use of the legal authorities of other departments and agencies. In particular, by attributing malicious cyber activity to its source, lawyers and investigators enable smart, targeted action to punish cyber criminals and deter future would-be bad actors.

For example, attribution will play a critical role in using economic sanctions to counter malicious cyber activity. On April 1, 2015, the President issued an Executive Order (EO) that will allow the use of America's economic power against the foreign cyber threat. EO 13,694, entitled "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," authorizes the Treasury Secretary, in consultation with the Attorney General and the Secretary of State, to impose targeted sanctions on and block the assets of individuals and entities whose "malicious cyber-enabled activities" originating from outside the United States contribute to a significant threat to the national security, foreign policy, economic health, or financial stability of the United States.[155]

---

[153] Letter from Mythili Raman, Acting Assistant Att'y Gen., Crim. Div., U.S. Dep't of Justice (Sept. 18, 2013) (on file with author).

[154] *Pending Rules Amendments*, U.S. COURTS, http://www.uscourts.gov/rules-policies/pending-rules-amendments.

[155] Press Release, White House, Statement by the President on Executive Order "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities" (Apr. 2, 2015), https://www.whitehouse.gov/the-press-office/2015/04/02/statement-president-executive-order-blocking-property-certain-persons-en.

Among other things, this EO allows the U.S. government to target certain companies that benefit from trade-secrets theft. Specifically, if a foreign individual or entity receives or uses a trade secret misappropriated through cyber-enabled means, knows the trade secret was misappropriated, and meets certain other criteria, then they could be subject to sanctions under the EO. Economic sanctions carry severe consequences: access to company property in the United States is blocked and U.S. individuals and firms are generally prohibited from engaging in transactions or dealing with that company. This EO has the potential to successfully deter foreign companies and individuals outside our jurisdiction. The types of narrowly tailored sanctions authorized by the EO have the potential to "make clear that the United States and its partners are willing to take a more forceful stance to uphold norms of good conduct in cyberspace," without eliciting the damaging impact on the U.S. and world economies that broad-based sanctions might.[156] Although the EO has not yet been used, it will no doubt change the calculation of foreign parties, including those who are contemplating whether to accept or use American trade secrets stolen by their governments. Similarly, sharing information with partners in the State Department and the U.S. Trade Representative's Office allow those partners to use the tools available to them more effectively.

Imposing economic sanctions on an entity often requires tracing the misappropriated trade secrets to their source—in other words, attributing the cyber intrusion and theft. In addition, knowing who stole the data can be helpful in tracing the spread of that data to companies that use it despite knowing that it's stolen. Accordingly, DOJ investigations will undoubtedly contribute substantially to the development of sanctions targets under this EO, as they often do under other legal tools. Such tools include the Commerce Department–administered Entity List, by which individuals or organizations can be barred from receiving U.S. exports if their activities are contrary to U.S. national security or foreign policy interests.[157] For example, the Commerce Department placed both Su Bin and his aviation company on the Entity List around the time of his indictment.[158] In addition, there are EOs that block property of, and prohibit transactions with, individuals who commit or support terrorism or the proliferation of WMDs.[159]

Finally, effective diplomatic and military responses to malicious cyber activity also require knowing who committed the bad acts. For example, the public criticism of North Korea for the Sony hacks, as well as the additional

---

[156] Zack Cooper & Eric Lorber, *Sanctioning the Dragon: Using Statecraft to Shape Chinese Behavior*, LAWFARE (Mar. 13, 2016), https://www.lawfareblog.com/sanctioning-dragon-using-statecraft-shape-chinese-behavior.

[157] *See Entity List*, BUREAU OF INDUS. & SEC., U.S. DEP'T OF COMMERCE, https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list.

[158] *See* 78 Fed. Reg. 44,680, 44,681 (Aug. 1, 2014); *see also* 81 Fed. Reg. 14,953, 14,957 (Mar. 21, 2016).

[159] *See* Exec. Order No. 13,224, 66 Fed. Reg. 49,079 (Sept. 25, 2001) (terrorism); Exec. Order No. 13,382, 70 Fed. Reg. 38,567 (July 1, 2005) (WMD).

economic sanctions imposed in early 2015,[160] could not have occurred without the FBI's activities, in partnership with Sony, to uncover who was responsible for the intrusion into Sony's systems. Nor could an important collateral benefit of the PLA indictment—the pressure it put on China to agree to change its behavior with respect to economic espionage—have occurred had DOJ been unable to identify the Pittsburgh hackers as PLA officers. Diplomatic efforts have proven critical in China's acceptance of international security norms in the past—notably in the field of export control and nonproliferation, where, as former National Security Council Director for Asian Affairs Evan Medeiros has noted, U.S. pressure "played an important role."[161] DOJ contributed to that effort by, in the words of former AAG for National Security J. Patrick Rowan, "taking many of the concepts used in combatting terrorism—namely, prevention, cooperation and coordination—and applying them to the efforts to prevent the illegal export of sensitive U.S. technology."[162] In a similar way, we will be able to use our ability to attribute malicious cyber activity to push other countries toward accepting and abiding by cyber norms. Finally, if the U.S. government ever needs to respond to a major cyber attack with military or intelligence operations,[163] accurate and rapid attribution will be critical.

C. *Public-Private Collaboration*

The private sector and government have long worked together to strengthen the national defense. During the Cold War, this generally involved volunteers and civil defense functions largely divorced from actual conflict—the battlefields were never on U.S. soil.[164] Today, some of the greatest dangers to national security transit electronic networks reside *within* our borders, threatening, among other things, critical infrastructure that supports our domestic economy

---

[160] Exec. Order No. 13,687, 80 Fed. Reg. 819 (Jan. 6, 2015).

[161] EVAN S. MEDEIROS, RAND CORP., CHASING THE DRAGON: ASSESSING CHINA'S SYSTEM OF EXPORT CONTROLS FOR WMD-RELATED GOODS AND TECHNOLOGIES 17 (2005), http://www.rand.org/content/dam/rand/pubs/monographs/2005/RAND_MG353.pdf; *see also* EVAN S. MEDEIROS, RAND CORP., CHINA'S INTERNATIONAL BEHAVIOR: ACTIVISM, OPPORTUNISM, AND DIVERSIFICATION 98 (2009), http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG850.pdf ("Chinese policymakers and analysts regularly stress the high quality of U.S.-China cooperation on combating global terrorism and WMD proliferation, highlighting it as a new basis of stability in bilateral relations.").

[162] *Enforcement of Federal Espionage Laws: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary*, 110th Cong. 5 (2008) (statement of J. Patrick Rowan, Dep. Assistant Att'y Gen., Nat'l Sec. Div., U.S. Dep't of Just.).

[163] *See, e.g.*, DEP'T OF DEF., THE DOD CYBER STRATEGY 11 (2015), http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf ("The United States has been clear that it will respond to a cyberattack on U.S. interests through its defense capabilities. . . . The United States will continue to respond to cyberattacks against U.S. interests at a time, in a manner, and in a place of our choosing, using appropriate instruments of U.S. power and in accordance with applicable law.").

[164] NAT'L PREPAREDNESS TASK FORCE, U.S. DEP'T OF HOMELAND SEC., CIVIL DEFENSE AND HOMELAND SECURITY: A SHORT HISTORY OF NATIONAL PREPAREDNESS EFFORTS 5–7 (2006), http://training.fema.gov/hiedu/docs/dhs%20civil%20defense-hs%20-%20short%20history.pdf.

and our health and safety. Private actors, not the government, are the dominant players, and the role of the private sector will only continue to increase as the "Internet of Things" gains increasing importance in our daily lives.[165] Cybersecurity must be built into all phases of development of Internet-connected systems and devices. This need was made evident when, just last July, security researchers remotely hacked a Jeep Cherokee as it was being driven down a highway, gaining the ability to shut down the engine, disable the brakes, and affect steering.[166] As a result of that controlled experiment, Chrysler issued a recall for 1.4 million vehicles.[167] It will be far cheaper, and far more beneficial to our collective security, if companies invest in cybersecurity at the front end of the product design and development process.

Not only is the majority of Internet-connected devices and Internet software and traffic privately used and generated, but the Internet's physical networks are also managed by private corporations. Over 80% of the critical infrastructure in the United States is owned and controlled by private firms.[168] Despite the tremendous resources and expertise available to federal agencies, the private sector is an indispensable partner in securing our nation's digital systems.[169] As my predecessor Lisa Monaco explained: "Private companies are on the front lines. Individual defenses, as well as broader efforts to reform . . . will require our joint efforts."[170] ISPs, critical-infrastructure operators, software vendors, security researchers, and industry associations all have important roles to play. Our collective success in protecting the country from the economic and physical consequences of network intrusions will depend in large part on the effectiveness of public-private collaborations.

As in the days after 9/11, when we tore down the wall between law enforcement and intelligence, now we facilitate information and threat sharing between the government and the private sector. Without cooperation and information from the private sector, the government would have a much harder

---

[165] For an analysis of coming cybersecurity risks, see SOFTWARE ENG'G INST., CARNEGIE MELLON UNIV., 2016 EMERGING TECHNOLOGY DOMAINS RISK SURVEY (2016), http://resources.sei.cmu.edu/asset_files/TechnicalReport/2016_005_001_453825.pdf.

[166] Michael E. Miller, *"Car Hacking" Just Got Real: In Experiment, Hackers Disable SUV on Busy Highway*, WASH. POST (July 22, 2015), https://www.washingtonpost.com/news/morning-mix/wp/2015/07/22/car-hacking-just-got-real-hackers-disable-suv-on-busy-highway/.

[167] Andy Greenberg, *After Jeep Hack, Chrysler Recalls 1.4M Vehicles for Bug Fix*, WIRED (July 24, 2015), http://www.wired.com/2015/07/jeep-hack-chrysler-recalls-1-4m-vehicles-bug-fix/.

[168] U.S. GOV'T ACCOUNTABILITY OFFICE, CRITICAL INFRASTRUCTURE PROTECTION: PROGRESS COORDINATING GOVERNMENT AND PRIVATE SECTOR EFFORTS VARIES BY SECTORS' CHARACTERISTICS (2006) http://www.gao.gov/assets/260/252603.pdf.

[169] *See Critical Infrastructure Sector Partnerships*, U.S. DEP'T OF HOMELAND SEC., http://www.dhs.gov/critical-infrastructure-sector-partnerships; Myriam Dunn Cavelty & Manuel Suter, *Public-Private Partnerships Are No Silver Bullet: An Expanded Governance Model for Critical Infrastructure Protection*, 4 INT'L J. CRITICAL INFRASTRUCTURE PROTECTION 179 (2009).

[170] Lisa Monaco, Assistant Att'y Gen. for Nat'l Sec., U.S. Dep't of Justice, Speech at the 2012 Cybercrime Conference, Seattle (Oct. 25, 2012), http://www.justice.gov/nsd/justice-news-2.

time attributing malicious cyber activity and understanding its motivations. At the same time, the private sector relies on the government for information about the latest threats and to take investigative and deterrent actions unavailable to the private sector. Senator Dianne Feinstein has emphasized the importance of public-private cooperation in cybersecurity: "To strengthen our networks, the government and private sector need to share information about the attacks they are facing and how best to defend against them."[171]

Companies sometimes hesitate to voluntarily share information with the government. This is understandable. They may worry that sharing information about cyber intrusions with law enforcement or regulators might risk their public reputation, customer confidence, or stock prices, and that doing so could expose them to litigation, enforcement actions, or even criminal sanctions. Even where regulatory guidance requires disclosure, "companies have tended to include generic risk factors rather than disclose specific incidents," according to former Acting AAG Todd Hinnen.[172] With business concerns in mind, companies may prefer to conduct an investigation internally in an attempt to resolve the problem on their own before involving law enforcement. If they do resolve it, the incident may never be reported; if they do not, the reporting and subsequent investigation will be delayed.

There are risks to going it alone, both for the individual victim company and the public at large, and reasons why reporting intrusions to law enforcement is to a company's advantage. First and foremost, the government can help victims understand what happened. Experienced law enforcement agents (with access to the intelligence and resources of other parts of the government) are often familiar with patterns of malicious cyber activity across the country. They can help a company's security and technical teams identify and stop the malicious activity and better understand the context of the incident.

As a result, private reporting can help reveal what may have initially appeared to be a simple criminal enterprise as something much more sinister. Consider the complaint in the Ferizi case, mentioned above.[173] To the victim company, the intrusion into its network and the theft of personally identifiable information may have appeared to be simple identity theft of a sort perpetrated every day in this country. But the government was in the position to uncover that, as alleged in the complaint, the cyber activity was part of a transnational terrorist threat, involving a Kosovar citizen in Malaysia providing personally identifiable information on American service members to ISIL. But imagine

---

[171] Press Release, U.S. Senate Select Comm. on Intelligence, Senate Intelligence Committee Approves Cybersecurity Bill (July 10, 2014), http://www.intelligence.senate.gov/press/senate-intelligence-committee-approves-cybersecurity-bill.

[172] *See* Karen Freifeld, *U.S. Companies Allowed to Delay Disclosure of Data Breaches*, REUTERS (Jan. 16, 2014), http://www.reuters.com/article/us-target-data-notification-idUSBREA0F1LO20140116.

[173] *See supra* notes 38–39 and accompanying text.

(counterfactually) if the victim decided not to cooperate with law enforcement to investigate the origin and scope of the intrusion, and physical harm befell one of the individuals whose data was stolen. The repercussions to the victim company might go beyond the data breach alone.

Furthermore, if one company discovers a cyber intrusion, it is likely that other companies in the industry have been breached as well. Usually, perpetrators of cyber intrusions use exploits that target common vulnerabilities, and many perpetrators engage in mass exploitation of targets. Reporting the incident allows law enforcement to identify broader trends in the cyber threat environment and to disseminate information that helps other potential victims protect their own networks. And disclosing information about the intrusion to the U.S. government often enables us to share valuable insights and information from other investigations with the reporting victim. The more complete a victim's understanding of what happened, the better its ability to mitigate any damage and to identify and defend against similar activity in the future.

Second, proactive cooperation may assist victims in dealing with government regulators and other constituents. For instance, the Federal Trade Commission has said that it's "likely" that it will view a company that has suffered a breach "more favorably" if "it cooperated with criminal and other law enforcement agencies in their efforts to apprehend the people responsible for the intrusion."[174] And the Securities and Exchange Commission has signaled that it "will give substantial credit" to companies that proactively self-report cyber intrusions.[175] Cooperation also often strengthens a victim's position before shareholders, insurers, lawmakers, the media, and others observing how it responds. As our outreach has shown, those constituents want to know whether the company did everything in its power to protect itself (and often its customers), and that includes cooperating with law enforcement.

Third, the federal government is uniquely positioned to win some measure of justice for victims and to deter malicious activity. This may, of course, be through criminal charges, arrest, and prosecution. But when victims report intrusions and cooperate in ensuing investigations, they also enable every one of the other legal tools and actions discussed in the foregoing sections. These include diplomatic pressure, intelligence operations, military action, enforcement of

---

[174] Mark Eichorn, *If the FTC Comes to Call*, FED. TRADE COMM'N BUS. BLOG (May 20, 2015), https://www.ftc.gov/news-events/blogs/business-blog/2015/05/if-ftc-comes-call ("We'll also consider the steps the company took to help affected consumers, and whether it cooperated with criminal and other law enforcement agencies in their efforts to apprehend the people responsible for the intrusion. In our eyes, a company that has reported a breach to the appropriate law enforcers and cooperated with them has taken an important step to reduce the harm from the breach. Therefore, in the course of conducting an investigation, it's likely we'd view that company more favorably than a company that hasn't cooperated.").

[175] Ken Herzinger et al., *SEC Speaks—What to Expect in 2016*, ORRICK (Feb. 23, 2016), http://blogs.orrick.com/securities-litigation/2016/02/23/sec-speaks-what-to-expect-in-2016/.

multilateral trade agreements, and economic sanctions. These tools not only deter foreign actors generally, but also can potentially target the individual companies that benefit from the economic espionage, thus providing a measure of specific deterrence and possibly mitigation of damage.

Because electronic evidence dissipates over time, speed is essential in breach investigations. We can't know today whether we will charge a case, arrest a defendant, or take some other action, but quick action to report and investigate a breach maximizes the chances that we are able to take some legal or other action to disrupt the perpetrators.

On the other hand, without private reporting of cyber incidents and indicators, there is little deterrence: hackers can easily find new targets and run little risk of punishment. Fortunately, last December, and after close to eight years of congressional consideration of legislation to address this problem, the President signed legislation to encourage public-private collaboration related to the sharing of certain types of cyber information. The Cybersecurity Information Sharing Act of 2015 provides companies with certain liability protection when they share indicators of cyber threats, or techniques to defend against cyber threats, with each other and with the government.[176] The legislation also includes rigorous requirements and restrictions to ensure that privacy and civil liberties are protected, including through requirements to remove personal or identifying information[177] and guidelines to "limit the receipt, retention, use, and dissemination of cyber threat indicators containing personal information or information that identifies specific persons."[178]

Finally, sometimes the government alone has access to the critical cyber threat signatures that private industry needs to effectively defend itself. In addition to the Department of Homeland Security, which runs the important Computer Emergency Readiness Team (US-CERT) and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT),[179] the FBI works closely with the private sector through its InfraGard program, a public-private partnership with over 30,000 members. The program securely distributes unclassified intelligence products relating to threats to critical infrastructure and

---

[176] Consolidated Appropriations Act, 2016, Pub. L. 114-113, div. N, tit. I, 129 Stat. 2241, 2936 (2015) (codified at 6 U.S.C. §§ 1501–1510).
[177] 6 U.S.C. § 1503(d)(2).
[178] *Id.* § 1504(b)(3)(B). On February 16, 2016, the DOJ and the Department of Homeland security issued interim guidelines, as required by the law. U.S. DEP'T OF HOMELAND SEC. & U.S. DEP'T OF JUSTICE, PRIVACY AND CIVIL LIBERTY INTERIM GUIDELINES (2016), https://www.us-cert.gov/sites/default/files/ais_files/Privacy_and_Civil_Liberties_Guidelines_(Sec%20105(b)).pdf.
[179] Pursuant to EOs 13,636 and 13,691, the Department of Homeland Security's National Cybersecurity and Communications Integration Center (NCCIC) collaborates closely with private sector entities to ensure access to classified and unclassified information about cyber risks and incidents. NCCIC includes US-CERT and ICS-CERT, which together publish hundreds of products each year and provide classified and unclassified briefings.

allows affected stakeholders to report incidents directly to the FBI. Furthermore, the FBI has presented over three dozen sector-specific threat briefings to companies in the past year alone. Through such efforts, law enforcement has also attempted to advise private sector actors on the steps they can take to keep their own networks safe. For example, in April 2015, the Cybersecurity Unit of the Computer Crime and Intellectual Property Section of the Criminal Division released a guidance document advising private companies on best practices for preparing for and responding to security breaches.[180]

These initiatives capitalize on the comparative advantages of the public and private sectors, while generating the type of persistent coordination required in a threat environment characterized by constantly evolving challenges. The private sector enjoys remarkable expertise, enormous manpower, and an ability to quickly act to protect its own systems. In some cases it also has a technological advantage, at least in relation to monitoring and guarding its own networks.[181] The government has a different kind of expertise, with legal authority to take decisive action and the power to compel cooperation at home using legal process and persuade (or pressure) foreign governments to do the same. In the most important cases, the government can also bring enormous manpower to the table. Together, the private sector and the government each amplifies and strengthens the other, holding out our best chance to disrupt and deter cyber intrusions before they cause real harm to our economy, our security, and our way of life.

Ultimately, we must find the right balance of industry protections, government action, and civil and regulatory liability—the right combination of carrots and sticks—that incentivizes companies to improve their cybersecurity without revictimizing them or creating perverse incentives to underreport. Where to strike this balance might change over time. This Article doesn't purport to give the answer. Rather, it sets out a research agenda that will hopefully be taken up by industry and researchers.

Conclusion

We are at the early stages of what will be a long fight against national security cyber threats, and DOJ is only beginning to play a significant role in this fight. A good analogy is DOJ's counterterrorism activities shortly after 9/11. Although terrorists had been prosecuted in federal courts before 9/11, the FBI had no National Security Branch, the National Security Division hadn't been created, the relationship between foreign intelligence gathering and law enforcement activities was rapidly transforming, and there were active debates about whether

---

[180] CYBERSECURITY UNIT, U.S. DEP'T OF JUSTICE, BEST PRACTICES FOR VICTIM RESPONSE AND REPORTING OF CYBER INCIDENTS (2015), https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/04/30/04272015reporting-cyber-incidents-final.pdf.

[181] *See* Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 HARV. J.L. & TECH. 429, 448–49 (2012).

terrorists could be adequately investigated, disrupted, and prosecuted through the domestic criminal justice system. We now use the criminal justice system more effectively than ever before in combatting terrorist threats and gaining vital intelligence on terrorist plots, while at the same time using other tools.

It took multiple years, with occasional course corrections, for the government to develop its strategy—and that strategy is still evolving to meet a changing terrorist threat. Such is the case now with the cyber threat. The tools described above show great promise, and have already made significant improvements, but they can be used to do more. Prosecutions, takedowns, public attribution, diplomatic and economic pressure—all of these techniques will evolve over the next decade and beyond. And no doubt an article on this subject written ten years from now will highlight tools and activities as yet unimagined.

So although we'll need to race to catch up to today's threat, that will not be enough. The dynamism of the Internet is reflected in the rapidly evolving nature of the cyber threat: its actors, their motivations, and their tools. The government, and society at large will have to continue to think creatively about how to keep ourselves safe while preserving the dynamism and openness that has made the Internet such a revolutionary invention.

There will be false starts, and even more false peaks. But we must resist cynicism or desperation. Throwing up our collective hands is not an option—not for the engineers who design the technologies and services we use, the public that benefits from them, the academics and researchers who study how to manage these complex systems, and especially not for those tasked with protecting our nation.