Vanderbilt Journal of Transnational Law

Volume 50
Issue 4 *October 2017*

Article 2

2017

Hidden by Sovereign Shadows: Improving the Domestic Framework for Deterring State-Sponsored Cybercrime

Eric Blinderman
Therium, Inc.

Myra Din
U.S. District Court for the Eastern District of New York

Hidden by Sovereign Shadows: Improving the Domestic Framework for Deterring State-Sponsored Cybercrime

Eric Blinderman[*] *& Myra Din*[**]

ABSTRACT

This Article analyzes the domestic legal framework applicable to state-sponsored cybercrime. The Article describes several instances where state sovereigns perpetrated cybercrimes in the United States. It then outlines the legal framework that the US government utilizes to hold accountable those who perpetrate such crimes. This Article argues that the current legal framework does not have a deterrence effect on sovereign states engaged in such activity and that prosecutors who seek to apply the current framework against state sovereigns or who misattribute the source of such attacks could negatively impact US foreign policy. To remedy these defects, this Article asserts that relevant US law should apply extraterritorially and that Congress should contemplate passing a statute that abrogates sovereign immunity for state sponsors of cybercrime and subjects such states to civil liability.

TABLE OF CONTENTS

---

[*] Eric Blinderman is the CEO of Therium, Inc.

[**] Myra Din is a judicial law clerk in the U.S. District Court for the Eastern District of New York.

I. INTRODUCTION

Since the first tribes evolved into sovereign states and began competing with one another for resources, power, and influence, they have sought to obtain advantage over the others through the gathering and use of confidential and sensitive information and the forcible destruction of a competitor and its resources.[1] Traditional diplomacy, spying, monitoring of foreign news outlets, military force, and other similar tools have long been deployed to allow sovereigns to gain and utilize such information and/or to obtain advantage over a competitor. Since the advent of the information age, however, these tools have evolved radically as sovereigns seek to exploit the

1. Even the Bible chronicles that espionage has been consistent with the law of nations since Moses sent spies into Israel. "Yet there is no doubt, but the law of nations allows any one to send spies, as Moses did to the land of promise, of whom Joshua was one." HUGO GROTIUS, THE RIGHTS OF WAR AND PEACE, INCLUDING THE LAW OF NATURE AND OF NATIONS 331 (A.C. Campbell, trans., M. Walter Dunne 1901) (1625).

vulnerabilities that attach to the mass storage and transmission of information across a variety of digital platforms.[2]

This technological complexity has also given rise to equally complicated legal issues that attach when a sovereign deploys its digital arsenal against another state in a manner which violates the domestic laws of the target state. For example, attributing cyber action to a sovereign is often a difficult task given the multitude of state and non-state actors that perpetrate such actions.[3] Additionally, if a sovereign is implicated in such an action, the international and domestic legal framework designed to hold the sovereign responsible for such criminal activity is nearly nonexistent.[4] Likewise, the domestic legal norms across each state pertaining to these types of cyber activities vary wildly.[5] This lack of uniformity makes it

---

2. *See, e.g.*, Julian Borger, *Brazilian President: US Surveillance a "breach of international law,"* THE GUARDIAN (Sept. 24, 2013), https://www.theguardian.com/world/2013/sep/24/brazil-president-un-speech-nsa-surveillance [https://perma.cc/5FGC-88JP] (archived Aug. 26, 2017); David E. Sanger, *Document Reveals Growth of Cyberwarfare Between the U.S. and Iran*, N.Y. TIMES (Feb. 22, 2015), https://www.nytimes.com/ 2015/02/23/us/document-reveals-growth-of-cyberwarfare-between-the-us-and-iran.html?_r=2 [https://perma.cc/7T8C-UNHX] (archived Aug. 25, 2017); David E. Sanger, *Iran Fights Malware Attacking Computers*, N.Y. TIMES (Sept. 25, 2010), http://www.nytimes.com/2010/09/26/world/middleeast/26iran.html [https://perma.cc/2J3P=2Q4C] (archived Aug. 26, 2017); Ian Traynor, *Russia accused of unleashing cyberwar to disable Estonia*, THE GUARDIAN (May 17, 2007), https://www.theguardian.com/world/2007/may/17/topstories3.russia [https://perma.cc/9NVU-HM7X] (archived Aug. 26, 2017).

3. One of the leading international sources on international cybercrime is the Tallinn Manual. This comprehensive manual is the product of a study conducted by an International Group of Experts that purports to apply existing international law to the cyber warfare context. Several rules in this manual govern attribution, underscoring the innate complexities when attributing cyberattacks to sovereign states. *See generally* INTERNATIONAL GROUP OF EXPERTS, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt et al. eds., 2013) [hereinafter TALLINN MANUAL].

4. Indeed, while the European Convention on Cybercrime is designed to simplify some of the jurisdictional issues that arise when cross-border cyberattacks occur, the convention was designed to address cybercrime perpetrated by private actors as opposed to government actors. *See* Convention on Cybercrime, Jan. 7, 2004, C.E.T.S. No. 185; *Professor Kesan on the Sony Hack, North Korea and the Laws Governing Cyber-Attack*, ILL. L. FACULTY BLOG (Jan. 13, 2015), http://uiuclawfaculty.typepad.com/facultyblog/2015/01/professor-kesan-on-the-sony-hack.html [https://perma.cc/4P5E-DWH8] (archived Aug. 26, 2017).

5. Consider the example of China. Just this past November, China implemented new cybersecurity regulations to increase dramatically data localization and state surveillance. These laws require all technology companies in China to require users to register with their real names and personal information and to censor content that is "prohibited." Kate Conger, *China's new cybersecurity law is bad for business*, TECHCRUNCH (Nov. 6 2016), https://techcrunch.com/2016/11/06/chinas-new-cybersecurity-law-is-bad-news-for-business/ [https://perma.cc/LYL7-RLRU] (archived Aug. 29, 2017). Such a regime stands in stark contrast to the European Union, which has gradually expanded privacy rights. Indeed, in 2014, the European Court of Justice held that the Data Retention Directive, a mandate that required each member state to

extraordinarily difficult for any enforcement authority to make a reasoned judgement about when permissible information-gathering crosses into the realm of impermissible cybercrime. In addition, the diplomatic consequences of misattribution make the stakes for assessing cybercrime especially high.[6]

Although analyzing the multitude of these challenges is beyond the scope of this Article, it is important to understand the basic framework within the United States that federal prosecutors rely upon when trying to hold accountable actors who perpetrate such crimes.[7] Even more relevant is understanding how this framework applies in the unique context when a sovereign state is implicated in such criminal activity. By better understanding this framework and applying it to instances where sovereigns have seized information from persons, juridical or natural, located in the United States, one can understand the limitations current law enforcement faces when seeking to punish such activity. Most importantly, by understanding these limitations, one can also propose changes to the current domestic framework so that such criminal activity is effectively deterred and perpetrators are held accountable for their actions.

This Article does the following. Part I describes recent instances of sovereign use of digital tools to perpetrate various crimes. Part II describes the legal framework that the US government utilizes when it concludes that a sovereign was implicated in a crime. It also discusses the international legal framework that could be (but is generally not) employed by the United States to address such criminal activity. Part III argues that there are two main shortcomings with the present domestic legal framework applicable to such sovereign criminal activity, including but not limited to whether: (1) domestic prosecutions actually have a deterrence effect on sovereign states perpetrating such crimes, and (2) prosecutors who overreach in their application of US law against foreign actors or misattribute the source of cyberattacks on the basis of insufficient evidence negatively impact US foreign policy. This Article then concludes by arguing that if the public wishes for the government to prosecute effectively state-sponsored actors, then the domestic legal framework should allow for the robust extraterritorial application of

---

retain citizens' personal data, violated the fundamental right to privacy enshrined under European Union Law. Joined Cases C-293/12 & C594/12, Digital Rights Ir. Ltd. v. Minister for Commc'n, 2014 E.C.R. I-238.

6. *See* Howard Lipson, *Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues*, CERT COORDINATION CENTER (Nov. 2002), http://resources.sei.cmu.edu/asset_files/SpecialReport/2002_003_001_13928.pdf [https://perma.cc/PM92-XVKQ] (archived Aug. 26, 2017).

7. One thing that is clear. The US Intelligence Community's desired method for prosecuting sovereign state actors is through domestic legal frameworks. *See* John P. Carlin, *The FBI Wants to Try North Korean Sony Hackers in US Courts*, MOTHERBOARD (Feb. 23, 2015), https://motherboard.vice.com/en_us/article/the-fbi-wants-to-try-north-korean-sony-hackers-in-us-courts [https://perma.cc/VBH8-AUTS] (archived Aug. 26, 2017).

US laws. Further, this Article concludes by arguing that Congress should contemplate passing a statute that exposes sovereign state perpetrators to civil liability.

II. DESCRIPTION OF SOVEREIGN INVOLVEMENT IN CYBERCRIME

On a nearly daily basis, news outlets report alleged instances in which a sovereign state has engaged in digital espionage or sabotage against another.[8] Each instance of such activity raises fundamental definitional problems as to what constitutes cybercrime and when law enforcement officials should attribute digital criminal activity to a sovereign state as opposed to a non-state actor. To answer these definitional problems, the next Parts of the Article analyze four specific instances of alleged cybercriminal activity directed against the United States and in violation of US domestic law: (a) the People's Liberation Army of China's (PLA) alleged theft of digitally stored trade secrets and information from various US companies, which was then used to benefit Chinese companies; (b) the Russian government's

---

8. *See, e.g.*, Andrzej Kozlowski, *Comparative Analysis of Cyberattack on Estonia, Georgia and Kyrgyzstan*, 3 EUR. SCI. J. 237, 238 (2014), http://www.eujournal.org/index.php/esj/article/viewFile/2941/2770 [https://perma.cc/T3QV-4N76] (archived Aug. 27, 2017) (comparing three allegedly Russian state-sponsored cyberattacks against Estonia in 2007, Georgia in 2008, and Kyrgyzstan in 2009 respectively); Michael Cieply & Brooks Barnes, *Sony Cyberattack, First a Nuisance, Swiftly Grew Into a Firestorm*, N.Y. TIMES (Dec. 30 2014), https://www.nytimes.com/2014/12/31/business/media/sony-attack-first-a-nuisance-swiftly-grew-into-a-firestorm-.html [https://perma.cc/BQ7N-Y82W] (archived Aug. 27, 2017) (describing a 2014 cyberattack believed to be launched by North Korea against Sony Pictures Entertainment, located in the United States); *Hackers Leak Emails from UAE Ambassador to US*, AL JAZEERA (June 4, 2017), http://www.aljazeera.com/news/2017/06/hackers-leak-emails-uae-ambassador-170603153956229.html [https://perma.cc/95L2-Q5H6] (archived Aug. 26, 2017) (describing how recently the United Arab Emirates' Ambassador to the United States, Yousef al-Otaiba, was hacked); Steve Lohr & Liz Alderman, *The Fallout From a Global Cyberattack: 'A Battle We're Fighting Every Day'*, N.Y. TIMES (May 15, 2017), https://www.nytimes.com/2017/05/15/world/asia/china-cyberattack-hack-ransomware.html [https://perma.cc/334M-TDJ5] (archived Aug. 26, 2017) (describing a recent global hack which was first detected in Britain but also infiltrated many computer systems of prestigious institutions and healthcare services systems throughout China, India, and Russia); Gerry Mullany & Paul Mozur, *Cyberattack Spreads in Asia; Thousands of Groups Affected*, BERKSHIRE EAGLE (May 16, 2017), http://www.berkshireeagle.com/stories/cyberattack-spreads-in-asia,507471; Choe Sang-Hun, Paul Mozur, Nicole Perlroth & David E. Sanger, *Focus Turns to North Korea Sleeper Cells as Possible Culprits in Cyberattack*, N.Y. TIMES (May 16, 2017), https://www.nytimes.com/2017/05/16/world/asia/north-korea-cyber-sleeper-cells-ransomware.html [https://perma.cc/3Q8Y-ST7Y] (archived Aug. 27, 2017) (describing how cybersecurity experts believe North Korea has spread "cadres of digital soldiers" across the border to China and other countries who are trained to engage in electronic warfare against South Korea and the United States).

hacking into and seizing of over 500 million Yahoo user accounts in 2014; (c) the Iranian Islamic Revolutionary Guard Corps' coordinated attack on forty-six major US companies mostly in the financial sector in order to harm American infrastructure and American people; and (d) the Russian government's alleged theft of politically sensitive information from the Democratic National Committee and subsequent leaking of that information to cause damage to the US democratic system.

After reviewing the facts pertaining to these four instances of purported sovereign state cybercrime, this Article defines "cybercrime" as any digital activity which runs afoul of US domestic criminal statutes.[9] Secondly, it argues that sovereign attribution to cybercrime should attach when any individual, arm, or agency of a sovereign acts, or acting at the direction of a sovereign, is directly responsible, aids or abets those responsible, conspires with those responsible, or otherwise facilitates the perpetration of such cybercriminal activity.[10]

---

9. This definition is based upon analogous reasoning included in the latest edition of the Tallinn Manual. In the Manual's Section on Sovereignty, Jurisdiction, and Control, Rule 5 explains that unlawful cyber activity denotes an activity "that is contrary to the legal rights of the affected State." *See* TALLINN MANUAL, *supra* note 3 (providing the definition of "unlawful" as it is used in Rule 5 – Control of Cyber Infrastructure, designed not limiting the prohibition to narrower concepts). The International Group of Experts that drafted the Manual further explain that they "deliberately chose not to limit the prohibition to narrower concepts, such as use of force (Rule 11) or armed attack (Rule 13), in order to emphasize that the prohibition extends to all cyber activities from one State's territory that affect the rights of other States and have detrimental effects on another State's territory." *Id.*

10. This standard too derives from the latest determinations made by the International Group of Experts in the Tallinn Manual. In Rule 5, the Manual instructs that for purposes of attribution, "A state shall not knowingly allow the cyber infrastructure located in its territory or under its exclusive governmental control to be used for acts that adversely and unlawfully affect other States." The manual further explains there is not yet consensus as to whether state attribution is appropriate where a state has constructive knowledge of cyber activities occurring from its territory or governmental structures. As such, the Tallinn Manual imposes a high standard for state attribution, one close to effective or direct control, with a high bar for specific intent, rather than applying the more lenient overall control standard that has occasionally been employed in international law. *Id.*; *see also* G.A. Res. 56/83, Responsibility of States for Internationally Wrongful Acts, U.N. Doc. A/56/83 (Dec. 12, 2001). For a discussion about the competing standards for state attribution under modern international law, see Scott J. Shackleford, *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem,* CONF. ON CYBER CONFLICT 197–198 (2010), https://ccdcoe.org/sites/default/files/multimedia/pdf/Shackelford%20-%20State%20Responsibility%20for%20Cyber%20Attacks%20Competing%20Standards%20for%20a%20Growing%20Problem.pdf [https://perma.cc/HB4E-Y88C] (archived Aug. 26, 2017).

A. *China: The People's Liberation Army's Hack of US Companies*

On May 1, 2014, the U.S. Department of Justice formally charged five Chinese officers of the PLA with various crimes related to computer hacking and economic espionage.[11] Specifically, defendants Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, and Gu Chunhui were indicted by a grand jury in the Western District of Pennsylvania for violating and conspiring to violate the Computer Fraud and Abuse Act (CFAA),[12] aggravated identity theft,[13] economic espionage,[14] and trade secret theft. [15] The indictment states:

> From at least in or about 2006 up to and including at least in or about April 2014, members of the People's Liberation Army ("PLA"), the military of the People's Republic of China ("China"), conspired together with each other to hack into the computers of commercial entities located in the Western District of Pennsylvania and elsewhere in the United States, to maintain unauthorized access to those computers, and to steal information from those entities that would be useful to their competitors in China, including state-owned enterprises ("SOEs").[16]

The six companies named as victims of the computer hacking were: Westinghouse, an electronic and nuclear power company; SolarWorld, a German solar products manufacturer; United States Steel Corporation, the largest steel company in the United States; Alleghany Technologies Incorporated, a large specialty metals company; United Steel Workers International Union, the largest industrial labor union in North America; and Alcoa, the largest aluminum company in the United States.[17] Taken together, the six victims represent major segments of American nuclear power, metals production, and solar power.

The indictment describes how the PLA systematically stole trade secrets at moments that were particularly opportune for Chinese companies.[18] For example, the indictment describes how during 2011

---

11. Press Release, The 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), https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor_[https://perma.cc/TY7G-C4ME] (archived Aug. 26, 2017).

12. Indictment at 35–38, U.S. v. Wang Dong et. al., No. 14-118 (W.D. Pa. May 1, 2014); *see* Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030 (2016).

13. Indictment at 43, *Wang Dong*, No. 14-118; *see* 18 U.S.C. § 1028A (2016).

14. Indictment at 45, *Wang Dong*, No. 14-118; *see* 18 U.S.C. § 1831 (2016).

15. Indictment at 47, *Wang Dong*, No. 14-118; *see* 18 U.S.C. § 1832 (2016).

16. Indictment at 1, *Wang Dong*, No. 14-118.

17. *Id.* at 4–7.

18. *Id.* at 2.

and 2012, around the time when Oregon-based solar products manufacturer SolarWorld was losing market share to Chinese competitors and was active in trade litigation, Chinese solar manufacturers were continually dumping large volumes of solar products into US markets at below-fair-value market prices.[19] Then in May 2012, Defendant Wen "hacked into SolarWorld's computers and stole e-mails and files belonging to three senior executives."[20] Following that hack, Wen and at least one other member of the conspiracy conducted at least twelve more intrusions into and exfiltrations from SolarWorld's computers, enabling them to steal thousands of e-mail messages and other files containing detailed financial information, production capabilities, business strategies, litigation strategies, and confidential cost-structure information from SolarWorld employees.[21]

The indictment similarly alleges that right around when nuclear power developer Westinghouse was in negotiations with a Chinese company over the construction and operation of four power plants in China, PLA conspirators stole proprietary and confidential technical and design specifications for pipes, pipe supports, and pipe routing for nuclear power plants.[22] Given that Westinghouse's designs are the basis for approximately half of the world's currently operating nuclear power plants and given that many of these plants have unique safety features that have taken Westinghouse over fifteen years to develop,[23] the theft provided Chinese competitors with critical information to build similar plants without having to undertake significant research and development costs.

While the indictment further details the timing and methodology behind several cyberattacks committed on the other four American corporate victims, numerous research organizations, such as the prominent cybersecurity firm, Mandiant, have published reports delineating how the PLA's systematic espionage of these victims represents only a fraction of the numerous US companies that state-sponsored actors have targeted in recent years.[24]

Members of the intelligence community continually warn that China presents "one of the most significant economic and national

---

19. *Id.* at 17.
20. *Id.*
21. *Id.* at 17–18.
22. *Id.* at 13–15.
23. *Id.*
24. *See* MANDIANT APT 1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS (2013). "The indictment announced today is an important step. But there are many more victims, and there is much more to be done. With our unique criminal and national security authorities, we will continue to use all legal tools at our disposal to counter cyber espionage from all sources." U.S. Dep't of Justice, *supra* note 11.

security challenges facing the U.S."[25] Thus, shortly after the PLA indictment was filed, then FBI Director James Comey commented that "[f]or too long, the Chinese Government has blatantly sought to use cyber espionage to obtain economic advantage for its state-owned industries."[26] He added:

> Success in the global market place should be based solely on a company's ability to innovate and compete, not on a sponsor government's ability to spy and steal business secrets. This administration will not tolerate actions by any nation that seeks to illegally sabotage American companies and undermine the integrity of fair competition in the operation of the free market.[27]

Although the indictment has limited reach, insofar as the defendants will unlikely ever be extradited to the United States, its issuance represents a watershed moment in US history. According to former U.S. Attorney General Eric Holder, the case "represents the first ever charges against a state actor for this type of hacking," and "[t]he range of trade secrets and other sensitive business information stolen in this case . . . demand an aggressive response."[28] John Carlin, the former Assistant Attorney General for National Security, agrees, emphasizing: "State actors engaged in cyber espionage for economic advantage are not immune from the law just because they hack under the shadow of their country's flag."[29]

Despite the fact that none of the defendants has yet stood trial in the United States, the mere existence of this attack and subsequent indictment illustrates how sovereigns can utilize cyber warfare techniques to gain financial or legal advantage for the benefit of domestic constituents. Likewise, it raises the prospect (at least with respect to the seizure of nuclear information) that sovereigns could seize sensitive designs and information to benefit their military.[30] In

---

25. *Hearing on Commercial Cyber Espionage and Barriers to Digital Trade in China Before the U.S. – China Economic and Security Review Commission*, 114th Cong. 1 (2015) (statement of Paul M. Tiao, Partner, Hunton & Williams LLP).

26. U.S. Dep't of Justice, *supra* note 11.

27. *Id.*

28. *Id.*

29. *Id.*

30. In fact, the PLA was alleged to have done exactly this. According to an indictment issued against a Chinese National named Su Bin who was resident in Canada, members of the PLA sent spear phishing emails to various military contractors located in the United States including Boeing and Lockheed Martin. The military then copied relevant directories and transmitted them to Mr. Bin who (in turn) advised the PLA about which directories to copy. The PLA transmitted all copied information to Mr. Bin who translated them into Chinese and prepared reports on their contents, which included technical and highly sensitive information about the F-22 fighter jet, the C-17, and the F-35 fighter jet. Mr. Bin was extradited from Canada to the United States and pled guilty to violating the CFAA.

this case, however, all that transpired was the seizure of industrial information.

B. *Russia: The Federal Security Service's Hack of Yahoo*

On March 15, 2017, the U.S. Department of Justice formally charged two Russian intelligence agents and two hackers with orchestrating the theft of 500 million Yahoo accounts starting in January 2014.[31] The indictment, issued by a grand jury in the Northern District of California, alleges that at least two officers of the Russian Federal Security Service (FSB) engaged in computer hacking, economic espionage, and other criminal offenses in connection with a conspiracy to access Yahoo's network and the contents of webmail accounts.[32] Significantly, this represents the first instance where the United States criminally charged Russian spies for cybercriminal conduct.[33]

The indictment provides that "[f]rom at least in or about 2014 up to and including at least in or about December 2016, officers of the [FSB] . . . conspired together and with each other to protect, direct, facilitate, and pay criminal hackers to collect information through computer intrusions in the United States and elsewhere."[34] It further explains that the conspirators gained "unauthorized access to the computers of companies providing webmail and internet-related services located in the Northern District of California and elsewhere, to maintain unauthorized access to those computers, and to steal information from those computers, including information regarding, and communications of, the providers' users."[35]

The indictment states that some of the information the conspirators sought was of "predictable interest" to the FSB, such as Yahoo email accounts of Russian journalists, Russian and US government officials, employees of a prominent Russian cybersecurity company, and numerous employees of US, Russian, and other foreign

---

31. Dustin Volz, *U.S. authorities charge Russian spies, hackers in huge Yahoo hack*, REUTERS (Mar. 16, 2017), http://www.reuters.com/article/us-yahoo-hack-indictments-fsb-idUSKBN16N0CO [https://perma.cc/R596-VDKA] (archived Aug. 27, 2017).

32. U.S. Dep't of Justice, *supra* note 11 (reporting the identity of the defendants: "Dmitry Aleksandrovich Dokuchaev, 33, a Russian national and resident; Igor Anatolyevich Sushchin, 43, a Russian national and resident; Alexsey Alexseyevich Belan, aka "Magg," 29, a Russian national and resident; and Karim Baratov, aka "Kay," "Karim Taloverov" and "Karim Akehmet Tokbergenov," 22, a Canadian national and a resident of Canada).

33. Volz, *supra* note 31.

34. The FSB is "an intelligence and law enforcement agency of the Russian Federation ("Russia") headquartered in Lubyanka Square, Moscow, Russia, and a successor service to the Soviet Union's Committee of State Security ("KGB") . . . ." Indictment at 2, U.S. v. Dmitry Dokuchaev et. al., No. 17-103 (N.D. Cal. Feb. 28, 2017).

35. *Id.*

webmail and Internet-related service providers whose networks the conspirators sought to further exploit.[36] In addition, the conspirators allegedly sought access to accounts of employees of commercial entities, including a prominent Russian investment banking firm, a French transportation company, a US financial services firm, a Swiss banking firm, and a US airline.[37]

Importantly, Interpol had issued a "Red Notice" and the United States had listed one of the hackers, Alexsey Alexseyevich Belan, on its "Most Wanted" list in 2012, prior to the Yahoo incident.[38] Instead of cooperating with US authorities by either extraditing Belan or prosecuting him in Russia, Russian intelligence instead decided to use him for assistance with FSB investigations and to rely upon his skills as a hacker to gather sensitive intelligence information without detection.[39] Indeed, Belan is alleged to have led the successful infiltration of Yahoo's network and also used his access to Yahoo's network to personally enrich himself through a scam marketing scheme.[40] As to the other three defendants, the indictment alleges that the two FSB agents named as defendants, Igor Anatolyevich Sushchin and Dmitry Dokuchaev, paid bounties to the other hacker defendants, such as Karim Baratov, when they successfully hacked into the email accounts of individuals who were FSB "targets of interest."[41]

The indictment charges all four defendants with conspiring to commit computer fraud and abuse under the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030(b).[42] In addition, it charges three of the defendants (Dokuchaev, Sushchin, and Belan) with conspiring to engage in economic espionage and theft of trade secrets under 18 U.S.C. § 1831(a)(5) and 18 U.S.C. § 1832(a)(5), respectively.[43] Further, all four defendants were charged with theft of trade secrets, conspiracy to commit wire fraud, and various other counts under the CFAA.[44] Finally, Defendants Dokuchaev and Baratov were also charged with aggravated identity theft.[45]

In response to issuance of the indictment, Attorney General Jeff Sessions stated:

> Cyber crime poses a significant threat to our nation's security and prosperity, and this is one of the largest data breaches in history. . . . But thanks to the

---

36. *Id.*
37. *Id.*
38. *Id.*
39. *Id.* at 2–3.
40. *Id.* at 3.
41. *Id.*
42. *Id.* at 5–16.
43. *Id.* at 17–19.
44. *Id.* at 20–24.
45. *Id.* at 29–30.

> tireless efforts of U.S. prosecutors and investigators, . . . [t]he United States will vigorously investigate and prosecute the people behind such attacks to the fullest extent of the law.[46]

As the next two subparts explain, sovereigns often perpetrate cybercrimes for even more nefarious purposes, such as to harm a target's economy or to sabotage its infrastructure.

C. *Iran: The Islamic Revolutionary Guard Corps' Hack of the US Financial Sector and Infrastructure*

On March 24, 2016, the U.S. Attorney for the Southern District of New York announced the indictment of seven Iranians for conducting a coordinated campaign of cyberattacks against the US financial sector on behalf of Iran's Islamic Revolutionary Guard Corps (IRGC) and other Iranian state entities.[47] The seven named defendants, Ahmad Fathi, Hamid Firoozi, Amin Shokohi, Sadegh Ahmadzadegan, Omid Ghaffarinia, Sina Keissar, and Nader Saedi, were alleged experienced computer hackers employed by two private computer security companies based in Iran but who performed work on behalf of the Iranian government, including specifically the IRGC.[48]

As alleged in the indictment, the defendants "conducted extensive computer network exploitation and computer network attacks against victim corporations in the United States [including] approximately 46 major financial institutions and other financial-sector corporations . . . over a total of at least approximately 176 days."[49] Specifically, the defendants were alleged to have begun perpetrating distributed denial of service (DDoS) attacks[50] against the US financial industry, commencing in December 2011, which "variously disabled and attempted to disable computer servers belonging to these corporations in an effort to prevent the corporations from conducting business with customers online during the course of the attacks, including, among other things, providing

---

46. U.S. Dep't of Justice, *supra* note 11.

47. *See* United States v. Fathi, No. 16-48 (S.D.N.Y. filed Jan. 21, 2016).

48. *Id.* at 1–2.

49. *Id.* at 3. Targeted companies included Bank of America, N.A., NASDAQ, the New York Stock Exchange, Capital One Bank, N.A., PNC Bank, AT&T, Inc., Ally Bank, American Express, Ameriprise, Bank of Montreal, BB&T, Banco Nilbao Vizyana Argentaria, J.P. Morgan, Chase Bank, Citibank, N.A. Citizens Bank, Fifth Third Bank, FirstBank, HSBC, Key Bank, Regions Bank, State Street Bank, SunTrust Bank, Union Bank, N.A., US Bank, Wells Fargo, and Zions First National Bank. *Id.* at 5, 10.

50. A DDoS occurs when a malicious actor takes control of many computers and servers (often numbering hundreds of thousands, with each individual computer referred to as a "bot" and the collective referred to as a "botnet") and directs those computers and servers to flood a victim server with electronic communications in order to disable the server and prevent it from receiving and maintaining connections with legitimate internet traffic. *Id.* at 2.

online banking services and other information to customers."[51] These attacks resulted on certain days in hundreds of thousands of customers failing to access their online bank accounts and caused tens of millions of dollars in remediation costs for the affected companies.[52]

To perpetrate this attack, the defendants were alleged to have created malicious computer scripts on thousands of computers and computer servers, some of which were located in the United States, which allowed them to obtain remote access and control of the compromised computers.[53] Further, the defendants were alleged to have leased computer servers in the United States, allowing them to coordinate and direct their DDoS attacks.[54] To attribute the attack to the Iranian government, the indictment noted that at least one defendant received credit for his computer intrusion work towards completion of his mandatory military service in Iran.[55] All seven defendants were charged with computer hacking in violation of the CFAA,[56] while four defendants[57] were also charged with conspiracy to violate the CFAA.[58]

One defendant, Hamid Firoozi, was additionally charged with a single count of unauthorized access to a protected computer in violation of the CFAA.[59] According to the indictment, Mr. Firoozi, obtained repeated and unauthorized access from August 28, 2013 to September 18, 2013 to a computer that controlled a dam located in Rye, New York.[60] Upon hacking into the dam's computer, Mr. Firoozi was able to obtain information about water levels and temperature

---

51. *Id.* at 3–4.

52. *See id.*

53. *Id.* at 7–8.

54. *Id.*

55. *Id.* at 6.

56. *Id.* at 8–9. All the Defendants were charged with violating 18 U.S.C. §§ 1030(a)(5)(A), (c)(4)(B)(i), (c)(4)(A)(i)(I), (c)(4)(A)(i)(VI).

57. Defendants Sadegh Ahmadzadegan, Omid Ghaffarinia, Sina Keissar, and Nader Saedi (referred to in the indictment as the "Mersad Defendants" since the computer security company that employed them was named Mersad Co.) were charged with a single count of conspiracy. *Id.* at 10–12.

58. *Id.* at 15–16. The Mersad Defendants were also charged with conspiracy to violate 18 U.S.C. §§ 1030(a)(5)(A), (c)(4)(B)(i), (c)(4)(A)(i)(I), (c)(4)(A)(i)(VI) and 2. *Id.*

59. *Id.* at 15. Mr. Firoozi was charged specifically with violating 18 U.S.C. §§ 1030(a)(5)(B), (c)(4)(A)(i)(i), (c)(4)(A)(i)(IV) and 2. *Id.*

60. *Id.*; 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 [https://perma.cc/9NTP-QSUZ] (archived Aug. 29, 2017); *see also* David E. Sanger, *U.S. Indicts 7 Tied to Iranian Unit in Cyberattacks*, N.Y. TIMES (Mar. 25, 2016), https://www.nytimes.com/2016/03/25/world/middleeast/us-indicts-iranians-in-cyberattacks-on-banks-and-a-dam.html?_r=0 [https://perma.cc/4GXU-SVNR] (archived Aug. 29, 2017).

and the status of the dam's sluice gate, which controls water levels and flow rates.[61] Indeed, Mr. Firoozi's access would have allowed him to "remotely operate and manipulate the sluice gate on the Bowman Dam," but fortunately the gate was manually disconnected for maintenance at the time he gained access to the systems.[62]

As this example of sovereign state cybercrime illustrates, the motives for such an attack may extend to the crippling of a target's economy and its basic infrastructure. The next illustration of cybercrime goes even further and points out how such activities can be utilized to effect regime change in a target.

D. *Russia: Cyber Interference with the 2016 US Election*

On June 14, 2016, the *Washington Post* reported that: "Russian government hackers penetrated the computer network of the Democratic National Committee [(DNC)] and gained access to the entire database of opposition research on GOP Presidential candidate Donald Trump . . . [and] so thoroughly compromised the DNC's system that they also were able to read all email and chat traffic."[63] On July 26, 2016, the *New York Times* also reported that American intelligence had concluded with "'high confidence' that the Russian Government was behind the theft of emails and documents from the Democratic National Committee" and was motivated by either "routine espionage," or "an effort to manipulate" the election.[64]

In January 2017, the U.S. Director of National Intelligence released a comprehensive report entitled *Assessing Russian Activities and Intentions in Recent US Elections*.[65] The report observed that Russian cyber activities went far beyond the mere theft of email and information from the DNC.[66] It described how Russian President Vladimir Putin and the Russian government employed a unique strategy that blended covert intelligence operations with overt efforts by state-funded media, third party intermediaries, and paid social

---

61. U.S. Dep't of Justice, *supra* note 60.

62. *Id.*

63. Ellen Nakashima, *Russian government hackers penetrated DNC, stole opposition research on Trump*, WASH. POST. (June 14, 2016), https://www.washingtonpost.com/world/national-security/russian-government-hackers-penetrated-dnc-stole-opposition-research-on-trump/2016/06/14/cf006cb4-316e-11e6-8ff7-7b6c1998b7a0_story.html?utm_term=.415605a77d24 [https://perma.cc/MT5F-VMHB] (archived Aug. 29, 2017).

64. David E. Sanger & Eric Schmitt, *Spy Agency Consensus Grows That Russia Hacked D.N.C.*, N.Y. TIMES (July 26, 2016), https://www.nytimes.com/2016/07/27/us/politics/spy-agency-consensus-grows-that-russia-hacked-dnc.html [https://perma.cc/NMC8-626F] (archived Aug. 29, 2017).

65. OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, NAT'L INTELLIGENCE COUNCIL, ICA 2017-01D, ASSESSING RUSSIAN ACTIVITIES AND INTENTIONS IN RECENT US ELECTIONS (2017).

66. *Id.* at ii.

media users (trolls) to gain access to and information from specific targets of both major political parties, which was then relayed to select media sources.[67]

Most significantly, the report concluded that "Russian President Vladimir Putin *ordered* an influence campaign," with the goals of "undermin[ing] public faith in the US democratic process," "denigrat[ing] Secretary Clinton, and harm[ing] her electability and potential presidency."[68] Admiral Michael Rogers, Director of the National Security Agency (NSA) and Commander of U.S. Cyber Command, stated that these activities constituted a "conscious effort by a nation-state to attempt to achieve a specific effect," namely to elect Donald Trump as President of the United States.[69]

The genesis of this attack began in the summer of 2015 when a Russian hacking group named Cozy Bear sent spear phishing emails[70] to multiple government agencies, non-profits, and various government contractors.[71] Upon the exfiltration of documents from the DNC, the Russian government expanded the scope of their information-gathering activities to also include the Democratic Congressional Campaign Committee. By September 2015, the FBI reported to the DNC that at least one DNC computer had been hacked by an entity referred to as "the Dukes,"[72] which the FBI explained was a "cyberespionage team linked to the Russian government."[73]

The DNC largely ignored the FBI's warning, unsure of its legitimacy.[74] In November 2015, the FBI telephoned the DNC again to report that at least one DNC computer was now "calling home" or sending information to Moscow.[75] Distracted with allegations that

---

67. *Id.*

68. *Id.* (emphasis added).

69. Eric Lipton, David E. Sanger & Scott Shane, *The Perfect Weapon: How Russian Cyberpower Invaded the United States*, N.Y. TIMES (Dec. 14, 2016), https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html [https://perma.cc/A86E-KPAH] (archived Aug. 29, 2017). According to the article, prior to the release of the report, Commander of the United States Cyber Command, Admiral Michael S. Rogers, stated "This was not something that was done casually, this was not something that was done by chance, this was not a target that was selected purely arbitrarily." *Id.*

70. A spear phishing email is an email that appears to be from a known individual or business but is in fact from a criminal hacker seeking access to credit card information, bank account numbers, passwords, and financial or other information on a computer. *See Spear Phishing: Scam, Not Sport*, NORTON, https://us.norton.com/spear-phishing-scam-not-sport/article [https://perma.cc/2Q9H-JMRA] (archived Aug. 29, 2017).

71. Lipton et al., *supra* note 69.

72. *Id.* The "Dukes" was also known as Cozy Bear and A.P.T.29, which stands for advanced persistent threat. *Id.*

73. *Id.*

74. *Id.*

75. *Id.*

Senator Bernie Sanders had improperly gained access to confidential campaign data, the DNC failed to respond to this warning.[76] In March 2016, the FBI finally met with representatives of the DNC to convince them that the threat from Russia was real.[77] By then, however, a second set of Russian operatives had begun to attack DNC computers.[78] Operating under the pseudonym Fancy Bear or APT 28, this second group of hackers allegedly took direct orders from Russia's military intelligence agency, the GRU.[79]

Fancy Bear first successfully breached the emails of Billy Rinehart, a regional field director then working for Secretary Clinton. Fancy Bear sent Rinehart a spear phishing email, purportedly from Google, falsely stating that someone attempted to use Mr. Rinehart's password to sign into his email and urging Mr. Rinehart to change his password immediately through an embedded link.[80] When he followed these instructions, the Russian government received access to his emails.[81] Likewise, Secretary Clinton's campaign manager, John Podesta, received a similar email notification. Although his aides attempted to verify its legitimacy, the DNC technician drafted a hasty response, intending to notify Mr. Podesta and his aides that the email was "illegitimate", but instead misstated that the email was "legitimate."[82] Consequently, when Mr. Podesta's aides clicked on the link to change his password, the Russian government received access to approximately sixty thousand of his emails.[83]

The Russian government's initial strategy purportedly was to gather information. It later evolved into a broader effort to assist Donald Trump win the election by weaponizing its information.[84] To do this, a Russian government operative, utilizing the *nom de guerre* Gucifer 2.0, bragged on Twitter that he had successfully hacked the DNC computers and provided all his materials to WikiLeaks.[85] Around the same time, the Russian government, through third parties, created at least one website, www.DCleaks.com, to disseminate data that it had collected.[86]

In July, Gucifer 2.0 began engaging directly with media outlets and transmitting documents designed to contradict Democratic messaging.[87] Twelve days before the Republican National Convention, Gucifer 2.0 released the Democratic Party's campaign

---

76. *Id.*
77. *Id.*
78. *Id.*
79. *Id.*
80. *Id.*
81. *Id.*
82. *Id.*
83. *Id.*
84. *Id.*
85. *Id.*
86. *Id.*
87. *Id.*

battle plan.[88] Three weeks before the Democratic National Convention, WikiLeaks published 44,053 DNC emails,[89] causing allegations that the DNC was favoring Hillary Clinton over Senator Bernie Sanders.[90] Then, about one month before the election, WikiLeaks published thousands of emails from John Podesta's account.[91] WikiLeaks continued publishing material from John Podesta's account each day in the lead up to the election, which media outlets continuously covered.[92]

Whether these actions directly caused Secretary Clinton to lose the campaign can never be known. Yet the Russian government's clear breach of email servers and theft of information violated a host of US domestic legal statutes for which no indictments have been issued. Instead, in December 2016, then President Obama retaliated against Russia by issuing Executive Order 13757 entitled *Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities*,[93] which sanctioned four Russian individuals[94] and five Russian entities for the

---

88. *Id.*

89. *Search the DNC Email*, WIKILEAKS, https://wikileaks.org/dnc-emails/ (last visited Aug. 25, 2017) [https://perma.cc/V57W-2TQB] (archived Aug. 25, 2017).

90. Lipton et al., *supra* note 69 (claiming Donald J. Trump incessantly highlighted the publication of these documents. At a minimum, Donald Trump's campaign was aware that such leaks were imminent as a Republican operative named Roger Stone tweeted on October 2, 2016 (five days before the Podesta emails were first leaked) that "Wednesday @HillaryClinton is done. #Wikileaks.").

91. Aaron Sharockman, *It's True: Wikileaks dumped Podesta emails hour after Trump Video Surfaced*, POLITIFACT (Dec. 18, 2016), http://www.politifact.com/truth-o-meter/statements/2016/dec/18/john-podesta/its-true-wikileaks-dumped-podesta-emails-hour-afte/ [https://perma.cc/7QPF-3WDS] (archived Aug. 25, 2017); *The Podesta Emails*, WIKILEAKS, (last visited Aug. 25, 2017) https://wikileaks.org/podesta-emails/ [https://perma.cc/6HU2-2X5A] (archived Aug. 25, 2017).

92. *See, e.g.*, Amy Chozick & Nicholas Confessore, *Hillary Clinton's Campaign Strained to Hone Her Message, Hacked Emails Show*, N.Y. TIMES (Oct. 10, 2016), https://www.nytimes.com/2016/10/11/us/politics/hillary-clinton-emails.html?action=click&contentCollection=Politics&module=RelatedCoverage&region=EndOfArticle&pgtype=article [https://perma.cc/LQW7-LYLV] (archived Aug. 25, 2017); Peter Nicholas, Colleen Nelson & James Grimaldi, *Hacked Emails Show Hillary Clinton Team Trying to Navigate Bill Clinton*, WALL ST. J. (Oct. 14, 2016), https://www.wsj.com/articles/hacked-emails-show-hillary-clinton-team-trying-to-navigate-bill-clinton-1476485243 [https://perma.cc/T7BX-CWLA] (archived Aug. 25, 2017); Abby Phillip & John Wagner, *Hacked WikiLeaks emails show concerns about Clinton candidacy, email server*, WASH. POST (Oct. 12, 2016), https://www.washingtonpost.com/politics/hacked-wikileaks-emails-show-concerns-about-clinton-candidacy-email-server/2016/10/12/cdacbbd0-908f-11e6-a6a3-d50061aa9fae_story.html?utm_term=.5613486178c6 [https://perma.cc/WL9H-XMYC] (archived Aug. 25, 2017).

93. Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities, Exec. Order No. 13757, 82 Fed. Reg. 1 (Jan. 3, 2017), https://www.gpo.gov/fdsys/pkg/FR-2017-01-03/pdf/2016-31922.pdf [https://perma.cc/HH9K-KHM2] (archived Aug. 25, 2017).

94. These were Lieutenant General Igor Valentinovich Korobov (chief of the GRU), Sergey Aleksandrovich Gizunov (deputy chief of the GRU), Igor Olegovich

interference in the US election.[95] In addition, then President Obama ordered thirty-five Russian diplomats to leave the country and Russia to close two diplomatic compounds.[96]

III. DOMESTIC AND INTERNATIONAL LEGAL FRAMEWORK APPLICABLE TO STATE-SPONSORED CYBERCRIME

This Article next provides an explanation of the various domestic statutes and foreign principles of law that could apply to the conduct outlined in Part I.

A. *Domestic Framework: The Computer Fraud and Abuse Act*

Congress enacted the precursor to the CFAA in 1984, when computers were new in the workplace, recognizing that computer hacking posed novel threats to national security.[97] At the time, the media's depiction of computer hacking led to Congress conceiving a computer hacker as "'a bright, intellectually curious, and rebellious youth,' who could 'become the white-collar crime superstar of tomorrow.'"[98] The original act, known as the Counterfeit Access

---

Kostyukov (a first deputy chief of the GRU), and Vladimir Stepanovich Alexseyev (another first deputy chief of the GRU). *FACT SHEET: Actions in Response to Russian Malicious Cyber Activity and Harassment,* THE WHITE HOUSE OFFICE OF THE PRESS SECRETARY (Dec. 29, 2016), https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/fact-sheet-actions-response-russian-malicious-cyber-activity-and [https://perma.cc/PA7N-5ULF] (archived Aug. 25, 2017).

95. These were the GRU, Russia's Federal Security Service (Russia's main security agency, commonly referred to as the FSB, and the successor to the Soviet Union's KGB), STLC, Ltd. Special Technology Center of St. Petersburg (an entity which assisted the GRU in conducting signals intelligence operations), Zoresecurity, aka Esage Lab (an entity which provided the GRU with technical research), and the Autonomous Noncommercial Organization "Professional Association of Designers of Data Processing Systems" (an organization which provided specialized training to the GRU). *Id.*

96. Evan Perez & Daniella Diaz, *White House announces retaliation against Russia: Sanctions, ejecting diplomats,* CNN (Jan. 2, 2017), http://www.cnn.com/2016/12/29/politics/russia-sanctions-announced-by-white-house/ [https://perma.cc/E9T3-B4GC] (archived Aug. 25, 2017).

97. Myra F. Din, *Breaching and Entering: When Data Scraping should be a Federal Computer Hacking Crime,* 81 BROOK. L. REV. 405, 415 (2016); Glenn R. Schieck, *Undercutting Employee Mobility: The Computer Fraud and Abuse Act in the Trade Secret Context,* 79 BROOK. L. REV. 831, 831–32 (2014) (citing Greggory S. Blundell, *Personal Computers in the Eighties,* BYTE (Jan. 1983), at 168).

98. *See* Laura Bernescu, *When Is A Hack Not A Hack: Addressing the CFAA's Applicability to the Internet Service Context,* 2013 U. CHI. LEGAL F. 633, 637 (2013); Joseph M. Olivenbaum, *<Ctrl> <Alt> <Delete>: Rethinking Federal Computer Crime Legislation,* 27 SETON HALL L. REV. 574, 582 (1997); Schieck, *supra* note 97, at 831 (all describing the history of personal computers and hacking in popular culture). (Ironically, the movie War Games, rumored to have inspired Congress's legislation, depicts a complacent teenager who spends much of his time procrastinating on video games and on his computer, until one day, when he accidentally hacks into the United States' military system and nearly launches a nuclear attack against Russia).

Device and Computer Fraud and Abuse Act (CADCFAA),[99] imposed criminal sanctions on hackers and other criminals who accessed computers "without authorization."[100]

In proscribing computer fraud and use of counterfeit access devices in the same act, Congress likened computer hacking to the crimes of credit card fraud and identity theft.[101] In 1986, Congress passed the CFAA,[102] proscribing more anti-hacking conduct.[103] Due to the basic understanding of computers and the internet when the CFAA was enacted, the CFAA was amended numerous times between 1990 and 2001. Its most notable expansion was in 1994, when Congress established a private right of action for individuals harmed by certain violations of the CFAA.[104]

The majority of hacking crimes brought under the CFAA arise under sections 1030(a)(2) and 1030(a)(4). Section 1030(a)(2), the broadest provision of the statute, makes it unlawful for a person to access intentionally "a computer without authorization" or to exceed "authorized access" to obtain information belonging to a financial institution or agency of the United States, or from any protected computer.[105] Section 1030(a)(4) has a narrower focus and makes it illegal for a person to "knowingly . . . access[] a protected computer without authorization, or [to] exceed[] authorized access, and by means of such conduct further[] the intended fraud and obtain[] anything of value."[106]

Data-breaching crimes are also covered under section 1030(a)(5), which penalizes one who knowingly "causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization to a protected computer[,]" intentionally "accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage[,]" or intentionally "accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss."[107]

Sections 1030(a)(2), 1030(a)(4), and 1030(a)(5) all include either the phrase "without authorization" or "exceeds authorized access."

---

99. Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, 18 U.S.C. § 1030 (2008).

100. H.R. REP. NO. 98-894 at 14–15 (1984).

101. *See id.* at 4 ("[T]here are indications of a growing problem in counterfeit credit cards and unauthorized use of account numbers or access codes to banking system accounts. . . .").

102. Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, *supra* note 99.

103. *See generally* S. REP. NO. 99-432 (1986).

104. CFAA, *supra* note 12.

105. *Id.* § 1030(a)(2)(A)–(C).

106. *Id.* § 1030(a)(4).

107. *Id.* § 1030(a)(5)(A)–(C).

The phrase "exceeds authorized access" is defined in the statute as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled to so obtain or alter." However, the word "authorization" is nowhere defined. Consequently, circuit courts have applied inconsistent definitions of the term.[108]

1. Narrow View of Authorization

The Ninth Circuit promulgated the narrow view of authorization in the seminal case *United States v. Nosal*.[109] In *Nosal*, employees of an executive search firm obtained and passed along confidential company information from their employer's database to a former employee who was trying to set up a competing business. The court held that, because the current employees had logged into the firm's database with valid credentials, they did not violate the CFAA, even though their ultimate *use* of the information did not align with the purpose for which they had access. The court thus held that the phrase "exceeds authorized access" requires hacking to be akin to intentional trespass and does not refer to mere *misuse* of information.[110]

The Second Circuit recently joined the Fourth and Ninth Circuits in adopting a narrow definition of authorization in *United States v. Valle*.[111] That case involved a defendant who was an officer of the New York Police Department (NYPD).[112] As an NYPD employee, he had access to restricted computer databases, which allowed him to attain the home addresses and dates of birth of certain individuals.[113] Despite the NYPD's clear policy that restricted use of this database to conduct in the course of official job duties, Valle used this database to

---

108. *See, e.g.*, United States v. Nosal, 676 F.3d 854, 864 (9th Cir. 2012) (en banc) (holding that the phrase "exceeds authorized access" is limited to access restrictions, not use restrictions); *See* Din, *supra* note 97, at 418–26; Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1596 (2003). *But see* Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1125, 1129 (W.D. Wash. 2000) (holding that Shurgard lost authorization and breached the CFAA when he became an agent of a direct competitor and used his employer's proprietary information in a way that damaged his employer).

109. *See Nosal*, 676 F.3d at 863.

110. *Id.* at 863–64 ("Therefore, we hold that 'exceeds authorized access' in the CFAA is limited to violations of restrictions on *access* to information, and not restrictions on its *use*.").

111. United States v. Valle, 807 F.3d 508 (2d Cir. 2015); *Nosal*, 676 F.3d at 864 (holding that the phrase "exceeds authorized access" is limited to *access* restrictions, not *use* restrictions); WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199, 206 (4th Cir. 2012), *cert. dismissed*, 133 S. Ct. 831 (2013); LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1134–35 (9th Cir. 2009).

112. *Valle*, 807 F.3d at 512.

113. *Id.* at 512–13.

attain information on women about whom he fantasized torturing, raping, and murdering. He then posted graphic descriptions about these fantasies in internet chat rooms.[114]

In deciding whether Valle "exceeded authorized access" under the CFAA, the court focused on the rule of lenity, a canon of statutory interpretation, which states that, when construing a criminal statute with ambiguous language, after "seizing everything from which aid can be derived," any ambiguity must be resolved in favor of a defendant so as to not "penalize those whose conduct does not create the risks of harm at which the statute aims."[115] Because the court concluded that the there was "doubt" as to whether the CFAA made Valle's conduct unlawful, it had no choice but to apply the rule of lenity, narrowly construe the statute in favor of Valle, and reverse his CFAA conviction.[116]

2. Broad View of Authorization

In contrast to the Second, Fourth, and Ninth Circuits, the First, Fifth, and Eleventh Circuits have adopted broad definitions of authorization.[117] This is largely because, ever since the CFAA's civil liability provision was added in 1994, employers have increasingly used section 1030(g) to bring disloyal employees into federal court. In response, the First, Fifth, and Eleventh Circuits have adapted agency theories, duty of loyalty theories, contract theories, and use-based theories to find CFAA liability.

The duty of loyalty theory provides that authorization implicitly ends as soon as an employee becomes disloyal to his/her employer, even if he or she still has technical authorization. Thus, in *International Airport Centers v. Citrin*, the Seventh Circuit held that an employee exceeded authorized access and therefore violated the CFAA when, after deciding to go into business for himself, he erased certain programs belonging to his former employer.[118]

---

114. *Id.* at 512.

115. Muscarello v. United States, 524 U.S. 125, 138–39 (1998).

116. *Valle*, 807 F.3d at 527.

117. *See, e.g.*, United States v. John, 597 F.3d 263, 271 (5th Cir. 2010); United States v. Rodriguez, 628 F.3d 1258, 1261–63 (11th Cir. 2010) United States v. Czubinski, 106 F.3d 1069, 1078–79 (1st Cir. 1997).

118. Once the employee breached his duty of loyalty to the company, he terminated the agency relationship, and "with it his authority to access the laptop, because the only basis of his authority had been that relationship." Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 420–21 (7th Cir. 2006); *see also* Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1129 (W.D. Wash. 2000). In *Shurgard*, the Western District of Washington held that Shurgard lost authorization and breached the CFAA when he became an agent of a direct competitor and used his employer's proprietary information in a way that damaged his employer.

The contract-based interpretation of authorization provides that if an individual acquires or utilizes information in breach of a written policy, such as a confidentiality agreement, workplace rules of conduct, or a terms-of-service agreement, then use of that information is unauthorized under the CFAA. Therefore, in *EF Cultural Travel BV v. Explorica, Inc.*, the First Circuit held that a company likely violated the CFAA when it used a computer robot to glean information from its competitor because the breach of a binding confidentiality agreement constituted a breach of authorization.[119]

The Fifth and Eleventh Circuits have both employed an "intended use" analysis. Under this theory, courts look at the underlying purpose of certain company policies to determine whether an employee breached or exceeded authorized access. The analysis is broader than that under the contract theory, as it considers how employees used information they obtained even if they did not contravene a written policy or contract. Thus, in *United States v. John*, the Fifth Circuit held that an employee violated the CFAA when she used data from Citigroup's internal computer system to obtain customer account information, which she then shared with a third party in order to engage in fraudulent activity.[120] The court deduced that the company did not likely intend to permit such a use when it granted her access.[121] Similarly, in *United States v. Rodriguez*, the Eleventh Circuit held that an employee of the U.S. Social Security Administration violated the CFAA when, in violation of the agency's policy against the taking of information for non-business purposes, he obtained confidential information from the agency's computers such as the social security numbers, birthdates, income, and home addresses of his former friends and co-workers for personal use.[122]

B. *International Framework: The Tallinn Manual 2.0*

The Tallinn Manual is a comprehensive manual authored by a group of widely respected international law experts. It seeks to develop a framework of international law applicable to cyber warfare.[123] The second version of the manual (Tallinn Manual 2.0) was released in February 2017.[124] Supported by the NATO Cooperative Cyber Defense Centre of Excellence, the manual is regarded as containing the most comprehensive analysis of how

---

119. EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 582–84 (1st Cir. 2001).
120. *John*, 597 F.3d at 270–74.
121. *Id.* at 272.
122. *Rodriguez*, 628 F.3d at 1260–63.
123. TALLINN MANUAL, *supra* note 3.
124. *Id.*

existing international law applies to cyber operations.[125] Although it focuses on cyber operations that occur during armed conflict, the framework of law applicable to cyberattacks that occur during peacetime is also discussed.[126] The new edition analyzes the applicable international legal principles to cyberattacks committed against states, individuals, and companies.[127]

Section 1 outlines issues pertaining to state sovereignty, jurisdiction, and control. This section posits that customary international law applies to cyberspace.[128] It also explains that, when a cyberattack does not rise to the level of "use of force" as the term is understood in the *jus ad bellum* context,[129] the international legal framework for cyber criminality is still unsettled.[130]

Rule 1 provides that states enjoy sovereignty over the cyber infrastructure and activities within their sovereign territory and on any territory that gives them *control* over cyber infrastructure and cyber activities within their territory.[131] Because sovereignty incorporates the limits set by treaties and customary international law, cyber operations are understood as subject to state legal and regulatory control. As such, a cyber operation directed at a structure in another state violates the other state's sovereignty.[132] Similarly, cyber operations intended to coerce another government can constitute a prohibited "intervention" under international law or a prohibited "use of force."[133] Certain attacks can even qualify as "armed attacks," thereby triggering the right of individual or

125. *Tallinn Manual: Research*, NATO COOPERATIVE CYBER DEFENSE, https://ccdcoe.org/research.html [http://perma.cc/BCX3-244W] (archived Aug. 25, 2017).

126. *Id.*

127. *International Law and Cyber Operations – Launch of the Tallinn Manual 2.0*, ATLANTIC COUNCIL (2017), http://www.atlanticcouncil.org/events/upcoming-events/detail/international-law-and-cyber-operations-launch-of-the-tallinn-manual-20 [http://perma.cc/N7K6-TNKQ] (archived Aug. 25, 2017).

128. TALLINN MANUAL, *supra* note 3, at 15.

129. *Jus ad bellum* refers to the context in which States may resort to war or the general use of armed forces.

130. TALLINN MANUAL, *supra* note 3, at 4. The fact that many cyber-attacks that occur today are state-sponsored, but do not occur during the course of armed conflict, means that understanding cyber criminality in the *jus ad bello* is critical. For the same reason, it is equally important to understand the implications of domestic frameworks for prosecuting cybercrime since these mechanisms are increasingly employed against state actors. *See id.* at 4.

131. *Id.* at 15–16. Thus, any cyber infrastructure that a state can control from sea or space falls within its sovereign territory. *Id.* at 16.

132. *Id.* at 16.

133. *Id.* at 17.

collective self-defense.[134] Consequently, cyberattacks that violate international law can entitle victim states to use countermeasures.[135]

Rule 2 provides that a state may exercise jurisdiction: a) over persons engaged in cyber activities within its own territory, b) over cyber infrastructure within its territory, and c) over persons and cyber infrastructure extraterritorially, in accordance with international law.[136] With regard to territorial jurisdiction, the Manual provides that, although users of cyber infrastructure may move, and even though some infrastructure may be located in a cloud, a state has jurisdiction over any individual who conducts cyber operations within that state.[137] In addition, Rule 3 governs the jurisdiction of flag states and Rule 4 governs sovereign immunity and inviolability.[138] These rules provide that a state waives any claims of immunity over cyber structures that are used for both governmental and private purposes.[139]

The last rule in Section 1 is Rule 5. This rule provides that if a state *knowingly* permits its territory to facilitate cyberattacks in breach of other states' sovereign rights, then the host state is deemed to have "controlled" that attack.[140] Rule 5 also establishes that any cyberattack that broadly violates another country's domestic laws violates international law.[141] The duty to prevent a cyberattack, however, is still unsettled in international law.[142]

Section 2, beginning with Rule 6, sets forth the rules governing state responsibility and is therefore the most relevant section to understand sovereign state attribution. Rule 6 provides that "a state bears international legal responsibility for a cyber operation: a) attributable to it and b) which constitutes a breach of an international obligation."[143] Within this framework, a state's failure to act may also constitute a breach of international law.

Importantly, state responsibility under Rule 6 does not require damage to be caused in the victim state.[144] As such, if a state organ

---

134. *Id.* Notably, there is no consensus yet whether a malware attack that occurs in another country's territory but causes the other country no physical damage constitutes a violation of the targeted state's sovereignty. *Id.* at 16.

135. *Id.* at 17.

136. *Id.* at 18.

137. *Id.* at 19. The Manual also warns that even though geo-location technology is constantly improving, the risk of spoofing the origin of a cyber-attack is real. *Id.*

138. *Id.* at 21–23. The present Manual does not deal with diplomatic immunity or immunity of government officials.

139. *See id.* at 24.

140. *See id.* at 26.

141. *See id.* at 27.

142. *See id.* This Section discusses the four levels of knowledge that determine whether a state had "control" when an attack is perpetrated. *See id.* at 26–29.

143. *Id.* at 29. Importantly, the Manual here explains that the prevailing international legal attribution standard is very high and requires a sovereign state to have "effective control" over the perpetrators of an attack. *See id.* at 32.

144. *See id.* at 30.

perpetrates an act, "[i]t does not matter whether that organ in question acted in compliance with, beyond, or without any instruction" from persons or entities outside those organs; a state is responsible for a cyber act so long as the state "specifically empowered" the actors.[145] Similarly, this rule provides that, for purposes of state control, the focus is not on the location where the act in question takes place, but rather, on the state's level of involvement in the act.[146]

Rule 7 provides that it is not sufficient to attribute a cyber operation to a particular state simply because an operation has been launched or otherwise originates from governmental cyber infrastructure within that state.[147] Rather, the context of the entire situation must be considered. This means that state attribution can attach if, for example, patterns of non-state actors launch hacks that serve state purposes.[148] Similarly, attribution principles must take into account situations in which private or public actors are able to spoof IP addresses and make it appear that a cyberattack originated from a false point of origin.[149] Rule 8 complements Rule 7 and provides that the mere routing of a cyber operation through the cyber infrastructure of a state is not sufficient evidence alone to attribute that operation to the state through which the operation was routed.[150]

Rule 9 governs countermeasures and provides that "[a] state injured by an internationally wrongful act may resort to proportionate countermeasures, including cyber countermeasures, against the responsible state."[151] This rule is derived from Articles 22 and 49 to 53 of the International Law Commission's Articles on State Responsibility.[152] Although the Manual contains an additional ten sections detailing rules related to the law of cyber armed conflict, the details of such rules are beyond the scope of this Article and will not be discussed. Rather, this Article will now discuss the European Convention on Cybercrime.

---

145. *See id.* at 31.

146. *See id.* at 30–33.

147. *Id.* at 34.

148. *See id.* at 35.

149. *See id.* For illustrative examples of IP spoofing used in connection with cyberattacks, see generally Kozlowski, *supra* note 8.

150. TALLINN MANUAL, *supra* note 3, at 36.

151. *Id.*

152. *See* Int'l Law Comm'n, Rep. on the Work of Its Fifty-Third Session, U.N. Doc. A/56/49 (2001).

C. *European Convention on Cybercrime*

The European Convention on Cybercrime was passed in 2001 and entered into force in 2004.[153] The first convention to address Internet policy and cybercrime in a comprehensive manner, the Convention seeks to foster cooperation with other state parties and develop common rules and policies in order to protect societies against cybercrime while facilitating the development of information technologies.[154]

The Convention lists numerous substantive criminal offenses for member and signatory states to incorporate into their domestic legislation. These include, *inter alia*, intentional access to whole or part of a computer system without right; illegal interception of computer data to, from, or within a computer system; damaging, deleting, deteriorating, altering, or suppressing computer data without right; interfering with computer data; misusing vis-à-vis procuring, importing, distributing, or possessing devices; committing computer-related fraud or forgery; and committing offenses such as distribution of child pornography and copyright infringement.[155]

Unlike the Tallinn Manual, this Convention focuses on common domestic threats that result from transnational cybercriminal conduct, regardless of who perpetrates such crimes. Based on the crimes listed, it primarily seeks to facilitate cooperation in combatting cybercrime committed by *private actors* located out-of-state. The Convention does not target state-sponsored cybercrime, and is less helpful in providing guidance to deter state-sponsored cyberattacks. Nevertheless, the guide provides a useful framework for identifying common cyber threats and the challenges connected to cyberattacks such as the lack of extradition mechanisms, the need to preserve endangered data, and the need to enact mutual assistance procedures.

IV. SHORTCOMINGS IN THE US DOMESTIC LEGAL FRAMEWORK

With the above principles set forth, this Part discusses shortcomings in the US domestic framework applicable to state-sponsored cybercrime. Specifically, the next two subparts of this Article discuss: (1) shortcomings with respect to achieving deterrence and (2) foreign policy considerations which arise when seeking to prosecute state actors for cybercrime under US law.

---

153. *See generally* Convention on Cybercrime, *supra* note 4 (adopting a common criminal policy to protect society against cybercrime).

154. *Id.*

155. *Id.* at 4–8.

A. *Achieving Deterrence*

One of the main shortcomings with the use of domestic legislation to prosecute state-sponsored cybercrime is that it is unclear whether it deters cybercrime. In a paper entitled *Deterring Financially Motivated Cybercrime*, Professors Zachary Goldman and Damon McCoy write about many challenges of cyber deterrence that are due to the unique nature of cyber space.[156] They discuss problems with "publicly attributing cyberattacks with confidence" and "the unwillingness of states to discuss publicly capabilities that they treat as highly classified."[157] They also emphasize that motivations for cyberattacks vary greatly and require tailored deterrence strategies.[158] They further argue that the majority of cyberattacks are "financially motivated cyberattacks"—that is, the attacks are effectuated so that the perpetrators can generate a profit.[159] Hence, Goldman and McCoy argue that the best way to deter such attacks is to make it harder for criminals to monetize the goods they have counterfeited or data they have stolen.[160]

Interestingly, McCoy and Goldman argue that in the case of the PLA cyberattacks, the use of financial sanctions would have been powerful regardless of whether the United States issued the indictment.[161] They contend that the United States is still uniquely positioned to project financial power in a world in which the majority of commercial transactions, including the global energy trade, are conducted in US dollars.[162] The potency of financial sanctions is due to the fact that once the United States sanctions another government, international financial institutions become wary of doing business with that entity as a result of the reputational risks involved.[163]

Recall that although the PLA is a Chinese government entity, the attacks were effectuated for the theft of industrial and nuclear trade secrets, as opposed to direct regime change, as was the case in the Russia-United States election hack. As such, the PLA hack was more akin to the types of financially motivated cybercrimes committed by rogue independent actors as opposed to the type of hack one would associate with classic espionage. For state-sponsored cyberattacks aimed against military targets or critical infrastructure, McCoy and Goldman acknowledge that financial sanctions are less

---

156. *See generally* Zachary K. Goldman & Damon McCoy, *Deterring Financially Motivated Cybercrime*, 8 J. NAT'L SECURITY L. & POL'Y 595, 595–619 (2016).
157. *Id.* at 595.
158. *Id.* at 595–596.
159. *Id.* at 596.
160. *See id.* at 597.
161. *See id.* at 603–605.
162. *See id.* at 603.
163. *See id.*

likely to be effective in most instances and that alternative deterrence tools are required.[164]

Ultimately, any effective deterrence strategy must increase the perceived costs and lower the perceived benefits of engaging in a particular criminal activity.[165] That begs the question of how the US government came to believe that issuing indictments under the CFAA for hacks that were believed to be state-sponsored would affect the cost/benefit calculations of the sovereign state actors who ordered them. On that point, it is important to note that an indictment is only one tool in the arsenal of deterrence which the United States has employed against state actors who engaged in cybercriminal activity against it. Other tools the United States has (sparingly) used in lieu of issuing an indictment include diplomatic and/or economic sanctions and cyber and/or military retaliation against a perpetrator.

For example, in response to Russia's interference in the US presidential election, then President Obama expelled thirty-five Russian diplomats from the United States, imposed financial sanctions on Russia's intelligence services, its top officers, and various companies and organizations complicit in the attack, and ordered the closure of two Russian diplomatic compounds.[166] He also signed an executive order allowing himself and any future president to retaliate further against the Russian government for its interference in the US election or for any interference perpetrated against US allies. Such retaliation was stated as being likely "covert . . . , one that would be obvious to Mr. Putin but not to the public."[167]

Unfortunately, the effectiveness of any deterrence strategy requires the imposition of such a high cost on an adversary that the adversary decides "not to act aggressively."[168] Measured against this standard, the United States' response to Russia's actions against it in the 2016 election (or for that matter any of the state-sponsored cyberattacks outlined in Part I) has not proven successful. This is because Russia and other state actors continue to engage in

---

164. *See id.* at 597.

165. *See generally id.* Goldman and McCoy highlight Patrick Morgan's formulation of deterrence: "deterrence has generally been conceived as an effort by one actor to convince another to not attack by using threats of a forceful response to alter the other's cost-benefit calculations." PATRICK MORGAN, DETERRENCE NOW 44 (2003).

166. David E. Sanger, *Obama Strikes Back at Russia for Election Hacking*, N.Y. TIMES (Dec. 30, 2016), https://www.nytimes.com/2016/12/29/us/politics/russia-election-hacking-sanctions.html?mcubz=0 [https://perma.cc/BCH8-WQV9] (archived Aug. 29, 2017).

167. *Id.*

168. *See* Will Goodman, *Cyber Deterrence: Tougher in Theory than in Practice*, STRATEGIC STUD. Q. 107 (2010).

significant cyber operations against the United States and its allies.[169]

Applying this basic fact to traditional theories of deterrence reveals an inevitable conclusion: The United States needs to increase the costs of cyber aggression against it such that the actual and/or perceived costs outweigh the benefits of any future attacks. Given the narrow range of options currently present, and given the reality of increasingly frequent and potent cybercriminal conduct, indictments without actual extradition and punishment, although helpful, are not going to alter the activities of state actors. This leaves the United States with a series of least good alternatives.

First, it can simply accept that such attacks are an inherent part of the new national security order requiring the devotion of significant resources to cyber-defensive strategies designed to ensure that such attacks are less likely to result in a successful outcome. Given the rapidly evolving cat-and-mouse nature of aggressive cyber activities, such an approach would need to accept a certain percentage of failure as it is likely impossible that any defensive strategy will prevent all future attacks from occurring.

Second, the United States can retaliate against perpetrators of cyberattacks by deploying its offensive cyber capabilities in a manner that is so overwhelming to the attacker that any future attackers recognize that engaging in such activities will result in tremendous cost to it. This approach is also fraught with difficulty because any such activity will likely result in the disclosure of US cyber assets which in turn will lead to countermeasures against those assets making them ineffective in the future.[170] Moreover, recent news reports reflect that the United States lags behind certain states, such as Israel, with regards to its cyber expertise, and even rogue criminal

---

169. Although certain United States officials assert that Chinese hacking against United States targets decreased immediately after the 2014 indictment was issued, recent news reports tend to show that on the aggregate, the frequency of global cyber-attacks has only increased in recent months. *See* Vindu Goel & Eric Lichtblau, *Russian Agents were Behind Yahoo Hack, U.S. Says*, N.Y. TIMES (March 15, 2017), https://www.nytimes.com/2017/03/15/technology/yahoo-hack-indictment.html?mcubz=0 [https://perma.cc/5RFH-WSPH] (archived Aug. 29, 2017); Lohr & Alderman, *supra* note 8; *see also supra* text accompanying note 8.

170. Such efforts would also likely be of little avail because in addition to the United States risking full disclosure of its cyber weaponry, cyber actors, including Islamic State fighters for example, are so mobile that they reconfigure their cyber communication strategies with high frequency. David E. Sanger & Eric Schmitt, *U.S. Cyberweapons, Used Against Iran and North Korea, Are a Disappointment Against ISIS*, N.Y. TIMES (June 12, 2017), https://www.nytimes.com/2017/06/12/world/middleeast/isis-cyber.html?_r=0 [https://perma.cc/KLM4-C7Y7] (archived Aug. 29, 2017).

groups, such as the Islamic State, have recently found ways to evade the efforts of US cyber experts.[171]

Third, the United States could impose diplomatic or economic sanctions against a perpetrator, which may have limited effect. In the case of the Russia-United States election hack, the United States implemented a combination of economic and diplomatic sanctions. In addition, the indictments that the United States issued in the other three instances discussed in Part I were akin to diplomatic sanctions, insofar as they resulted in the same type of naming and shaming that diplomatic sanctions effectuate. To date, there is no clear sign that these indictments or any other diplomatic sanctions issued during the election hack have slowed down cyber activities. And in fact, recent reports tend to reflect that the opposite is true.[172]

Fourth, the United States can deploy actual military force against the perpetrators of cyber aggression against it provided that any such use of force qualifies as self-defense under Article 51 of the United Nations Charter and otherwise complies with international law. Given the legal and foreign policy implications of using force against the perpetrators of cyber aggression, this should be a consideration of last resort and only turned to when the cyber aggression at issue is of such magnitude that it would qualify as an armed attack under Article 51 and other measures would be unsuccessful. On this point, it is important to remember that what type of "cyberattack" qualifies as an armed attack in the *jus ad bellum* is still subject to debate in the international legal community.[173] As it could be a while before a global consensus is reached as to what types of cyberattacks rise to the level of an armed attack and are legally sufficient to trigger a right of self-defense, the premature use of self-defense measures (cyber or otherwise) should be avoided because of its high costs.[174]

---

171. *See id.* (discussing the failures and successes of cyber weapons used against ISIS, mainly focusing on why ISIS proves to be a more difficult target of cyberattacks than Iran, which began to be targeted under the Bush administration).

172. *See supra* text accompanying note 8.

173. Although the Tallinn Manual and The Tallinn Manual 2.0 attempt to fill in definitional holes and address the types of cyber operations which are the most severe violations of international law and which are more innocuous, the manuals are replete with references to the many cyber operations over which international consensus has yet to be reached.

174. *See generally* Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue & Julia Spiegel, *The Law of Cyber-Attack*, Faculty Scholarship Series (2012), http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=4844&context=fss_papers [https://perma.cc/87NW-76DU] (archived Aug. 29, 2017) (calling for a consensus as to the definitions of cyber-attack, cyber-crime, and cyber-warfare).

B. *Foreign Policy Implications*

As just noted, indictments and diplomatic sanctions alone will unlikely alter a state's calculations when deciding whether to conduct cyber operations against the United States. Having said that, indictments do carry with them foreign policy impacts, a topic that this Article next explores. First, this Article explores the foreign policy impacts that might arise if US courts were to apply its domestic cybercriminal framework extraterritorially. Second, it discusses the competing tests required to attribute any such cybercriminal activity to a state actor and the foreign policy implications of doing so.

1. Impact of Applying Domestic Laws Extraterritorially

Chief among these foreign policy implications is the risk that prosecutors overreach in the application of US domestic laws, such that they infringe upon another state's sovereignty. For example, the United States Supreme Court is now reviewing a July 2016, decision in the widely publicized case *Microsoft Corp. v. United States* where the Second Circuit held it unlawful for a US magistrate judge to issue a warrant, pursuant to the Stored Communications Act (SCA), to attain emails that were stored on a server located in Ireland.[175]

The case arose when a prosecutor for the U.S. Department of Justice (DOJ) made a request to Magistrate Judge James Francis IV for a search warrant to be issued against Microsoft Corporation.[176] The DOJ presented probable cause to believe that a Microsoft-based email account, located on a server in Ireland, was being used in furtherance of narcotics trafficking.[177] In analyzing whether the SCA could be employed extraterritorially, the Second Circuit focused on the Supreme Court's recent holdings in *RJR Nabisco, Inc. v. European Cmty.*[178] and *Morrison v. National Australian Bank.*[179] Both of these Supreme Court cases bolstered the presumption against extraterritoriality—the notion that "[w]hen interpreting the laws of the United States, [courts] presume that legislation of Congress 'is

175. *See generally* Microsoft Corp. v. United States, 829 F.3d 197 (2d Cir. 2016); *see also* Myra F. Din, *Data Without Borders: Resolving Extraterritorial Data Disputes*, 26 J. TRANSNAT'L L. & POL'Y (forthcoming 2017). On October 16, 2017, the United States Supreme Court granted the Department of Justice's Petition for Certiorari. *See* Order List: 583 US (Oct. 16, 2017) https://www.supremecourt.gov/orders/courtorders/101617zr_6k37.pdf [https://perma.cc/VL6M-N7BD] (archived Oct. 29, 2017).

176. *In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., 15 F. Supp. 3d 466, 477 (S.D.N.Y. 2014).

177. *Id.*

178. RJR Nabisco, Inc. v. European Cmty., 136 S. Ct. 2090 (2016).

179. Morrison v. Nat'l Australian Bank Ltd., 561 U.S. 247 (2010).

meant to apply only within the territorial jurisdiction of the United States,' unless a contrary intent clearly appears."[180]

The Second Circuit therefore engaged in a two-part inquiry laid out in *Morrison* to assess whether the SCA could either be read as extraterritorial or applied in such a manner.[181] First, the court ascertained that the relevant statutory provisions did not expressly "contemplate extraterritorial application."[182] Second, the court assessed the statute's "focus" to determine whether in light of the statute's intended purpose and structure, and based on the facts presented in the case, application of the statute would be impermissibly extraterritorial.[183] Ultimately, the Second Circuit held that the SCA could neither be read nor applied in an extraterritorial manner as the district court had permitted.

A key takeaway from *Microsoft* is that, although the underlying narcotics trafficking may have been committed within the United States, the prosecutor's requested extraterritorial application of the SCA was of greater concern. This takeaway lies in contrast to the long-standing objective territorial jurisdiction principle contained in international law, which provides that a sovereign can generally exercise jurisdiction over persons who engage in criminal conduct outside of the sovereign's borders when those acts produce "substantial detrimental effects" within the sovereign's borders.[184] Nevertheless, in *Microsoft* the court effectively held that this principle did not apply where the foreign link was merely stored *communications* related to the underlying domestic crime, regardless of how intertwined they were.

For purposes of prosecuting state-sponsored cybercrime under the CFAA and similar domestic statutes as was laid out in the PLA, Iran, and Russia (Yahoo) indictments, the implications of *Microsoft* (assuming the Supreme Court upholds the Second Circuit's decision) are twofold. If an investigation were to continue beyond the issuance of indictments, a court would need to assess whether the CFAA applied extraterritorially and whether, considering the Second Circuit's interpretation of the SCA, US prosecutors could attain digital evidence stored abroad without violating the presumption against extraterritoriality. This second concern is especially important because, as the numerous amicus briefs from *Microsoft*

---

180. *Microsoft Corp.*, 829 F.3d at 210 (citing *Morrison*, 561 U.S. at 255).

181. *Id.* at 209–10.

182. *Id.* at 210–11.

183. *Id.* at 210, 216.

184. Edward Carter, *Examining Cybercrime: Tactics for Investigation and Prosecution*, 99 n.23 (2002), pb.univd.edu.ua/?controller=service&action=download&download=25257 (citing United States v. Roberts, 1 F. Supp. 2d 601, 603 (E.D. La. 1998)); *see also* Andrew Clapham, BRIERLY'S LAW OF NATIONS: AN INTRODUCTION TO THE ROLE OF INTERNATIONAL LAW IN INTERNATIONAL RELATIONS 242–47 (Oxford University Press 7th Ed. 2012).

indicated, a US prosecutor's unilateral seizure of evidence located abroad through a US court order could cause that other state to retaliate against the United States. This could include the imposition of sanctions or trade restrictions, the suspension of judicial, military, economic, or other cooperation, or the seizure by that state of information located here, any of which could have a deleterious impact on the US economy and/or foreign policy.[185]

Indeed, on October 6, 2015, just about one year after the district court affirmed the extraterritorial email warrant's issuance (and about ten months before the Second Circuit reversed that decision), the European Court of Justice issued a milestone decision in *Maximillian Schrems v. Data Protection Commissioner.*[186] That decision struck down the "safe harbor" provisions between a multitude of US digital services providers and EU member countries on the basis that the United States was not providing "adequate protection" of EU members' personal data.[187] Some viewed this decision as retaliation for the United States' decision to infringe Irish sovereignty in *Microsoft,* as the European Court of Justice decision resulted in companies such as Facebook, Google, Amazon, and thousands of other smaller businesses having to renegotiate their contracts and data protection policies in order to preserve their European consumer base.[188]

---

185. Numerous *amici* filed briefs in the Microsoft litigation to explain how an over-application of U.S. law could infringe Ireland's sovereignty and negatively harm foreign relations. *See, e.g.*, Brief for Apple as Amici Curiae Supporting Appellants at 21–22, *In re* Warrant to Search a Certain E-mail Account Controlled & Maintained by Microsoft Corp., 829 F.3d 197 (2016) (No. 14-2985); Brief for Brennan Center for Justice at NYU School of Law et al. as Amici Curiae Supporting Appellants at 14, *In re* Warrant to Search a Certain E-mail Account Controlled & Maintained by Microsoft Corp., 829 F.3d at 197; Brief for Anthony J. Colangelo, International Law Scholar as Amici Curiae Supporting Appellants at 11–12, *In re* Warrant to Search a Certain E-mail Account Controlled & Maintained by Microsoft Corp., 829 F.3d at 197 (describing how the principles of sovereignty and non-intervention are well-established under customary international law and preclude one state from exercising law enforcement jurisdiction in the territory of another state); Brief for Digital Rights Ireland Limited et al. as Amici Curiae Supporting Appellants at 16–18, *In re* Warrant to Search a Certain E-mail Account Controlled & Maintained by Microsoft Corp., 829 F.3d at 197; Brief for Ireland as Amici Curiae Supporting Appellants at 3–4, *In re Warrant to Search a Certain E-mail Account Controlled & Maintained by Microsoft Corp.*, 829 F.3d at 197 (arguing that national sovereignty is never waived by non-intervention in foreign domestic court proceedings and endorsing application of the MLAT process in order to avoid conflicts as much as possible).

186. Case C-362/14, Maximillian Schrems v. Data Protection Commissioner, EU:C:2015:627 (Judgment of the Court).

187. *Id.* ¶ 107.

188. *See, e.g.*, Natalia Drozdiak and Sam Schechner, *EU Court Says Data-Transfer Pact With U.S. Violates Privacy,* WALL ST. J., (Oct. 6, 2015), https://www.wsj.com/articles/eu-court-strikes-down-trans-atlantic-safe-harbor-data-transfer-pact-1444121361 [https://perma.cc/6XAH-JGMR] (archived Sep. 27, 2017); Mark Scott, *Data Transfer Pact Between U.S. and Europe if Ruled Invalid,* N.Y. TIMES

2. Costs Connected with Attribution

A second challenge that implicates foreign sovereignty is the issue of attribution, a subject which scholars and jurists have long debated.[189] For this reason, a critical development in international law involved the codification of rules for state responsibility in the Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA), which is now generally accepted as representing customary international law.[190] Under the ARSIWA, a state is responsible for all the acts of its organs, which include the executive branch, legislature, judiciary, and armed forces.

In contrast, the conduct of private persons or entities is generally not attributable to states other than in select instances in which a sufficient factual "link" exists between the person or entity engaging in the conduct and the state. What types of links are sufficient for private conduct to be deemed state-sponsored is crucial to attribute cybercrime to a state, where there is often an unapparent connection between cyber conduct and its effects.[191]

Article 8 of ARSIWA explains when acts that are not effectuated by state organs may be attributed to a state:

> The conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of that State in carrying out the conduct.[192]

Consequently, a state may assume responsibility for conduct by either 1) issuing specific directions or 2) exercising sufficient "control" over a group. While situations in which a state issues instructions or directions are relatively clear, instances in which states have been responsible for the conduct of non-state actors who were deemed to be

---

(Oct. 6, 2015), https://www.nytimes.com/2015/10/07/technology/european-union-us-data-collection.html?_r=0 [https://perma.cc/E5WN-4DR7] (archived Sep. 27, 2017); Mark Scott, *U.S. and Europe in 'Safe Harbor' Data Deal, but Legal Fight May Await*, N.Y. TIMES (Feb. 2, 2016), https://www.nytimes.com/2016/02/03/technology/us-europe-safe-harbor-data-deal.html [https://perma.cc/USU7-Y2G5] (archived Sep. 27, 2017).

189. *See, e.g.*, The Corfu Channel Case (U.K. v. Alb.), Judgment, 1949 I.C.J. 4, at 18 (Apr. 9); The Lotus Case (Fr. v. Turk.), Judgment, 1927 P.C.I.J. (ser. A) No. 10, at 18–26 (Sep. 7). Both of these were monumental contentious international law cases that hinged upon state attribution issues. Ultimately, they established the legal foundations for when states may be held responsible for conduct that occurs outside of their sovereign borders and the evidentiary burdens that must be met for state attribution to lie.

190. *See generally* G.A. Res. 56/83, *supra* note 10 (delineating the many circumstances in which States can be held responsible for internationally wrongful acts).

191. *See* Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L. J. 326, 365–66 (2015) (describing how the unique properties of data, such as its mobility, divisibility, unpredictability, and interconnectedness create fragmentation between the location of data and its effects); Din, *supra* note 175.

192. G.A. Res. 56/83, *supra* note 10, at art. 8.

under state control are murkier, and international courts have applied varying definitions of control.

Because misattributing cyberattacks and cyber espionage to sovereign states carries grave consequences, the international legal community recently began to apply a higher standard of "control" before attributing the actions of an independent actor to a state. In the past, however, international courts were wary of employing too high a standard of control, as such a standard could result in the failure to attribute sovereign sponsored conduct to states at all. This, in turn, would have allowed states to commit grave crimes with impunity. This risk is exacerbated in the cyber context where directions are much harder to detect due to the amorphous and fragmented nature of digital communications that can be invisible to the naked eye and disconnected from the location at which cyberattacks occur.[193] As such, this Article will next discuss the competing standards for control under international law and explain the implications of using US domestic laws for attributing cyber conduct to state actors.

a. Effective (Operational) Control

The International Court of Justice (ICJ) promulgated the effective control standard in *The Case Concerning Military and Paramilitary Activities in and against Nicaragua.*[194] In that case, the ICJ had to decide if human rights violations committed by the *Contras*, a rebel group fighting the Nicaraguan army, could be attributed to the United States. The question of attribution arose because the United States had financed and given the Contras logistical and military support.[195] The ICJ considered that, while the United States had not created the Contras, it had played a significant role in assisting their efforts. Ultimately, however, the ICJ held that the conduct of the Contras was not attributable to the United States because "a country's control over paramilitaries or other non-State

193. *See* Daskal *supra* note 191; Din, *supra* note 175; Kozlowski, *supra* note 8 ("The Georgian authorities in the wake of massive disruption of Internet websites firstly tried to filter Russian IP addresses but the Russian[s] very quickly changed their tactic[s] and used non-Russian servers."); David E. McNabb, *Russia's Undeclared Cyber Wars*, INFO. SECURITY TODAY, http://www.infosectoday.com/Articles/Undeclared-Cyber-Wars.htm#.WT7qplXytyw [https://perma.cc/M8KU-DAW7] (archived Aug. 29, 2017) (describing instances in which Russian employed IP spoofing and other cyberattacks against Lithuania, Estonia, and Georgia).

194. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. Rep. 14, ¶ 18 (June 27).

195. *Id.*

actors can only be established if the actors in questions act in 'complete dependence' on the State."[196]

b. Overall Control

The International Criminal Tribunal for the former Yugoslavia (ICTY) took a different approach in *Prosecutor v. Tadic*.[197] There, the ICTY had to determine whether it had jurisdiction over Dusko Tadic, who was charged with committing crimes against humanity, violating the Geneva Conventions, and violating the customs of war in various Serb-run concentration camps in Bosnia-Herzegovina.[198] Jurisdiction over Dusko depended upon whether his acts were attributable to a state.[199] The ICTY employed a lower attribution standard than the ICJ in *Nicaragua* holding that "where a state has a role in organizing and coordinating, in addition to providing support for a group, it has sufficient *overall* control, and the group's acts are attributable to the State."[200]

c. Prevailing Test

The ICJ had to revisit this issue in the *Application of the Genocide Convention* (Bosnian Genocide case), nearly a decade after *Tadic*.[201] Upon reviewing both the effective and overall control standards for state attribution, the ICJ reiterated that the effective control standard promulgated in *Nicaragua* was appropriate.[202] The ICJ, in reaffirming the effective control test for state attribution, required that a non-state actor be a "de facto organ" of the state. This ruling is also important from an evidentiary perspective because it required the equivalent of "smoking gun" evidence—or proof beyond *any* doubt—for state attribution to attach.[203]

In discussing state responsibility, the Tallinn Manual acknowledges the validity of the Articles on State Responsibility as

---

196. Scott J. Shackelford, *State Responsibility For Cyber Attacks: Competing Standards For A Growing Problem*, NORTH ATLANTIC TREATY ORGANIZATION [NATO], COOPERATIVE CYBER DEFENSE CENTER OF EXCELLENCE 197, 201 (2010); *see* Military and Paramilitary Activities in and Against Nicaragua, *supra* note 194.

197. Prosecutor v. Tadic, Case No. IT-94-1-ar72, Decision on Interlocutory Appeal on Jurisdiction (Int'l Crim. Trib. for the Former Yugoslavia Oct. 2, 1995).

198. Prosecutor v. Tadic, Case No. IT-94-1-A, Judgment, ¶ 2 (Int'l Crim. Trib. for the Former Yugoslavia July 15, 1999).

199. *Id.*

200. Shackelford, *supra* note 196 (emphasis added); *see* Prosecutor v. Tadic, Case No. IT-94-1-A, Judgment, ¶ 122 (Int'l Crim. Trib. for the Former Yugoslavia July 15, 1999).

201. Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro), Judgment, I.C.J. Rep. 2007, p. 43, ¶ 402 (Feb. 26).

202. *Id.*

203. *Id.*; Shackelford, *supra* note 196, at 201.

codifying customary international law and articulates the competing standards for state control as articulated in the *Nicaragua* and *Tadic* cases.[204] The Manual further distinguishes instances in which private citizens conduct cyber operations on their own initiative (such as "hacktivists" or "patriotic hackers"), from instances in which military or other organized groups engage in acts that may violate international law, such as in the case of the Contras.[205] However, while the Manual acknowledges that there is a split in the standard that governs state control over military or group actions, it implies that at least in the case of *individuals or groups not organized into military structures*, the higher standard for control applies, and a state "needs to have issued specific instructions or directed or controlled a particular operation to engage State responsibility." [206]

Each of the three indictments discussed in Part I of this Article highlights the foreign policy implications that arise when a state suffering from such malfeasance attributes that malfeasance to another state, regardless of the test used. For example, the Chinese government suspended high-level diplomatic talks regarding cyber activities after the PLA indictment was issued and also summoned the US ambassador over the hacking charges.[207] Similarly, the Iran hack was itself said to be retaliatory in nature, conducted as retribution for an American led cyberattack against Iran's main nuclear enrichment plant.[208] To avoid escalating global tensions further, prosecutors carefully refrained from alleging that the IRGC *directed* the Iran attacks, instead alleging merely that the defendants performed work *on behalf of* the Iranian government, including the IRGC. And the diplomatic fallout from the Russian election and Yahoo hacks (along with the accompanying indictment) continue to cause severe tension between the United States and Russia,[209] albeit

---

204. *See* TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE, *supra* note 3, at 29–34.

205. *Id.* at 33.

206. *See id.*

207. Ellen Nakashima & William Wan, *U.S. Announces First Charges Against Foreign Country in Connection with Cyberspying*, WASH. POST (May 19, 2014), https://www.washingtonpost.com/world/national-security/us-to-announce-first-criminal-charges-against-foreign-country-for-cyberspying/2014/05/19/586c9992-df45-11e3-810f-764fe508b82d_story.html [https://perma.cc/EN6W-VTSG] (archived Aug. 29, 2017).

208. *Id.*

209. On June 22, 2017, the US Congress reached agreement to impose additional sanctions on Russia because of its interference in the 2016 election. *See* Matt Flegenheimer & David E. Sanger, *Congress Reaches Deal on Russia Sanctions, Setting up Tough Choice for Trump*, N.Y. TIMES (July 22, 2017), https://www.nytimes.com/2017/07/22/us/politics/congress-sanctions-russia.html (subscription required) [https://perma.cc/JVV3-PH7D] (archived Aug. 29, 2017). In response, Russia ordered 755 US diplomats to cease their work. *See* Neil MacFarquhar, *Putin, Responding to Sanctions, Orders U.S. to Cut Diplomatic Staff by 755*, N.Y.

without any accompanying alterations or changes to Russia's behavior.[210]

V. SUGGESTED LEGISLATIVE OR OTHER PROPOSALS

Part III of this Article explained how the US domestic legal framework is not effective at imposing sufficient cost on a state-sponsored perpetrator of cybercrime so as to deter it from future transgressions. Additionally, Part III touched upon the foreign policy challenges that attach when seeking to indict and prosecute individuals who perpetrate such acts on behalf of a state sovereign. The following sections of this Article argue that the United States needs to modify the framework applicable to such crimes to deter states more effectively from engaging in such acts in the future. Specifically, the final sections of the article argue that Congress should (i) permit its domestic statutes to apply extraterritorially and (ii) pass a statute that exposes sovereign state perpetrators of such acts to civil liability.

A. *Extraterritorial Application of CFAA and SCA*

Self-evidently, ambiguity regarding the extraterritorial reach of the CFAA and SCA requires resolution. Specifically, Congress should incorporate language explicitly incorporating extraterritorial application of these two statutes much as Congress has done with other statutes that are used to combat transnational crimes such as the Racketeer Influenced Corrupt Organizations Act (RICO), the wire fraud statute, and other similar type statutes. As the Supreme Court noted in *RJR Nabisco, Inc. v. European Cmty.*, when analyzing whether RICO applied extraterritorially, a clear indication of Congress's intent for a statute to have extraterritorial effect is sufficient for a court to apply it as such.[211]

Confirming the CFAA's extraterritorial reach will ensure that state sovereign actors who are nearly always working abroad and who are charged with violating the CFAA will be denied the ability to challenge the statute's applicability to their actions. This issue may become immediately pressing as one of the named defendants in the

---

TIMES (July 30, 2017), https://www.nytimes.com/2017/08/02/world/europe/trump-russia-sanctions.html (subscription required) [https://perma.cc/A4YD-W5PG] (archived Aug. 29, 2017). President Trump signed the Russia sanctions bill into law on August 2, 2017. *See* Peter Baker & Sophia Kishkovsky, *Trump Signs Russian Sanctions into Law, with Caveats*, N.Y. TIMES (Aug. 2, 2017), https://www.nytimes.com/2017/07/30/world/europe/ russia-sanctions-us-diplomats-expelled.html (subscription required) [https://perma.cc/ZVK8-7MD8] (archived Aug. 29, 2017).

210. *See* Goel & Lichtblau, *supra* note 169.

211. RJR Nabisco, Inc. v. European Cmty., 136 S. Ct. 2090, 2101–03 (2016).

Russia election and Yahoo hacks, Karim Baratov, was recently arrested in Canada. Should Canada extradite him to the United States, it can be expected that his attorneys will file a legal challenge based on the extraterritorial reach of the CFAA which, if resolved in his favor, could undercut prosecutorial efforts to hold him accountable.

Congress should also include similarly clear language in the SCA. Doing this will overcome evidentiary issues that could arise if the government requires evidence stored on a server located abroad as occurred in the *Microsoft* case. As Judge Gerald Lynch explained in that case, the lack of any such language yields unfair results. Specifically, a service provider's decision to store emails in another country, whether for cost or other reasons, can now defeat the "government's demand" for such emails, notwithstanding that such emails are needed to prosecute criminal activity occurring here.[212] This result is even more unfair considering that such storage is merely virtual as computer files can be fragmented and stored across many servers, and because service provider employees in the United States are capable in the ordinary course of business—and without ever leaving their desks—to review such data. Accordingly, the SCA as drafted imposes an unfair penalty on criminal prosecutors so long as the Supreme Court does not alter this interpretation and the statute is deemed applicable only to files held domestically.

Of course, any alterations to either the text or judicial interpretation of the CFAA or SCA which confirms their extraterritorial reach are bound to have foreign policy implications as applied to specific acts. But that is not unusual. Consider the pending prosecution of members Fédération Internationale de Football Association (FIFA) by the U.S. Attorney's Office for the Eastern District of New York for corruption. Despite critiques of the United States for overreaching in the application of its laws[213] and for acting as a "world police," the case proceeds apace with little diplomatic fallout for the simple reason that the "world is not insular to a particular country any longer."[214]

---

212. *In re* Warrant to Search a Certain E-mail Account Controlled & Maintained by Microsoft Corp., 829 F.3d 197, 224 (2016) (No. 14-2985).

213. Jon Sopel, *Fifa scandal: Is the long arm of US law now overreaching?*, BBC (June 4 2015), http://www.bbc.com/news/world-us-canada-33011847 [https://perma.cc/FP7Z-4X5Q] (archived Aug. 29, 2017); Raymond J. de Souza, *America's Prosecutorial Overreach*, NAT'L POST (June 10, 2015), http://nationalpost.com/opinion/father-raymond-j-de-souza-why-is-the-u-s-prosecuting-fifa-over-corruption-scandals-that-largely-took-place-elsewhere (subscription required) [https://perma.cc/AHN3-DM8P] (archived Aug. 29, 2017).

214. Everett Rosenfeld, *Why the FIFA case is being prosecuted in the US*, CNBC (May 27, 2015), http://www.cnbc.com/2015/05/27/why-fifa-is-being-prosecuted-in-the-us.html [https://perma.cc/H8FY-8KMR] (archived Aug. 29, 2017).

This argument applies even more forcefully in the cybercrime context and also serves a deterrent effect. Bluntly put, if Chinese hackers associated with the PLA or Russian hackers associated with the FSB are indicted and such governments are made aware that evidence pertaining to their actions, which are stored on commercially available servers outside the United States, are subject to seizure, then the costs for engaging in such activities rise. This is so because the seizure and publication of such evidence in the form of an indictment can result in diplomatic pressures on an aggressor country and the development of countermeasures by victims of such attacks when they are made aware of how the original attack occurred.

B. *Removal of Sovereign Immunity for State Sponsors of Cyber Crime*

Congress should also consider amending the Foreign Sovereign Immunities Act (FSIA) or otherwise passing special legislation to permit civil litigants to file claims directly against a state implicated in a cyberattack. Such an approach may seem outlandish, but it has precedent. In 2016, Congress overrode a presidential veto to pass a bill entitled the Justice Against Sponsors of Terrorism Act (JASTA).[215] JASTA provides a private right of action against state sponsors of terrorism.[216] More specifically, it authorizes federal court jurisdiction over civil claims against a foreign state for physical injury to a person or property or death that occurs inside the United States as a result of an act of international terrorism or a tort committed anywhere by an official, agent, or employee of a foreign state acting within the scope of his or her employment.[217]

When the bill was debated, Saudi Arabia protested vigorously as its passage allowed the continuation of a longstanding civil suit brought by victims of the September 11, 2001 terror attacks against Saudi Arabia.[218] In fact, Saudi Arabia threatened to destabilize the US economy by selling up to $750 billion in US securities if the bill passed.[219] Likewise, the U.S. Department of State warned that the

---

215. 18 U.S.C. § 2333 (2012).

216. *Id.*

217. *Id.*

218. *See, e.g.*, Callum Paton, *Saudi Arabia Paid Veterans to Lobby Congress Against 9/11 Lawsuit Bill*, NEWSWEEK (May 11, 2017), http://www.newsweek.com/saudi-arabia-paid-veterans-lobby-congress-against-911-lawsuit-law-607655 [https://perma.cc/66FG-5JFH] (archived Aug. 29, 2017).

219. *See* Mark Mazzetti, *Saudi Arabia Warns of Economic Fallout if Congress Passes 9/11 Bill*, N.Y. TIMES (April 15, 2016), https://www.nytimes.com/2016/04/16/world/middleeast/saudi-arabia-warns-ofeconomic-fallout-if-congress-passes-9-11-bill.html?_r=0 (subscription required) [https://perma.cc/FM73-BEMZ] (archived Aug. 29, 2017); Larry McShane, *Saudi Arabia Threatens to Pull $750B from U.S. Economy if Congress Allows them to be Sued for 9/11 Terror Attacks*, DAILY NEWS (April 16, 2016),

bill's passage could cause other states to pass similar measures abrogating sovereign immunity defenses of the United States for drone strikes or other foreign economic, military, or diplomatic activity which caused harm.[220] Although Saudi Arabia never followed through on its threats, it continues to lobby heavily to amend JASTA and restore the protections it previously enjoyed as a sovereign state.[221]

Applying the JASTA model to sovereign state perpetrators of cybercrimes would likely be far less controversial from a foreign policy and legal perspective for a variety of reasons. This is so because JASTA was widely understood as specifically targeting Saudi Arabia, whereas removing sovereign immunity defenses for state sponsors of cybercrime would apply generally to any state. Furthermore, customary international law, as codified in the FSIA, already strips away sovereign immunity defenses for state actions that qualify as: (a) commercial activities performed in the United States; (b) an act performed by a state in the United States in connection with a commercial activity outside the United States; or (c) an act performed by a state outside the United States in connection with a commercial activity outside the United States but which causes a direct effect in the United States.[222] This is important because a host of state-sponsored criminal activity directed against the United States arguably qualifies as commercial in nature, such as occurred when the PLA hacked US commercial entities and stole their trade secrets ostensibly to benefit Chinese competitors, meaning that the passage of a law removing a state's claim of sovereign immunity for such actions would arguably fall within existing law.

Take the PLA hack. If Westinghouse, Alcoa, or any of the other victims of that incident could file a civil cause of action against China directly for theft of their trade secrets, which went to benefit Chinese competitors, they could recover significant damages which would (in turn) raise the cost benefit analysis future hackers would undertake

---

http://www.nydailynews.com/news/world/saudi-arabia-warns-750b-response-9-11-liability-suit-article-1.2603675 (subscription required) [https://perma.cc/4ET7-MBSS] (archived Aug. 29, 2017).

220. 162 CONG. REC. 147, at 19 (Sept. 28, 2016) (Justice Against Sponsors Of Terrorism Act—Veto Message From The President Of The United States), https://www.congress.gov/crec/2016/09/28/CREC-2016-09-28.pdf. [https://perma.cc/UQD4-M3FN] (archived Aug. 29, 2017); *See* Mazzetti, *supra* note 219.

221. Bruce Riedel, *What JASTA Will Mean for U.S.-Saudi Relations*, BROOKINGS (Oct. 3, 2016), https://www.brookings.edu/blog/markaz/2016/10/03/what-jasta-will-mean-for-u-s-saudi-relations/ [https://perma.cc/S4A4-GZPQ] (archived Aug. 29, 2017); Ananya Sreekanth, *Justice Against Sponsors of Terrorism Act: The Bad and the Ugly*, BERK. POL. REV. (Nov. 14, 2016); *see also* Lee Fang, *As Trump Travels to Saudi Arabia, the Kingdom's D.C. Lobbying Surge is Paying Off*, THE INTERCEPT (May 19, 2017), https://theintercept.com/2017/05/19/as-trump-travels-to-saudi-arabia-the-kingdoms-d-c-lobbying-surge-is-paying-off/.

222. 28 U.S.C. § 1605(a)(2) (2012).

before deciding to launch future attacks. On the negative side, however, it could be presumed that other states would pass similar legislation which could be directed towards deterring aggressive cyber espionage activities of the United States.[223] But that is not necessarily a negative outcome, as a mutual deterrence legal regime broadly directed against a variety of state actors could militate against the continued perpetration of such attacks in the future.

Of course, opening the courthouse doors to civil litigants who suffer when a state perpetrates a cyberattack for purely commercial reasons is different from the situation when a state perpetrates such an attack for political or other noncommercial reasons. That said, this approach could prove attractive for policy makers given that the alternative solutions are (as explained above): (1) to do nothing except strengthen cyber defenses; (2) institute a counter cyberattack against a perpetrator; (3) impose diplomatic or economic sanctions against a perpetrator; or (4) use military force against a perpetrator. Stated differently, if Russia's actions in the Yahoo attack were not purely commercial but its actions were still subject to civil penalties in the United States, its calculus in launching such an attack might change.

Similarly, Congress can set the threshold level of attribution required for liability to attach in any such legislation. In so doing, Congress could harmonize the holdings in *Nicaragua* and *Tadic* by establishing a standard of attribution flexible enough to account for the amorphous nature of how states perpetrate cyberattacks yet robust enough to satisfy those instances when attribution truly cannot be determined. At a minimum, by equipping the United States with such a statutory remedy, when combined with more traditional responses, it is at least theoretically possible that the instances of such cyberattacks would be decreased and/or that the victims of such attacks located here would recover some form of compensation for their losses.

VI. CONCLUSION

This Article has provided an overview of instances in which sovereign states have perpetrated cybercrimes against the United States. This Article also has set forth the domestic legal framework applicable to the prosecution of such crimes. After opining that the current legal framework does little to deter states from engaging in such attacks, this Article argues that: (1) the CFAA and SCA should either be modified or interpreted to apply extraterritorially, and (2) Congress should provide civil litigants a private right of action against state sovereign perpetrators of cybercrimes. If these

223. Ananya Sreekanth, *Justice Against Sponsors of Terrorism Act: The Bad and the Ugly*, BERK. POL. REV. (Nov. 14, 2016).

recommendations were adopted, it by no means assure that such activity would decrease or that state actors would find themselves deterred from committing such acts in the future. Notwithstanding, it would certainly raise the stakes for such actors should they decide to engage in such activity, which would further the goal of deterrence while also ensuring that the victims of such attacks have a vehicle to obtain compensation.

***