Nebraska Law Review

Volume 96 | Issue 2 Article 5

2017

From Russia with Love: Understanding the Russian Cyber Threat to U.S. Critical Infrastructure and What to Do about It

Scott J. Shackelford
Indiana University, sjshacke@indiana.edu

Michael Sulmeyer
Harvard University, michael_sulmeyer@hks.harvard.edu

Amanda N. Craig Deckard
Microsoft

Ben Buchanan
Harvard University, ben_buchanan@hks.harvard.edu

Brian Micic
Indiana University Maurer School of Law

Scott J. Shackelford, Michael Sulmeyer, Amanda N. Craig Deckard, Ben Buchanan & Brian Micic*

From Russia with Love: Understanding the Russian Cyber Threat to U.S. Critical Infrastructure and What to Do About It

TABLE OF CONTENTS

* Scott J. Shackelford, J.D., Ph.D., Associate Professor, Indiana University Kelley School of Business; Director, Ostrom Workshop Program on Cybersecurity and Internet Governance; Research Fellow, Harvard Kennedy School Belfer Center on Science and International Affairs Cyber Security Project. Michael Sulmeyer, J.D., Ph.D., Director, Harvard Kennedy School Belfer Center on Science and International Affairs Cyber Security Project. Amanda N. Craig Deckard, J.D., M.Sc., Senior Cybersecurity Strategist, Microsoft Corporation. The views expressed in this Article are solely those of the author and do not necessarily represent or reflect the position of Microsoft Corporation. Ben Buchanan, Ph.D., Postdoctoral Research Fellow, Harvard Kennedy School Belfer Center on Science and International Affairs Cyber Security Project. Brian Micic, J.D. candidate, Indiana University Maurer School of Law.

I. INTRODUCTION

In December 2016, the U.S. Department of Homeland Security disclosed that malicious software (malware) found on a computer system owned by a Vermont utility called the Burlington Electric Company was the same variant as that used to breach the Democratic National Committee (DNC).[1] This admittedly overhyped episode is the latest in a string of cybersecurity incidents that involve U.S. critical infrastructure (CI) and that have been linked to Russia. Already, a number of nations have seen their systems compromised by such attempts, such as Ukraine, which experienced several of its substations crashing in December 2015 in "the first-ever confirmed cyberattack against grid infrastructure."[2] Unfortunately, the same type of attack played out again in Ukraine on December 23, 2016.[3] This Article examines the most recent of such hacks and investigates the current state of U.S. efforts to advance cybersecurity, including to what extent the recently released draft Version 1.1 of the National Institute of Standards and Technology (NIST) Cybersecurity Framework will contribute to safeguarding vulnerable U.S. CI and what further steps—such as an effective deterrence strategy—are needed going forward.

This Article is structured as follows: Part II briefly summarizes the history of alleged Russian hacking on U.S. critical infrastructure and government networks from the 1990s to 2016.[4] Part III builds from

1. *See* Evan Perez, *Vermont Utility Finds Alleged Russian Malware on Computer*, CNN (Dec. 31, 2016), http://www.cnn.com/2016/12/30/us/grizzly-steppe-malware-burlington-electric [https://perma.unl.edu/TWE3-BBW2].
2. Jeff St. John, *The Real Cybersecurity Issues Behind the Overhyped "Russia Hacks the Grid" Story*, GREENTECH MEDIA (Jan. 4, 2017), https://www.greentechmedia.com/articles/read/the-real-cybersecurity-issues-behind-the-overhyped-russia-hacks-the-grid-st [https://perma.unl.edu/4RJK-NDC5].
3. *See* Thomas Fox-Brewster, *Ukraine Claims Hackers Caused Christmas Power Outage*, FORBES (Jan. 4, 2016), http://www.forbes.com/sites/thomasbrewster/2016/01/04/ukraine-power-out-cyber-attack/#77b6ed5d5e6f [https://perma.unl.edu/AG5E-T6QE].
4. *See What Is Critical Infrastructure?*, U.S. DEP'T HOMELAND SEC., http://www.dhs.gov/what-critical-infrastructure [https://perma.unl.edu/H5EG-TWZ4]; *What Is ICS-CERT's Mission?*, INDUS. CONTROL SYS. CYBER EMERGENCY RESPONSE TEAM, http://ics-cert.us-cert.gov/Frequently-Asked-Questions [https://perma.unl.edu/QW8H-VJET] (giving sixteen critical-infrastructure sectors the U.S. Cyber Emergency Response Team has identified, consistent with Homeland Security Presidential Directive 21, including: chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, health care and public health, information technology, nuclear reactors and materials, transportation systems, and water and wastewater systems).

the foundation laid in Part II with a comparative case study exploring the 2015 and 2016 cyber attacks on the Ukraine power grid. Part IV explores policy prescriptions to enhance U.S. critical-infrastructure cybersecurity with a focus on unpacking draft Version 1.1 of the 2017 NIST Cybersecurity Framework, exploring international cybersecurity norm building in the CI context and laying out a deterrence strategy for mitigating the Russian cyber threat to U.S. CI and government systems.

II. A SHORT HISTORY OF RUSSIAN HACKING OF U.S. GOVERNMENT NETWORKS AND CRITICAL INFRASTRUCTURE

A comprehensive rendering of Russia's alleged and now decades-long information-warfare campaign against the U.S. government and U.S.-based critical infrastructure is beyond the scope of this Article. Rather, this Part helps inform the following discussion on contemporary challenges and policy prescriptions by briefly summarizing several of the early Russian campaigns and comparing them to what has transpired since. In particular, we focus on two episodes—the late 1990s "Moonlight Maze" campaign and the 2016 DNC hack—to gain a better understanding of how Russian cybersecurity strategy has evolved in the nearly twenty-year span bookending these events.

The Moonlight Maze attacks of the late 1990s became among the most extensive cyber attacks aimed at the U.S. government to that point, involving attackers gaining access to thousands of sensitive files.[5] According to U.S. officials, state-sponsored Russian hackers penetrated U.S. Department of Defense (DoD) computers for more than one year, stealing data from U.S. agencies such as the Department of Energy and NASA, as well as from military contractors and universities.[6] Damage from the attacks was limited to unclassified networks but prompted a great deal of concern in the U.S. government. Some officials, including then-Coordinator for Counterterrorism Richard Clarke, likened it to pre-war reconnaissance.[7]

While Moonlight Maze in many respects introduced the risk of Russian and other state-sponsored hacking into the consciousness of U.S. officials, later events would show how widespread the threat was and continues to be. In 2015, it was reported that Russian hackers had gained access to the unclassified White House email network that was used for scheduling, personnel matters, correspondence with overseas

5. *See* Major Arie J. Schaap, *Cyber Warfare Operations: Development and Use Under International Law*, 64 A.F. L. REV. 121, 141 (2009).

6. *See id.*

7. *Id.*; *see* BENJAMIN BUCHANAN, THE CYBERSECURITY DILEMMA (2017); THOMAS RID, RISE OF THE MACHINES: A CYBERNETIC HISTORY 314 (2016).

diplomats, and more.[8] The same group of hackers was reportedly able to access key networks in the Pentagon, such as the email systems used by the Joint Chiefs of Staff; in the State Department, where remediation proved to be an ongoing challenge;[9] and in a wide variety of other targets.

The election year of 2016 brought even greater attention to potential Russian cyber operations. According to CrowdStrike, not one but two Russian intelligence agencies, the nominally domestic FSB and the military-intelligence-focused GRU, gained access to the networks of the Democratic National Committee and to the email accounts of staffers on the Hillary Clinton campaign.[10] While much cyber espionage up to this point involved using the stolen secrets out of view, those involved in this hack took a different tack. They splayed stolen data out on social media, on the anti-secrecy site WikiLeaks, and in newspapers.[11] While the individual revelations themselves were not enormously consequential—the most significant email forced the ouster of Democratic National Committee Chairwoman Debbie Wasserman Schultz because of the party's perceived favoritism towards Hillary Clinton over primary rival Bernie Sanders—they consumed an enormous amount of media attention.[12] Historians will debate the degree to which the hacking and information operation persuaded voters to choose Donald Trump over Hillary Clinton; an assessment by the U.S. intelligence community later concluded that this was the Russians' aim.[13]

The ongoing drip of hacked files and emails throughout the summer and fall of 2016 raised the concern about Russian cyber capabilities to a previously unprecedented level. Reportedly, President Obama

8. Michael S. Schmidt & David E. Sanger, *Russian Hackers Read Obama's Unclassified Emails, Officials Say*, N.Y. TIMES, Apr. 26, 2015, at A1, https://www.nytimes.com/2015/04/26/us/russian-hackers-read-obamas-unclassified-emails-officials-say.html?_r=0.

9. *See* Justin Fishel & Lee Ferran, *State Dept. Shuts Down Email After Cyber Attack*, ABC NEWS (Mar. 13, 2015), http://abcnews.go.com/US/state-dept-shuts-email-cyber-attack/story?id=29624866 [https://perma.unl.edu/QZ8R-3FUQ].

10. Dmitri Alperovitch, *Bears in the Midst: Intrusion into the Democratic National Committee*, CROWDSTRIKE (June 15, 2016), https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee [https://perma.unl.edu/4PCY-Y8VV].

11. Thomas Rid, *All Signs Point to Russia Being Behind the DNC Hack*, VICE (July 24, 2016), https://motherboard.vice.com/en_us/article/all-signs-point-to-russia-being-behind-the-dnc-hack [https://perma.unl.edu/6L2P-MAPM].

12. *See, e.g.*, *id.*

13. Adam Entous, Ellen Nakashima & Greg Miller, *Secret CIA Assessment Says Russia Was Trying to Help Trump Win White House*, WASH. POST (Dec. 9, 2016), https://www.washingtonpost.com/world/national-security/obama-orders-review-of-russian-hacking-during-presidential-campaign/2016/12/09/31d6b300-be2a-11e6-94ac-3d324840106c_story.html?utm_term=.4992441a5ab3 [https://perma.unl.edu/3SS4-B4NG].

attempted to achieve bipartisan consensus in condemning the hacks but was rebuffed by Senator Mitch McConnell.[14] In lieu of that feat, and wary of Russian operations that might change votes rather than target voters, it is reported that the United States used a Cold War-like communications mechanism to warn Russia against targeting election infrastructure itself. Specifically, as Election Day came and went without Russian manipulation of vote-counting mechanisms, this warning can be perhaps be viewed as an instance of successful deterrence.[15] Nonetheless, towards the end of the Obama presidency, he saw fit to punish the Russians for their reported interference in the electoral process, levying sanctions, expelling diplomats, and closing two Russian compounds in the United States.[16] It was a watershed moment, as the intersection of computer hacking and international intrigue emerged more fully than ever before into public view. This sets the stage for other, more explicitly damaging hacks of Ukraine's grid, showing a broader range of possible Russian cyber operations.

III. UNPACKING THE UKRAINE GRID HACKS AND THEIR AFTERMATH

While cyber attacks on critical infrastructure are not unprecedented, the recent penetrations in December 2015 and December 2016 against the electrical grid in Ukraine have gained widespread notoriety given that they show what is possible for unprepared sectors.[17] As a result, thoroughly understanding the Ukrainian cyber attacks provides governments a glimpse into the strategies adversarial hackers use and helps to underscore what can be done about it.

To set the stage, the recent cyber attacks on Ukraine's electrical grid were not the first to plague the country. Since 2014, there has been a string of cyber attacks that have targeted—with varying degrees of success—various industries within Ukraine.[18] In May 2014,

14. *Id.*
15. David E. Sanger, *White House Confirms Pre-Election Warning to Russia over Hacking*, N.Y. TIMES, Nov. 17, 2016, at A20, https://www.nytimes.com/2016/11/17/us/politics/white-house-confirms-pre-election-warning-to-russia-over-hacking.html?_r=0.
16. David E. Sanger, *Obama Strikes Back at Russia for Election Hacking*, N.Y. TIMES, Dec. 30, 2016, at A1, https://www.nytimes.com/2016/12/29/us/politics/russia-election-hacking-sanctions.html.
17. *See, e.g.*, Darlene Storm, *Cyberwarfare: Digital Weapons Causing Physical Damage*, COMPUTERWORLD (Dec. 22, 2014), http://www.computerworld.com/article/2861531/cyberwarfare-digital-weapons-causing-physical-damage.html [https://perma.unl.edu/H67W-TBUD].
18. JAKE STYCZYNSKI, NATE BEACH-WESTMORELAND & SCOTT STABLES, WHEN THE LIGHTS WENT OUT: A COMPREHENSIVE REVIEW OF THE 2015 ATTACKS ON UKRAINIAN CRITICAL INFRASTRUCTURE 7 (2016), http://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf [https://perma.unl.edu/F9MF-SXGV].

threat actors targeted Ukrainian electricity distributor Prykarpattyaoblenergo and all six of Ukraine's state railway transportation-system operators as part of a phishing campaign.[19] In August 2014, a similar campaign attacked five Ukrainian regional government sources and state archives.[20] This occurred again in March 2015, with the target this time being Ukrainian television broadcasters.[21] In October 2015, on Ukraine's election day, BlackEnergy and KillDisk malware were used to hack into numerous government workstations.[22] A similar attack was also used to target Ukrainian mining firms.[23] These attacks shared similar characteristics in both their methodology of operation and use of certain malware. As such, the cyber attacks in December 2015 may be considered the climax of a chain of exploits that sought to obtain valuable information from, and eventually cripple, specific industry sectors within Ukraine.

In December 2015, adversarial hackers successfully infiltrated workstations within three Ukrainian energy-distribution companies—Prykarpattyoblenergo, Kyivoblenergo, and Chernivtsioblenergo—and caused physical damage to the electrical grid.[24] This left over two hundred thousand people in western Ukraine without power for several hours.[25] The threat actors were able to change security measures and disable communication channels, prolonging the blackout and preventing recovery efforts by the respective company employees.[26] Several sources, including Booz Allen, attributed the cyber attacks to Russian hackers who may have been acting under the direction of the Kremlin.[27]

Almost one year after the December 2015 cyber attacks, another campaign was conducted against the Ukrainian electrical grid. This time, a power substation was targeted, leaving 100,000 to 200,000 residents of Kiev without power.[28] Eventually, approximately one-fifth

19. *Id.*
20. *Id.*
21. *Id.*
22. *Id.*
23. *Id.*
24. *Id.* at 3.
25. *See* James Temperton, *Hackers Were Behind Ukraine Power Outage*, WIRED (Feb. 26, 2016), http://www.wired.co.uk/article/ukrainian-power-station-cyber-attack [https://perma.unl.edu/MF2F-9YTQ].
26. *See* Kim Zetter, *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid*, WIRED (Mar. 3, 2016), https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid [https://perma.unl.edu/U9J2-MTKZ].
27. STYCZYNSKI ET AL., *supra* note 18, at 8.
28. Patrick Tucker, *Ukrainian Power Company "99% Certain" Blackout Result of Cyber Attack*, DEF. ONE (Dec. 21, 2016), http://www.defenseone.com/technology/2016/12/ukrainian-power-company-99-certain-blackout-result-cyber-attack/134099/ [https://perma.unl.edu/D4LT-G3B7].

of Kiev's electrical power was cut as a result of the attack.[29] Further investigation has linked this cyber attack with the December 2015 attack.[30]

While the direct effects of these incidents unnerved the Ukrainian government and contributed to increased tensions between Ukraine and Russia, these cyber attacks had far-reaching effects beyond Eastern Europe. The threat-actor group, dubbed SandWorm, believed to have conducted the aforementioned cyber attacks is also thought to have conducted attacks against NATO and Western European governmental targets,[31] which raises the question as to the sufficiency of other nations' ability to prevent attacks against their own electrical grids. Numerous nations, including the United States, took notice of the swiftness and sophistication of these attacks and responded by reevaluating their own respective security systems. In turn, numerous issues were discovered concerning the safety of CI during future attacks, in particular focusing on the vulnerability of smart-grid tech, international norm building, and the increasing sophistication of attackers.[32]

First, many electrical grids are using outdated industrial control systems that are unable to prevent adversarial hackers from infiltrating vulnerable networks; in particular, "[t]he underlying protocols and components take no account of modern internet threats and so are inherently insecure."[33] In response, some nations have attempted to update their grids; ironically, though, this has multiplied vulnerabilities through the rise of smart-grid systems.[34] According to a report by the Congressional Research Service:

> [N]ew intelligent technologies utilizing two-way communications and other digital advantages are being optimized by Internet connectivity. Moderniza-

29. *Ukraine Power Cut "Was Cyber-Attack,"* BBC (Jan. 11, 2017), http://www.bbc.com/news/technology-38573074 [https://perma.unl.edu/Y2VA-AKSH].

30. *Id.*

31. Ellen Nakashima, *Russian Hackers Suspected in Attack that Blacked Out Parts of Ukraine*, WASH. POST (Jan. 5, 2016), https://www.washingtonpost.com/world/national-security/russian-hackers-suspected-in-attack-that-blacked-out-parts-of-ukraine/2016/01/05/4056a4dc-b3de-11e5-a842-0feb51d1d124_story.html?utm_term=.3602b71d8e8c [https://perma.unl.edu/Q7BB-FJGC].

32. *Cf.* BEN BUCHANAN, THE LEGEND OF SOPHISTICATION IN CYBER OPERATIONS 1 (2017), https://www.belfercenter.org/sites/default/files/files/publication/Legend%20Sophistication%20-%20web.pdf [https://perma.unl.edu/FJS6-VA4H] (exploring what the term "sophistication" means in the context of cyber operations).

33. Nilufer Tuptuk & Stephen Hailes, *The Cyberattack on Ukraine's Power Grid Is a Warning of What's to Come*, PHYS.ORG (Jan. 13, 2016), https://phys.org/news/2016-01-cyberattack-ukraine-power-grid.html [https://perma.unl.edu/4CFZ-GLWG].

34. Loren Thompson, *Five Reasons the U.S. Power Grid Is Overdue for a Cyber Catastrophe*, FORBES (Aug. 19, 2015), http://www.forbes.com/sites/lorenthompson/2015/08/19/five-reasons-the-u-s-power-grid-is-overdue-for-a-cyber-catastrophe/2/#2e670805513c [https://perma.unl.edu/2FBQ-7ZR9].

> tion of many IC [industrial control] systems . . . has resulted in connections to the Internet. While these advances will improve the efficiency and performance of the grid, they also will increase its vulnerability to potential cyberattacks.[35]

Thus, modernized "smart" grids may in fact increase, not limit, the number of avenues that hackers can exploit.

Second, the use of cyber attacks to damage critical infrastructure has increased international tensions and undermined cybersecurity norm-building efforts (a topic discussed further in Part IV). Specifically, the cyber attacks against Ukraine in December 2015 and 2016 have been linked to Russia, though the degree of state sponsorship remains an area of active debate.[36] This has made the international community weary of Russia and other nations using cyber attacks to cause similar damage, especially considering that, by some estimates, the electrical control systems that were hacked were in fact more secure than some U.S. counterparts.[37]

Finally, the sophistication of threat actors has increased to an alarming level, though not across the board.[38] While governments and security firms try to stay one step ahead, the ability of adversarial hackers and their tools means that they are able to penetrate ever more sophisticated defenses[39] to achieve a large range of motivations.[40] Whether it be retribution, monetary gain, or a social or political cause, a successful hack of a power grid holds the promise for causing far-reaching consequences. In turn, the increased number of potential suspects makes it more difficult to identify, locate, and prevent possible cyber attacks, which can lead to an increase in spending

---

35. RICHARD J. CAMPBELL, CONG. RESEARCH SERV., R43989, CYBERSECURITY ISSUES FOR THE BULK POWER SYSTEM (2015), https://fas.org/sgp/crs/misc/R43989.pdf [https://perma.unl.edu/J2GR-9UMP]; *see also* AM. SOC'Y OF CIVIL ENG'RS, 2013 REPORT CARD FOR AMERICA'S INFRASTRUCTURE (2013), http://2013.infrastructurereportcard.org/a/#p/energy/overview [https://perma.unl.edu/VA4C-TN5A] ("America relies on an aging electrical grid and pipeline distribution systems, some of which originated in the 1880s. Investment in power transmission has increased since 2005, but ongoing permitting issues, weather events, and limited maintenance have contributed to an increasing number of failures and power interruptions.").

36. *See* Pavel Polityuk, *Ukraine Investigates Suspected Cyber Attack on Kiev Power Grid*, REUTERS (Dec. 20, 2016), http://www.reuters.com/article/us-ukraine-crisis-cyber-attacks-idUSKBN1491ZF [https://perma.unl.edu/2RNZ-9L7C].

37. *See* Daniel Wagner & Dante Disparte, *The Growing Severity of Cyber-Attacks and How to Protect Against Them*, HUFFINGTON POST (Dec. 14, 2016), http://www.huffingtonpost.com/daniel-wagner/the-growing-severity-of-c_b_13601810.html [https://perma.unl.edu/M3FM-8VDH].

38. *See, e.g.*, BUCHANAN, *supra* note 32.

39. *See generally* Trevor McDougal, Note, *Establishing Russia's Responsibility for Cyber-Crime Based on Its Hacker Culture*, 11 BYU INT'L L. & MGMT. REV. 55 (2015).

40. *See* Tuptuk & Hailes, *supra* note 33.

by these industries to implement sufficient cyber defenses—with the cost ultimately being born by consumers.[41]

The cyber attacks on Ukraine's critical infrastructure have raised awareness with regards to the vulnerabilities of numerous industries and have led some governments to take action to mitigate the risk of future attacks.[42] In the United States, this has fed into the narrative surrounding cybersecurity regulation or other approaches to risk mitigation, in particular as it relates to the role of the NIST Cybersecurity Framework and the overall need for effective cyber deterrence to safeguard vulnerable U.S. CI. Part IV analyzes these steps in an effort to understand whether they are, in fact, sufficient to ensure that the cyber attacks against Ukraine's power grid are not repeated domestically.

IV. ANALYZING POLICY OPTIONS TO HELP PROMOTE THE RESILIENCE OF U.S. GOVERNMENT SYSTEMS AND CRITICAL INFRASTRUCTURE

There is no perfect solution to the issue of safeguarding vulnerable government systems and diverse CI systems. As a result, a range of policy tools and strategies are needed to address the threat of advanced nation-state actors. The U.S. government has taken some steps forward in this vein with the development and dissemination of the NIST Cybersecurity Framework, including the recent 2017 Version 1.1 Draft, along with intensive cybersecurity norm-building efforts. This Part reviews these developments along with the potential for an effective deterrence strategy to help mitigate the cyber threat to U.S. systems—from Russia or otherwise—going forward.

A. Contextualizing and Introducing Draft Version 1.1 of the NIST Cybersecurity Framework

Efforts to identify and protect U.S. CI have been ongoing for decades. In 1998, Presidential Decision Directive No. 63 (PPD-63) designated authorities to protect U.S. CI from intentional physical and cyber attacks; in October 2001, two Executive Orders (EOs) were signed, establishing new authorities and coordination mechanisms to protect U.S. CI and recover from incidents; and in 2003, the Homeland Security Presidential Directive 7 (HSPD-7) updated agencies' roles and responsibilities in protecting CI.[43] Keeping in place much of the

41. CAMPBELL, *supra* note 35, at 30.

42. *See* Wagner & Disparte, *supra* note 37 ("Despite the fact that cyber-attacks occur with greater frequency and intensity around the world, many either go unreported or are under-reported, leaving the public with a false sense of security about the threat they pose and the lives and property they impact.").

43. JOHN D. MOTEFF, CONG. RESEARCH SERV., RL30153, CRITICAL INFRASTRUCTURES: BACKGROUND, POLICY, AND IMPLEMENTATION 11 (2015) ("The Bush Administration

policy and organization established by the Bush Administration, the Obama Administration declared U.S. CI to be a "strategic national asset" back in 2009, but little progress was made following the pronouncement, and 2012 legislative proposals to strengthen cybersecurity were filibustered.[44] In response, in 2013, President Obama issued EO 13,636 that, among other things, expanded public–private information sharing and tasked NIST to work with the private sector and other stakeholders to develop a cybersecurity framework for CI. In addition, from 2013 to 2016, the Obama Administration issued PPD-21 and a draft update to the National Infrastructure Protection Plan, conducted a "Cyber Sprint" to assess agency defenses, and developed the Cybersecurity Strategy and Implementation Plan (CSIP) and Cybersecurity National Action Plan (CNAP) to drive improvements to federal cybersecurity and resilience.

As it was tasked in EO 13,636, NIST partnered with its stakeholder community to develop the *Framework for Improving Critical Infrastructure Cybersecurity* (the Cybersecurity Framework or Framework), Version 1 of which it released in 2014.[45] Both the Framework itself and the process through which it was developed represented an important step forward for the U.S. government and CI; the focus was on reaching consensus through an inclusive process on best practices that the private sector could adopt to better secure systems.[46] In particular, the NIST Cybersecurity Framework captures industry best practices to provide—its proponents argue—a flexible approach to boosting cybersecurity governance, assisting owners and operators of CI in managing cyber risk and engaging executives in enterprise risk-management conversations that scope in cybersecurity. In addition,

---

policy and approach regarding critical infrastructure protection can be described as an evolutionary expansion of the policies and approaches laid out in PPD-63. The fundamental policy statements were essentially the same . . . . Also, the stated goal of the government's efforts is to ensure that any disruption of the services provided by these infrastructures be infrequent, of minimal duration, and manageable. . . . Finally, the primary effort was directed at working collaboratively and voluntarily with the private sector owners and operators of critical infrastructure . . . .").

44. *Id.* at 12–13. One notable organizational change directed by President Obama was the appointment of a White House official to coordinate cybersecurity policies and activities. *Id.*; *A Better Defined and Implemented National Strategy Is Needed to Address Persistent Challenges*, GAO (Mar. 7, 2013), http://www.gao.gov/products/GAO-13-462T [https://perma.unl.edu/YL7V-LSKY] ("Further, without an integrated strategy that includes key characteristics, the federal government will be hindered in making further progress in addressing cybersecurity challenges.").

45. NAT'L INST. STANDARDS & TECH., IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY EXECUTIVE ORDER 13636: PRELIMINARY CYBERSECURITY FRAMEWORK (2013), http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf [https://perma.unl.edu/K3BX-2LSG].

46. *See id.* at 1.

the Framework is particularly relevant for CI because it acts as a baseline that is relevant across sectors, many of which are independent and thus reap security benefits from compatible guidance or requirements, recognizing that it may also be necessary to have sector-specific guidance or requirements to complement a cross-sector baseline.

This Framework is also important since—even though its critics argue that it helps to solidify a reactive stance to the nation's cybersecurity challenges[47]—it is arguably spurring the development of a standard of cybersecurity care in the United States, which is an important step given how fragmented this process has been to date.[48] Although the Framework has only been available since 2014,[49] already some private-sector clients are receiving the advice that if their "cybersecurity practices were ever questioned during litigation or a regulatory investigation, the 'standard' for 'due diligence' was now the NIST Cybersecurity Framework."[50] Eventually, the Framework could help shape a standard of care for domestic CI organizations while also driving collaboration and compatibility in global cybersecurity best practices, especially given active NIST collaborations with a number of nations including the U.K., Japan, and Korea.[51]

Consistent with the roadmap that NIST issued along with the Framework Version 1 (v1) in 2014 as well as the comments and feedback that NIST has collected through Requests for Information and public workshops since the release of v1, in January 2017, NIST is-

47. Taylor Armerding, *NIST's Finalized Cybersecurity Framework Receives Mixed Reviews*, CSO ONLINE (Jan. 31, 2014), http://www.csoonline.com/article/2134338/security-leadership/nist-s-finalized-cybersecurity-framework-receives-mixed-reviews.html [https://perma.unl.edu/AF3P-U2W2]. For more on the benefits of a more proactive approach to cybersecurity, see Amanda N. Craig, Scott J. Shackelford & Janine S. Hiller, *Proactive Cybersecurity: A Comparative Industry and Regulatory Analysis*, 52 AM. BUS. L.J. 721 (2015).

48. *See, e.g.*, Scott J. Shackelford et al., *Toward a Global Cybersecurity Standard of Care?: Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices*, 50 TEX. INT'L L.J. 305 (2015).

49. *See* NAT'L INST. STANDARDS & TECH, FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY 26 (2015), http://www.nist.gov/cyberframework/upload/cybersecurity_framework_bsi_2015-04-08.pdf [https://perma.unl.edu/W7C6-SV3V] ("To allow for adoption, Framework version 2.0 is not planned for the near term.").

50. John Verry, *Why the NIST Cybersecurity Framework Isn't Really Voluntary*, PIVOTPOINT SECURITY (Feb. 25, 2014), https://www.pivotpointsecurity.com/blog/nist-cybersecurity-framework [https://perma.unl.edu/Q3Y9-RGVN]; *see* Andrea Arias, *The NIST Cybersecurity Framework and the FTC*, FED. TRADE COMMISSION (Aug. 31, 2016), https://www.ftc.gov/news-events/blogs/business-blog/2016/08/nist-cybersecurity-framework-ftc [https://perma.unl.edu/8Q7S-EU4R].

51. For more on this topic, see Scott J. Shackelford, Scott Russel & Jeffrey Haut, *Bottoms Up: A Comparison of "Voluntary" Cybersecurity Frameworks*, 16 U.C. DAVIS BUS. L.J. 217, 222 (2016).

sued a draft update to the Framework: v1.1. Rather than aiming for fundamental changes to the Framework, the draft update is intended to clarify and enhance v1. To that end, the basic structure of the Framework is unchanged; the components of the Core, Tiers, and Profiles remain intact.[52] Indeed, within the Framework's Core, no Functions were added; just one Category was added ("Supply Chain Risk Management"—along with five accompanying Subcategories); and only three additional Subcategories were included (bringing the total to 106). Meanwhile, in other Categories and Subcategories, language was updated and clarified (e.g., within the "Risk Assessment" and "Identity Management, Authentication and Access Control" Categories), and NIST is continuing to assess potential updates to Information References. Keeping the structure of the Core, as well as much of its content, consistent was a critically important step since the structure and content of the Core have proved fundamental to the Framework's success.

In addition to minor updates to the Core and other sections, within draft v1.1 of the Framework, NIST has also incorporated some significant new content, including a section on metrics and measures, and an expanded explanation on how to use the Framework for cyber supply-chain risk management (C-SCRM). Among the most dramatic changes is the inclusion of Section 4.0—"Measuring and Demonstrating Cybersecurity"—which proposes that the Framework can be used as the basis for "comprehensive measurement"—both "metrics," which facilitate decision-making, and the "measures," or quantifiable data, that inform those metrics. In addition, within the Implementation Tiers and Sections 3.3 and 3.4, there is substantial new C-SCRM content intended to inform both organizations' assessment of their C-SCRM practices as well as their conversations with information and communication technology (ICT) suppliers and buyers.

While some of the Framework's draft v1.1 updates are indeed helpful, others may risk undermining the unique value of the Framework as a cross-sector baseline and be better incorporated as evolving documents that supplement the Framework. Because the cyber-threat landscape is rapidly evolving and security technologies are continually advancing, so too must government entities, CI, and other enterprises continually adapt and improve their defenses. Likewise, policy and guidance documents must also be updated to capture recent best prac-

52. The Core outlines cybersecurity risk-management best practices, organized according to five Functions (Identify, Protect, Detect, Respond, and Recover), along with increasingly specific and practitioner-oriented Categories, Subcategories, and Informative References. The "Implementation Tiers" enable organizations to assess the extent to which they've implemented those best practices, and the "Profiles" enable organizations to establish current and target Profiles and to track their progress in closing any implementation gaps.

tices. However, guidance intended for a broad, cross-sector audience that supports risk-management conversations and advancements across interdependent sectors and enterprises may compromise relevance with an ever-expanding scope. For example, as draft v1.1 describes, using metrics and measures to understand and convey meaningful risk information to partners and customers would be valuable, providing a basis for trust both within and between organizations. Yet meaningful ways to demonstrate the effectiveness of cybersecurity practices and investments are still developing. As this effort is ongoing, guidance for measuring and demonstrating cybersecurity may more appropriately supplement rather than be integrated into the NIST Cybersecurity Framework, promoting its continued relevance as a cross-sector baseline.

NIST has released information about its intended next steps, including its intention to release another draft v1.1 and to receive another round of comments from stakeholders.[53] In doing so, NIST in particular recognized the importance of adjusting both the metrics and measurement and supply-chain risk management sections. NIST's continued responsiveness to stakeholders and commitment to open and iterative engagements is critical to the Framework's ongoing use in the ecosystem and its potential to drive advancements in cybersecurity risk management across sectors.

In capturing and promoting baseline best practices in cybersecurity risk management, the Framework has represented an important step forward for U.S. CI protection, and the draft v1.1 update process demonstrates sustained investment by the U.S. government in the Framework's continued relevance and success. The Framework filled a gap by incorporating an array of information-security controls into the risk-management context. One outcome has been the increasing use of a consistent language, both within and between organizations, which supports continuous improvements in cybersecurity risk management and supply-chain security.

The Framework's functioning as a baseline set of best practices has been critical to this success; however, by definition, implementing a baseline may not be sufficient to mitigate significantly advanced threats. Rather than trying to capture every action that a differently situated CI or U.S. government entity might undertake to reduce or mitigate advanced, persistent, targeted threats, the Framework has captured, in a flexible way, a core set of activities and outcomes that are relevant to mitigate threats that are common across many sectors and enterprises, including smaller companies integrated into CI sup-

53. NAT'L INST. STANDARDS & TECH., CYBERSECURITY FRAMEWORK WORKSHOP 2017 SUMMARY (2017), https://www.nist.gov/sites/default/files/documents/2017/07/21/cybersecurity_framework_workshop_2017_summary_20170721_1.pdf [https://perma.unl.edu/KP7X-Q7NC].

ply chains. Moreover, the Framework has been structured to institutionalize processes of continuous improvement, which may help many organizations drive more meaningful investments in cybersecurity risk management. To mitigate the issue of targeted attacks by advanced nation-state threat actors, some organizations need to do more than just the baseline best practices. They might implement security in a way that increases the investment required by threat actors to accomplish nefarious activities, track repeat threat actors to better understand their techniques and improve targeted mitigations, or work with others in the ecosystem to track advanced threat-actor behavior and share effective mitigations. Ultimately, these advanced actions, undertaken by organizations with a security mission and sufficient resources, compliment the Framework's approach to establishing processes in support of strategic cybersecurity risk management.

In summary, the widespread adoption of a baseline set of cybersecurity best practices is a necessary but not sufficient condition to boosting U.S. CI protection across a range of CI providers with different threat profiles. In addition to more advanced defensive measures responsive to sector- or organization-specific risk scenarios—such as advanced information sharing and behavioral analytics, pen testing, red and blue teams, and decoys—other developments or mechanisms may help to deter or raise the cost of such attacks. The following two sections turn to two ways that the U.S. and other partner governments might work to do so—namely through international cybersecurity norms and deterrence—including deterrence based on sharing information publicly about the security benefits of using the NIST Cybersecurity Framework.

B. Operationalizing International Cybersecurity Norms on Critical Infrastructure

In addition to promoting U.S. government and CI adoption of baseline best practices in cybersecurity risk management and sector- or organization-specific investments in advanced defensive measures, the U.S. government—in partnership with other governments and private-sector entities—can help to secure CI by advancing cybersecurity norms intended to limit destructive attacks of the kind discussed in Part III. Positive progress has been made in 2015–16 in relation to the distillation and propagation of cybersecurity norms that may be applied to enhancing critical-infrastructure protection. The G2 Cybersecurity Code of Conduct between the U.S. and China, for example, calls for mutual restraint in economic cyber espionage, particularly

the theft of trade secrets. It could be expanded to include mutual respect for one another's critical infrastructure.[54]

Similarly, the G7 continued its work on cybersecurity in 2016, publishing its view that "no country should conduct or knowingly support [information and communication technology-enabled] theft of intellectual property" and that all G7 nations should work to "preserve the global nature of the Internet," including the free flow of information in a nod to the notion of cyberspace as a "global networked commons."[55] Such information could explicitly include the protection of data vital to CI systems. The G20 has taken similar steps to help reinforce a norm against attacking vulnerable civilian critical infrastructure,[56] as has the U.N. Security Council in 2017.[57]

The Obama Administration also proposed peacetime norms on CI protection that were included in the 2015 UN Group of Governmental Experts (GGE) consensus report.[58] In particular, the UN GGE agreed that, during peacetime, "[a] State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public."[59] This CI norm could be operationalized to better define the notion of cybersecurity due diligence,[60] but the failure of the 2017 UN GGE to reach agreement bodes ill for further progress in the near term.[61] On the lead up to this meeting, though, it looked like

54. *See* Teri Robinson, *U.S., China Agree to Cybersecurity Code of Conduct*, SC MEDIA (June 26, 2015), http://www.scmagazine.com/us-china-summit-talks-turn-to-cybersecurity/article/423175 [https://perma.unl.edu/4G8B-655M].

55. *G7 Leaders Approve Historic Cybersecurity Agreement*, BOS. GLOBAL F., http://bostonglobalforum.org/2016/06/g7-leaders-produce-historic-cybersecurity-agreement [https://perma.unl.edu/FL2Y-QZZR].

56. *See* Tom Simonite, *Do We Need a Digital Geneva Convention?*, MIT TECH. REV. (Feb. 15, 2017), https://www.technologyreview.com/s/603639/do-we-need-a-digital-geneva-convention [https://perma.unl.edu/K63K-3WK9].

57. *UN Security Council Urges Joint Measures to Protect "Critical Infrastructure" from Terrorist Attacks*, UN NEWS CTR. (Feb. 13, 2017), http://www.un.org/apps/news/story.asp?NewsID=56163#.WKczuJMrJE4 [https://perma.unl.edu/MT5Q-JYLR].

58. *See* U.N. Secretary-General, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,* UN General Assembly, U.N. Doc. A/70/174 (July 22, 2015).

59. *Id.* ¶ 13(f).

60. An earlier version of this research appeared as Scott Shackelford, *Opinion: How to Make Democracy Harder to Hack*, CHRISTIAN SCI. MONITOR (July 29, 2016), http://www.csmonitor.com/World/Passcode/Passcode-Voices/2016/0729/Opinion-How-to-make-democracy-harder-to-hack [https://perma.unl.edu/8RKH-PUM3]; *see also* Scott J. Shackelford et al., *Making Democracy Harder to Hack*, 50 MICH. J.L. REFORM 629 (2017) (analyzing the applicability of these norms in the context of election security).

61. *See* Arun Mohan Sukumar, *The UN GGE Failed. Is International Law in Cyberspace Doomed as Well?*, LAWFARE (July 4, 2017), https://lawfareblog.com/un-gge-

a different result was possible. In February 2017, for example, U.S. State Department Deputy Coordinator for Cyber Issues Michele Markoff, who attended the 2017 UN GGE meeting on behalf of the U.S. government, called for the UN GGE to turn its focus to pushing adoption of norms and confidence-building measures. Addressing an audience at the Carnegie Endowment for International Peace, Markoff was optimistic about U.S.–Russia cooperation on international cybersecurity issues, noting that Russia-linked attacks on Ukraine's power grid in 2016 did not violate the UN GGE norm because Russia and Ukraine were in open conflict rather than peacetime. But an open question remains: given the cyber instability of the recent past, how can the U.S. deterrence strategy be updated to help safeguard vulnerable U.S. government and CI systems?

C. Deterrence and a Path Forward

As discussed above, the NIST Cybersecurity Framework offers one approach that companies, individuals, and government agencies might utilize to improve their cybersecurity practices. Such improvements should help defend against intrusions and other cyber-related compromises. But can the Framework actually deter such malicious acts? In this section, we offer one way to link defense with deterrence and then propose options to strengthen the deterrent value of such steps.

Simply put, deterrence is about perception. If individual A wants to prevent individual B from undertaking action X, A has several options. Usually, scholarship considers A's options in terms of threats: if A threatens B with unacceptable costs that will result from B undertaking X, then B may think twice and not go forward with X. In that scenario, A would deter B from taking action X with a credible threat of cost imposition. The key is that B must perceive that A's threat is credible and that the cost A threatens to impose will indeed be costly and not a mere nuisance. Otherwise, B may not undertake action X for reasons that have nothing to do with A's threat to impose cost. For example, B may simply be unable to underake action X at the present time, but once he gains the capabilities necessary, he will act. In this situation, A is not detering B, who still has the will to act. Instead, B just lacks the means.

Another form of deterrence, also premised on perception, envisions A deterring B from taking action X not by threatening cost but instead by denying B's objectives. B may not think A's threats are credible or costly, but if B does not think he will be able to accomplish X because B perceives A's defenses to be robust, then B has been deterred. This

---

failed-international-law-cyberspace-doomed-well [https://perma.unl.edu/93HY-5PGC].

method of deterence, often referred to as "deterrence by denial" is often seen as a goal of a vulnerable party improving its defenses.

Indeed, a 2015 document by the Obama Administration that outlined a policy of cyber deterrence envisions the Framework as having just a "deterrence by denial" benefit.[62] In that document, they contend that "[t]he Administration will continue to promote the adoption of the Framework as a key means of improving U.S. cyber defenses and, by extension, decreasing adversaries' perceptions of the benefits to be gained from engaging in malicious cyber activities against U.S. computers and networks."[63] As the adoption of a set of technical standards is difficult to politicize, it is possible that the Trump Administration continues to think of the Framework (or some other related approach) in similar ways.

The challenge for U.S. policy makers, and for those who adopt the standards contained within the Framework, is that for the adoption of those standards to deter an adversary, the adversary has to believe that the standards, processes, and practices have been implemented and that the standards, processes, and practices are likely to deny the adversary from achieving his objectives. Merely adopting the Framework does not deter anyone from doing anything. This is not to say that the Framework is not worthwhile; it most certainly is, but primarily as a way to improve defenses and increase resiliency. To deter by denial, the adversary has to believe that Framework adoption makes it harder to accomplish objectives. Despite the merits of the Framework, it is not clear that, all things being equal, advanced nation-state threat actors would be deterred from hacking a U.S. utility because they believed it had adopted the Framework.

It is worth noting that since the adversary's perception is what is most key when trying to deter him, making material improvements to one's defenses is not necessarily required. If the adversary believes—rightly or wrongly—that the defenses will deny him his objectives and if he therefore does not act, then he is deterred. Theoretically, it is possible to imagine such a scenario: a sophisticated propoganda or psychological operations campaign might do much to sow doubt in an adversary's mind that his attack will be successful, independent of the true state of his would-be victim's defenses. While it strains credulity to imagine A can deter B because B thinks A has adopted the NIST Cybersecurity Framework when in fact A has not, the broader point is that B's perception remains the key variable to determining if deterence is at work.

62. REPORT ON CYBER DETERRENCE POLICY 5 (2015), http://1yxsm73j7aop3quc9y5ifaw3.wpengine.netdna-cdn.com/wp-content/uploads/2015/12/Report-on-Cyber-Deterrence-Policy-Final.pdf [https://perma.unl.edu/LMS8-ASWN].

63. *Id.* at 14.

In other words, there are options for those wishing to think of the Framework through the construct of deterrence. Three options are presented below that can help to influence a would-be attacker's perceptions.

1. Publicize Benefits as Applied

To have a chance at deterring a would-be attacker, there needs to be more of a public effort to explain why the Framework's standards, processes, and practices would deny that attacker his objectives. In its cyber-deterrence policy quoted previously, the Obama Administration asserted this link, but it did not explain it. If the Trump Administration shares the previous team's thinking, it could do more to stress why three or four key principles in the Framework stand to deter an adversary. One example is the adoption of multifactor authentication. The task is not to explain the merits of this rather obvious security measure but to message just how successful it is at blunting an adversarial hacker's efforts to gain unauthorized access to an account by harvesting user credentials. Statistics can be gathered and publicized about how many intrusions in previous years exploited the absence of a second factor of authentication. Given that adding a second factor of authentication can be as simple as a mere configuration change, more can be said about the relative ease and lack of expense to adopt it versus the additional effort an adversary may need to expend to overcome it and achieve his objectives.

2. Publicize Exercise Results

Those who have adopted, or are adopting, the Framework would be wise to exercise how a range of cyber attacks by a determined attacker would fare. While deep technical details need not be publicized, thorough explanations of the scenarios tested, how defenses associated with the Framework functioned, and how much more damage could have been wrought without adopting the Framework could be useful areas about which to message.

3. Publicize Updates

Some of the recommendations contained in the NIST Cybersecurity Framework risk being outdated as attackers evolve their techniques. It would be wise for NIST to commit to an update cycle and for those who adopt the Framework to stress their continuing commitment to put in place recommended updates in a timely manner. And of course, the key is to publicize the commitment and evidence of adhering to it.

To be sure, public messaging about adopting the Framework is unlikely to deter an advanced and determined adversary. But at this point, the prevailing culture of defending against cyber attacks em-

phasizes secrecy more than publicity. A less public posture may be wise for operational security and other practical reasons, but it undermines the opportunity for deterrence by denial. Companies and agencies may, when given the choice, still choose a subtler approach to public engagement—and that may be the most prudent course of action—but they should be aware that, by doing so, they will have to look to shape the adversary's perceptions by other means.

V. CONCLUSION

This Article has examined the multifaceted cyber threat to U.S. government systems and CI by exploring campaigns from Moonlight Maze to the 2016 DNC hacks that have been linked to Russia, as well as the 2015 and 2016 attacks against Ukraine. These incidents demonstrate a need for strengthening defenses on the part of governmental and critical-infrastructure providers and a credible deterrence strategy going forward. The Framework, including the most recent v1.1 update, is a helpful step forward in this regard, especially considering its utility in establishing a common baseline and a common vocabulary based around cybersecurity risk management. However, to deter advanced threat actors from especially valuable CI targets, use of the Framework should be considered one step in a multipronged campaign that includes the further definition and dissemination of international cybersecurity norms to help safeguard critical infrastructure, along with publicizing the benefits of the Framework itself to help deter foreign adversaries. None of these recommendations are a magic bullet, of course. But perhaps they do not need to be. After all, the Australian government, for example, has reportedly been successful in preventing eighty-five percent of cyber attacks on its networks through following three common-sense techniques: application whitelisting (only permitting pre-approved programs to operate on networks), regularly patching applications and operating systems, and minimizing "the number of users with administrative privileges"—all baseline best practices promoted through the Framework.[64] Though U.S. systems are at a different scale, such efforts help to highlight the fact that the cyber threat may be complex and sophisticated, but individual attacks are not. As such, by leveraging cybersecurity risk-management best practices, such as those promoted within the Framework, many attacks can be thwarted. In addition, deterrence and international norm-building efforts can shift the calculus of more advanced, state-sponsored cyber attacks in favor of making them an exception to a relative state of cyber peace.

64. JAMES A. LEWIS, RAISING THE BAR FOR CYBERSECURITY 7–8 (2013), http://csis.org/files/publication/130212_Lewis_RaisingBarCybersecurity.pdf [https://perma.unl.edu/6Z2B-AJBV].