Boston College Law Review

Volume 59 | Issue 6 Article 7

7-11-2018

A Slap on the Wrist: Combatting Russia's Cyber Attack on the 2016 U.S. Presidential Election

Christina Lam
Boston College Law School, christina.lam@bc.edu

A SLAP ON THE WRIST: COMBATTING RUSSIA'S CYBER ATTACK ON THE 2016 U.S. PRESIDENTIAL ELECTION

Abstract: On June 14, 2016, suspicions emerged that Russia launched a cyber attack on the U.S. Democratic National Committee in the midst of an extremely contentious presidential election season. The damage was extensive, occurring over a series of months and resulting in numerous leaks of highly sensitive information regarding Democratic Presidential Candidate Hillary Clinton. After it was verified that Russia was behind the cyber attack, President Barack Obama relied on general and anachronistic principles of international law to issue a grossly ineffective response. Russia's cyber attack and the U.S. response thus highlighted the ways in which international law fails to guard against and remedy state-sponsored cyber attacks. These attacks will continue to occur at an alarming rate and without adequate recourse unless a new international treaty is implemented. In order to be successful, this treaty would need to garner the support of the major cyber powers and be specifically tailored towards combatting state-sponsored cyber attacks.

INTRODUCTION

The 2016 U.S. presidential election was highly contentious from the start.[1] Americans were deeply divided over the issues, even within the Republican and Democratic parties.[2] A lot was at stake: the next President would have the power to shape the Supreme Court, decide the future of Obamacare, and transform immigration policies.[3] Republican candidate

[1] *See, e.g.*, Joshua Green, *Why 2016 May Be the Most Important Election of Our Lifetime*, BLOOMBERG BUSINESSWEEK (Nov. 5, 2015), https://www.bloomberg.com/news/articles/2015-11-05/why-2016-may-be-the-most-important-election-of-our-lifetime [http://perma.cc/B5K9-JPSM] (recognizing that "the chasm" between the Republican and Democratic parties was "the greatest it's ever been"); Danielle Kurtzleben, *The Most 'Unprecedented' Election Ever? 65 Ways It Has Been*, NPR (July 3, 2016), http://www.npr.org/2016/07/03/484214413/the-most-unprecedented-election-ever-65-ways-it-has-been [http://perma.cc/86BJ-JJZU] (listing the ways in which the 2016 presidential election was "unprecedented").

[2] William A. Galston, *Republicans and Democrats Divided on Important Issues for a Presidential Nominee*, BROOKINGS (June 3, 2015), https://www.brookings.edu/blog/fixgov/2015/06/03/republicans-and-democrats-divided-on-important-issues-for-a-presidential-nominee/ [http://perma.cc/VAQ9-VKMQ]; Green, *supra* note 1.

[3] *See* Green, *supra* note 1 (stating that Democratic and Republican presidential candidates point the country towards entirely different futures in regards to the Affordable Care Act, the make-up of the Supreme Court, and immigration policies); Bradley Klapper et al., *Why It Matters: Issues at Stake in Election*, U.S. NEWS (Sept. 17, 2016), https://www.usnews.com/news/politics/articles/2016-09-17/

Donald Trump and Democratic candidate Hillary Clinton appealed to the many voters who were angry and frustrated with the status quo, thereby securing their party's presidential nomination in a bitterly fought primary election.[4] Both candidates only grew more extreme in their views and shrouded in controversy as Election Day neared and, in fact, were deemed the two most disliked presidential candidates in nearly forty years.[5] Once it seemed as though the election could not possibly create more media headlines, suspicions emerged that Russia hacked the Democratic National Committee ("DNC").[6]

The DNC reported a breach of its computer network on June 14, 2016, which was quickly attributed to Russian hackers.[7] The devastating fallout occurred in waves beginning on July 22, 2016 when WikiLeaks published nearly twenty thousand e-mails and eight thousand attachments from top DNC officials.[8] The hackers continued to leak massive amounts of sensitive

---

why-it-matters-issues-at-stake-in-election [http://perma.cc/TZ65-L7R8] (describing the Democratic and Republican stance on major issues such as immigration and health care).

[4] Caitlin Huey-Burns, *Angry Voters: Who Will They Support?*, REALCLEARPOLITICS (Jan. 12, 2016), http://www.realclearpolitics.com/articles/2016/01/12/angry_voters_who_will_they_support.html [http://perma.cc/SD2J-QRRQ]; Maria Liasson, *Here's Why Voters Are So Anxious This Election*, NPR (Jan. 25, 2016), http://www.npr.org/2016/01/25/464217330/heres-why-voters-are-so-anxious-this-election [http://perma.cc/Z2NB-REFF].

[5] Eliza Collins, *Poll: Clinton, Trump Most Unfavorable Candidates Ever*, USA TODAY (Aug. 31, 2016), http://www.usatoday.com/story/news/politics/onpolitics/2016/08/31/poll-clinton-trump-most-unfavorable-candidates-ever/89644296/ [http://perma.cc/N64U-XX3V]; Harry Enten, *Americans' Distaste for Both Trump and Clinton Is Record-Breaking*, FIVETHIRTYEIGHT (May 5, 2016), https://fivethirtyeight.com/features/americans-distaste-for-both-trump-and-clinton-is-record-breaking/ [http://perma.cc/XQ2T-5FJC].

[6] Justin Fishel & Veronica Stracqualursi, *A Timeline of Russia's Hacking into US Political Organizations Before the Election*, ABC NEWS (Dec. 15, 2016), http://abcnews.go.com/Politics/timeline-russias-hacking-us-political-organizations-ahead-election/story?id=44140526 [http://perma.cc/3DL9-4QC7]; 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 [http://perma.cc/R54P-9LH5]. "Hacking" is defined as "deliberately gain[ing] (or attempt[ing] to gain) unauthorized access to computer systems." S.M. Furnell & M.J. Warren, *Computer Hacking and Cyber Terrorism: The Real Threats in the New Millennium?*, 18 COMPUTERS & SECURITY 28, 29 (1999). The Democratic National Committee ("DNC") is an organization responsible for raising money, hiring staff, and coordinating strategies to assist Democratic candidates. *The Democratic National Committee*, DEMOCRATS, https://www.democrats.org/organization/the-democratic-national-committee [http://perma.cc/P7J2-MY26].

[7] Fishel & Stracqualursi, *supra* note 6; Eric Lipton et al., *The Perfect Weapon: How Russian Cyberpower Invaded the U.S.*, N.Y. TIMES (Dec. 13, 2016), https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html [http://perma.cc/6VJZ-CQSK]; Nakashima, *supra* note 6; Dmitri Alperovitch, *Bears in the Midst: Intrusion into the Democratic National Committee*, CROWDSTRIKE BLOG (June 15, 2016), https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/ [http://perma.cc/3MKY-XT3W].

[8] Fishel & Stracqualursi, *supra* note 6; Tom Hamburger & Karen Tumulty, *WikiLeaks Releases Thousands of Documents About Clinton and Internal Deliberations*, WASH. POST (July 22, 2016),

campaign information in the days leading up to the November 7, 2016 U.S. presidential election.[9]

On October 7, 2016, the U.S. Intelligence Community publicly expressed confidence that the Russian government was behind the cyber attack on the DNC.[10] Then, on December 29, 2016, U.S. President Barack Obama issued an Executive Order, taking measures against Russia for perpetrating the cyber attack.[11] Specifically, the order blocked five Russian entities and four Russian individuals from engaging in business with the United States and seized all of their assets in the United States.[12] Obama also authorized the U.S. Department of State to declare thirty-five Russian

---

https://www.washingtonpost.com/news/post-politics/wp/2016/07/22/on-eve-of-democratic-convention-wikileaks-releases-thousands-of-documents-about-clinton-the-campaign-and-internal-deliberations/ [http://perma.cc/MZ3R-QK2R]. WikiLeaks was created in 2006 by Julian Assange as a non-profit organization for releasing documents obtained from anonymous sources. Jonathan Zittrain & Molly Sauter, *Everything You Need to Know About Wikileaks*, MIT TECH. REV. (Dec. 9, 2010), https://www.technologyreview.com/s/421949/everything-you-need-to-know-about-wikileaks/ [http://perma.cc/R2WH-9284].

[9] Fishel & Stracqualursi, *supra* note 6; Maggie Haberman & Alan Rappeport, *Presidential Election: The Day Before the Storm*, N.Y. TIMES (Nov. 7, 2016), https://www.nytimes.com/2016/11/07/us/politics/presidential-election.html [http://perma.cc/66FZ-BQ59]; Katiana Krawchenko et al., *The John Podesta Emails Released by WikiLeaks*, CBS NEWS (Oct. 13, 2016), http://www.cbsnews.com/news/the-john-podesta-emails-released-by-wikileaks/ [http://perma.cc/94WM-Q53F]; Michael Sainato, *DC Leaks Exposes Clinton Insider's Elitist and Embarrassing Emails*, OBSERVER (Oct. 7, 2016), http://observer.com/2016/10/dc-leaks-exposes-clinton-insiders-elitist-and-embarrassing-emails/ [http://perma.cc/8V6N-3BBE].

[10] Fishel & Stracqualursi, *supra* note 6; *Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security*, DEP'T OF HOMELAND SECURITY (Oct. 7, 2016), https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national [http://perma.cc/JW2V-M26Y]. The U.S. Intelligence Community is comprised of seventeen separate organizations including the Central Intelligence Agency, Federal Bureau of Investigation, Department of Homeland Security, National Security Agency, and U.S. Army. *Member Agencies*, THE U.S. INTELLIGENCE COMMUNITY INTELLIGENCE CAREERS, https://www.intelligencecareers.gov/icmembers.html [http://perma.cc/G7TC-QZTR].

[11] Exec. Order No. 13,757, 82 Fed. Reg. 1 (Dec. 28, 2016); Lauren Gambino et al., *Obama Expels 35 Russian Diplomats in Retaliation for US Election Hacking*, THE GUARDIAN (Dec. 30, 2016), https://www.theguardian.com/us-news/2016/dec/29/barack-obama-sanctions-russia-election-hack [http://perma.cc/3B75-FSZS]; David E. Sanger, *Obama Strikes Back at Russia for Election Hacking*, N.Y. TIMES (Dec. 29, 2016), https://www.nytimes.com/2016/12/29/us/politics/russia-election-hacking-sanctions.html [http://perma.cc/9HG8-VL68]; Lesley Wroughton, *US Expels 35 Russian Diplomats, Closes 2 Russian Compounds*, BUS. INSIDER (Dec. 29, 2016), http://www.businessinsider.com/us-expels-35-russian-diplomats-closes-2-russian-compounds-2016-12 [http://perma.cc/6GHR-DK52].

[12] Exec. Order No. 13,757; Gambino et al., *supra* note 11; Sanger, *supra* note 11; Press Release, The White House, Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment (Dec. 29, 2016) (on file with the White House Office of the Press Secretary).

diplomats "persona non grata" and close two Russian compounds on U.S. territory.[13]

On January 6, 2017, the U.S. Director of National Intelligence released its official conclusion that the Russian government was behind the DNC hacks.[14] Although Russia's motives for interfering with the election are still not entirely clear, the Director of National Intelligence and many others believe that the hacks were intended to help Donald Trump win the presidency.[15] There was, however, no indication that the Russian government tampered with the voting process itself.[16]

This Note examines the legal ramifications of the U.S. response to Russia's cyber attack on the DNC.[17] Part I links this attack to the alarming rise of state-sponsored hacking aimed at the United States.[18] Part II discusses the international law of response, focusing on the provisions relevant to the U.S. response to Russia's cyber attack.[19] Lastly, Part III argues that the United States was forced to rely on general and outdated international law principles when responding to Russia's cyber attack, emphasizing the need for a new international treaty that would guard against state-sponsored cyber attacks and punish them effectively when they occur.[20]

---

[13] Gambino et al., *supra* note 11; Sanger, *supra* note 11; Press Release, The White House, *supra* note 12; *see* Exec. Order No. 13,757; *infra* notes 149–151 and accompanying text (explaining that "persona non grata" means "not acceptable" and its declaration requires the sending state to "recall the diplomat concerned or terminate his functions with the mission").

[14] 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). The U.S. Director of National Intelligence is the head of the U.S. Intelligence Community. *Careers at ODNI*, OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, https://www.dni.gov/index.php/careers/careers-at-odni [http://perma.cc/3HMS-QCMM].

[15] OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *supra* note 14; Craig Forcese, *The "Hacked" US Election: Is International Law Silent, Faced with the Clatter of Cyrillic Keyboards?*, JUST SECURITY (Dec. 16, 2016), https://www.justsecurity.org/35652/hacked-election-international-law-silent-faced-clatter-cyrillic-keyboards/ [http://perma.cc/636S-WNJ3]; Kathy Gilsinian & Krishnadev Calamur, *Did Putin Direct Russian Hacking? And Other Big Questions*, THE ATLANTIC (Jan. 6, 2017), https://www.theatlantic.com/international/archive/2017/01/russian-hacking-trump/510689/ [http://perma.cc/S49E-C9J8]. There was rampant speculation about Russia's impetus for interfering with the 2016 U.S. Presidential Election. Kurt Eichenwald, *Why Vladimir Putin's Russia Is Backing Donald Trump*, NEWSWEEK (Nov. 4, 2016), http://www.newsweek.com/donald-trump-vladimir-putin-russia-hillary-clinton-united-states-europe-516895 [http://perma.cc/ZGR3-QMFQ]. For example, some claimed that Russia was more concerned with lessening Clinton's chances of winning because it was believed that she improperly interfered with Russian affairs while serving as Secretary of State. *Id.*

[16] OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *supra* note 14; Forcese, *supra* note 15; Gilsinian & Calamur, *supra* note 15.

[17] *See infra* notes 21–236 and accompanying text.

[18] *See infra* notes 21–93 and accompanying text.

[19] *See infra* notes 94–189 and accompanying text.

[20] *See infra* notes 190–236 and accompanying text.

I. THE ESCALATING TREND OF STATE-SPONSORED CYBER ATTACKS ON THE UNITED STATES

In light of the heightened dependence on technology in the digital age, it was inevitable that states would add computers to their arsenal.[21] Traditionally, a government sponsoring an attack would send armed nationals into enemy territory, potentially placing them in grave danger.[22] With the advent of technology, however, states are now able to wreak havoc on any target without even crossing a border.[23] States have already wielded their technological capabilities to undermine the infrastructure of countries around the world, and Russia's cyber attack on the DNC was merely the latest in an escalating trend of state-sponsored hacking directed at the United States.[24] Each of these events elicited a drastically different U.S. re-

---

[21] Irène Couzigou, *The Challenges Posed by Cyber-Attacks to the Law on Self-Defense*, *in* SELECT PROCEEDINGS OF THE EUROPEAN SOCIETY OF INTERNATIONAL LAW 245 (Christina Binder et al. eds., 2016); Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE J. INT'L L., 421, 422–23 (2011); Daniel D. Brecht, *Are Cyber Threats the New Terrorism Frontier?*, CYBER DEF. MAG., Dec. 2014, at 28; Ian Sherr & Seth Rosenblatt, *Sony and the Rise of State-Sponsored Hacking*, CNET (Dec. 20, 2014), https://www.cnet.com/news/sony-and-the-rise-of-state-sponsored-hacking/ [http://perma.cc/4BBZ-VL8C].

[22] Brecht, *supra* note 21; Gavin Millard, *How Can You Fend Off a Nation?*, INFOSECURITY (Jan. 18, 2016), https://www.infosecurity-magazine.com/opinions/how-can-you-fend-off-a-nation/ [http://perma.cc/9XEP-ER5J].

[23] Brecht, *supra* note 21, at 28–29; *see* Waxman, *supra* note 21, at 422–23 (noting that, due to cyber attacks, "[m]ilitary defense networks can be remotely disabled or damaged" and "[p]rivate sector networks can be infiltrated, disrupted, or destroyed"); Millard, *supra* note 22 (noting that "hired thugs, instead of being given swords and guns, are afforded extensive resources and technologies . . . " to carry out cyber attacks). State-sponsored attacks are carried out at the direction of the government for a political purpose. Millard, *supra* note 22. In contrast, attacks that are not state-sponsored (sometimes referred to as "private") are merely an individual or group operation to achieve a personal end. Kimberly Peretti & Jared Slade, *State-Sponsored Cybercrime from Exploitation to Disruption to Destruction*, 10 SCITECH LAW. 12, 13 (2014); Millard, *supra* note 22.

[24] *See, e.g.*, Elizabeth A. Rowe, *RATs, TRAPs, and Trade Secrets*, 57 B.C. L. REV. 381, 400 (2016) (recognizing that "[f]oreign governments have used strategic cyberattacks in growing numbers "); Peretti & Slade, *supra* note 23, at 13 (identifying significant state-sponsored cyber attacks on China, Iran, South Korea, and Australia); Sherr & Rosenblatt, *supra* note 21 (identifying North Korea's cyber attacks on the United States). There is not a generally agreed-upon definition of the term "cyber attack" or related terms such as "cyber espionage" and "cyber terrorism," largely because questionable cyber activities are constantly evolving. *See* MICHAEL N. SCHMITT, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 106 (2013) (defining cyber attack as "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects"); Waxman, *supra* note 21, at 422 (defining cyber attack as the "efforts to alter, disrupt, or destroy computer systems or networks or the information or programs on them"); Memorandum from Gen. James E. Cartwright for Chiefs of the Military Servs., Commanders of the Combatant Commands, Dirs. of the Joint Staff Directories on Joint Terminology for Cyberspace Operations 5 (Nov. 2011) (defining cyber attack as "[a] hostile act using computer or related networks or systems, and intended to disrupt and/or destroy an adversary's critical cyber systems, assets, or functions"). In fact, there is not even a consensus as to whether "cyber attack" should be written as one word or two. Gary D.

sponse.[25] This Part illustrates this trend with two state-sponsored hacks on the United States that occurred prior to the Russian cyber attack on the DNC.[26] Section A identifies a few of China's numerous hacks on the U.S. government.[27] Section B describes North Korea's highly invasive hacks on a U.S. company, Sony Pictures Entertainment.[28] Section C then provides a detailed account of the Russian cyber attack on the DNC and the U.S. response.[29]

A. China's Hacks on the U.S. Government

The Chinese government has been a usual suspect in hacks on various U.S. government agencies and companies.[30] For example, China was accused of hacking the Federal Deposit Insurance Corporation's ("FDIC") computer network between 2010 and 2013.[31] According to investigators,

---

Solis, *Cyber Warfare*, 219 MIL. L. REV. 1, 2 (2014). The DNC's computer network breach was arguably an act of cyber espionage (i.e., "unauthorized viewing and copying of data files") or cyber terrorism (i.e. "unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives"). OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *supra* note 14; Michael Gervais, *Cyber Attacks and the Laws of War*, 30 BERKLEY J. INT'L L. 525, 534; Solis, *supra*, at 3 (quoting CLAY WILSON, CONGRESSIONAL RESEARCH SERVICE, RL32114, BOTNETS, CYBERCRIME, AND CYBERTERRORISM: VULNERABILITIES AND POLICY ISSUES FOR CONGRESS 12 (2008)). This Note, however, refers to the breach of the DNC's computer network as a cyber attack because its information was not only viewed and copied, but also disseminated to the public without a clear motive. *See* OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *supra* note 14; Waxman, *supra* note 21, at 422.

[25] *Compare* Gary Brown & Christopher D. Yung, *Evaluating the US-China Cybersecurity Agreement, Part 1: The US Approach to Cyberspace*, THE DIPLOMAT (Jan. 19, 2017), http://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-1-the-us-approach-to-cyberspace/ [http://perma.cc/H98N-VVYR] (reaching cyber security agreement with China in response to hacks), *with* Exec. Order No. 13,687, 80 Fed. Reg. 819 (Jan. 2, 2015) (barring certain North Korean individuals and organizations from accessing U.S. financial systems in response to hacks), *and* Press Release, The White House, *supra* note 12 (freezing assets of certain Russian individuals and entities and barring them from doing business with the United States as well as expelling Russian diplomats and closing two Russian compounds).

[26] *See infra* notes 30–93 and accompanying text.

[27] *See infra* notes 30–37 and accompanying text.

[28] *See infra* notes 38–58 and accompanying text.

[29] *See infra* notes 59–93 and accompanying text.

[30] Brown & Yung, *supra* note 25; Robert Windrem, *Exclusive: Secret NSA Map Shows China Cyber Attacks on U.S. Targets*, NBC NEWS (July 30, 2015), http://www.nbcnews.com/news/us-news/exclusive-secret-nsa-map-shows-china-cyber-attacks-us-targets-n401211 [http://perma.cc/D6A4-UXK6].

[31] MAJORITY STAFF OF HOUSE COMM. ON SCIENCE, SPACE, & TECH., INTERIM STAFF REPORT: COMM.'S INVESTIGATION OF FDIC'S CYBERSECURITY 6 (2016) [hereinafter H. FDIC REPORT]; Aaron Mamiit, *FBI Launched Probe into FDIC Hack: Was China Really Behind the Security Breach?*, TECHTIMES (Dec. 24, 2016), http://www.techtimes.com/articles/190030/20161224/fbi-launched-probe-into-fdic-hack-was-china-really-behind-the-security-breach.htm [http://perma.cc/6UAD-QKGJ]; Jose Pagliery, *China Hacked the FDIC—and US Officials Covered it up,*

viruses were installed on twelve computers and ten servers at the FDIC, including personal computers belonging to high-ranking FDIC officials.[32] These viruses enabled the installer to access information on the computers and servers, such as banking data and employee records.[33]

China was also accused of hacking the U.S. Office of Personnel Management in December 2014, obtaining the personal information of over twenty million federal employees.[34] The damage was so extensive that it prompted the United States to negotiate a cyber security agreement with China.[35] On September 25, 2015, President Barack Obama of the United States and President Xi Jinping of China officially agreed that their respective governments would not engage in or support cyber-enabled theft for commercial gain.[36] At least one report showed that Chinese government hacking activity decreased ninety percent in the months following the agreement.[37]

B. North Korea's Hacks on Sony

On November 24, 2014, Sony Pictures Entertainment ("Sony") discovered a major breach of its computer network.[38] Employees at all Sony

---

Report Says, CNN TECH (July 13, 2016), http://money.cnn.com/2016/07/13/technology/china-fdic-hack/ [http://perma.cc/QF69-N6RF]. The Federal Deposit Insurance Corporation is a government agency that regulates U.S. commercial banks. Mamiit, *supra*; Pagliery, *supra.*

[32] H. FDIC REPORT, *supra* note 31, at 6; Pagliery, *supra* note 31.

[33] Mamiit, *supra* note 31; Pagliery, *supra* note 31.

[34] Ellen Nakashima, *Chinese Breach Data of 4 Million Federal Workers*, WASH. POST (June 4, 2015), https://www.washingtonpost.com/world/national-security/chinese-hackers-breach-federal-governments-personnel-office/2015/06/04/889c0e52-0af7-11e5-95fd-d580f1c5d44e_story.html [http://perma.cc/FAA9-3DWT]; David E. Sanger, *U.S. Decides to Retaliate Against China's Hacking*, N.Y. TIMES (July 31, 2015), https://www.nytimes.com/2015/08/01/world/asia/us-decides-to-retaliate-against-chinas-hacking.html [http://perma.cc/FLW6-E8KX]. The Office of Personnel Management is a federal agency responsible for recruiting and retaining federal employees. *Our Agency*, OPM.GOV, https://www.opm.gov/about-us/ [http://perma.cc/BT2S-Z4P3].

[35] Brown & Yung, *supra* note 30; Ellen Nakashima & Steven Mufson, *U.S., China Vow Not to Engage in Economic Cyberespionage*, WASH. POST (Sept. 25, 2015), http://www.washingtonpost.com/national/us-china-vow-not-to-engage-in-economic-cyberespionage/2015/09/25/90e74b6a-63b9-11e5-8e9e-dce8a2a2a679_story.html [http://perma.cc/QR6P-3CS2].

[36] Brown & Yung, *supra* note 30; Nakashima & Mufson, *supra* note 35.

[37] Joseph Menn & Jim Finkle, *Chinese Economic Cyber-Espionage Plummets in U.S.: Experts*, REUTERS (June 21, 2016), http://www.reuters.com/article/us-cyber-spying-china-idUSKCN0Z700D [http://perma.cc/6KR6-VQL8]; Nafeesa Syeed, *U.S. Cyber Deal with China Is Reducing Hacking, Official Says*, BLOOMBERG TECH. (June 28, 2016), https://www.bloomberg.com/news/articles/2016-06-28/u-s-cyber-deal-with-china-is-reducing-hacking-official-says [http://perma.cc/8XJL-FBMZ].

[38] Alex Altman & Alex Fitzpatrick, *Everything We Know About Sony,* The Interview*, and North Korea*, TIME (Dec. 17, 2014), http://time.com/3639275/the-interview-sony-hack-north-korea/ [http://perma.cc/SS8V-TXHG]; Lori Grisham, *Timeline: North Korea and the Sony Pictures Hack*, USA TODAY (Dec. 18, 2014), http://www.usatoday.com/story/news/nation-now/2014/12/18/sony-hack-timeline-interview-north-korea/20601645/ [http://perma.cc/YV6L-T9G3].

offices worldwide found themselves unable to login to their computers.[39] In addition, glowing, red skeletons displayed on their screens along with the message "Hacked By #GOP . . . . We've already warned you, and this is just a beginning . . . . We've obtained all of your internal data including your secrets . . . ."[40] The "GOP," or Guardians of Peace, also posted a message using at least three of Sony's Twitter accounts specifically threatening Sony's Chief Executive Officer.[41] The hacks brought Sony to a standstill as employees were forced to shut down their computers.[42]

Almost immediately, North Korea was accused of orchestrating the attack as revenge for Sony's production of "The Interview."[43] The timing was indeed suspicious, occurring just a month away from the scheduled release date of the comedy about two journalists recruited by the U.S. Central Intelligence Agency to assassinate North Korean leader Kim Jong-un.[44] In June 2014, the isolationist, totalitarian state sent a letter to the United Nations Secretary General condemning the movie.[45] Specifically, North Korea referred to the "The Interview" as the "undisguised sponsoring of terrorism, as well as an act of war" and pledged "decisive and merciless countermeasure" if "the U.S. administration tacitly approves or supports" the movie.[46]

---

[39] James Cook, *Staff at Sony Pictures Are Being Forced to Use Pens and Paper After a Massive Hack*, BUS. INSIDER (Nov. 28, 2014), http://www.businessinsider.com/staff-at-sony-pictures-are-using-pens-and-paper-after-a-massive-hack-2014-11 [http://perma.cc/WL2S-WVSN]; Grisham, *supra* note 38; Elizabeth Weise & Claudia Puig, *Sony Hack May Be Linked to James Franco Comedy*, USA TODAY (Dec. 1, 2014), http://www.usatoday.com/story/tech/2014/12/01/hack-attack-sony-pictures-north-korea-the-interview/19733463 [http://perma.cc/YQ5Y-XLG7].

[40] Grisham, *supra* note 38; Weise & Puig, *supra* note 39; Aly Weisman, *A Timeline of the Crazy Events in the Sony Hacking Scandal*, BUS. INSIDER (Dec. 9, 2014), http://www.businessinsider.com/sony-cyber-hack-timeline-2014-12 [http://perma.cc/W344-VBQV].

[41] Sean Gallagher, *Sony Pictures Hackers Release List of Stolen Corporate Files*, ARS TECHNICA (Nov. 26, 2014), https://arstechnica.com/security/2014/11/sony-pictures-hackers-release-list-of-stolen-corporate-files/ [http://perma.cc/BXP3-PMYW]; Weisman, *supra* note 40.

[42] Cook, *supra* note 39; Weisman, *supra* note 40.

[43] Grisham, *supra* note 38; Weise & Puig, *supra* note 39; Weisman, *supra* note 40.

[44] Grisham, *supra* note 38; Weisman, *supra* note 40. Kim Jong-un became the third "supreme leader" of North Korea immediately after the death of his father, Kim Jong-il, on December 17, 2011. *Profile: Kim Jong-un, North Korea's Supreme Commander*, BBC NEWS (Jan. 6, 2016), http://www.bbc.com/news/world-asia-pacific-11388628 [http://perma.cc/9G4Z-4LFS]; Paul Szoldra et al., *How a Quiet Boy from North Korea Became One of the World's Scariest Dictators*, BUS. INSIDER (Sept. 9, 2016), http://www.businessinsider.com/kim-jong-un-life-2016-9/#some-originally-believed-that-kim-jong-uns-aunt-and-uncle-were-actually-calling-the-shots-9 [http://perma.cc/36HF-FNSD]. As "supreme leader," Kim Jong-un has complete control over the country, including the world's fourth-largest military. Szoldra et al., *supra*. Under the Kim family regime, North Korea is known as "the world's most oppressed nation" where there is "no freedom of speech or religion," "the world's most closed nation" where there is "no freedom of information," and the "world's darkest nation" where there is "little light, politically, spiritually, and even physically." Benedict Rogers, *North Korea in the Dark*, N.Y. TIMES (Jan. 28, 2013), http://www.nytimes.com/2013/01/29/opinion/north-korea-in-the-dark.html [http://perma.cc/6PP7-BJFS].

[45] Weise & Puig, *supra* note 39; Weisman, *supra* note 40.

[46] Weise & Puig, *supra* note 39; Weisman, *supra* note 40.

North Korea publicly denied responsibility for the Sony hacks, but called it a "righteous deed."[47]

The hackers' reign of terror continued when, on November 27, 2014, five of Sony's films were posted on illegal file-sharing sites.[48] By December 2, 2014, thousands of Sony documents were leaked and many contained sensitive employee data such as employees' social security numbers, home addresses, and salaries.[49] Soon after, Sony staff received an e-mail threatening to harm their families if they did not promote the GOP's goals.[50] The hackers also posted a message demanding that Sony cancel the release of "The Interview" and distributed links to thousands of e-mail exchanges from top Sony executives' accounts.[51]

Sony ultimately surrendered to the hackers' demands on December 17, 2014, cancelling "The Interview's" release.[52] This announcement came only shortly after the hackers' threat to execute attacks on movie theaters prompted several major theater chains to back out of showing the film.[53] On December 19, 2014, the U.S. Federal Bureau of Investigation publicly announced its official conclusion that North Korea was responsible for the cyber attack on Sony.[54]

On January 2, 2015, President Obama signed an Executive Order imposing sanctions on North Korea for the cyber attack on Sony.[55] This

---

[47] Grisham, *supra* note 38; Weisman, *supra* note 40.

[48] Weise & Puig, *supra* note 39; Weisman, *supra* note 40.

[49] Kevin Roose, *Hacked Documents Reveal a Hollywood Studio's Stunning Gender and Race Gap*, SPLINTER (Dec. 1, 2014), http://fusion.net/story/30789/hacked-documents-reveal-a-hollywood-studios-stunning-gender-and-race-gap/ [http://perma.cc/JA46-4VA3]; Weisman, *supra* note 40.

[50] Andrea Mandell & Elizabeth Weise, *Sony Hit Again, Employee Families Threatened, Files Released*, USA TODAY (Dec. 5, 2014), http://www.usatoday.com/story/life/movies/2014/12/05/sony-hacked-again-this-time-employee-families-threatened/19970141/ [http://perma.cc/ZPU9-REYD]; Weisman, *supra* note 40.

[51] Sherr & Rosenblatt, *supra* note 21; Weisman, *supra* note 40.

[52] Grisham, *supra* note 38; Sherr & Rosenblatt, *supra* note 21.

[53] Altman & Fitzpatrick, *supra* note 38; Grisham, *supra* note 38.

[54] Grisham, *supra* note 38; *see* Press Release, FBI, Update on Sony Investigation (Dec. 19, 2014) (on file with FBI National Press Office) (basing conclusion, in part, on "links to other malware that the FBI knows North Korean actors previously developed," "significant overlap between the infrastructure used in this attack and other malicious cyber activity . . . linked to North Korea," and "similarities to a cyber attack . . . against South Korean banks and media outlets, which was carried out by North Korea"). *But see* Altman & Fitzpatrick, *supra* note 38 (acknowledging that the evidence indicated that North Korea was behind the hacks, but "hackers will often dissect and imitate successful techniques"); Paul, *New Clues in Sony Hack Point to Insiders, Away from DPRK*, SECURITY LEDGER (Dec. 28, 2014), https://securityledger.com/2014/12/new-clues-in-sony-hack-point-to-insiders-away-from-dprk/ [http://perma.cc/Q23M-L928] (detailing cyber security firm Norse's allegation that their investigation revealed that six individuals—one a former Sony employee and none based in North Korea—were directly involved in the Sony hacks).

[55] Dan Roberts, *Obama Imposes New Sanctions Against North Korea in Response to Sony Hack*, THE GUARDIAN (Jan. 2, 2015), https://www.theguardian.com/us-news/2015/jan/02/obama-

marked the first time in history that the United States had retaliated in response to a foreign cyber attack on a U.S. company.[56] Specifically, the Executive Order barred ten individuals and three organizations, including North Korea's main intelligence agency and primary arms exporter, from accessing U.S. financial systems.[57] In reality, these sanctions only minimally affected North Korea because it has long been one of the most isolated countries in the world.[58]

C. Russia's Cyber Attack on the DNC

The media first reported that Russian hackers breached the DNC's computer network on June 14, 2016 and shortly thereafter, a hacker named Guccifer 2.0 claimed responsibility.[59] Crowdstrike, an American cyber security firm, promptly analyzed the breach and confirmed the initial reports.[60] The fallout began on July 22, 2016—just three days before the Democratic National Convention—when WikiLeaks published "part one" of a "new Hillary Leaks series."[61] Part one was comprised of 19,252 e-mails

---

imposes-sanctions-north-korea-sony-hack-the-interview [http://perma.cc/GR5A-KTTY]; *see* Exec. Order No. 13687 (sanctioning North Korea).

[56] Ellen Nakashima, *Why the Sony Hack Drew an Unprecedented U.S. Response Against North Korea*, WASH. POST (Jan. 15, 2015), https://www.washingtonpost.com/world/national-security/why-the-sony-hack-drew-an-unprecedented-us-response-against-north-korea/2015/01/14/679185d4-9a63-11e4-96cc-e858eba91ced_story.html [http://perma.cc/A4N3-QPP9]; Roberts, *supra* note 55.

[57] Exec. Order No. 13,687; Roberts, *supra* note 55.

[58] *See* Roberts, *supra* note 55 (recognizing that the sanctions "barr[ed] only limited further commercial engagement with the already heavily-isolated state").

[59] Alperovitch, *supra* note 7; Fishel & Stracqualursi, *supra* note 6; Adi Robertson, *WikiLeaks Posts Leaked DNC Emails, Including Donor Personal Information*, THE VERGE (July 22, 2016), http://www.theverge.com/2016/7/22/12259258/wikileaks-leaked-democratic-national-committee-emails-personal-information [http://perma.cc/56B8-FSTN]. Guccifer 2.0 claimed to be a lone, Romanian hacker. OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *supra* note 14. Investigators found, however, that the hacker "made multiple contradictory statements and false claims about his likely Russian identity . . . ." *Id.*

[60] Alperovitch, *supra* note 7; Fishel & Stracqualursi, *supra* note 6; Lipton et al., *supra* note 7; Nakashima, *supra* note 6. Crowdstrike recognized two known Russian hacking groups' "distinctive handiwork" in the DNC hacks and assigned them the code names "Cozy Bear" and "Fancy Bear." Alperovitch, *supra* note 7; Lipton et al., *supra* note 7. Around June 2015, Cozy Bear sent spear-phishing e-mails to a number of American government agencies, nonprofits, and government contractors including the DNC. Alperovitch, *supra* note 7; Lipton et al., *supra* note 7. As soon as someone clicked on one of these e-mails, the hackers were able to enter the network and download documents. Alperovitch, *supra* note 7; Lipton et al., *supra* note 7. Fancy Bear did not become involved until sometime around April 2016, first hacking the Democratic Congressional Campaign Committee and then the DNC. Alperovitch, *supra* note 7; Lipton et al., *supra* note 7.

[61] Fishel & Stracqualursi, *supra* note 6; Hamburger & Tumulty, *supra* note 8. The main objective of the Democratic National Convention is to nominate the party's presidential candidate. Michael Saul, *Democratic National Convention 101*, DAILY NEWS (Aug. 21, 2008), http://www.nydailynews.com/news/politics/democratic-national-convention-101-article-1.317252 [http://perma.cc/78K9-2JV9].

and 8,034 attachments from high-ranking DNC officials.[62] The e-mails spanned from January 2015 to May 2016 and contained a number of important conversations.[63] For example, one e-mail showed party officials discussing a campaign strategy to undermine Clinton's main competitor for the Democratic presidential nomination, Bernie Sanders.[64] The e-mails also disclosed party donors' personal information including their addresses, credit card numbers, and even some passport and social security numbers.[65]

The hacks again incited chaos when, on October 6, 2016, DCLeaks published e-mails from Capricia Marshall's account.[66] Marshall worked closely with Clinton on her campaign and the e-mails thus divulged sensitive information about campaign efforts, including conversations with the media and networking strategies.[67]

The day after DCLeaks released Marshall's e-mails, WikiLeaks published the first batch in a series of fifty thousand e-mails from an account belonging to Clinton campaign chairman John Podesta.[68] At least some of

---

[62] Fishel & Stracqualursi, *supra* note 6; Hamburger & Tumulty, *supra* note 8; Robertson, *supra* note 59. Some of the high-ranking DNC officials involved were Communications Director Luis Miranda, National Finance Director Jordan Kaplan, and Finance Chief of Staff Scott Comer. Fishel & Stracqualursi, *supra* note 6; Hamburger & Tumulty, *supra* note 8; Robertson, *supra* note 59.

[63] Fishel & Stracqualursi, *supra* note 6; Hamburger & Tumulty, *supra* note 8; Robertson, *supra* note 59.

[64] *See* Hamburger & Tumulty, *supra* note 8 (quoting email from Marshall to Miranda discussing plan to publicly question Sanders' religious beliefs); Tobias Salinger, *Leaked DNC Email Floated Plan to Question Sanders' Religion*, N.Y. DAILY NEWS (July 23, 2016), http://www.nydailynews.com/news/politics/leaked-dnc-email-floated-plan-question-sanders-religion-article-1.2722203 [http://perma.cc/DB52-RWMQ] (quoting same email).

[65] Hamburger & Tumulty, *supra* note 8; Robertson, *supra* note 59.

[66] Rosalind S. Helderman & Tom Hamburger, *Hacked Emails Appear to Reveal Excerpts of Speech Transcripts Clinton Refused to Release*, WASH. POST (Oct. 7, 2016), https://www.washingtonpost.com/politics/hacked-emails-appear-to-reveal-excerpts-of-speech-transcripts-clinton-refused-to-release/2016/10/07/235c26ac-8cd4-11e6-bf8a-3d26847eeed4_story.html [http://perma.cc/L76P-ZQ9K]; Sainato, *supra* note 9. The e-mails were made publicly available at *Capricia Marshall*, DC LEAKS, http://dcleaks.com/index.php/portfolio_page/capricia-marshall/ [http://perma.cc/TN58-NXCC]. DCLeaks' website states that it was created by "American hacktivists" to collect, analyze, and publish e-mails from high-level officials. DCLEAKS, http://dcleaks.com/index.php/about/ [http://perma.cc/PQ36-KDC9]. There is strong evidence, however, that DCLeaks is actually managed by Russian hackers. *Does a Bear Leak in the Woods?*, THREATCONNECT (Aug. 12, 2016), https://www.threatconnect.com/blog/does-a-bear-leak-in-the-woods/ [http://perma.cc/9PQQ-YBMJ].

[67] Helderman & Hamburger, *supra* note 55; Sainato, *supra* note 9. For example, one e-mail from MSNBC News producer Sheara Braun to a Clinton campaign spokesman and Marshall detailed a weekly piece to "inform young people" about how Clinton is an "amazing, intelligent woman who probably faced more nonsense back in the day because she is a woman . . . ." Sainato, *supra* note 9.

[68] Eliza Collins, *Four of the Juiciest Leaked Podesta Emails*, USA TODAY (Oct. 13, 2016), http://www.usatoday.com/story/news/politics/onpolitics/2016/10/13/four-juiciest-leaked-podesta-emails/92014368/ [http://perma.cc/B6KW-M8G2]; Fishel & Stracqualursi, *supra* note 6; Kraw-

the e-mails brought the Clinton Campaign into disrepute.[69] For example, an email exchange between a Center for American Progress fellow and Clinton's Communications Director stated that conservatives are attracted to Catholicism due to "the systematic thought and severely backwards gender relations" and because "[t]heir rich friends wouldn't understand if they became evangelicals."[70]

On November 7, 2016—the day before the presidential election—WikiLeaks published thousands of additional e-mails from DNC officials.[71] This was yet another massive leak of information that should have been kept confidential, including an e-mail attachment regarding Clinton's efforts to raise millions of dollars for the United States to host a pavilion at the World Exposition 2010 Shanghai China.[72] According to the e-mail attachment, Clinton, as Secretary of State, ignored ethics guidelines in the process of soliciting donations for the U.S. pavilion and the donors later received "favorable treatment" from the U.S. Department of State.[73]

---

chenko et al., *supra* note 9. The e-mails were made publicly available at *The Podesta Emails*, WIKILEAKS, https://wikileaks.org/podesta-emails/ [http://perma.cc/8H3Q-DEGL].

[69] *See* Collins, *supra* note 68 (identifying four leaked e-mails that "reflect poorly on the campaign and raise question about relationships"); Krawchenko et al., *supra* note 9 (detailing numerous leaked e-mails, including some that reveal "a penchant for secrecy that has fueled questions about Clinton's trustworthiness"). Former New Hampshire Governor John H. Sununu stated on the Trump Campaign's behalf that the e-mails "revealed an underlying sense of religious bigotry." Collins, *supra* note 68. Other e-mails that brought the Clinton Campaign into disrepute: (1) indicated that Hillary Clinton unfairly received debate questions in advance; (2) disclosed information from the Department of Justice about upcoming hearings on the release of Secretary Clinton's State Department e-mails; (3) discussed soliciting support from "needy Latinos"; and (4) considered including jokes about Mrs. Clinton's private e-mail server into speeches. Collins, *supra* note 68; Krawchenko et al., *supra* note 9.

[70] Collins, *supra* note 68.

[71] Fishel & Stracqualursi, *supra* note 6; Haberman & Rappeport, *supra* note 9.

[72] '*Disregarded Ethics Guidelines': Clinton Document Raised Issues with 2010 Shanghai Expo*, FOX NEWS (Nov. 7, 2016), http://www.foxnews.com/politics/2016/11/07/disregarded-ethics-guidelines-clinton-document-raised-issues-with-2010-shanghai-expo.html [http://perma.cc/Q3L5-CYLD]. The World Exposition 2010 Shanghai China was a six-month event and had seventy million visitors. Kenneth Pletcher, *Expo Shanghai 2010*, ENCY. BRITANNICA, https://www.britannica.com/event/Expo-Shanghai-2010 [http://perma.cc/F2HN-L2MB]. Its goal was to highlight urban life using massive structures, or pavilions, which over 190 countries and 50 organizations constructed. *Id.* The Obama administration let construction plans for the U.S. pavilion fall to the wayside. Kim Ghattas, *Hillary Clinton Visits 'Her' Shanghai Expo Pavilion*, BBC NEWS (May 23, 2010), http://www.bbc.com/news/10142881 [http://perma.cc/8VV7-K6QA]. Secretary Clinton believed a U.S. pavilion was necessary to maintaining its relationship with China and took over the project. *Id.* The final product was heavily criticized: a "dull steel structure" with three short movies intended to portray the "American spirit." *Id.*

[73] *'Disregarded Ethics Guidelines,' supra* note 72; Richard Pollock, *WIKILEAKS: Campaign Manager Says "Clinton Had Little Consideration for Ethics,"* DAILY CALLER (Nov. 6, 2016), http://dailycaller.com/2016/11/06/wikileaks-campaign-manager-says-clinton-had-little-consideration-for-ethics/ [http://perma.cc/C54K-AZR4]. For example, Secretary Clinton influenced Russia to sign a multi-billion aircraft deal with The Boeing Company. Pollock, *supra*. Two days later, Boe-

On January 6, 2017, the Office of the Director of National Intelligence released an assessment laying out the conclusion that President of Russia Vladimir Putin "ordered an influence campaign" intentionally designed to challenge public confidence in the American democracy, destroy Clinton's credibility, and increase Trump's chances of winning the 2016 U.S. presidential election.[74] According to investigators, the Russian government directed its intelligence agencies to obtain information from U.S. campaign organizations, think tanks, and lobbying groups.[75] The assessment pinpointed Russia's Main Intelligence Directorate (known as the GRU) as responsible for breaching the DNC's computer network and using the Guccifer 2.0 persona, DCLeaks, and WikiLeaks to release the acquired data.[76]

In response to Russia's cyber attack on the DNC, U.S. President Barack Obama issued an Executive Order on December 28, 2016.[77] It amended an April 1, 2015 Executive Order, under which anyone found engaging in or responsible for certain cyber-enabled activities outside the United States would have their assets in the United States frozen and be prohibited from participating in business transactions in the United States.[78] Specifically, the April 1, 2015 Executive Order applied to cyber-enabled activities with the purpose or effect of "harming . . . a critical infrastructure sector," "causing a significant disrupt to the availability of a computer or

---

ing gave over two million dollars to the pavilion even though it was on a list of companies to avoid for donations because it would likely "be seen as an attempt to curry favor with American officials." *Id.* As an example of favorable treatment, Proctor & Gamble gave three million dollars to the pavilion and, allegedly, received the Secretary's Corporate Excellence Award from Mrs. Clinton in exchange. *Id.*

[74] OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *supra* note 14; Gilsinian & Calamur, *supra* note 15; Michael D. Shear & David E. Sanger, *Putin Led a Complex Cyberattack Scheme to Aid Trump, Report Finds*, N.Y. TIMES (Jan. 6, 2017), https://www.nytimes.com/2017/01/06/us/politics/donald-trump-wall-hack-russia.html [http://perma.cc/RS6W-5WT2].

[75] OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *supra* note 14.

[76] *Id.* The Main Intelligence Directorate, or GRU, is the Russian army's intelligence branch. Shaun Walker, *US Expulsions Put Spotlight on Russia's GRU Intelligence Agency*, THE GUARDIAN (Dec. 30, 2016), https://www.theguardian.com/world/2016/dec/30/us-expulsions-put-spotlight-on-russias-gru-intelligence-agency [http://perma.cc/6QC8-75SN].

[77] Gambino et al., *supra* note 11; Sanger, *supra* note 11; Wroughton, *supra* note 11; *see* Exec. Order No. 13,757, 82 Fed. Reg. 1 (Dec. 28, 2016) (responding to Russia's cyber attack).

[78] James Killick et al., *U.S. Expands Cyber-Related Sanctions Executive Order and Designates Russian Parties*, WHITE & CASE (Jan. 2, 2017), https://www.whitecase.com/publications/alert/us-expands-cyber-related-sanctions-executive-order-and-designates-russian-parties [http://perma.cc/5XKL-X66R]; *see* Exec. Order No. 13,757; Exec. Order No. 13,694, 80 Fed. Reg. 18,077 (Apr. 1, 2015). The April 1, 2015 Executive Order stated, in relevant part:

> All property and interests in property that are in the United States, that hereafter come within the United States, or that are or hereafter come within the possession or control of any United States person of the following persons are blocked and may not be transferred, paid, exported, withdrawn, or otherwise dealt in . . . .

Exec. Order No. 13,694, at 18,077.

network . . .” or “causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or financial gain.”[79]

The December 28, 2016 Executive Order expanded the list of cyber-enabled activities covered to include “tampering with, altering, or causing a misappropriation of information with the purpose or effect of interfering with or undermining election processes or institutions . . . .”[80] The December 28 Executive Order also explicitly identified five Russian entities (including the GRU) and four Russian individuals that violated the new provision.[81] Accordingly, their assets in the United States were frozen and they were barred from doing business with anyone in the United States.[82]

After issuing the December 28, 2016 Executive Order, President Obama announced that the U.S. Department of State declared thirty-five Russian diplomats and consular officials in the United States “persona non grata.”[83] Accordingly, the diplomats were expelled from the United States and given seventy-two hours to leave.[84] The U.S. Department of State also informed the Russian government that it could no longer access two compounds it owned in the United States.[85] According to U.S. officials, the Russians primarily used them to conduct intelligence activities.[86] Russian offi-

---

[79] *Id.*

[80] Exec. Order No. 13,757; Killick et al., *supra* note 72.

[81] Exec. Order No. 13,757. The five entities were: (1) Main Intelligence Directorate (a.k.a GRU); (2) Federal Security Service (a.k.a FSB); (3) Special Technology Center; (4) Zorsecurity; and (5) Autonomous Noncommercial Organization “Professional Association of Designers of Data Processing Systems.” *Id.* The four individuals were: (1) Igor Valentinovich Korobov; (2) Sergey Aleksandrovich Gizunov; (3) Igor Olegovich Kostyukov; and (4) Vladimir Stepanovich Alexseyev. *Id.*

[82] *Id.*

[83] Gambino et al., *supra* note 11; Sanger, *supra* note 11; Press Release, The White House, *supra* note 12.

[84] Gambino et al., *supra* note 11; Sanger, *supra* note 11; Press Release, The White House, *supra* note 12.

[85] Mark Mazzetti & Michael S. Schmidt, *Two Russian Compounds, Caught Up in History’s Echoes*, N.Y. TIMES (Dec. 29, 2016), https://www.nytimes.com/2016/12/29/us/politics/russia-spy-compounds-maryland-long-island.html [http://perma.cc/TSD8-3M7N]; Press Release, The White House, *supra* note 12; Killick et al., *supra* note 78. One of the compounds was a fourteen-acre property in Upper Brookville, New York known as “Norwich House.” Killick et al., *supra* note 78; Mazzetti & Schmidt, *supra*. The other was located along the Corsica River in Centreville, Maryland and included a three-story brick mansion, a swimming pool, a soccer field, and tennis courts. Killick et al., *supra* note 78; Mazzetti & Schmidt, *supra*.

[86] Daniella Diaz, *What Do We Know About the Russian Compounds in the US?*, CNN POL. (Dec. 30, 2016), http://www.cnn.com/2016/12/30/politics/russian-federation-compounds-what-do-we-know/ [http://perma.cc/6HRN-6C3S]; Mazzetti & Schmidt, *supra* note 85; Robert Windrem et al., *The Spy Next Door: What Went on in Russia’s Shuttered U.S. Compounds?*, NBC NEWS (Dec. 31, 2016), http://www.nbcnews.com/news/us-news/spy-next-door-what-went-russia-s-shuttered-u-s-n701581 [http://perma.cc/26EV-3PAT].

cials, however, insisted that the compounds were merely used as vacation homes for Russian diplomats.[87]

President Obama announced that the sanctions came after his administration issued multiple warnings to the Russian government and were a "necessary and appropriate response to efforts to harm U.S. interests in violation of established international norms of behavior."[88] He went on to give assurance that these actions were only the beginning of the U.S. response to Russia's hacks.[89] It was widely speculated that further U.S. action involved executing retaliatory hacks on Russian intelligence agencies.[90]

Russia openly condemned the sanctions, particularly because they were imposed just three weeks before President Obama was leaving office.[91] Specifically, a spokesperson for Russia President Vladimir Putin stated that the order was intended "to further harm Russian-American ties, which are at a low point as it is" and "deal a blow on the foreign policy plans of the incoming administration[.]"[92] Russia denied responsibility for the hacks and vowed to retaliate against the United States for imposing sanctions.[93]

---

[87] *See* Mazzetti & Schmidt, *supra* note 85 (describing the compounds as "[a] pair of luxurious waterfront compounds . . . [that] have for decades been a retreat for Russian diplomats, places to frolic in the water, play tennis and take lengthy steam baths" and noting that "Obama administration officials described the compounds differently: as beachside spy nests sometimes used by Russian intelligence operatives to have long conversations on the sand to avoid being snared by American electronic surveillance"); Andrey Rezchikov et al., *Russia Wants the Return of Its American Dachas Illegally Taken by Obama*, RUSS. BEYOND THE HEADLINES (Feb. 13, 2017), http://rbth.com/international/2017/02/13/russia-wants-the-return-of-its-american-dachas-illegally-taken-by-obama_701328 [http://perma.cc/66WW-H2J8] (noting that Russian diplomats used both compounds to host receptions and festivities, including Victory Day celebrations and New Year's parties for children); Adam Taylor, *The Luxurious, 45-Acre Compound in Maryland Being Shut Down for Alleged Russian Espionage*, WASH. POST (Dec. 29, 2016), https://www.washingtonpost.com/news/worldviews/wp/2016/12/29/the-luxurious-45-acre-compound-in-maryland-being-shut-down-for-alleged-russian-espionage/?utm_term=.239a51cee77d [http://perma.cc/TA7S-NHAR] (identifying a Russian ambassador that previously described one of the compounds as a "traditional Russian summer house, or dacha, he was used to back home" and quoting his wife as saying that they went there "to hide for a while" from their "hectic life").

[88] Press Release, The White House, *supra* note 12.

[89] *Id.*

[90] Lee Ferran, *The NSA Is Likely 'Hacking Back' Russia's Cyber Squads*, ABC NEWS (July 30, 2016), http://abcnews.go.com/International/nsa-hacking-back-russias-cyber-squads/story?id=41010651 [http://perma.cc/BQN8-QXHP]; Ellen Nakashima, *Obama Administration Is Close to Announcing Measures to Punish Russia for Election Interference*, WASH. POST (Dec. 27, 2016), https://www.washingtonpost.com/world/national-security/the-white-house-is-scrambling-for-a-way-to-punish-russian-hackers-via-sanctions/2016/12/27/0eee2fdc-c58f-11e6-85b5-76616a33048d_story.html?utm_term=.70fe81b3a3da [http://perma.cc/RWS5-BFZ6].

[91] Gambino et al., *supra* note 11; Sanger, *supra* note 11.

[92] David Jackson, *Obama Sanctions Russian Officials Over Election Hacking*, USA TODAY (Dec. 29, 2016), https://www.usatoday.com/story/news/politics/2016/12/29/barack-obama-russia-sanctions-vladimir-putin/95958472/ [http://perma.cc/5CG4-WLEV]; Sanger, *supra* note 11.

[93] Jackson, *supra* note 92; Sanger, *supra* note 11.

II. THE INTERNATIONAL LAWS AND PRINCIPLES UNDERLYING THE U.S. RESPONSE TO RUSSIA'S CYBER ATTACK

There is not a comprehensive, international legal framework that explicitly prohibits state-sponsored cyber attacks, let alone one that prescribes a punishment.[94] Consequently, in responding to Russia's cyber attack on the DNC, the United States was forced to rely on international laws and principles that were not directly applicable.[95] Specifically, the U.S. response involved the doctrine of retorsions, economic sanctions law and practice, and the Vienna Convention on Diplomatic Relations.[96] This Part discusses these international laws and principles generally and in the context of the U.S.

---

[94] Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CAL. L. REV. 817, 840–41 (2012); Duncan B. Hollis, *Why States Need an International Law for Information Operations*, 11 LEWIS & CLARK L. REV. 1023, 1037 (2007); Jens David Ohlin, *Did Russian Cyber Interference in the 2016 Election Violate International Law?*, 95 TEX. L. REV. 1579, 1579–80 (2017); Matthew J. Sklerov, Solving the Dilemma of State Responses to Cyber Attacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent 6 (Apr. 2009) (unpublished LL.M. thesis, The Judge Advocate General's School) (on file with the Homeland Security Digital Library). The only international law that address any form of cyber crime is the Convention on Cybercrime (also referred to as the Budapest Convention). The Council of Europe drafted the Convention on Cybercrime and submitted it for signatures in 2001. Hathaway et al., *supra*, at 862–63; *Chart of Signatures and Ratifications of Treaty 185*, COUNCIL OF EUR., https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=W4JU5WPj [http://perma.cc/3BGD-U4DR]. As of April 17, 2018, fifty-seven countries ratified it; the United States is one, Russia and China are not. *Chart of Signatures and Ratifications of Treaty 185, supra*. The Convention on Cybercrime requires states to criminalize a broad range of cyber crimes under domestic law including child pornography and copyright infringement. Convention on Cybercrime, Nov. 23, 2001, E.T.S. 185, T.I.A.S. 13174. It does not apply to government action, such as state-sponsored cyber attacks. Hathaway et al., *supra*, at 877; *see* Convention on Cybercrime, *supra*. There are arguments that Russia's cyber attack on the DNC violated an international law that does not explicitly address cyber crime, such as the right to self-determination—a country's right to structure their own government. Ohlin, *supra*.

[95] *See* Hathaway et al., *supra* note 94, 840–41(arguing that laws of war are extremely hard to apply to cyber attacks); Hollis, *supra* note 94, at 1037, 1039–40 (acknowledging that "there are no specific rules" for information operations such as cyber attacks and the laws of war apply by analogy); Sklerov, *supra* note 94 (recognizing that there is not a comprehensive treaty for international cyber attacks and states are forced to "practice law by analogy").

[96] *See* Philip Bump, *How to Be Declared 'Persona Non Grata' and Get Yourself Kicked Out of the United States*, WASH. POST (Dec. 29, 2016), https://www.washingtonpost.com/news/the-fix/wp/2016/12/29/how-to-be-declared-a-persona-non-grata-and-get-yourself-kicked-out-of-the-united-states/?utm_term=.bf73f6087adb [http://perma.cc/K6NJ-MHF2] (identifying U.S. reliance on the Vienna Convention on Diplomatic Relations ("VCDR") in responding to Russia's cyber attack); Ryan Goodman, *International Law and the US Response to Russian Election Interference*, JUST SECURITY (Jan. 5, 2017), https://www.justsecurity.org/35999/international-law-response-russian-election-interference/ [http://perma.cc/H8KM-DWMC] (identifying U.S. use of retorsions in responding to Russia's cyber attack); Greg Miller et al., *Obama's Secret Struggle to Punish Russia for Putin's Election Assault*, WASH. POST (June 23, 2017), https://www.washingtonpost.com/graphics/2017/world/national-security/obama-putin-election-hacking/?utm_term=.f24db992492e [http://perma.cc/QZT5-789X] (identifying U.S. use of economic sanctions in responding to Russia's cyber attack).

response to Russia's cyber attack on the DNC.[97] Section A of this Part explains the doctrine of retorsions.[98] Section B provides a detailed overview of economic sanctions.[99] Section C addresses the Vienna Convention on Diplomatic Relations.[100] Lastly, Section D shows how each of these international laws and principles were in play in the U.S. response to Russia's cyber attack on the DNC.[101]

A. Retorsions

Retorsions, or unfriendly acts taken consistently with the acting state's international obligations, have long been recognized as a remedy in international law.[102] They are often referred to as a form of "self-help," actions that states take to enforce their rights or protect their interests without authorization from an international organization.[103] Retorsions typically involve one state acting against another, but international organizations may use them or be subject to them.[104]

---

[97] *See infra* notes 102–189 and accompanying text.

[98] *See infra* notes 102–117 and accompanying text.

[99] *See infra* notes 118–145 and accompanying text.

[100] *See infra* notes 146–167 and accompanying text.

[101] *See infra* notes 168–189 and accompanying text.

[102] Int'l Law Comm'n, *Rep. on the Work of its Fifty-Third Session,* U.N. Doc. A/56/10, at 325 (2001); Tom Ruys, *Sanctions, Retorsions and Countermeasures: Concepts and International Legal Framework*, *in* RESEARCH HANDBOOK ON UN SANCTIONS AND INTERNATIONAL LAW 24 (Larissa van den Herik ed. 2017); THOMAS GIEGERICH, RETORSION, MAX PLANCK ENCY. OF PUB. INT'L L. ¶ 2; Joacquín Alcaide Fernández, *Countermeasures*, OXFORD BIBLIOGRAPHIES, http://www.oxfordbibliographies.com/view/document/obo-9780199796953/obo-9780199796953-0072.xml [http://perma.cc/86CN-TCBP] (last updated Oct. 29, 2013). Retorsions are distinguished from countermeasures, which have effectively replaced the nineteenth century idea of reprisals, or "acts of self-help by the injured State, acts in retaliation for acts contrary to international law on the part of the offending State, which have remained unredressed after a demand for amends." Ruys, *supra*, at 32; Matthias Ruffert, *Reprisals*, OXFORD PUB. INT'L L., http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1771 [http://perma.cc/3NMS-VDC8] (last updated Sept. 2015). Unlike retorsions, countermeasures are unlawful acts; they are *inconsistent* with the imposing state's international obligations, and *must* be taken in response to an international law violation. ECONOMIC SANCTIONS AND INTERNATIONAL LAW 42 (Matthew Happold & Paul Eden ed. 2016); Hathaway et al., *supra* note 94, at 845 n.109. The rules on countermeasures are mainly found in the Draft Articles on Responsibility of States for Internationally Wrongful Acts, which provide that an injured state may employ countermeasures in response to an "internationally wrongful act." Int'l Law Comm'n, *Rep. on the Work of Its Fifty-Third Session*, *supra*, at 324. In order for an act to be deemed "internationally wrongful," it must satisfy two conditions set forth in Article 2: (1) it must violate one of the perpetrating state's international obligations; and (2) the act must be attributable to the state against which countermeasures are sought. *Id.* at 68.

[103] Ruys, *supra* note 102, at 24; GIEGERICH, *supra* note 102, ¶ 1. State action taken without support from another state or an international organization is often called "unilateral" action. Richard B. Bilder, *The Role of Unilateral State Action in Preventing International Environmental Injury*, 14 VAND. J. TRANSNAT'L L. 51, 54 (1981).

[104] Ruys, *supra* note 102, at 24; GIEGERICH, *supra* note 102, ¶ 1.

International law does not explicitly restrain the use of retorsions and states generally view them as a right rather than a privilege.[105] In fact, an international law violation is not required to justify retorsions, but they sometimes succeed international law violations.[106] States enjoy wide discretion when imposing retorsions; the only real limitation is that they must be consistent with the imposing state's international obligations.[107]

What an individual state's international obligations are—and whether a certain act violates one of those obligations—is far from clear under the current international law framework.[108] Article 38 of the Statute of the International Court of Justice provides some guidance, identifying the primary sources of law as international conventions, international custom, general principles of law, and the judicial decisions and teachings from the most highly qualified publicists.[109] Given the ever-expanding regulatory breadth of international law and the constantly developing, complex relationships between countries, many states have countless international obligations that are difficult to ascertain.[110] Thus, the limitation that retorsions must be consistent with the acting state's international obligations is a significant and unclear one.[111]

---

[105] Ruys, *supra* note 102, at 24; GIEGERICH, *supra* note 102, ¶ 1; *see* Fernández, *supra* note 102 (stating that the doctrine of retorsions is not covered by the International Law Commission's work on international responsibility).

[106] CHARLES CHENEY HYDE, INTERNATIONAL LAW CHIEFLY AS INTERPRETED AND APPLIED BY THE UNITED STATES VOLUME II 169–70 (1922); Ruys, *supra* note 102, at 24; GIEGERICH, *supra* note 102, ¶ 1.

[107] Ruys, *supra* note 102, at 24; GIEGERICH, *supra* note 102, ¶¶ 1, 14. Retorsions are not legally required to be proportional to the act they are in response to. GIEGERICH, *supra* note 102, ¶ 14.

[108] MATH NOORTMANN, ENFORCING INTERNATIONAL LAW: FROM SELF-HELP TO SELF-CONTAINED REGIMES 44 (2016); *see* Ruys, *supra* note 102, at 24 (recognizing the difficulty "in determining whether or not certain measures do or do not amount to a breach of an international obligation of the State (or organization) engaging in them").

[109] Statute of the International Court of Justice art. 38. The Statute of the International Court of Justice (ICJ) is annexed to the United Nations (UN) Charter. *Basic Documents*, INT'L CT. OF JUST., http://www.icj-cij.org/en/basic-documents [http://perma.cc/44NN-7GYK]. The UN Charter established the ICJ as the UN's "principal judicial organ." U.N. Charter art. 92, 93 ¶ 1. The Statute of the ICJ sets forth the rules and procedures for the ICJ. *See* Statute of the International Court of Justice.

[110] *See* NOORTMANN, *supra* note 108 ("Considering the increasing sophistication of international regulation and law-making, the very question of whether a specific measure constitutes a violation of an international obligation or not is likely to become the very subject of the dispute."); Ruys, *supra* note 102, at 24 (determining whether an act is consistent with a state's international obligations may require "careful scrutiny . . . under relevant customary law, bilateral treaty law and multilateral treaty law").

[111] *See* NOORTMANN, *supra* note 108 (recognizing that "it is not easy to determine whether a specific measure violates a legal obligation in a given situation or not"); *see* Ruys, *supra* note 102, at 24 (recognizing the difficulty in determining whether certain measures are a breach of the imposing state's international obligations).

Nevertheless, certain retorsions are ordinarily considered legal, especially those by which the imposing state revokes a privilege that it was under no obligation to give at the outset.[112] For instance, retorsions may involve refusing access to ports, canceling diplomatic visits, and declaring diplomats "personas non grata."[113] They may also involve revoking international aid, recalling military assistance, or withdrawing from an international organization.[114] States usually cannot take more severe action without violating one of its international obligations.[115] For example, if a state were to impose a trade embargo or threaten military intervention, it would likely violate the principle of non-intervention or the prohibition on the threat or use of force set forth in Article 2(4) of the United Nations (UN) Charter.[116] Therefore, retorsions are typically a very mild form of retaliation, causing only minimal disruption to the receiving state's affairs.[117]

---

[112] *See* NOORTMANN, *supra* note 108 (acknowledging the ICJ's holding in *Nicaragua v. United States*); GIEGERICH, *supra* note 102, ¶ 10 (identifying retorsions which involve a state invoking a privilege such as denying ship access to ports and terminating economic aid). In *Nicaragua v. United States*, Nicaragua argued that the United States illegally intervened in its affairs in ceasing U.S. economic aid to Nicaragua out of vehement disapproval of the Nicaraguan government. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, 67 (June 27). The ICJ held, rather vaguely, that "the cessation of economic aid, the giving of which is more of a unilateral and voluntary nature, could be regarded as such a violation [of the obligation not to defeat the object and purpose of the treaty] only in exceptional circumstances." *Id.*

[113] Ruys, *supra* note 102, at 24; YONG ZHOU, INTERNATIONAL RELATIONS AND LEGAL COOPERATION IN GENERAL DIPLOMACY AND CONSULAR RELATIONS 336 (2014); GIEGERICH, *supra* note 102, ¶ 10.

[114] ZHOU, *supra* note 113; GIEGERICH, *supra* note 102, ¶ 10.

[115] Ruys, *supra* note 102; *see* GIEGERICH, *supra* note 102, ¶ 24 ("Even though a specific measure of retorsion does not as such violate international law, its use for an illegitimate end, namely an intervention, will render it unlawful if its coercive force is strong enough to pose a serious threat to the self-determination of the target State . . . .").

[116] Ruys, *supra* note 102; *see* GIEGERICH, *supra* note 102, ¶ 25 (recognizing that interrupting the supply of critical goods to another state is illegal). The customary international principle of non-intervention was codified in the UN General Assembly's 1965 Declaration on the Inadmissibility of Intervention and Interference in the Domestic Affairs of States. William Mattesich, *Digital Destruction: Applying the Principle of Non-Intervention to Distributed Denial of Service Attacks Manifesting No Physical Damage*, 54 COLUM. J. TRANSNAT'L L. 873, 879–80 (2016); Carolyn Dubay, *A Refresher on the Principle of Non-Intervention*, INT'L JUDICIAL MONITOR (2014), http://www.judicialmonitor.org/archive_spring2014/generalprinciples.html [http://perma.cc/EX7J-XF86]. There, the principle of non-intervention is formulated as: "[n]o State has the right to intervent, directly or indirectly, for any reason whatsoever, in the internal or external affairs of any other State." G.A. Res. 36/103 (Dec. 9, 1981). Article 2(4) of the UN Charter declares that "[a]ll Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations." U.N. Charter art. 2, ¶ 4.

[117] GBENGA ODUNTAN, INTERNATIONAL LAW AND BOUNDARY DISPUTES IN AFRICA 326 (2015); GIEGERICH, *supra* note 102, ¶ 29.

B. Economic Sanctions

Like retorsions, sanctions are measures intended to enforce states' rights or protect their interests.[118] In fact, sanctions are often confused with retorsions or considered an umbrella term that includes retorsions.[119] Unlike retorsions, though, sanctions are not usually defined as limited to actions that are consistent with the state's international obligations.[120] There is, however, not a widely agreed upon definition of the term "sanctions" and there are at least three different ways of defining it.[121]

The first way is to broadly define sanctions as any action, whether taken by a state or institution, "against a State to compel it to obey international law or to punish it for a breach of international law."[122] The second is much narrower: sanctions are the UN Security Council's actions pursuant to Article 41 of the UN Charter.[123] A number of scholars embrace a third, more middle ground approach, recognizing sanctions as any international organizations' actions taken against its members and in accordance with its rules.[124]

---

[118] Natalino Ronzitti, *Conclusion, in* COERCIVE DIPLOMACY, SANCTIONS AND INTERNATIONAL LAW 287 (Natalino Ronzitti ed. 2016); *see* Ruys, *supra* note 102, at 22–23 (recognizing "sanction" as referring to a certain type of measure to "(i) coerce or change behavior; (ii) to constrain access to resources needed to engage in certain activities; or (iii) to signal and stigmatize").

[119] CHRISTINA ECKES, EU COUNTER-TERRORIST POLICIES AND FUNDAMENTAL RIGHTS: THE CASE OF INDIVIDUAL SANCTIONS 16 (2009); *see* JAN KLABBERS, INTERNATIONAL LAW 183 (2017) (describing retorsions as "the most ubiquitous of sanctions"); Hans-Martien ten Napel, *The Concept of International Crimes of States: Walking the Thin Line Between Progressive Development and Disintegration of the International Legal Order*, 1 LEIDEN J. INT'L L. 149, 151 (1988) (describing retorsions as individual sanctions).

[120] *See* KLABBERS, *supra* note 119, at 183 ("[W]hat characterizes the retorsion is that it remains within the law"); ALAIN PELLET & ALINA MIRON, SANCTIONS, MAX PLANCK ENCY. OF PUB. INT'L L., ¶ 4 (declining to limit sanctions to actions consistent with a state's international obligations).

[121] Ruys, *supra* note 102, at 19–22; Clara Portela, *The EU's Use of 'Targeted Sanctions'* 3 (CEPS, Working Paper No. 391, 2014); Boris Kondoch, *Sanctions in International Law*, OXFORD BIBLIOGRAPHIES, http://www.oxfordbibliographies.com/view/document/obo-9780199743292/obo-9780199743292-0191.xml#obo-9780199743292-0191-bibItem-0002 [http://perma.cc/Z8ZW-4DYN] (last updated Sept. 28, 2016).

[122] Ruys, *supra* note 102, at 19 *(*quoting *Sanctions*, A DICTIONARY OF LAW (Johnathan Law ed. 2015)); *see* PELLET & MIRON, *supra* note 120, ¶ 4 (defining sanctions broadly as "all types of consequences triggered by the violation of an international legal rule").

[123] Ruys, *supra* note 102, at 20; PELLET & MIRON, *supra* note 120, ¶ 11; *see* U.N. Charter art. 41 ("The Security Council may decide what measures not involving the use of armed force are to be employed to give effect to its decisions . . . . These may include complete or partial interruption of economic relations and of . . . means of communication, and the severance of diplomatic relations.").

[124] Ruys, *supra* note 102, at 21; Michael Brzoska, *International Sanctions Before and Beyond UN Sanctions*, 91 INT'L AFF. 1339, 1345 (2015); PELLET & MIRON, *supra* note 120, ¶ 10; *see* Kondoch, *supra* note 121 (recognizing a common understanding that sanctions "refers to the multilateral measures adopted by states through the United Nations or another international organization").

Under any definition, sanctions may take a variety of forms including trade embargos, travel bans, and asset freezes.[125] Sanctions may also serve a number of different purposes.[126] For instance, they may be designed to alter behavior, inhibit access to resources, or send a message.[127] Furthermore, sanctions may be specifically targeted to affect only certain individuals deemed responsible for objectionable activity, rather than broadly affecting a country's population as a whole.[128]

Sanctions imposed today are most frequently in the category of "economic sanctions."[129] "Economic sanctions" are sometimes defined as the "deliberate, government inspired withdrawal, or threat of withdrawal, of customary trade or financial relations."[130] For instance, economic sanctions may take the form of freezing or seizing assets, trade embargoes, tariff increases, or bans on cash transfers.[131]

Economic sanctions have a long and contentious history.[132] The UN Charter merely states that the UN Security Council may impose economic and certain other sanctions, but is silent as to whether individual states may impose sanctions.[133] Nevertheless, many argue that economic sanctions are contrary to international law because they are coercive to an extent that they

---

[125] Ruys, *supra* note 102, at 21; Brzoska, *supra* note 124, at 1343–45; Meredith Rathbone et al., *Sanctions, Sanctions Everywhere: Forging a Path Through Complex Transnational Sanctions Laws*, 44 GEO. J. INT'L L. 1055, 1057 (2013).

[126] Ruys, *supra* note 102, at 22; Jonathan Masters, *What Are Economic Sanctions?*, COUNCIL ON FOREIGN REL., https://www.cfr.org/backgrounder/what-are-economic-sanctions [http://perma.cc/ATR7-KHEX] (last updated Aug. 7, 2017).

[127] Ruys, *supra* note 102, at 22–23; Masters, *supra* note 126.

[128] Portela, *supra* note 121, at 4; Gary Clyde Hufbauer & Barbara Oegg, *Targeted Sanctions: A Policy Alternative*, PETERSON INST. FOR INT'L ECON. (Feb. 23, 2000), https://piie.com/commentary/speeches-papers/targeted-sanctions-policy-alternative [http://perma.cc/5JMV-2V99]. Sanctions specifically targeted to affect only certain individuals are sometimes referred to as "smart sanctions." Portela, *supra* note 121, at 4; Hufbauer & Oegg, *supra*.

[129] Paul Szasz, *The Law of Economic Sanctions*, *in* 71 INTERNATIONAL LAW STUDIES 455; BARRY E. CARTER, ECONOMIC SANCTIONS, MAX PLANCK ENCY. OF PUB. INT'L L., ¶ 33.

[130] GARY CLYDE HUFBAUER ET AL., ECONOMIC SANCTIONS RECONSIDERED 3 (3d ed. 2009).

[131] Barry Klodokin, *What Are Sanctions?*, THOUGHTCO., https://www.thoughtco.com/what-are-sanctions-3310373[http://perma.cc/TL3N-C8N2] (last updated May 15, 2017); Masters, *supra* note 126.

[132] CARTER, *supra* note 129, ¶ 7; *see* Szasz, *supra* note 129, at 455 (acknowledging that there are numerous instances in which economic sanctions have been imposed with questionable effectiveness and legal issues). Economic sanctions were imposed as early as 432 B.C. when Pericles limited the entry of products from Megara, Greece to Athens, Greece in retaliation for Megara adding new territory and kidnapping three women. CARTER, *supra* note 129, ¶ 7. In the years since then, states have continued to impose economic sanctions to achieve various, and often controversial, objectives such as inciting a governmental regime change, interfering with a state's development of nuclear weapons, protecting human rights, and fighting terrorism. *Id.*

[133] UN Charter art. 41; Mergen Doraev, *The "Memory Effect" of Economic Sanctions Against Russia: Opposing Approaches to the Legality of Unilateral Sanctions Clash Again*, 37 U. PA. J. INT'L L. 355, 373–74 (2015).

are a prohibited use of force under Article 2(4) of the UN Charter and violate the customary international law principle of non-intervention.[134] Accordingly, the UN General Assembly has adopted a number of resolutions in attempt to bar states from imposing economic measures—including both sanctions and retorsions—without UN authorization.[135] One such resolution is the 1965 "Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty."[136] This resolution prohibited states from coercing another state using economic, political, or other measures to interfere with its sovereignty or receive a benefit.[137] A similar resolution was adopted in 1995 and entitled "Economic Measures as a Means of Political and Economic Coercion against Developing Countries."[138] There, the UN General Assembly strongly encouraged states to adopt urgent and effective measures to cease employing coercive measures against developing countries that are not authorized by the UN or are inconsistent with the UN Charter.[139] Even if these UN resolutions are not binding upon UN member states, the international community has repeatedly acknowledged that economic sanctions are illegal.[140]

These resolutions and other organizational attempts to limit the use of economic sanctions were largely unsuccessful.[141] Many only bind a few states, contain vague or overly broad provisions, or lack an effective enforcement mechanism.[142] Many states, especially the United States, routinely impose economic sanctions on their own accord without formal consequences.[143] Economic sanctions thus remain an optimal yet legally dubious choice for states and international organizations seeking to pressure, punish,

---

[134] Szasz, *supra* note 129, at 456; CARTER, *supra* note 129, ¶¶ 12–13.

[135] *See* G.A. Res. 46/210, ¶ 1 (Dec. 20, 1991); G.A. Res. 2131 (XX), ¶ 2 (Dec. 21, 1965); Szasz, *supra* note 129, at 456.

[136] G.A. Res. 2131, *supra* note 135; Szasz, *supra* note 129, at 457.

[137] G.A. Res. 46/210, *supra* note 135.

[138] *Id.*; Szasz, *supra* note 129, at 457.

[139] G.A. Res. 46/210, *supra* note 135; Szasz, *supra* note 129, at 457.

[140] Doraev, *supra* note 133, at 376–77; *see* Szasz, *supra* note 129, at 458 (noting that the international community has adopted strong resolutions of condemnation of the U.S. economic sanctions on Cuba).

[141] CARTER, *supra* note 129, ¶ 18; *see* Szasz, *supra* note 129, at 455, 458 (stating that economic sanctions are widely used even though states cannot claim a general legal right to impose them).

[142] CARTER, *supra* note 129, ¶ 13; *see* HUFBAUER ET AL., *supra* note 130, at 139–40 (noting that the UN does not have a military to enforce its arms embargos and UN resolutions on arms embargos are vague).

[143] *See* CARTER, *supra* note 129, ¶ 33 (acknowledging that "[e]conomic sanctions have become a fact of international life and a tool of international diplomacy" and "[e]fforts . . . to somehow limit these sanctions under the UN Charter or customary international law made little headway"); Masters, *supra* note 126 (acknowledging that economic sanctions are widely used and, although U.S. sanctions have evoked anger, the United States was never formally reprimanded).

or shame states.[144] This is mainly due to their cost-efficient, low-risk nature—not necessarily their effectiveness which is generally inconsistent and intensely debated.[145]

C. The Vienna Convention on Diplomatic Relations

The Vienna Convention on Diplomatic Relations ("VCDR") was signed in 1961 and nearly all countries have agreed to be bound to it.[146] It culminated the effort to codify customary international law on diplomatic relations between states.[147] The VCDR now serves as a comprehensive framework for creating, maintaining, and ceasing diplomatic relations on a consensual basis.[148]

Under Article 9 of the VCDR, a state is allowed to pronounce a diplomat it has received into its territory "persona non grata."[149] States' right to

---

[144] CARTER, *supra* note 129, ¶ 33; Masters, *supra* note 126; *see* Doraev, *supra* note 133, at 388 ("[T]he United States historically considers economic sanctions as a legitimate tool of its foreign policy . . . . Nevertheless, although this practice might be supported by the ancient 'Lotus principle' that a state is permitted to do everything, which is not affirmatively prohibited, the United States prefers to keep a distance from debates on the legality of sanctions.").

[145] CARTER, *supra* note 129, ¶ 33; Richard N. Haass, *Economic Sanctions: Too Much of a Bad Thing*, BROOKINGS (June 1, 1998), https://www.brookings.edu/research/economic-sanctions-too-much-of-a-bad-thing/ [http://perma.cc/7SPZ-58JG] ("In a global economy, unilateral sanctions tend to impose greater costs on American firms than on the target, which can usually find substitute sources of supply and financing."); Masters, *supra* note 126.

[146] *Vienna Convention on Diplomatic Relations*, AM. SOC'Y INT'L L., https://www.asil.org/eisil/vienna-convention-diplomatic-relations [http://perma.cc/4YM5-W3UG] [hereinafter *VCDR,* AM. SOC'Y INT'L L.]; Jan Wouters & Sanderjin Duquet, *The Vienna Conventions on Diplomacy and Consular Relations*, OXFORD BIBLIOGRAPHIES, http://www.oxfordbibliographies.com/view/document/obo-9780199743292/obo-9780199743292-0112.xml [http://perma.cc/97GQ-XDH9] (last updated Jan. 11, 2018). As of August 16, 2017, the VCDR has 191 parties. *Vienna Convention on Diplomatic Relations*, UN TREATY COLLECTION, https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=III-3&chapter=3&lang=en [http://perma.cc/9MEF-FXEW].

[147] *VCDR,* AM. SOC'Y INT'L L., *supra* note 146; Wouters & Duquet, *supra* note 146.

[148] *VCDR,* AM. SOC'Y INT'L L., *supra* note 146; Wouters & Duquet, *supra* note 146. The VCDR is similar to the Vienna Convention on Consular Relations ("VCCR"), which was signed in 1963. Wouters & Duquet, *supra* note 146. Whereas the VCDR pertains to diplomats, the VCCR governs consuls. *Id.* Both diplomats and consuls are representative of foreign governments, but consuls receive less extensive immunities under the VCCR than diplomats under the VCDR. Cami Green, *Counsel, Consul, or Diplomat: Is There Any Practical Significance for Practitioners?*, 1 U. MIAMI INT'L & COMP. L. REV. 143, 148–49 (1991). Whether a foreign representative is a diplomat or consular is usually determined simply by how the receiving state identifies them. *Id.* at 149.

[149] Vienna Convention on Diplomatic Relations, Apr. 18, 1961, 23 U.S.T. 3227, 3233–34, 500 U.N.T.S. 95, 102 [hereinafter VCDR]; CRAIG BARKER, INTERNATIONAL LAW AND INTERNATIONAL RELATIONS 167 (2000). Article 9 of the VCDR is as follows:

> 1. The receiving State may at any time and without having to explain its decision, notify the sending State that the head of the mission or any member of the diplomatic staff of the mission is persona non grata or that any other member of the staff of the mission is not acceptable.

declare a diplomat "persona non grata" pre-dates the VCDR and is one of the most ancient principles of diplomatic law.[150] In declaring a diplomat "persona non grata," the diplomat is "not acceptable" and the state that sent the diplomat must "recall the person concerned or terminate his functions with the mission."[151]

Article 9 of the VCDR does not entitle the receiving state to physically remove the diplomat.[152] Rather, the sending state must tell them to return.[153] If, for whatever reason, the diplomat does not leave within a reasonable time, the receiving state may treat them as any other foreign individual—that is, without diplomatic immunity or privileges.[154] Aside from these procedural limitations, states have free-reign to declare diplomats "persona non grata"; they can make the declaration at any time, for any reason.[155] The right is not susceptible to abuse, because in reality, its exercise minimally disrupts the sending state's affairs, merely requiring them to ensure that the unwelcome diplomat departs and perhaps reorganize the diplomatic mission to some extent.[156]

Although the VCDR permits a state to expel foreign diplomats, it heavily restricts a state's ability to interfere with the premises of a diplomat-

---

> 2. If the sending state refuses or fails within a reasonable period to carry out its obligations under paragraph 1 of this article, the receiving State may refuse to recognize the person concerned as a member of the mission.

VCDR, *supra*.

[150] Amer Fakhoury, *Persona Non Grata: The Obligation of Diplomats to Respect the Laws and Regulations of the Hosting State*, 57 J.L. POL'Y & GLOBALIZATION 110, 111 (2017); JEAN D'ASPREMONT, PERSONA NON GRATA, MAX PLANCK ENCY. OF PUB. INT'L L., ¶ 1 [hereinafter PERSONA NON GRATA].

[151] VCDR, *supra* note 149, 23 U.S.T. at 3233–34, 500 U.N.T.S. at 102.

[152] *Id.*; PERSONA NON GRATA, *supra* note 150, ¶¶ 10, 12.

[153] VCDR, *supra* note 149, 23 U.S.T. at 3233–34, 500 U.N.T.S. at 102; PERSONA NON GRATA, *supra* note 150, ¶ 12; *VCDR,* AM. SOC'Y INT'L L., *supra* note 146.

[154] VCDR, *supra* note 149, 23 U.S.T. at 3234, 500 U.N.T.S. at 102; PERSONA NON GRATA, *supra* note 150, ¶¶ 12–13. Forty-eight hours is typically considered a reasonable time after which a diplomat declared "persona non grata" must leave the receiving state. PERSONA NON GRATA, *supra* note 150, ¶ 13.

[155] *Id.* ¶ 5; *see* VCDR, *supra* note 149, 23 U.S.T. at 3233–34, 500 U.N.T.S. at 102 (providing that states may declare a diplomat "persona non grata" at any time and without explanation).

[156] *See* BARKER, *supra* note 149, at 168 (showing that the right is not susceptible to abuse because states are strongly hesitant to declare diplomats "persona non grata," likely because they fear retaliatory action); PERSONA NON GRATA, *supra* note 150, ¶ 14 (showing that the right is not susceptible to abuse because diplomats declared "persona non grata" are not "automatically dismissed" and "[i]t is incumbent upon the sending State to decide on the ensuing career of the agent concerned"). Although the declaration of "persona non grata" declaration is considered a powerful and controversial one, it is mainly the unwelcome diplomat that feels its effects, rather than the sending state's government. *See* Bump, *supra* note 96; PERSONA NON GRATA, *supra* note 150, ¶¶ 16–17.

ic mission such as embassies or consulates.[157] The idea that diplomatic premises are protected is central to diplomatic law and was widely recognized as early as the eighteenth century.[158] In the VCDR, the premises of a diplomatic mission are expansively defined as "the buildings or parts of buildings and the land ancillary thereto, irrespective of ownership, used for the purposes of the mission including the residence of the head of the mission."[159] In particular, Article 22 of the VCDR plainly states that "[t]he premises of the mission shall be inviolable" and "their furnishings and other property thereon . . . shall be immune from search, requisition, attachment or execution."[160] Article 30 extends the same inviolability and protection granted to premises of diplomatic missions to a diplomatic agent's private residence.[161] The VCDR does not prescribe a punishment for a violation of its terms, other than that a state may expel diplomats and sever all diplomatic relations with the offending state.[162] The offended state has the option to appeal to the world's primary judicial body—the International Court of Justice (ICJ). [163] States rarely pursue this option, however.[164] The ICJ must agree to hear the case and have jurisdiction over the parties, which is not automatic. [165] Even if the ICJ hears the case and finds in the offended state's favor, its decisions are often not adhered to and it lacks an effective en-

---

[157] *See* VCDR, *supra* note 149, 23 U.S.T. at 3233–34, 3237, 500 U.N.T.S. at 102, 106 (recognizing right to expel diplomats and heavily restricting interference with diplomatic premises); *see also* United States Diplomatic and Consular Staff in Tehran (U.S. v. Iran), Judgment, 1980 I.C.J. Rep. 64, ¶ 62 (May 24) (recognizing the inviolability of diplomatic premises under the VCDR).

[158] ERNEST MASON SATOW, SATOW'S DIPLOMATIC PRACTICE 101 (6th ed. 2009); JEAN D'ASPREMONT, PREMISES OF DIPLOMATIC MISSIONS, MAX PLANCK ENCY. OF PUB. INT'L L., ¶ 1 [hereinafter PREMISES OF DIPLOMATIC MISSIONS].

[159] VCDR, *supra* note 149, 23 U.S.T. at 3231, 500 U.N.T.S. at 98.

[160] *Id.* at 3237, 500 U.N.T.S. at 106.

[161] *Id.* at 3240, 500 U.N.T.S. at 110.

[162] *See* VCDR, *supra* note 149, 23 U.S.T. at 3233–34, 500 U.N.T.S. at 102 (permitting states to declare diplomats "persona non grata" and sever diplomatic relations).

[163] David A. Koplow, *Indisputable Violations: What Happens When the United States Unambiguously Breaches a Treaty?*, 37 FLETCHER F. WORLD AFF. 53, 54–55 (2013); *see* Tehran, 1980 I.C.J. Rep., ¶¶ 62–63 (deciding case between Iran and United States regarding VCDR violations, including the inviolability of premises provision).

[164] *See* Koplow, *supra* note 163, at 54–55 (noting that the ICJ resolves only two to three cases a year and it does not have automatic jurisdiction); S. Gozie Ogbodo, *An Overview of the Challenges Facing the International Court of Justice in the 21st Century*, 18 ANN. SURV. OF INT'L & COMP. L. 93, 107 (2012) (identifying that four out of five permanent Security Council members have rejected the ICJ's compulsory jurisdiction, severely reducing its power and influence).

[165] *See* Koplow, *supra* note 163, at 54–55 (noting that the ICJ does not have automatic jurisdiction over the United States, Russia, and other key international actors); *Basis of the Court's Jurisdiction*, INT'L CT. OF JUST., http://www.icj-cij.org/en/basis-of-jurisdiction [http://perma.cc/MH4T-DDFS] (identifying the ways in which the ICJ is granted jurisdictional authority, which are based on consent of the states involved in contentious proceedings).

forcement mechanism.[166] Consequently, many international law violations go unpunished.[167]

D. The Legality of the U.S. Response to Russia's Cyber Attack

President Obama's press release in conjunction with the December 29, 2016 Executive Order referred to the measures taken against Russia in response to its cyber attack on the DNC as "sanctions."[168] The United States, however, imposed the measures without support from the UN Security Council or other international organization and therefore do not qualify as sanctions under the two more restrictive definitions.[169] Even under the broadest definition of sanctions as "any action against a State to compel it to obey international law or to punish it for a breach of international law," the U.S. measures fall short.[170] The Obama Administration did not state whether Russia's cyber attack violated international law, only that it violated "established international norms of behavior."[171] This is not a distinction without a difference, as the term "international norms" does not indicate an international legal obligation.[172]

---

[166] *See, e.g.*, Amuda-Kannike Abiodun et al., *An Examination of the Enforcement of ICJ Decisions Through Regional Organizations and Specialized Agencies*, 59 J.L. POL'Y & GLOBALIZATION 21, 21 (2017) (stating that ICJ enforcement is inadequate); Aloysius P. Llamzon, *Jurisdiction and Compliance in Recent Decisions of the International Court of Justice*, 18 EUR. J. INT'L L. 815, 825–44 (detailing five recent instances of non-compliance with ICJ decisions). *But see* PHILIPPE COUVREUR, THE INTERNATIONAL COURT OF JUSTICE AND THE EFFECTIVENESS OF INTERNATIONAL LAW 80 n.128 (2016) (noting that non-compliance with the ICJ's decisions is "extremely rare" but acknowledging a number of cases of non-compliance); *How the Court Works*, INT'L CT. OF JUST., http://www.icj-cij.org/en/how-the-court-works [http://perma.cc/37DJ-D2EY] (explaining that it is rare for an ICJ decision to go unimplemented because cases have to be submitted and parties have to consent to jurisdiction).

[167] *See* Abram Chayes & Antonia Handler Chayes, *On Compliance*, 47 INT'L ORG. 175, 197–201 (1993) (recognizing that the international legal system tolerates a lot of non-compliance); Koplow, *supra* note 163, at 54–55 (pointing out that treaty violations are often inconclusive).

[168] Press Release, The White House, *supra* note 12.

[169] *See* Exec. Order No. 13,757 (taking measures pursuant to U.S. law only); Ruys, *supra* note 102, at 20–21 (identifying two more restrictive definitions of sanctions).

[170] Ruys, *supra* note 102, at 19 (quoting *Sanctions*, *supra* note 122); *see* Goodman, *supra* note 96 (recognizing that the question of whether Russia violated international law is irrelevant to determining the legality of the U.S. measures against Russia because they were retorsions); Patrick Tucker, *Did Russia's Election Meddling Break International Law? Experts Can't Agree*, GOV'T EXEC. (Feb. 8, 2017), http://www.govexec.com/technology/2017/02/did-russias-election-meddling-break-international-law-experts-cant-agree/135260/ [http://perma.cc/DW77-B7SA] (recognizing the U.S. expulsion of diplomats and economic measures as retorsions).

[171] Press Release, The White House, *supra* note 12; Goodman, *supra* note 96.

[172] Goodman, *supra* note 96; *see* Jelena Cupac, *Emerging International Norms and State Behavior: Chinese Foreign Policy Between "Pluraist Pull" and "Solidarist Push*,*"* 9 CEU POL. SCI. J. 39, 39–40 (recognizing international norms of behavior as "ingredients of international politics").

In actuality, the United States largely executed its response to Russia pursuant to the doctrine of retorsions, unfriendly acts that do not violate the acting state's international obligations.[173] Although retorsions are the most unregulated mode of international response, the United States had numerous international legal obligations in responding to Russia's cyber attack, including the VCDR and the prohibition on imposing coercive economic measures without support from an international organization.[174] Pursuant to Article 9 of the VCDR, the United States was undoubtedly permitted to declare thirty-five Russian diplomats "personas non grata."[175] It is less clear, though, whether the United States acted consistently with its international obligations when closing two Russian compounds on U.S. territory and taking economic measures against certain Russian entities and individuals.[176]

In regards to the U.S. closure of two Russian compounds, Article 22 of the VCDR prohibited it if the compounds were "premises of a mission."[177] Media reports conflicted as to whether the two Russian compounds were mainly used as surveillance outposts for Russian spies or as vacation homes for Russian diplomats.[178] Either way, the two compounds were reasonably considered protected premises under the VCDR.[179] The VCDR defines "premises of the mission" quite broadly, extending it to any building and the land connected with it used for "the purposes of the mission."[180] In fact, records showed that at least one of the compounds received a partial tax

---

[173] Int'l Law Comm'n, *Report on the Work of Its Fifty-Third Session*, *supra* note 102, at 325; Goodman, *supra* note 96; Tucker, *supra* note 170.

[174] Ruys, *supra* note 102, at 24; Doraev, *supra* note 133, at 376–77; GIEGERICH, *supra* note 102, ¶ 1.

[175] Bump, *supra* note 96; *see* VCDR, *supra* note 149, 23 U.S.T. at 3233–34, 500 U.N.T.S. at 102 (establishing right to declare diplomats "personas non grata").

[176] *See* VCDR, *supra* note 149, 23 U.S.T. at 3237, 500 U.N.T.S. at 106 (recognizing inviolability of premises of diplomatic missions); Doraev, *supra* note 133, at 376–77 (recognizing customary international law prohibition on coercive, economic measures imposed unilaterally); Press Release, The White House, *supra* note 12 (announcing closure of two Russian compound on U.S. territory and economic measures against four Russian entities and five Russian individuals).

[177] *See* VCDR, *supra* note 149, 23 U.S.T. at 3237, 500 U.N.T.S. at 106 (recognizing inviolability of premises of diplomatic missions); Rezchikov et al., *supra* note 87 (quoting Professor Dmitry Labin of Moscow State Institute of International Relations as stating that the VCDR "establishes the immunity of a state and its property used for [diplomatic purposes]" and the U.S. seizure of the Russian compounds was "a blatant violation" of the VCDR).

[178] *See* Diaz, *supra* note 86 (describing Russian compounds as quiet); Mazzetti & Schmidt, *supra* note 85 (describing Russian compounds as "luxurious waterfront compounds" used as "a retreat for Russian diplomats"); Windrem et al., *supra* note 86 (describing Russian compounds as "festooned with all manner of antenna for capturing communications" and having "clear electronic views of several critical U.S. facilities").

[179] *See* VCDR, *supra* note 149, 23 U.S.T. at 3231, 500 U.N.T.S. at 98 (defining "premises of the mission"); Rezchikov et al., *supra* note 87 (arguing that the Russian compounds were protected premises under the VCDR).

[180] VCDR, *supra* note 149, 23 U.S.T. at 3231, 500 U.N.T.S. at 98.

exemption due to its status as a government embassy, which is typically considered a protected diplomatic premises under Article 22 of the VCDR.[181] The VCDR does not define what constitutes "purposes of the mission" and does not expressly require that the premises be used solely for "purposes of the mission."[182] The phrase therefore arguably encompasses both surveillance and vacationing, and likely neither served as the sole purpose of the Russian compounds.[183] Alternatively, the Russian compounds could have been rendered inviolable under Article 30 because they were "[t]he private residence of a diplomatic agent," which the VCDR also does not define.[184] It was therefore highly likely that the United States acted contrary to its international law obligations under the VCDR in closing the two Russian compounds.[185]

Similarly, the U.S. economic measures taken against Russia were in conflict with UN resolutions prohibiting the use of coercive, economic measures without UN authorization.[186] The U.S. measures are reasonably deemed coercive to the extent that they were aimed at changing Russian policies, such as those regarding cyber surveillance.[187] The United States

---

[181] Tehran, 1980 I.C.J. Rep., ¶ 19; Diaz, *supra* note 86.

[182] *See* VCDR, *supra* note 149, 23 U.S.T. at 3231, 500 U.N.T.S. at 98 (neglecting to define "purposes of the mission"); PREMISES OF DIPLOMATIC MISSIONS, *supra* note 158, ¶ 17 (noting that conducting activities contrary to diplomatic missions, such as smuggling, on diplomatic premises does not affect inviolability).

[183] *See* VCDR, *supra* note 149, 23 U.S.T. at 3231, 500 U.N.T.S. at 98 (neglecting to define "purposes of the mission"); PREMISES OF DIPLOMATIC MISSIONS, *supra* note 158, ¶ 17 (recognizing that diplomatic premises may be used for non-diplomatic purposes and remain inviolable); Diaz, *supra* note 86 (providing accounts of the Russian compounds as being used for surveillance and vacationing). "Purposes of the mission" in the VCDR could be construed to include vacation homes for diplomats because diplomatic missions often serve to maintain the sending state's presence in that country. *See* VCDR, *supra* note 149, 23 U.S.T. at 3231, 500 U.N.T.S. at 98 (identifying "functions of a diplomatic mission" as including "[r]epresenting the sending State in the receiving State"). Surveillance could also reasonably be considered a "purpose of the mission"; illicit or questionable activities do not impact the inviolability of the premises of a mission. PREMISES OF DIPLOMATIC MISSIONS, *supra* note 158, ¶ 17. Also, even if vacationing and surveillance are not proper purposes, the VCDR does not specify that a property must be used *solely* for "purposes of the mission" in order to be considered a "premises of a mission." *See* VCDR, *supra* note 149, 23 U.S.T. at 3231, 500 U.N.T.S. at 98. It is highly probable that the Russian diplomats also used the two compounds for some other purpose, such as for conducting negotiations in-person or over the phone. *See* Diaz, *supra* note 86.

[184] Rezchikov et al., *supra* note 87; *see* VCDR, *supra* note 149, 23 U.S.T. at 3240, 500 U.N.T.S. at 110 (neglecting to define "private residence of a diplomatic agent").

[185] Rezchikov et al., *supra* note 87; *see* VCDR, *supra* note 149, 23 U.S.T. at 3237, 500 U.N.T.S. at 106 (recognizing inviolability of premises of diplomatic missions).

[186] G.A. Res. 46/210, *supra* note 135; G.A. Res. 2131, *supra* note 135; Doraev, *supra* note 133, at 376–77.

[187] *See* Matthew Happold, *Economic Sanctions and International Law: An Introduction in* ECONOMIC SANCTIONS AND INTERNATIONAL LAW 3 (Matthew Happold & Paul Eden ed. 2016) ("[I]t is argued that all 'coercive measures' are unlawful; that is, measures which . . . seek[] to require the target State to change its policies on any matter within its domestic jurisdiction . . . .");

and other countries, however, have routinely taken economic measures without authorization from the UN or another international organization, and were never concretely reprimanded.[188] International practice therefore indicates that the U.S. economic measures were legal, but they were nevertheless contrary to several UN resolutions and the general trend in modern international law.[189]

III. COMBATTING STATE-SPONSORED CYBER ATTACKS WITH A NEW CYBER TREATY

There is not an international law that directly applied to Russia's cyber attack on the DNC.[190] Consequently, it was indeterminable whether Russia violated the law and the United States was extremely challenged to formulate a response consistent with international law.[191] The United States ultimately grounded its response in generic and anachronistic international law principles and thereby skirted the bounds of the law, if not violated it.[192]

John J.A. Burke, *Economic Sanctions Against the Russian Federation are Illegal Under Public International Law*, 3 RUSSIAN L. J. 126, 127 (2015) (arguing that the economic sanctions imposed on Russia for its annexation of Crimea were in violation of international law because they intended to cause change in Russia's foreign policy).

[188] *See* Doraev, *supra* note 133, at 388 (recognizing that U.S. use of economic measures may be justified by the Lotus principle because they are not affirmatively prohibited); PELLET & MIRON, *supra* note 120, ¶ 7 (stating that "[i]n a rather primitive legal order such as public international law, with no centralized institutions to establish a violation of rules and ensure their enforcement, [use of unilateral sanctions] is mainly incumbent upon States"); *see also* Haass, *supra* note 145 (identifying consequences of U.S. economic sanctions to include, for example, "increased economic distress on Haiti, triggering a dangerous and expensive exodus of people from Haiti to the United States" and increasing Pakistan's dependence on a nuclear option as opposed to concrete reprimands from other countries or an international organization).

[189] *See* G.A. Res. 46/210, *supra* note 135 (strongly discouraging unilateral, coercive economic measures); G.A. Res. 2131, *supra* note 135 (prohibiting unilateral, coercive economic measures); Int'l Law Comm'n, Rep. on the Work of its Thirty-First Session, U.N. Doc. A/34/10 (1979), *reprinted in* [1979] 2 Y.B. Int'l L. Comm'n 121, U.N. Doc. A/CN.4/SER.A/1979/Add.1 (Part 2) (allowing "for the trend in modern international law to reserve the term 'sanction' for reactive measures applied by virtue of a decision taken by an international organization following a breach of an international obligation"); Doraev, *supra* note 133, at 388 (recognizing that international practice considers U.S. unilateral, economic measures legal because they are not affirmatively prohibited).

[190] Ido Kilovaty & Itamar Mann, *Towards a Cyber-Security Treaty*, JUST SECURITY (Aug. 3, 2016), https://www.justsecurity.org/32268/cyber-security-treaty [http://perma.cc/U8XE-UE3T]; Miller et al., *supra* note 96; *see* Hathaway et al., *supra* note 94; Hollis, *supra* note 94, at 1037, 1039–40; Sklerov, *supra* note 94.

[191] Goodman, *supra* note 96; Miller et al., *supra* note 96.

[192] *See* GIEGERICH, *supra* note 102, ¶ 1 (recognizing retorsions as an ancient remedy in international law); Goodman, *supra* note 96 (identifying U.S. use of retorsions in responding to Russia's cyber attack on the DNC); PREMISES OF DIPLOMATIC MISSIONS, *supra* note 158, ¶ 1 (recognizing that inviolability of diplomatic premises under the VCDR is an ancient principle of international law); Rezchikov et al., *supra* note 87 (claiming that U.S. response to Russia's cyber attack on the DNC violated the VCDR).

Even so, the U.S. measures were far from effective in punishing Russia and deterring future cyber attacks.[193] As this Part argues, these issues emphasize the dire need for a new international treaty—one that specifically applies to state-sponsored cyber attacks, ensures detailed and unbiased investigations, sets forth a predetermined response, and provides an effective remedy.[194] This Part identifies three features the new cyber treaty needs to successfully combat future state-sponsored cyber attacks.[195] Section A recommends that the treaty clearly and precisely define "state-sponsored cyber attack."[196] Section B proposes that the treaty create an international cyber security council.[197] Lastly, Section C advocates for a punishment provision.[198]

A. Defining State-Sponsored Cyber Attacks

The new international cyber treaty should explicitly prohibit states sponsored cyber attacks and provide a definition that is as clear and concise as possible.[199] This definition would improve states' ability to quickly and

---

[193] *See* Miller et al., *supra* note 96 (stating that President "Obama approved a modest package combining measures that had been drawn up to punish Russia for other issues . . . with economic sanctions so narrowly targeted that . . . their impact [w]as largely symbolic"); Sanger, *supra* note 11 (stating that the U.S. measures against Russia were "not as biting as previous ones" and it is unclear what impact they will have except on the expelled diplomats); Rebecca Crootof, *The DNC Hack Demonstrates the Need for Cyber-Specific Deterrents*, LAWFARE (Jan. 9, 2017), https://lawfareblog.com/dnc-hack-demonstrates-need-cyber-specific-deterrents [http://perma.cc/MY96-D576] (characterizing the U.S. measures against Russia as "too little, too late," "confusing and weak," and "insufficient"). The U.S. measures taken against Russia for the cyber attack on the DNC were bound to fail for at least four reasons. *See* Miller et al., *supra* note 96; Sanger, *supra* note 11. First, the United States waited far too long to announce the measures—six months after it was first suspected that Russia hacked the DNC—and they appeared as an afterthought rather than a swift condemnation of the attack. *See* Miller et al., *supra* note 96; Sanger, *supra* note 11; Crootof, *supra*. Second, the U.S. measures were not clearly aimed at a particular Russian act connected with the DNC cyber attack and thus did not serve as a strong punishment or deterrent. *See* Miller et al., *supra* note 96; Sanger, *supra* note 11. Third, the United States already had numerous, highly burdensome sanctions in place against Russia for annexing Crimea in 2014; the new measures merely compounded these and were unlikely to encourage Russia to change its behavior. *See* Sanger, *supra* note 11. Fourth, the United States did not quickly provide adequate evidence to support its conclusion that Russia committed the cyber attack, thereby allowing Russia and President-elect Donald Trump to deny Russia's involvement. *See* Miller et al., *supra* note 96; Sanger, *supra* note 11.

[194] *See* Hathaway et al., *supra* note 94, at 877 (arguing for a new international cyber treaty); Kilovaty & Mann, *supra* note 190 (recognizing need for a new cyber treaty after Russia's cyber attack on the DNC); *infra* notes 199–236 and accompanying text.

[195] *See infra* notes 199–236 and accompanying text.

[196] *See infra* notes 199–210 and accompanying text.

[197] *See infra* notes 211–217 and accompanying text.

[198] *See infra* notes 218–236 and accompanying text.

[199] *See* Gary D. Brown, *The Wrong Questions About Cyberspace*, 217 MIL. L. REV. 214, 223–25 (2013) (understanding that any definition of cyber attack will not be perfect, but a necessary discussion and should not prevent the development of law and policy on the issue); Hathaway et al., *supra* note 94, at 881 (urging states to adopt a clear definition of cyber attack); Hollis, *supra*

accurately determine when a state-sponsored cyber attack has occurred.[200] It would also provide states with a defensible basis for relying on the treaty's provisions when executing a response.[201]

One appropriate definition of "state-sponsored cyber attack" is "the unauthorized viewing or copying of data of another state by a government agent which is used for any purpose other than to inform government officials of national security threats."[202] This definition is broad enough to account for the sophisticated and innovative nature of state-sponsored cyber attacks.[203] At the same time, it narrowly applies only to government agents' actions rather than, for example, lone credit card data thieves, which are usually not impactful enough to warrant an international response.[204] It also does not apply to government-executed, cyber espionage purely for national security purposes, such as a government agent tapping into a foreign terrorist cell's computer network to determine whether they plan to attack that agent's home state.[205] Many countries, including the United States, Russia,

---

note 94, at 1032–33 (explaining that information operations attacks have a variety of aims and methods and being overly narrow eliminates its aspects that should be legally analyzed).

[200] *See* Hathaway et al., *supra* note 94, at 823–26 (recognizing that definitions of cyber attack vary widely and it is difficult to determine what has occurred); Sklerov, *supra* note 94, at 14–19 (recognizing that conduct cannot be regulated effectively unless it is understood).

[201] *See* Hathaway et al., *supra* note 94 (implying that states do not have a strong basis for issuing a response to cyber attacks because the laws of war are extremely hard to apply); Hollis, *supra* note 94, at 1037, 1039–40 (implying that states do not have a strong basis for issuing a response to cyber attacks because there are not specific rules and states have to find analogies in the law); Sklerov, *supra* note 94 (implying that states do not have a strong basis for issuing a response to cyber attacks because there is not a comprehensive treaty for international cyber attacks and states must resort to applying law by analogy).

[202] *See* Gervais, *supra* note 24, at 534 (defining cyber espionage as "the unauthorized viewing and copying of data files"); Hathaway et al., *supra* note 94, at 826 (defining cyber attack as "any action taken to undermine the functions of a computer network for a political or national security purpose"); Solis, *supra* note 24, at 3, *quoting* WILSON, *supra* note 24, at 12 (defining cyber terrorism as "unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives").

[203] *See* Hathaway et al., *supra* note 94, at 824 (recognizing the need for a definition of cyber attack that does not exclude the broad range of potential threats to national security); Hollis, *supra* note 94, at 1032–33 (advocating for a broad definition of information operations attacks to avoid defining away important aspects); Sklerov, *supra* note 94, at 15 (recognizing that cyber attacks come in numerous different forms).

[204] *See* Hathaway et al., *supra* note 94, at 830–31 (arguing that cyber crimes not executed for a political or national security purpose such as Internet fraud and identity theft should not be considered cyber attacks because they do not raise the same international law questions); Peretti & Slade, *supra* note 23, at 13–14 (distinguishing credit card data theft as minor and straightforward unlike state-sponsored cyber attacks).

[205] *See* Brown & Yung, *supra* note 30 (identifying China's intrusion into U.S. networks to steal highly classified information such as trade secrets, intellectual property, and negotiating strategies for economic benefit as different and less acceptable than spying for national security reasons).

and China, routinely employ and heavily rely on cyber espionage activities to protect their citizenry.[206] The new treaty would therefore be more likely to obtain ratifications and other forms of consent if it did not govern this conduct.[207] A large number of ratifications is essential to the treaty's success because, as with any treaty, it will only bind the states that consent to be bound to it.[208] In other words, states that do not ratify or otherwise consent to the new cyber treaty will not be obligated under it to cease committing cyber attacks.[209] The treaty especially needs to be ratified by states that are strongly suspected of perpetrating cyber attacks in the past, such as Russia and China, in order to strongly deter them from committing future attacks.[210]

B. Creating an International Cyber Security Council

The new treaty should create an international cyber security council.[211] The Organisation for the Prohibition of Chemical Weapons ("OPCW") would serve as an appropriate model.[212] The OPCW is an independent international organization that was created by the Chemical Weapons Convention ("CWC"), a treaty that bans chemical weapons.[213] The OPCW has vast

---

[206] *See* Brown & Yung, *supra* note 30; *see* Jeffrey H. Smith, *Keynote Address*, 28 MICH. J. INT'L L. 543, 544 (2007) (stating that espionage is a "fixture in international affairs").

[207] *See* Waxman, *supra* note 21, at 435 (postulating that the U.S. government would be reluctant to interfere with their ability to prepare to eliminate hostile systems in advance of full-fledged attacks); Brown & Yung, *supra* note 30 (theorizing that the United States did not advocate to the UN in a 2015 report for an international norm of refraining from espionage because it would be rejected by countries like China and Russia).

[208] Vienna Convention on the Law of Treaties, May 23, 1969, 1155 U.N.T.S. 331, 335; Curtis A. Bradley, *Unratified Treaties, Domestic Politics, and the U.S. Constitution*, 48 HARV. INT'L L. J. 307, 307 (2007); *see* Hathaway et al., *supra* note 94, at 864, 883 (finding that the Convention on Cybercrime is limited because its members, for the most part, are only European countries).

[209] *See* Vienna Convention on the Law of Treaties, 1155 U.N.T.S. 331, 335 (providing means of expressing consent to be bound by a treaty); Bradley, *supra* note 208, at 307 (noting that nations become bound to a treaty upon ratification or accession); Kilovaty & Mann, *supra* note 190 (recognizing need for a binding cyber treaty).

[210] Hathaway et al., *supra* note 94, at 881; *see* Kilovaty & Mann, *supra* note 190 (identifying the United States, Russia, and China as major players in cyber operations).

[211] *See* KENNETH GEERS, STRATEGIC CYBER SECURITY, NATO COOPERATIVE CYBER DEFENCE CENTER OF EXCELLENCE 125 (2011) (advocating for an international cyber convention similar to the Chemical Weapons Convention ("CWC")); Kilovaty & Mann, *supra* note 190 (proposing an international cyber security organization).

[212] GEERS, *supra* note 213, at 123; Kilovaty & Mann, *supra* note 190; *see About OPCW*, ORGANISATION FOR THE PROHIBITION OF CHEMICAL WEAPONS, https://www.opcw.org/about-opcw/ [http://perma.cc/7ASB-LMB3] (describing the Organisation for the Prohibition of Chemical Weapons ("OPCW")).

[213] *About OPCW*, *supra* note 212; *Organisation for the Prohibition of Chemical Weapons*, THE HAGUE, http://www.haguejusticeportal.net/index.php?id=333 [http://perma.cc/3FVQ-QWFB]; *The Chemical Weapons Convention (CWC) at a Glance*, ARMS CONTROL ASS'N, https://www.armscontrol.org/factsheets/cwcglance [http://perma.cc/M72R-337Z]; *see* Convention on the Prohibition of

authority to enforce the CWC, such as by confirming that chemical weapons are destroyed and recommending that member states impose sanctions on non-compliant states.[214] Similarly, an international cyber security council should be an independent international organization with authority over the cyber treaty's member states.[215] It should also have expansive power to conduct investigations into suspected state-sponsored cyber attacks and to impose sanctions on perpetrators.[216] The international cyber security council would thereby ensure that state-sponsored cyber attacks are swiftly identified, attributed to the perpetrating state, and punished appropriately.[217]

C. Punishing State-Sponsored Cyber Attacks

The treaty should expressly authorize a punishment for state-sponsored cyber attacks.[218] The treaty should not identify the precise punishment, even though that would eliminate state discretion and promote consistency in punishing state-sponsored cyber attacks.[219] Due to the varied and increasingly sophisticated nature of state-sponsored cyber attacks, the punishment

---

the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction, April 29, 1997, 1974 U.N.T.S. 45, 319 (1993) [hereinafter CWC] (making numerous declarations with respect to chemical weapons including compelling their destruction).

[214] *About OPCW*, *supra* note 213; *Organisation for the Prohibition of Chemical Weapons*, *supra* note 213; *The Chemical Weapons Convention (CWC) at a Glance*, *supra* note 213; *see* CWC, *supra* note 214, 1974 U.N.T.S. at 335–36 (giving the Conference of the OPCW broad powers and functions).

[215] *See* GEERS, *supra* note 213, at 123, 130 (identifying the CWC as having authority to compel signatories not to produce, use, or keep existing chemical weapons and a useful model for a cyber weapons convention); Kilovaty & Mann, *supra* note 190 (advocating for an independent organization to monitor and assist with cyber attacks).

[216] *See* Mette Eilstrup-Sangiovanni, *Why the World Needs an International Cyberwar Convention*, PHIL. & TECH. ¶ 3.2.3 (2017) (recommending an international cyberwar convention that creates a collective mechanism for investigation, enforcement, and punishment); Kilovaty & Mann, *supra* note 190 (recommending an international cyber-security organization that has authority to investigate cyber attacks).

[217] *See* Eilstrup-Sangiovanni, *supra* note 216 (arguing that an international cyber convention would allow for collective action resulting in faster and more reliable attribution of cyber attacks and meaningful enforcement and punishment); Kilovaty & Mann, *supra* note 190 (arguing that an international cyber-security organization would be able to monitor and attribute cyber attacks).

[218] *See* Eilstrup-Sangiovanni, *supra* note 217, ¶ 3.2.5 (advocating for an international cyber convention that ensures cyber aggressors are consistently punished); John Markoff & Andrew E. Kramer, *U.S. and Russia Differ on a Treaty for Cyberspace*, N.Y. TIMES (June 27, 2009), https://www.nytimes.com/2009/06/28/world/28cyber.html [http://perma.cc/XN48-CHRC] (quoting a U.S. State Department official on the need for a cyber treaty to criminalize cyber attacks).

[219] *See* IRISH PENAL REFORM TRUST, IPRT POSITION PAPER 3: MANDATORY SENTENCING 2 (2013) (identifying mandatory minimum sentencing schemes as completely eradicating judges' discretion); Eilstrup-Sangiovanni, *supra* note 216, ¶ 3.2.5 (arguing that the international cyber convention should lay down clear rules for when punishment is appropriate, but not what exactly the punishment should be).

needs to be flexible to ensure that it is proportional.[220] Therefore, similar to the CWC, the cyber treaty should broadly authorize the international cyber security council to issue punitive action against the perpetrating state.[221] This punishment provision would significantly improve a victim state's ability to obtain adequate recourse against the perpetrating state in the wake of a state-sponsored cyber attack.[222] It would also deter states from perpetrating cyber attacks and ultimately reduce their occurrence.[223]

This punishment provision, together with the definition and cyber security council provisions, comprise a specific, comprehensive treaty to address state-sponsored cyber attacks.[224] Drafting this treaty, obtaining the necessary support, and implementing the recommended provisions will likely be an arduous process.[225] Also, like any treaty, it is not guaranteed to be successful. [226] Nevertheless, state-sponsored cyber attacks are wreaking havoc with increasing regularity and sophistication and a specific, comprehensive international cyber treaty is an imperative step towards combatting them.[227]

CONCLUSION

State-sponsored cyber attacks are a severe, global threat. Russia's cyber attack on the DNC demonstrated that the current international legal framework is woefully inadequate for combatting this threat. The United States was forced to apply general and outdated international law principles. As a result, the United States may have violated those principles and issued

---

[220] *See* IRISH PENAL REFORM TRUST, *supra* note 219 (recognizing that mandatory minimum sentencing schemes do not provide judges with flexibility to adjust the sentence according to the circumstances); Eilstrup-Sangiovanni, *supra* note 217, ¶ 3.2.5 (recognizing the need for a proportional response to cyber attacks).

[221] *See* CWC, *supra* note 213, 1974 U.N.T.S. at 336 (giving the Conference of the OPCW broad authority to take necessary measures to ensure compliance with the CWC and redress and remedy violations); Eilstrup-Sangiovanni, *supra* note 217, ¶ 3.2.5 (proposing an international cyber convention that allows for a punishment, but not specifying what the punishment should be).

[222] *See* Kilovaty & Mann, *supra* note 190 (acknowledging that international law does little to remdy state-sponsored cyber attacks and policymakers should consider a cyber-specific treaty).

[223] *See* Eilstrup-Sangiovanni, *supra* note 217, ¶ 3.2.5 (arguing that punishing cyber attacks will strengthen deterrence).

[224] *See* Hathaway et al., *supra* note 94, at 877; Kilovaty & Mann, *supra* note 190.

[225] *See* Eilstrup-Sangiovanni, *supra* note 217, ¶ 1 (admitting that coming to international agreement on cyber attacks will be extremely difficult and require lengthy and complex negotiations); Hathaway et al., *supra* note 94, at 882 (identifying challenge of bridging divides between the United States and other cyber powers when drafting a cyber treaty).

[226] *See* Hathaway et al., *supra* note 94, at 882–84 (laying out the challenges that an international cyber treaty will likely face); Kilovaty & Mann, *supra* note 190 (conceding that adapting the CWC to cyberspace will not resolve all threats and challenges).

[227] *See* Hathaway et al., *supra* note 94, at 883–85 (asserting need for international cyber treaty despite challenges it will face); Kilovaty & Mann, *supra* note 190 (recognizing growing issue of state-sponsored cyber attacks and need for international cyber treaty).

a response that was ill suited for its goals: to punish Russia and deter future cyber attacks. In the continued absence of legal reform, state-sponsored cyber attacks will continue to occur and grow in sophistication.

In order to effectively combat against state-sponsored cyber attacks, countries should come together and negotiate a new, international treaty specifically tailored to the issue. This treaty should contain three provisions. First, it should identify a clear and comprehensive definition of "state-sponsored cyber attack. Second, it should create an international cyber security council. Third, it should expressly authorize a punishment for state-sponsored cyber attacks. The treaty would thereby deter states from committing these attacks and provide an effective remedy when they occur.

CHRISTINA LAM