DECONSTRUCTING THE U.S. POLICY OF INDICTING MALICIOUS STATE CYBER ACTORS

*Peter G. Machtiger**

In 2014, the United States Justice Department announced its first indictment against foreign military hackers. Since then, the Justice Department has continued the practice, indicting military and intelligence personnel from China, Russia, Iran, and North Korea, as well as hackers-for-hire working at the behest of State handlers. Debates over the propriety and efficacy of the indictments have covered the benefits and downsides of the policy writ-large but have not analyzed the indictments in-depth to deconstruct the policy and identify first principles. This paper analyzes all of the indictments publicly released thus far and characterizes them along several axes, including the status of the hackers, the goal of the operation, the identity of the target, and the crimes charged, with additional discussion about the techniques involved in the various operations. After examining the trends identified in the analysis, this paper proposes a more nuanced framework for deciding whether or not to indict malicious State or State-sponsored cyber actors and recommends policies that will help the United States combat malicious State activity in cyberspace.

* J.D., New York University School of Law; A.B., Harvard College. The author would like to profusely thank all those who read early drafts. Additional thanks to the editors of the Journal of Legislation & Public Policy for their tireless efforts. The positions expressed in this Note are the author's alone and do not necessarily reflect the views of any employer or the United States government.

Introduction

In April 2018, four Russian men with diplomatic passports landed at Schiphol Airport in the Netherlands, rented a car, and checked into their hotel.[1] Several days later, the men were detained by Dutch authorities in the parking lot of a Marriott Hotel next to the Organisation for the Prohibition of Chemical Weapons (OPCW), an international chemical weapons watchdog.[2] The rental car was full of special equipment used to access the wireless network of the OPCW, which was in the midst of investigating the poisoning in the United Kingdom of Russian ex-spy Sergei Skripal.[3] The Dutch intelligence services seized the equipment and the men's possessions and escorted

1. *Западные спецслужбы раскрыли четырех ГРУ-шников, взломавших лабораторию ОЗХО и ЛГТ ОЗХО и ЛГТ*, The Insider (Oct. 4, 2018), https://theins.ru/news/120447; Laura Smith-Spark, *Netherlands Officials Say They Caught Russian Spies Targeting Chemical Weapons Body*, CNN (Oct. 5, 2018), https://www.cnn.com/2018/10/04/europe/netherlands-russia-gru-intl/index.html.

2. *See How the Dutch Foiled Russian 'Cyber-Attack' on OPCW*, BBC (Oct. 4, 2018), https://www.bbc.com/news/world-europe-45747472 [hereinafter *Dutch Foiled Russian Cyber Attack*]; Jon Henley, *Visual Guide: How Dutch Intelligence Thwarted a Russian Hacking Operation*, The Guardian (Oct. 4, 2018), https://www.theguardian.com/world/2018/oct/04/visual-guide-how-dutch-intelligence-thwarted-a-russian-hacking-operation.

3. *Dutch Foiled Russian Cyber Attack, supra* note 2, at 4–5.

them to the airport, where they were put on a plane back to Moscow.[4] Seven months later, the men, operatives of a Russian military intelligence agency called the GRU, were indicted by the United States Department of Justice as part of a conspiracy to commit malicious cyber activity around the world.[5] Two other GRU operatives named in that indictment had previously been charged by the Justice Department for their involvement in a series of hacks related to the 2016 U.S. presidential election.[6] These two indictments are part of a burgeoning U.S. practice of charging individual State-affiliated actors for State-directed malicious cyber activity.

Indictments of individual foreign government employees for malicious cyber activity have become increasingly frequent since the practice began in 2014, when the U.S. government unsealed an indictment against five Chinese military hackers for cyber espionage against U.S. companies.[7] Between 2015 and 2019, State-affiliated hackers caused 43% of the 103 most monetarily devastating global cyber incidents, causing $7.8 billion of damage.[8] According to one database, State-affiliated actors are suspected of conducting 155 different identifiable cyber operations that have affected U.S. targets from 2005 to 2020.[9] In response, there have been fifteen indictments of State-affiliated cyber actors by the Justice Department, with some of those covering multiple operations.[10] The previously mentioned database attributes seventeen cyber operations to the United States over the same time period, although the true number is surely orders of magnitude greater.[11]

---

4. *Id.* at 7–8.

5. Indictment, United States v. Morenets, No. 2:18-cr-00263 (W.D. Pa. Oct. 3, 2018).

6. Indictment, United States v. Netyksho, No. 1:18-cr-00215 (D.D.C. July 13, 2018). Catalin Cimpanu, *German Authorities Charge Russian Hacker for 2015 Bundestag Hack*, ZDNET (May 5, 2020), https://www.zdnet.com/article/german-authorities-charge-russian-hacker-for-2015-bundestag-hack/.

7. Indictment, United States v. Dong, No. 2:14-cr-00118 (W.D. Pa. May 1, 2014).

8. CYENTIA INST., INFORMATION RISK INSIGHTS STUDY 20/20 XTREME 23 (Nov. 10, 2020), https://www.cyentia.com/wp-content/uploads/IRIS2020-Xtreme.pdf.

9. The breakdown is: China – 71; Iran – 32; Russia – 29; North Korea – 13; Israel – 2; Ethiopia – 1; France – 1; Lebanon – 1; Pakistan – 1; Saudi Arabia – 1; Spain – 1; Syria – 1; Vietnam – 1. COUNCIL ON FOREIGN RELS., CYBER OPERATIONS TRACKER, https://www.cfr.org/cyber-operations/ (last visited Feb. 28, 2021).

10. *See infra* Section II.

11. Barton Gellman & Ellen Nakashima, *U.S. Spy Agencies Mounted 231 Offensive Cyber-Operations in 2011, Documents Show*, WASH. POST (Aug. 30, 2013), https://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html; Paul Kolbe, *With Hacking, the United States*

The Justice Department takes the position that "[c]omputer intrusions and attacks are crimes, and the Department of Justice fights crime. That is true regardless of whether the criminal is a transnational organized crime group, a lone hacker, or an officer of a foreign military or intelligence organization."[12] Assistant Attorney General for National Security John Demers has framed it as: "If the choice here is between remaining silent while we at the Department watch nations engage in malicious, norms-violating cyber activity, or charg[ing] these cases, the choice is obvious—we will charge them."[13]

For reasons that are not readily apparent, the United States is mostly unique among its allies in its pursuit of criminal indictments for State-affiliated malicious cyber activity.[14] This decision to criminally charge State-affiliated actors for their cyber activity may be because of the "increasingly blurring line between State and non-State actors" in cyberspace.[15] This is true both of offensive actors and of targets. In the words of former Principal Deputy Director of National Intelligence Sue Gordon:

> [I]t used to be that governments held all the vital information (kept the secrets worth stealing) and wielded all the power (made all the decisions worth influencing.) No longer. . . . Threat actors today target government and non-government, critical infrastructure and

Needs to Stop Playing the Victim, N.Y. TIMES (Dec. 23, 2020), https://www.nytimes.com/2020/12/23/opinion/russia-united-states-hack.html.

12. DEP'T OF JUST., REPORT OF THE ATTORNEY GENERAL'S CYBER DIGITAL TASK FORCE xii (July 2, 2018), https://www.justice.gov/archives/ag/page/file/1076696/download [hereinafter CYBER REPORT].

13. Press Release, Dep't of Just., Assistant Attorney General John C. Demers Delivers Remarks on the National Security Cyber Investigation into North Korean Operatives (Feb. 17, 2021), https://www.justice.gov/opa/pr/assistant-attorney-general-john-c-demers-delivers-remarks-national-security-cyber.

14. Garrett Hinck & Tim Maurer, *Persistent Enforcement: Criminal Charges as a Response to Nation-State Malicious Cyber Activity*, 10 J. NAT'L SEC. L. & POL'Y 525, 534 (2020); *but see* Cimpanu, *supra* note 6, at 1 (detailing a German arrest warrant for a GRU hacker—previously indicted by the United States for another incident—accused of breaching the network of the German Parliament). Swedish prosecutors have explicitly declined to prosecute GRU hackers because they were acting on behalf of the Russian government. Catalin Cimpanu, *Sweden Drops Russian Hacking Investigation Due to Legal Complications*, RECORD (Apr. 13, 2021), https://therecord.media/sweden-drops-russian-hacking-investigation-due-to-legal-complications/.

15. *Homeland Cybersecurity: Assessing Cyber Threats and Building Resilience: Hearings Before the H. Comm. on Homeland Sec.*, 117th Cong. 3 (2021) (statement of Christopher C. Krebs) [hereinafter Krebs Statement]. "State actors" are generally government personnel, but this can get complicated in cyberspace when some people work for both governments and private clients.

> private citizens, academic institutions and research centers, huge multi-national corporations and small businesses.[16]

The practice of indicting malicious State-affiliated cyber actors for State-directed activity has been met with mixed reviews. Proponents of the policy generally argue that there is a chance of eventual arrest and that the indictments have a specific and general deterrent effect, provide trustworthy attribution for cyber incidents, vindicate victims, and support further penalties, such as sanctions.[17] Further, proponents describe the indictments as just one tool in a whole-of-government approach, serving as a signal to foreign State actors that their behavior is not acceptable as a matter of international custom.[18]

Opponents of the indictment policy have called it "a magnificent failure" in the face of relentless State-sponsored cyber activity.[19] The indictments showcase U.S. attribution capabilities, but the lack of serious consequences has just emboldened malicious State actors in cyberspace.[20] Former Director of National Intelligence Denis Blair reportedly referred to the first indictment of Chinese military hackers as "speaking loudly and carrying a small stick."[21]

Many of the participants in this debate speak broadly about the U.S. policy of indicting State actor hackers.[22] The discourse has

---

16. *Homeland Cybersecurity: Assessing Cyber Threats and Building Resilience: Hearings Before the H. Comm. on Homeland Sec.*, 117th Cong. 1–2 (2021) (statement of Susan M. Gordon).

17. Press Release, Dep't of Just., Deputy Attorney General Rod J. Rosenstein Delivers Remarks at the Aspen Security Forum (July 19, 2018), https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-aspen-security-forum; *see also* Press Release, Dep't of Just., Deputy Assistant Attorney General Adam Hickey of the National Security Division Delivers Remarks at CyberNext DC (Oct. 4, 2018), https://www.justice.gov/opa/pr/deputy-assistant-attorney-general-adam-hickey-national-security-division-delivers-remarks; *see also* Press Release, Dep't of Just., Assistant Attorney General for National Security John P. Carlin Delivers Remarks on the National Security Cyber Threat at Harvard Law School (Dec. 3, 2015), https://www.justice.gov/opa/speech/assistant-attorney-general-national-security-john-p-carlin-delivers-remarks-national. For a more in-depth description of these features, *see* Hink & Maurer, *supra* note 14, at 530–35.

18. John P. Carlin, *Detect, Disrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats*, 7 HARV. NAT'L SEC. J. 391, 420–21 (2016).

19. Jack Goldsmith & Robert D. Williams, *The Failure of the United States' Chinese-Hacking Indictment Strategy*, LAWFARE (Dec. 28, 2018), https://www.lawfareblog.com/failure-united-states-chinese-hacking-indictment-strategy.

20. Jack Goldsmith, *The Puzzle of the GRU Indictment*, LAWFARE (Oct. 21, 2020), https://www.lawfareblog.com/puzzle-gru-indictment.

21. Michael S. Schmidt, David E. Sanger & Nicole Perlroth, *Chinese Hackers Pursue Key Data on U.S. Workers*, N.Y. TIMES (July 9, 2014), https://www.nytimes.com/2014/07/10/world/asia/chinese-hackers-pursue-key-data-on-us-workers.html.

22. *See, e.g.,* Peter Machtiger, *Disrupt, Don't Indict: Why the United States Should Stop Indicting Foreign State Actor Hackers*, JUST SECURITY (Apr. 3, 2020), https://

lacked a more granular analysis of various aspects of the existing indictments, such as the status of the actors, the goal of the operations, and the identities of the targets. If these indictments are to be useful to signal to foreign actors what is and is not acceptable behavior for government actors in cyberspace, the United States should be deliberate about which combinations of actors, goals, and targets trigger an indictment. This paper seeks to fill that gap and examine how the evolving U.S. policy in this space fits into historical practice and legal frameworks. Part I provides a brief overview of U.S. practice in modern history vis-à-vis the indictment or non-indictment of State actors for State-directed activity that violates U.S. domestic law. Part II analyzes the fourteen public indictments of State cyber actors for malicious cyber activity, breaking them down by the status of the hackers, the goal of the computer network operation, the identity of the target, and the crimes charged, with additional discussion about the characteristics of the various operations. Part III uses the trends identified in the comprehensive analysis to evaluate the indictment policy and provide a recommended course of action for dealing with State cyber actors going forward.

I.
An Overview of Historical U.S. Practice: Indictments of Foreign State Actors, State-Sponsored Actors, and Unrecognized State Actors

The Justice Department has historically prosecuted some, but not all, crimes committed by foreign State actors. A brief historical look at Justice Department behavior in the face of nations engaging in other kinds of malicious activity can help put the Justice Department's cyber indictment policy in context.

The Justice Department has indicted State-affiliated actors for intelligence activities, and in one instance terrorism, when they have caused injury to U.S. persons in the eyes of U.S. criminal law and when they were acting without declaring their government status. Prosecutors have also occasionally charged foreign government officials after the United States no longer recognizes the regime they work for as the legitimate government of a country. However, the Justice

---

www.justsecurity.org/69104/disrupt-dont-indict-why-the-united-states-should-stop-indicting-foreign-state-actor-hackers/; David Hechler, *What Is the Point of These Nation-State Indictments?*, Lawfare (Feb. 8, 2021), https://www.lawfareblog.com/what-point-these-nation-state-indictments; Goldsmith, *supra* note 20, at 1; Carlin, *supra* note 18, at 420–21.

Department has tended to avoid indictments when a State actor commits a crime that is nevertheless an accepted international practice—such as spying by a declared government employee working out of an embassy—or in situations where State actors have conducted intelligence, terrorist, or cyber activities but there is insufficient evidence, ambiguity over who would be charged, or a desire to protect sources and methods. One well-developed example of State action that does not trigger indictments is the conduct of war by military combatants.

Evaluating how the Justice Department has handled these various types of State action can shed light on what prosecutors may be considering or should be considering to craft a consistent policy when they decide to bring an indictment for State cyber activity.

A. State Action That Has Triggered Indictment of State-Affiliated Actors

1. Examples of State Action That Has Triggered Indictment

Aside from the recent indictments for State cyber activity, the Justice Department has historically indicted State actors in three sets of circumstances: certain intelligence operatives performing certain intelligence activities; limited instances of State-sponsored terrorism; and criminal activity by State leaders who the United States no longer recognizes as legitimate.

a. Certain Intelligence Activities

Historically, the Justice Department has arrested and charged foreign operatives conducting intelligence activities on U.S. soil. Prosecutors have seemed to restrict this to operatives who are undeclared, rather than those acting under "official diplomatic cover."[23] In some instances, prosecutors have indicted foreign operatives even when the plots are not fully carried out and the defendants cannot be immediately apprehended.

In the famous case *Ex parte Quirin*, 317 U.S. 1 (1942), eight Nazi saboteurs were charged after they entered the United States to blow up manufacturing plants and infrastructure. They were tried by a military commission and executed,[24] although the use of a military commission rather than a civilian court was somewhat controversial

23. Intelligence operatives are acting under "official diplomatic cover" when their government has openly declared them as an embassy employee or diplomat to a host country.

24. Jack Goldsmith & Cass R. Sunstein, *Military Tribunals and Legal Culture: What a Difference Sixty Years Makes*, 19 CONST. COMMENT. 261, 263–64 (2002).

amongst lawyers.[25] However, in other cases operatives are often returned to their home countries as part of diplomatic deals before serving their full sentences. For example, in 1939, a Soviet intelligence operative was convicted under the Espionage Act for spying in California.[26] He was released in 1941 and sent back to the Soviet Union at the request of the State Department.[27]

More recently, in 2010, ten Russian "Illegals" (intelligence operatives in the United States carrying out "long-term, 'deep cover' assignments") were arrested and charged in two criminal complaints with acting as unregistered agents of a foreign government and money laundering.[28] Less than two weeks later, they had already pled guilty and were sent back to Russia in exchange for "four Russians serving long prison terms in their homeland on charges of spying for the West."[29] In January 2015, an agent of Russia's foreign intelligence agency, the SVR, was arrested for acting as an unregistered agent of a foreign government. He, like the "Illegals," was collecting intelligence under "non-official cover," meaning "he entered and remained in the United States as a private citizen."[30] Two other SVR operatives were named in the indictment as co-conspirators, but they were no longer located in the United States. The Justice Department indicated that they had been "protected by diplomatic immunity from arrest and prosecution while in the United States" because they were operating under "official cover" as Russian diplomats.[31] The Russian intelli-

25. *See id.* at 264 ("Within the government . . . , there was considerable uncertainty about how to prosecute and punish the saboteurs. One complicating factor was that the laws applicable in civilian trials did not permit the death penalty for the non-U.S. citizen defendants. Another was a concern that Article III of the Constitution required the government to try the American citizens for treason.").

26. *See generally* Gorin v. United States, 111 F.2d 712 (9th Cir. 1940).

27. *Russian in Spy Case Free*, N.Y. TIMES (Mar. 22, 1941), https://timesmachine.nytimes.com/timesmachine/1941/03/23/85469501.pdf.

28. Press Release, Dep't of Just., Ten Alleged Secret Agents Arrested in the United States (June 28, 2010), https://www.justice.gov/opa/pr/ten-alleged-secret-agents-arrested-united-states.

29. Guy Faulconbridge & Heinz-Peter Bader, *Russia, U.S. Swap 14 in Cold War-Style Spy Exchange*, REUTERS (July 9, 2010), https://www.reuters.com/article/us-russia-usa-spies/russia-u-s-swap-14-in-cold-war-style-spy-exchange-idUSLDE6680KB20100709.

30. Press Release, Dep't of Just., Attorney General Holder Announces Charges Against Russian Spy Ring in New York City (Jan. 26, 2015) [hereinafter *Spy Ring Press Release*], https://www.justice.gov/opa/pr/attorney-general-holder-announces-charges-against-russian-spy-ring-new-york-city.

31. *Id.*

gence operative served 30 months in prison before being deported to Russia.[32]

In 2018, a Chinese intelligence operative became the first foreign intelligence operative to be arrested abroad and extradited to the United States to face criminal charges. The operative was detained in Belgium and extradited to the United States, where he was charged with economic espionage involving the theft of trade secrets from U.S. aviation and aerospace companies.[33] Pressure against Chinese intelligence activities has continued—four members of China's People's Liberation Army (PLA) were arrested in July 2020 and charged with visa fraud after coming to the United States and lying about their military affiliation. It is not entirely clear from the indictment what they were tasked with doing, but one said he was instructed to "observe the layout of the UCSF lab and bring back information on how to replicate it in China."[34]

In the summer of 2021, the Justice Department publicly indicted Iranian intelligence officials and assets for conspiring to kidnap on U.S. soil an American journalist and human rights activist critical of the Iranian regime.[35] Only a civilian co-conspirator was living in the United States, so none of the intelligence operatives were arrested. Even so, the indictment signals a willingness by the Justice Department to publicly indict foreign intelligence officials for their activities even when the plots are not fully carried out and the defendants cannot be immediately apprehended.

---

32. Brian Ross, Pete Madden & Michelle McPhee, *Russian Spy Evgeny Buryakov Deported From United States*, ABC NEWS (Apr. 5, 2017), https://abcnews.go.com/International/russian-spy-evgeny-buryakov-deported-united-states/story.

33. Press Release, Dep't of Just., Chinese Intelligence Officer Charged with Economic Espionage Involving Theft of Trade Secrets from Leading U.S. Aviation Companies (Oct. 10, 2018), https://www.justice.gov/opa/pr/chinese-intelligence-officer-charged-economic-espionage-involving-theft-trade-secrets-leading; *see also* Ellen Nakashima, *In a First, a Chinese Spy is Extradited to the U.S. After Stealing Technology Secrets, Justice Dept. Says*, WASH. POST (Oct. 10, 2018), https://www.washingtonpost.com/world/national-security/chinese-spy-charged-with-stealing-us-military-secrets-and-extradited-for-prosecution/2018/10/10/b2a7325c-cc97-11e8-920f-dd52e1ae4570_story.html.

34. Press Release, Dep't of Just., Chinese Intelligence Officer Charged with Economic Espionage Involving Theft of Trade Secrets from Leading U.S. Aviation Companies (Oct. 10, 2018), https://www.justice.gov/opa/pr/chinese-intelligence-officer-charged-economic-espionage-involving-theft-trade-secrets-leading.

35. Press Release, Dep't of Just., Iranian Intelligence Officials Indicted on Kidnapping Conspiracy Charges (July 13, 2021), https://www.justice.gov/opa/pr/iranian-intelligence-officials-indicted-kidnapping-conspiracy-charges.

b. Certain State-Sponsored Terrorism

The United States has only indicted State actors for acts of terrorism in one modern instance: the 1988 bombing of Pan Am Flight 103 over Lockerbie, Scotland, which killed 190 Americans. The Justice Department has charged three Libyan intelligence officers in the bombing. Two of the officers, charged in 1991, were tried in a "specially established Scottish court convened in The Netherlands" and the third, charged in 2020, is in Libyan custody.[36] The charged U.S. crimes included "destruction of aircraft resulting in death" and "destruction of vehicle used in interstate or foreign commerce by means of an explosive resulting in death."[37] According to remarks by Attorney General Bill Barr, the Justice Department will continue to move forward with the case against the recently charged conspirator, over three decades later.[38]

c. Unrecognized State Actors

The United States has on two occasions indicted individuals that some might consider State actors but that the U.S. government does not recognize to be part of the legitimate government of a country. The first example of this was the 1988 indictment of the unrecognized ruler of Panama, Manuel Noriega, and other Panamanian officials for drug trafficking.[39] According to one of the Noriega prosecutors, after the indictment but before the American invasion of Panama, "[s]ecret negotiations were conducted between high-level Justice and State Department officials and Noriega's lawyers, to arrange Noriega's graceful exit from Panama to a third country and the dismissal of all charges."[40] Noriega "rejected the proposal" and, eventually, "plans were orchestrated in Washington to invade Panama, capture General Noriega, and bring him back to stand trial . . . ."[41] Noriega eventually

36. Press Release, Dep't of Just., Attorney General William P. Barr Delivers Remarks at the Pan Am 103 Press Conference (Dec. 21, 2020), https://www.justice.gov/opa/speech/attorney-general-william-p-barr-delivers-remarks-pan-am-103-press-conference.

37. Criminal Complaint, United States v. Al-Marimi, No. 1:20-mj-00252 (D.D.C. Dec. 14, 2020).

38. Press Release, Pan Am 103 Press Conference, *supra* note 36.

39. Philip Shenon, *Noriega Indicted by U.S. for Links to Illegal Drugs*, N.Y. TIMES (Feb. 6, 1988), https://www.nytimes.com/1988/02/06/world/noriega-indicted-by-us-for-links-to-illegal-drugs.html; Associated Press, *U.S. Has Jurisdiction Over Noriega, Judge Rules*, N.Y. TIMES (June 9, 1990), https://www.nytimes.com/1990/06/09/us/us-has-jurisdiction-over-noriega-judge-rules.html.

40. Myles H. Malman, *United States v. Manuel Noriega: Never Before, Never Again*, 28 LITIG. 13, 17 (Winter 2002).

41. *Id*.

surrendered to U.S. military personnel and ultimately served 17 years in prison in the United States before being extradited first to France and then to Panama.[42]

In March 2020, the Justice Department indicted the former President of Venezuela, Nicolás Maduro Moros, and a host of current and former Venezuelan officials on charges related to narco-terrorism and drug trafficking.[43] The United States had ceased to recognize Maduro as the legitimate President of Venezuela in early 2019, although it is unclear how the Justice Department viewed the status of the co-conspirators it described as "current" Venezuelan officials.[44] The case has stalled as the Maduro regime remains in power in Venezuela.[45]

2. Characteristics of State Action That Has Triggered Indictment of State-Affiliated Actors

Indictments for State action seem to involve either crimes committed within the jurisdiction of the United States or crimes injuring U.S. persons. This falls in line with at least some international practice, such as the United Kingdom's decision to criminally charge two Russian GRU officers for their attempted assassination of Russian defector Sergei Skripal in southwest England.[46] While the 2018 Chinese espionage example and the two drug trafficking examples less obviously meet the "U.S. soil or injury to U.S. persons" standard, all three examples do involve injury to U.S. persons in the eyes of U.S. criminal law. However, the following section will explore instances in

---

42. *Obituary: General Manuel Noriega*, BBC NEWS (May 30, 2017), https://www.bbc.com/news/world-latin-america-16966007.

43. Press Release, Dep't of Just., Nicolás Maduro Moros and 14 Current and Former Venezuelan Officials Charged with Narco-Terrorism, Corruption, Drug Trafficking and Other Criminal Charges (Mar. 26, 2020), https://www.justice.gov/opa/pr/nicol-s-maduro-moros-and-14-current-and-former-venezuelan-officials-charged-narco-terrorism.

44. Ana Vanessa Herrero, *After U.S. Backs Juan Guaidó as Venezuela's Leader, Maduro Cuts Ties*, N.Y. TIMES (Jan. 23, 2019), https://www.nytimes.com/2019/01/23/world/americas/venezuela-protests-guaido-maduro.html.

45. Anthony Faiola & Ana Vanessa Herrero, *Maduro and Venezuela's Opposition Launch Fresh Talks. He Seems to Have the Upper Hand*, WASH. POST (Aug. 13, 2021), https://www.washingtonpost.com/world/2021/08/13/venezuela-maduro-guaido-talks-mexico/.

46. Richard Pérez-Peña & Ellen Barry, *U.K. Charges 2 Men in Novichok Poisoning, Saying They're Russian Agents*, N.Y. TIMES (Sept. 5, 2018), https://www.nytimes.com/2018/09/05/world/europe/russia-uk-novichok-skripal.html. The U.K. combined that indictment with sanctions, the expulsion of twenty-three Russian "diplomats," and the temporary suspension of high-level diplomatic contacts. Michel Paradis, *The U.K.'s Opportunity to Use Lawfare in Response to the Salisbury Attack*, LAWFARE (Mar. 15, 2018, 12:44 PM), https://www.lawfareblog.com/uks-opportunity-use-lawfare-response-salisbury-attack.

which State actors committed crimes either within the United States or that harmed U.S. persons and were nevertheless not indicted.

B. State Action That Has Not Triggered Indictment of State-Affiliated Actors

1. Examples of State Action That Has Not Triggered Legal Action Against State-Affiliated Actors

When State actors break U.S. laws, sometimes they are not indicted, generally due to some combination of international norms or law, insufficient evidence, or ambiguity about who specifically would be charged. This has occurred in the contexts of certain intelligence activities within the United States, State-sponsored terrorism and material support, military action, and many cyber incidents.

a. Certain Intelligence Activities

The Justice Department generally does not indict foreign intelligence officers operating in the United States under official diplomatic cover. Many of the public examples of this trend involve Russian intelligence operatives but occasionally operatives from China, too. In some cases, there might also be a lack of sufficient evidence for an indictment or a hesitancy to reveal U.S. investigatory sources and methods might explain the non-indictment policy.

In 1983, a Soviet military intelligence officer was caught spying in Virginia but was not arrested because he had diplomatic immunity—instead he was declared *persona non grata* and kicked out of the country the next day.[47] A few years later, two Chinese diplomats were asked to leave the United States under suspicion of espionage but were similarly "not arrested or charged with any crime because of the protections of diplomatic immunity."[48] Around the same time period, the Reagan Administration demanded that 55 Soviet intelligence operatives leave the United States after a series of escalating expulsions that started when a Soviet employee of the United Nations was arrested in New York on espionage charges.[49] The man was allowed to

47. Charles R. Babcock, *Soviet Military Spy Caught in FBI Trap*, WASH. POST (Sept. 16, 1983), https://www.washingtonpost.com/archive/politics/1983/09/16/soviet-military-spy-caught-in-fbi-trap/eab2d86f-405f-45bd-86dd-503e4e458f1b/.

48. Philip Shenon, *2 Chinese Depart in Espionage Case*, N.Y. TIMES (Dec. 31, 1987), https://www.nytimes.com/1987/12/31/world/2-chinese-depart-in-espionage-case.html.

49. David K. Shipler, *55 Expelled Russians Leave Washington*, N.Y. TIMES (Nov. 1, 1986), https://www.nytimes.com/1986/11/01/world/55-expelled-russians-leave-washington.html.

leave the country after pleading no contest to the charges.[50] More recently, after FBI agent Robert Hanssen was arrested for spying for the Soviet Union and Russia, the U.S. government declared fifty Russian "diplomats" *persona non grata* and ordered them to leave the country.[51]

One example that involves signals intelligence—electronic surveillance for intelligence purposes—rather than human intelligence (as in the above cases) is the instance of 2018 reporting sourced from American intelligence officials indicating that Russia and China were intercepting President Trump's cellphone calls.[52] While this interception technically violates the Wiretap Act, 18 U.S.C. § 2511, the Justice Department never charged any Chinese or Russian operatives, either because they did not know who to charge or perhaps because prosecutors would have been forced to disclose sensitive human sources and government surveillance.

b. State-Sponsored Terrorism & Material Support

The Justice Department has not charged State actors for State-sponsored terrorism or material support for terrorism on many occasions where other government officials have acknowledged the State involvement. There has also been a string of cases under an exception to the Foreign Sovereign Immunities Act (FSIA) where federal judges have determined that State entities were involved in acts of terrorism and the judges authorized monetary judgments against these State entities, although the Justice Department did not charge the individual perpetrators.

Members of Congress have said publicly that "Qatar has openly housed Hamas leaders [and] Taliban leaders" and "[a]t least one high-ranking Qatari official provided support to the mastermind of the 9/11 terror attacks against our country, Khalid Sheikh Mohammad."[53] Reportedly, Turkey also "provides financial, material, and political sup-

50. Leonard Buder, *A Final Day: 4 Minutes for Zakharov*, N.Y. TIMES (Oct. 1, 1986), https://www.nytimes.com/1986/10/01/world/a-final-day-4-minutes-for-zakharov.html.

51. *U.S. Expels 50 Russian Diplomats*, ABC NEWS (Mar. 22, 2001), https://abcnews.go.com/US/story?id=93757&page=1.

52. Matthew Rosenberg & Maggie Haberman, *When Trump Phones Friends, the Chinese and the Russians Listen and Learn*, N.Y. TIMES (Oct. 24, 2018), https://www.nytimes.com/2018/10/24/us/politics/trump-phone-security.html.

53. *Assessing the U.S.-Qatar Relationship: Hearing Before the Subcomm. on the Middle East and North Africa of the H. Comm. on Foreign Affairs*, 115th Cong. 2 (2017) (statement of Rep. Ileana Ros-Lehtinen, Chairwoman, Subcomm. on the Middle East and North Africa, H. Comm. on Foreign Affairs).

port" for Hamas, which the United States has designated a "Foreign Terrorist Organization."[54] Nevertheless, the Justice Department has not charged any Qatari or Turkish officials for this alleged behavior, which—if true—would likely violate the statutes prohibiting material support to terrorists and terrorist organizations.[55]

In response to decades of nefarious activity by Iran's Islamic Revolutionary Guard Corps (IRGC), the United States designated the group, which is officially part of Iran's military, a "Foreign Terrorist Organization."[56] In March 2020, the Treasury Department designated for sanctions "20 Iran- and Iraq-based front companies, senior officials, and business associates that provide support to or act for or on behalf of the Islamic Revolutionary Guards Corps-Qods Force (IRGC-QF)" building on the IRGC's Foreign Terrorist Organization status.[57] The individuals are alleged to have transferred weapons, dispensed funds, and conducted other malicious activity on behalf of the IRGC.[58] To date, none of these designated individuals has been indicted by the Justice Department.

Reporting backed up by statements from U.S. officials has indicated that Russia has provided weapons and military equipment to the Taliban, and members of the GRU have potentially, but not definitely, offered bounties to the Taliban for killing American troops.[59] While Russia is not a designated State sponsor of terrorism[60] and thus cannot

54. *Hamas' Benefactors: A Network of Terror: Joint Hearing Before the Subcomm. on the Middle East and North Africa & the Subcomm. on Terrorism, Nonproliferation, and Trade of the H. Comm. on Foreign Affairs*, 113th Cong. 2 (2014) (statement of Rep. Ileana Ros-Lehtinen, Chairwoman, Subcomm. on the Middle East and North Africa, H. Comm. on Foreign Affairs).

55. 18 U.S.C. §§ 2339A–2339B (1994).

56. Edward Wong & Eric Schmitt, *Trump Designates Iran's Revolutionary Guards a Foreign Terrorist Group*, N.Y. TIMES (Apr. 8, 2019), https://www.nytimes.com/2019/04/08/world/middleeast/trump-iran-revolutionary-guard-corps.html.

57. Press Release, Dep't of the Treasury, Treasury Designates Vast Network of IRGC-QF Officials and Front Companies in Iraq, Iran (Mar. 26, 2020), https://home.treasury.gov/news/press-releases/sm957.

58. *Id.*

59. Ryan Goodman, *Trump Pushed CIA to Give Intelligence to Kremlin, While Taking No Action Against Russia Arming Taliban*, JUST SECURITY (July 8, 2020), https://www.justsecurity.org/71279/trump-pushed-cia-to-give-intelligence-to-kremlin-while-taking-no-action-against-russia-arming-taliban/; Ellen Nakashima, *Biden Administration Imposes Significant Economic Sanctions on Russia Over Cyberspying, Efforts to Influence Presidential Election*, WASH. POST (Apr. 15, 2021), https://www.washingtonpost.com/national-security/biden-to-announce-tough-sanctions-on-russia-over-cyber-spying/2021/04/15/a4c1d260-746e-11eb-948d-19472e683521_story.html.

60. *State Sponsors of Terrorism*, U.S. DEP'T STATE, https://www.state.gov/state-sponsors-of-terrorism/ [https://perma.cc/HX9A-85EF] (last visited Nov. 4, 2021).

be sued under the State-sponsored terrorism exception, 28 U.S.C. § 1605A, of the FSIA, the GRU officers involved could theoretically be charged with providing material support to terrorists under 18 U.S.C. § 2339A, which prohibits furnishing weapons, equipment, and money, among other things, to terrorists.[61]

When designated State sponsors of terrorism are involved in terrorist acts, the terrorism exception to the FSIA has provided a civil path to judicial recognition of State entities' culpability. These cases—where federal judges determined that there was sufficient evidence to show State-sponsorship of certain terror attacks—would suggest that it has not been a lack of evidence that has prevented prosecutors from more indictments against State-sponsors of terrorism. After the 1996 Khobar Towers bombing in Saudi Arabia that killed 17 American servicemembers, the victims' families sued the Islamic Republic of Iran, the Iranian Ministry of Information and Security (MOIS), and the IRGC, citing the since-modified exception to the FSIA for acts of "state-sponsored terrorism."[62] Judge Royce Lamberth ruled that the attack was planned, funded, and carried out by Iran, the MOIS, and the IRGC and ordered a default judgment of over $250 million.[63] After Congress enacted 28 U.S.C. § 1605A, an amendment to the FSIA that expanded the exception for acts of State-sponsored terrorism and created a federal private right of action, victims of the 1983 and 1984 attacks on the U.S. Embassy in Beirut sued the government of Iran for its role in the attacks.[64] Judge John Bates found the Iranian government liable and awarded damages to the plaintiffs.[65] Following the 1998 al Qaeda bombings of the U.S. Embassies in Kenya and Tanzania, a group of victims and their families sued the governments of Sudan and Iran under 28 U.S.C. § 1605A. Judge John Bates found that "the governments of Sudan and Iran provided material support and resources to Bin Laden and al Qaeda for acts of terrorism, including extrajudicial killings."[66] Litigation over the damages is ongoing.[67] Further examples exist, including cases: against Cuba, after three Americans were held hostage and one killed in Colombia by a

61. Peter Machtiger, *Legally Available Options: A Case for Indicting Russian Officers for Providing Material Support to the Taliban*, JUST SECURITY (July 29, 2020), https://www.justsecurity.org/71609/legally-available-options-a-case-for-indicting-russian-officers-for-providing-material-support-to-the-taliban/.

62. Heiser v. Islamic Republic of Iran, 466 F. Supp. 2d 229, 248 (D.D.C. 2006) (citing 28 U.S.C. § 1605(a)(7)).

63. *Id.* at 265, 356.

64. Doe v. Islamic Republic of Iran, 808 F. Supp. 2d 1, 6 (D.D.C. 2011).

65. Doe v. Islamic Republic of Iran, 943 F. Supp. 2d 180, 192 (D.D.C. 2013).

66. Owens v. Republic of Sudan, 826 F. Supp. 2d 128, 150 (D.D.C. 2011).

67. Opati v. Republic of Sudan, 140 S. Ct. 1601, 1610 (2020).

terrorist organization supported by Cuba;[68] against Syria and Syrian Military Intelligence, after two Americans were killed in a terrorist attack in Jordan by a terrorist organization supported by Syria;[69] and against the Democratic People's Republic of Korea (North Korea), after an American student was detained and tortured to death by the North Korean government.[70]

It is unclear why these acts of terrorism have not led to State actor indictments like the Lockerbie bombing has, but it could be a combination of lack of evidence, ambiguity as to who to indict, foreign policy considerations, and wanting to conceal sources and methods.

c. Military Actions

Armed conflict is one classic example of a context where State actors commit acts against each other—such as killing enemy combatants—that would violate domestic criminal law if not for international consensus that a special framework is preferable. Military conflict is governed by an entire body of international law known as the law of armed conflict (LOAC).[71] LOAC is relevant not because of its applicability to cyber activity but because it is a classic example of international coalescence around the idea that some malicious action by States cannot be appropriately addressed by domestic criminal laws.[72]

One example of a rule unique to LOAC is the idea of "combatant immunity," which "prohibits the criminal prosecution of lawful com-

68. Stansell v. Republic of Cuba, 217 F. Supp. 3d 320, 328 (D.D.C. 2016).

69. Thuneibat v. Syrian Arab Republic, 167 F. Supp. 3d 22, 48 (D.D.C. 2016).

70. Warmbier v. Democratic People's Republic of Korea, 356 F. Supp. 3d 30, 60 (D.D.C. 2018).

71. The law of armed conflict is also known as international humanitarian law (IHL). For simplicity, references to "IHL" in cited sources have been replaced with "[LOAC]".

72. As stated by one international law and cyberspace expert, "international law represents consensus among states as to the rules of the game that govern their interactions." Michael N. Schmitt, *The Law of Cyber Warfare:* Quo Vadis*?*, 25 STAN. L. & POL'Y REV. 269, 272 (2014). In LOAC, these rules depend on the status of the actors (i.e. State or non-State), the status of the targets, the nature and intensity of the conflict, the location of the hostilities, and other factors. RYAN DOWDY ET AL., INT'L AND OPERATIONAL LAW DEPARTMENT, THE JUDGE ADVOC. GEN. LEGAL CTR. AND SCH., LAW OF ARMED CONFLICT DESKBOOK 24–26 (David Lee ed. 2015). The specific rules of LOAC have developed over time from international agreements and State practice to deal with the unique issues of armed conflict. *Id.* at 19–23. Stated simply, States came to the consensus that armed conflict was best regulated by a special body of law specifically designed for that purpose. The nuanced debate over whether or not armed conflict is *solely* governed by LOAC is beyond the scope of this paper. *See, e.g.*, Adil Haque, *Human Rights in Armed Conflict, Part I*, JUST SECURITY (Nov. 21, 2016), https://www.justsecurity.org/34631/human-rights-armed-conflict-part/.

batants by an adversary State for conduct that violates the domestic criminal law of that adversary State but does not also violate [LOAC]."[73] This narrow proscription does *not* protect a combatant from prosecution under the domestic law of their own State or other rules of international law.[74] Another LOAC rule is the principle of "distinction," which requires combatants to distinguish between civilian targets and military targets, and only operate against the military targets.[75]

While many scholars have examined the intersection of LOAC and cyberspace,[76] LOAC will generally not be triggered by cyber operations unless the traditional LOAC thresholds for an "attack" are met: "human death/injury or tangible property damage."[77] That said, the underlying principles of LOAC may help us think about the benefits and downsides of dealing with State action in certain ways.

d. Certain Cyber Incidents

While malicious State activity in cyberspace is a relatively recent phenomenon compared to espionage or warfare, there are still plenty of examples of State cyber activity that have not led to indictments. According to one database, State-affiliated actors are suspected of conducting 155 different identifiable cyber operations that have affected U.S. targets from 2005 to 2020.[78] In response, there have been fourteen indictments of State-affiliated cyber actors by the Justice Department, with some of those covering multiple operations.[79]

Iran committed one of the earliest attributed State cyberattacks, which rendered many computers belonging to the Las Vegas Sands

---

73. Adil Haque, *The Laws of War: Their Nature and Moral Function*, JUST SECURITY (Dec. 8, 2016), https://www.justsecurity.org/35386/laws-war-nature-moral-function/.

74. *See id*.

75. Schmitt, *supra* note 72, at 272.

76. *See, e.g.*, 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, 424 (2011). Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CAL. L. REV. 817 (2012). *See, e.g.*, Michael N. Schmitt, *Cyber Operations and the* Jus in Bello*: Key Issues*, 87 INT'L L. STUD. 89 (2011).

77. Yoram Dinstein, *Cyber War and International Law: Concluding Remarks at the 2012 Naval War College International Law Conference*, 89 INT'L L. STUD. 276, 284 (2013).

78. The breakdown is: China – 71; Iran – 32; Russia – 29; North Korea – 13; Israel – 2; Ethiopia – 1; France – 1; Lebanon – 1; Pakistan – 1; Saudi Arabia – 1; Spain – 1; Syria – 1; Vietnam – 1. *Cyber Operations Tracker*, *supra* note 9, at 2–18.

79. *See infra* Section II.

casino and hotel inoperable.[80] Iranian hackers have also accessed the email and social media accounts of State Department employees who focused on Iran and the Middle East.[81] Neither campaign led to an indictment.

In 2014, the same year as the first PLA indictment, Chinese hackers accessed the networks of the Office of Personnel Management, stealing the sensitive information of tens of millions of government employees from personnel records and security-clearance files.[82] The intelligence and counterintelligence value of this data makes it one of the most consequential State hacks ever, and, yet, there has not been an indictment for it.

Russia has also been active in cyberspace. In 2015, hackers "presumed to be linked to the Russian government, if not working for it" accessed an unclassified White House network, which included the emails of several White House officials.[83] A few years later, the U.S. Computer Emergency Readiness Team (US-CERT), published an alert warning of Russian government cyber actors infiltrating critical infrastructure systems in the United States.[84]

Although this activity and more like it has not led to an indictment, some activity has led to Treasury Department sanctions. As of the end of 2020, the United States has imposed sanctions for malicious cyber activity 35 times, targeting over 300 people and entities, including State entities like the GRU and FSB and their operatives.[85]

---

80. David E. Sanger & Nicole Perlroth, *Iran is Raising Sophistication and Frequency of Cyberattacks, Study Says*, N.Y. TIMES (Apr. 15, 2015), https://www.nytimes.com/2015/04/16/world/middleeast/iran-is-raising-sophistication-and-frequency-of-cyberattacks-study-says.html.

81. *Id*.

82. Ellen Nakashima, *Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say*, WASH. POST (July 9, 2015), https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/.

83. Michael S. Schmidt & David E. Sanger, *Russian Hackers Read Obama's Unclassified Emails, Officials Say*, N.Y. TIMES (Apr. 25, 2015), https://www.nytimes.com/2015/04/26/us/russian-hackers-read-obamas-unclassified-emails-officials-say.html?_r=0.

84. U.S. Cybersecurity & Infrastructure Agency, Alert TA18-074: Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure, (Mar. 15, 2018), https://www.us-cert.gov/ncas/alerts/TA18-074A [https://perma.cc/4C37-JNVM].

85. Allison Peters & Pierce MacConaghy, *Unpacking US Cyber Sanctions*, THIRD WAY (Jan. 29, 2021), https://www.thirdway.org/memo/unpacking-us-cyber-sanctions; Press Release, Dep't of the Treasury, Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks (Mar. 15, 2018), https://home.treasury.gov/news/press-releases/sm0312 [https://perma.cc/87TT-3PA2].

2. *Characteristics of State Action That Has Not Triggered Indictment of State-Affiliated Actors*

State action that has not led to indictment seems to involve international norms, insufficient evidence, ambiguity over who would be charged, or a desire to protect sources and methods.

In the case of armed conflict, international custom developed into an entire body of international law. In the case of espionage, international norms about diplomatic immunity have reinforced the custom of *persona non grata* declarations and expulsions rather than prosecutions. This international norm likely drove the Dutch decision not to indict the GRU operatives caught in The Hague trying to hack into the OCPW. Rather than criminally charge the operatives, as the U.S. Justice Department later did, the Dutch simply expelled them from the country because they had arrived on diplomatic passports.[86]

For State-sponsored terrorist activity, evidentiary issues might explain the lack of indictments. If it took over three decades to indict the third co-conspirator in the narrow case of the Lockerbie bombing, identifying sufficient evidence to indict specific conspirators in larger operations like the Beirut, Kenya, and Tanzania bombings must be even more difficult. When the State involvement is limited to material support, it can also be unclear who should be indicted. Should the low-level civil servant in the finance ministry be indicted for pushing "send" on a wire transfer? What about the mid-level manager that planned the execution of the money transfer? Or the senior policymaker that made the decision?

When sources and methods are particularly sensitive, prosecutors may choose not to indict because there might be no way to prove their case without revealing a classified source. For example, in the case of Russia and China intercepting President Trump's calls, officials indicated that this knowledge came from human sources and intercepted communications between foreign leaders.[87] Those sources and methods are undoubtedly more valuable than one indictment under the Wiretap Act.

It is unclear which of the above factors most contributed to the lack of indictments for the cyber incidents described above. Another possibility is simply a lack of prosecutorial capacity. As malicious

86. Press Release, Dep't of the Treasury, *supra* note 85. Press Release, Gov't of the Netherlands, Netherlands Defence Intelligence and Security Service Disrupts Russian Cyber Operation Targeting OCPW (Apr. 10, 2018), https://www.government.nl/latest/news/2018/10/04/netherlands-defence-intelligence-and-security-service-disrupts-russian-cyber-operation-targeting-opcw [https://perma.cc/9E5B-VKKQ].

87. Rosenberg & Haberman, *supra* note 52.

cyber activity has increased, there has not been a simultaneous decline in other crimes or a major increase in the number of federal prosecutors. Likely, decisions about which incidents to prosecute must be made based on time, resources, and the strength of the case based on the available evidence.

***

A brief overview of modern U.S. practice has shown a willingness to indict State actors for criminal activity in some instances, like intelligence operatives using non-official cover in the United States or conducting terrorist activity abroad, like the Lockerbie bombing. However, it also reveals a trend of not indicting State actors for nefarious activity if international norms or operational realities so dictate. These practices may help inform an analysis of the State actor cyber indictment policy as it has developed, as well as provide considerations to shape the policy moving forward.

II.
Analysis of Public U.S. Indictments of Malicious State and State-Sponsored Cyber Actors

A comprehensive analysis of the publicly released indictments for malicious State cyber activity makes it easier to deconstruct the practice and identify first principles. The findings do not reveal an overarching policy thus far but do reveal some trends that can inform a clearer policy going forward. First, this section will briefly discuss the methodology used in the analysis. Next, the section analyzes the indictments by the status of the hackers, the goal of the computer network operation, the identity of the target, and the crimes charged, with additional discussion about the characteristics of the various operations. Admittedly, breaking these indictments down along these metrics may be a uniquely American thing to do. Societies like Russia, China, Iran, and North Korea do not adhere to the same clean lines in these areas as the United States. Nevertheless, the analysis is helpful in this case because this paper seeks to understand U.S. decision-making in the cyber indictment context.

A. Methodology

This analysis is based solely on the Justice Department's public indictments for malicious State cyber activity. In some cases, information that was unknown or classified at the time of an indictment gets revealed later and would change the classification of a hacker's status

or an operation's goal—this analysis relies on the information provided by the original indictments because the analysis seeks to examine the decision-making process of the Justice Department at the time of the indictments' release.

One expert on State-related cyberattacks has laid out a very granular spectrum of State responsibility including: State-prohibited, State-prohibited-but-inadequate, State-ignored, State-encouraged, State-shaped, State-coordinated, State-ordered, State-rogue-conducted, State-executed, and State-integrated.[88] This paper strictly focuses on the fifteen DOJ indictments that explicitly declare the malicious cyber activity the work of State actors—i.e. government employees or organizations—or State-affiliated individuals acting on behalf of State actors—i.e. contractors identified as working directly for government employees or organizations. This paper does not include indictments of malicious cyber actors plausibly acting in support of foreign governments if the indictment does not explicitly link them to State actors, such as the Syrian Electronic Army hackers[89] and the Internet Research Agency indictment.[90]

The analysis also excludes cases where post-indictment reporting or revelations suggest a connection between a private hacker's activity and government support that was not described in the original indictment.[91] For example, one Iranian hacker, who was indicted in one instance for malicious cyber activity conducted on behalf of the IRGC, was also indicted separately for his own cyber-enabled extortion scheme against the cable television company HBO.[92] The former indictment is included in the data set below, but the latter indictment is

88. Jason Healey, *Beyond Attribution: Seeking National Responsibility for Cyber Attacks*, ATLANTIC COUNCIL (Feb. 22, 2012), https://www.atlanticcouncil.org/wp-content/uploads/2012/02/022212_ACUS_NatlResponsibilityCyber.PDF.

89. Press Release, Dep't of Just., Computer Hacking Conspiracy Charges Unsealed Against Members of Syrian Electronic Army (Mar. 22, 2016), https://www.justice.gov/opa/pr/computer-hacking-conspiracy-charges-unsealed-against-members-syrian-electronic-army [https://perma.cc/73XY-GY7F].

90. Press Release, Dep't of Just., Grand Jury Indicts Thirteen Russian Individuals and Three Russian Companies for Scheme to Interfere in the United States Political System (Feb. 16, 2018), https://www.justice.gov/opa/pr/grand-jury-indicts-thirteen-russian-individuals-and-three-russian-companies-scheme-interfere [https://perma.cc/M3RM-DQSM].

91. Michael Schwirtz & Joseph Goldstein, *Russian Espionage Piggybacks on a Cybercriminal's Hacking*, N.Y. TIMES (Mar. 12, 2017), https://www.nytimes.com/2017/03/12/world/europe/russia-hacker-evgeniy-bogachev.html.

92. Press Release, U.S. Att'ys Office, S.D.N.Y., Acting Manhattan U.S. Attorney Announces Charges Against Iranian National For Conducting Cyber Attack And $6 Million Extortion Scheme Against HBO (Nov. 21, 2017), https://www.justice.gov/usao-sdny/pr/acting-manhattan-us-attorney-announces-charges-against-iranian-national-conducting [https://perma.cc/J3WM-ENYD].

not. Similarly, in cases such as the twice-indicted North Korean hacker, the actor's status for purposes of the first indictment is characterized as it was in the original indictment, even though the Justice Department linked him to a specific North Korean intelligence service in the second indictment.[93] Indictments that include both activity on behalf of States and activity for private enrichment in the same indictment are included in the data set.

The descriptors used to classify the indictments within each category are defined in their respective sections. The classification determinations were made solely by the author and have not been comprehensively checked or spot-checked by a third-party.

B. Status of the Hackers

The first variable for analysis is the status of the hackers named in the indictments. For State actors, this breaks down into military personnel and intelligence personnel, with the exception of the first North Korean indictment where the classification was ambiguous. "State-sponsored" includes hackers that are not government personnel but are directed by government personnel. Indictments that contain defendants from multiple categories are listed in the table in each of the categories that apply.

TABLE 1. INDICTMENTS BY STATUS OF HACKER

Status of Hacker(s)	**Indictments With Defendant(s) of Indicated Status**
State (Military)	Russia (2018) – 1;[94] Russia (2018) – 2;[95] Russia (2020)[96] China (2014);[97] China (2020) – 1[98] Iran (2020)[99]
State (Intel)	Russia (2017)[100] China (2018)[101]; China (2021)[102] DPRK (2020)[103]
State (Other)	DPRK (2018)[104]
State-Sponsored	Russia (2017) China (2018); China (2020) – 2[105]; China (2021) Iran (2016);[106] Iran (2018);[107] Iran (2019);[108] Iran (2020)

93. Complaint at 3, United States v. Hyok, No. 2:18-mj-01479 (C.D. Cal. June 8, 2018). Indictment at 2, United States v. Hyok, No. 2:20-cr-00614-DMG (C.D. Cal. Dec. 8, 2020).

94. Indictment, United States v. Netyksho, No. 1:18-cr-00215 (D.D.C. July 13, 2018) [hereinafter Russia (2018) – 1].

1. State Actors

The data shows that military personnel show up in indictments more frequently than their counterparts from intelligence agencies. This has three potential explanations: (1) the offending countries tend to *use* military hackers more frequently than they use other kinds of State actor hackers; (2) the Justice Department tends to *catch* military hackers more frequently because their operational security is worse, their operations are less subtle, or the volume of their operations is greater; or (3) the Justice Department *chooses* to indict military hackers more frequently than hackers from intelligence services, perhaps to protect sources and methods associated with American penetrations of foreign intelligence services.

a. Military Personnel

The three military organizations featured in indictments have been the People's Liberation Army (PLA) in China, the GRU in Russia, and the Islamic Revolutionary Guard Corps (IRGC) in Iran. It can be hard to cabin individuals in other societies as purely military personnel the way one might in the United States. For example, the first

95. Indictment, United States v. Morenets, No. 2:18-cr-00263 (W.D. Pa. Oct. 3, 2018) [hereinafter Russia (2018) – 2].
96. Indictment, United States v. Andrienko, No. 2:20-cr-00316, (W.D. Pa. Oct. 15, 2020) [hereinafter Russia (2020)].
97. Indictment, United States v. Dong, No. 2:14-cr-00118 (W.D. Pa. May 1, 2014) [hereinafter China (2014)].
98. Indictment, United States v. Zhiyong, No. 1:20-cr-00046 (N.D. Ga. Jan. 28, 2020) [hereinafter China (2020) – 1].
99. Indictment, United States v. Arabi, No. 1:20-cr-217 (E.D. Va. Sept. 15, 2020) [hereinafter Iran (2020)].
100. Indictment, United States v. Dokuchaev, No. 3:17-cr-00103 (N.D. Cal. Feb. 28, 2017) [hereinafter Russia (2017)].
101. Indictment, United States v. Zhang-Gui, No. 3:13-cr-03132 (S.D. Cal. Oct. 25, 2018) [hereinafter China (2018)].
102. Indictment, United States v. Xiaoyang, No. 3:21-cr-01622 (S.D. Cal. May 28, 2021) [hereinafter China (2021)].
103. Indictment, United States v. Hyok, No. 2:20-cr-00614-DMG (C.D. Cal. Dec. 8, 2020) [hereinafter DPRK (2020)].
104. Complaint, United States v. Hyok, No. 2:18-mj-01479 (C.D. Cal. June 8, 2018) [hereinafter DPRK (2018)].
105. Indictment, United States v. Xiaoyu, No. 4:20-cr-06019 (E.D. Wash. July 7, 2020) [hereinafter China (2020) – 2]
106. Indictment, United States v. Fathi, No. 1:16-cr-00048 (S.D.N.Y. Jan. 21, 2016) [hereinafter Iran (2016)].
107. Indictment, United States v. Rafatnejad, No. 1:18-cr-00094-JMF (S.D.N.Y. Feb. 7, 2018) [hereinafter Iran (2018)].
108. Indictment, United States v. Witt, No. 1:19-cr-00043 (D.D.C. Feb. 8, 2019) [hereinafter Iran (2019)].

PLA indictment indicated that "during the period relevant to this Indictment, Chinese firms hired the same PLA Unit where the defendants worked to provide information technology services."[109] The GRU is tasked with "ensuring Russia's military, economic and technological security."[110] The IRGC is responsible for "protecting the country's political system[,]" but also has a role in "bolstering Iran's economy, including its telecommunications and aerospace industries."[111] These assigned responsibilities indicate a broader role for military organizations in those countries than the Department of Defense serves in the United States.

Thus, it may also be the case that military hackers are caught most often because the militaries of Russia, China, and Iran have a much larger remit than the U.S. military.

b. Intelligence Personnel

The Justice Department has only indicted intelligence agency hackers on four occasions. The first instance involved members of Russia's FSB, which is responsible for domestic intelligence and counterintelligence and which used to be run by Vladimir Putin.[112] Of note, there has not yet been an indictment of hackers from the SVR, Russia's foreign intelligence agency and the group behind the massive "Holiday Bear" or "SolarWinds" incidents, but there has been public attribution accompanied by sanctions and the expulsion of Russian diplomats.[113] This may indicate that the SVR is too "stealthy" and "ghostlike" for the Justice Department to build a case against com-

109. China (2014), *supra* note 97 at 3.

110. Guy Faulconbridge, *What is Russia's GRU Military Intelligence Agency?*, REUTERS (Oct. 5, 2018), https://www.reuters.com/article/us-britain-russia-gru-factbox/what-is-russias-gru-military-intelligence-agency-idUSKCN1MF1VK.

111. Iran (2020), *supra* note 99 at 2–3.

112. Jim Heintz, *What's GRU? A Look at Russia's Shadowy Military Spies*, ASSOCIATED PRESS (Sept. 6, 2018), https://perma.cc/6MMD-6EQB.

113. "Holiday Bear" and "SolarWinds" are both popular names for a string of operations uncovered in late 2020, in which Russian intelligence personnel hacked into numerous government and private sector systems in North America, Europe, Asia, and the Middle East. Ellen Nakashima & Craig Timberg, *Russian Government Hackers are Behind a Broad Espionage Campaign that has Compromised U.S. Agencies, Including Treasury and Commerce*, WASH. POST (Dec. 14, 2020), https://www.washingtonpost.com/national-security/russian-government-spies-are-behind-a-broad-hacking-campaign-that-has-breached-us-agencies-and-a-top-cyber-firm/2020/12/13/d5a53b88-3d7d-11eb-9453-fc36ba051781_story.html; Robert Chesney, *Solar Winds and the Holiday Bear Campaign: A Case Study for the Classroom*, LAWFARE (Aug. 25, 2021), https://www.lawfareblog.com/solarwinds-and-holiday-bear-campaign-case-study-classroom; Press Release, The White House, FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Gov't (Apr. 15, 2021), https://perma.cc/Y7PV-P56A.

pared to the "noisy" FSB, but it could just be that cases against SVR operatives are still being put together.[114] It might also indicate that the U.S. government has decided that the SVR's modus operandi is espionage, which is better fought via countersurveillance and disruption rather than an indictment that will reveal sources and methods.

In China, the Ministry of State Security has provincial divisions, such as the Jiangsu State Security Department (JSSD), the Guangdong State Security Department (GSSD), and the Hainan State Security Department (HSSD), that are responsible for domestic counter-intelligence and non-military foreign intelligence.[115] The Justice Department indicted two JSSD officers in 2018 for their role in a series of hacks primarily targeting aerospace companies.[116] However, a 2020 indictment of Chinese criminal hackers did not name as a defendant a GSSD officer who assisted the hackers and whose identity was apparently known to prosecutors.[117] The 2020 indictment does not explain this decision, but it might be another case of sources and methods protection or a case of lack of sufficient evidence. In 2021, the Justice Department named three HSSD officers in an indictment for cyberespionage and even provided photos of two of the individuals, an impressive demonstration of U.S. attribution capabilities.[118]

An indictment of North Korean members of the Reconnaissance General Bureau (RGB) poses a slightly difficult categorization challenge.[119] While the indictment describes the RGB as a "military intelligence agency[,]" the U.S. Department of Defense considers it "North Korea's primary foreign intelligence service" rather than a military organization, noting that it is responsible for intelligence collection and clandestine operations including in cyberspace.[120] Of note, the indictment mentions that the RGB hackers at times worked from China and Russia.[121] It is unclear whether or not China and Russia knew that North Korean intelligence personnel were conducting cyber operations

114. Krebs Statement, *supra* note 15, at 3.

115. *See, e.g.*, China (2018), *supra* note 101, at 2. *See also* China (2021), *supra* note 102.

116. *Id.*

117. China (2020) – 2, *supra* note 105, at 3.

118. China (2021), *supra* note 102, at 4.

119. DPRK (2020), *supra* note 103, at 1.

120. OFF. OF THE SEC'Y OF DEF., 9-600987B, MILITARY AND SECURITY DEVELOPMENTS INVOLVING THE DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA: REPORT TO CONGRESS 14 (2017), https://fas.org/irp/world/dprk/dod-2017.pdf.

121. DPRK (2020), *supra* note 103, at 2.

from within their borders, which could have implications under international law.[122]

c. Other Government Personnel

In one instance, a North Korean hacker was identified as a government employee, but not a member of the military or an intelligence service. The hacker was described as "a programmer employed by the government" that worked for a North Korean government front company and did some non-malicious work for paying clients on the side.[123] This hacker was subsequently identified as a member of the RGB in the 2020 North Korean indictment, showing the improved attribution capabilities of U.S. investigators.[124]

2. State-Sponsored Actors

Just as some of the State actors above moonlighted for private clients, some private criminal hackers do work for the government. One private hacker in Iran that was involved in cyberattacks against the U.S. financial industry even "received credit for his computer intrusion work from the Iranian Government towards completion of his mandatory military service in Iran."[125]

Typically, these hackers-for-hire are known criminal hackers within their home country. They might be international cybercriminals, like one hacker involved in the Russian hacks of Yahoo, who was the subject of an Interpol Red Notice and listed on the FBI's "Most Wanted" hackers list, before his work on behalf of the FSB.[126] Or, like in Iran, they might be more reminiscent of contractors, operating as corporate entities with "disbursed regular salaries, established work hours, issued assignments, and employed supervisors and managers" that enter into contracts to procure malware and provide ongoing support.[127] The hackers might also leverage the assistance of employees inside target companies, which seems to be a preferred method in China.[128]

---

122. Mari Dugas, *The Latest North Korea Cyber Indictment Should Serve as a Model*, JUST SECURITY (Feb. 24, 2021), https://www.justsecurity.org/74930/the-latest-north-korea-cyber-indictment-should-serve-as-a-model/.

123. DPRK (2018), *supra* note 104, at 5.

124. DPRK (2020), *supra* note 103, at 2.

125. Iran (2016), *supra* note 106, at 6.

126. Russia (2017), *supra* note 100, at 2–3.

127. Iran (2018), *supra* note 107, at 1; Iran (2019), *supra* note 108, at 9; *id.* at 20; Iran (2020), *supra* note 99, at 3–4.

128. China (2018), *supra* note 101, at 3–5.

On one occasion, the Russian FSB used a criminal hacker outside of Russia—a Canadian national and resident that assisted with the Yahoo hacks.[129] Either these countries or foreign hackers themselves have been hesitant to take this risk again, as the Canadian was arrested and extradited to the United States, where he was sentenced to five years in prison and a $250,000 fine.[130]

3. Previously Indicted Defendants

In several instances, defendants in these indictments are repeat-offenders. It is tempting to use this fact as evidence that the indictments do not have a deterrent effect, but in some cases, it seems to be a function of two indictments covering similar activity or a parallel time period. It may also be a function of U.S. investigators penetrating particular groups and indicting their members repeatedly while groups with better operational security go un-indicted.

One criminal Russian hacker indicted for his involvement in the Yahoo hacks had been indicted for computer fraud and abuse in 2012 in the District of Nevada and for intrusions into U.S. e-commerce companies in 2013 in the Northern District of California.[131] He was even once arrested in Europe on a U.S. provisional arrest warrant but was able to return to Russia before he could be extradited.[132]

The indictment of Russian GRU personnel for the hack-and-leak operation against the Democratic National Committee during the 2016 presidential election led to three repeat-offenders. Two of the hackers were indicted again a few months later for a campaign of cyber activity that spanned a similar time period, and one more was indicted for a second time in 2020 for his involvement in a global campaign of cyber operations.[133]

One North Korean hacker has been named in both North Korean indictments, although this is because the second indictment includes some of the same activity described in the first indictment.[134]

---

129. Russia (2017), *supra* note 100, at 4.

130. David Shepardson, *Canadian Who Helped Yahoo Email Hackers Gets Five Years in Prison*, REUTERS (May 29, 2018), https://www.reuters.com/article/us-yahoo-cyber/canadian-who-helped-yahoo-email-hackers-gets-five-years-in-prison-idUSKCN1IU2OE.

131. Russia (2017), *supra* note 100, at 4.

132. *Id.*

133. Russia (2018) – 2, *supra* note 95, at 1; Russia (2018) – 1, *supra* note 94, at 1; Russia (2020), *supra* note 96, at 5–6.

134. DPRK (2020), *supra* note 103, at 1.

***

The prevailing trend is that the Justice Department has indicted military personnel more frequently than intelligence personnel. This could be because countries tend to *use* military hackers the most. Alternatively, the U.S. government might *catch* military hackers more frequently because of worse operational security and tradecraft. A final possibility is that the Justice Department *chooses* to indict military hackers more frequently than hackers from intelligence services, perhaps to protect sources and methods associated with American penetrations of foreign intelligence services.

C. Goal of the Operation

The next variable to examine is the goal of the operation. Government lawyers will often look to the consequences of a cyber operation to determine whether the intrusion is an exploitation—"the unauthorized collection of information from a computer network"—or an attack—"the destruction or manipulation of data on a computer network."[135] While one scholar has examined cyber operations generally under the frameworks of "espionage" and "covert action," using more granular categories here may reveal more useful insights.[136]

In many cases, it is impossible to accurately categorize the exact nature of a cyber operation without information about the attackers' intent, which is usually unknown.[137] Additionally, if the operation is uncovered while it is ongoing, the intruders may have several options as to subsequent phases, rather than being locked into a single identifiable course of action.[138] A few lines of code can separate a computer network *exploitation* from a computer network *attack*.[139]

---

135. Robert D. Williams, *(Spy) Game Change: Cyber Networks, Intelligence Collection, and Covert Action*, 79 GEO. WASH. L. REV. 1162, 1192 (2011); BEN BUCHANAN, THE CYBERSECURITY DILEMMA: HACKING, TRUST, AND FEAR BETWEEN NATIONS 12 (2016).

136. *See generally*, Williams, *supra* note 135. It has been publicly reported that the Central Intelligence Agency operates under the legal framework for "covert action" for some U.S. cyber operations. Robert Chesney, *The CIA, Covert Action and Operations in Cyberspace*, LAWFARE (July 15, 2020), https://www.lawfareblog.com/cia-covert-action-and-operations-cyberspace (explaining that the CIA uses its legal authorities for "covert action" to conduct some cyber operations).

137. *See* NAT'L RESEARCH COUNCIL, TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 194 (William A. Owens et al. eds., 2009) (listing examples of covert actions where uncovering the activity itself still might not reveal a State's underlying motivation).

138. BUCHANAN, *supra* note 135, at 5.

139. Dave Aitel, *Responsible Cyber Offense* (Jan. 30, 2021) (unpublished working paper) (on file with author).

This analysis has identified six major categories that describe the goals of the operations described in the various indictments: (1) traditional espionage; (2) economic espionage; (3) direct financial gain; (4) election interference; (5) other disruptive activities; and (6) counterintelligence and internal security. The bounds of these categories are explained as each is addressed.

TABLE 2. INDICTMENTS BY GOAL OF OPERATION

Goal of Operation	Indictments With Indicated Goal of Operation
Traditional Espionage	Russia (2017); Russia (2018) – 1; Russia (2020) China (2020) – 1; China (2020) – 2; China (2021) Iran (2018); Iran (2019) DPRK (2018); DPRK (2020)
Economic Espionage	Russia (2017); Russia (2018) – 2 China (2014); China (2018); China (2020) – 1; China (2020) – 2; China (2021) Iran (2018); Iran (2020) DPRK (2018); DPRK (2020)
Direct Financial Gain	Russia (2017) China (2020) – 2 DPRK (2018); DPRK (2020)
Election Interference	Russia (2018) – 1; Russia (2020)
Other Disruptive Activities	Russia (2018) – 2; Russia (2020) Iran (2016) DPRK (2018); DPRK (2020)
Counterintelligence & Internal Security	Russia (2017) China (2020) – 2

1. Traditional Espionage

Traditional espionage involves stealing the kind of information that intelligence agencies typically seek, including material related to defense capabilities, political considerations, or adversary vulnerabilities.[140] This might involve accessing the communications of U.S. gov-

140. OFF. OF DIR. OF NAT'L INTEL., NATIONAL INTELLIGENCE STRATEGY 6–7 (2019), https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf.

ernment officials, like "cyber security, diplomatic, military, and White House personnel."[141] It might also involve hacking the government networks of a rival, as North Korea is described as doing to South Korea in the 2018 North Korean indictment.[142]

Hacking U.S. defense contractors or U.S. critical infrastructure might qualify as both traditional espionage and economic espionage—intelligence operatives seek this information for their own purposes, even if it also has potential commercial value.[143] For example, two Chinese criminal hackers "stole information regarding military satellite programs; military wireless networks and communications systems; high powered microwave and laser systems; a counter-chemical weapons system; and ship-to-helicopter integration systems" for Chinese intelligence and for commercial purposes.[144] Similarly, the hack of Equifax—one of America's three largest consumer credit reporting agencies—that stole the personal information of 145 million U.S. citizens likely provided valuable data to Chinese intelligence agencies and to Chinese companies.[145]

2. Economic Espionage

Economic espionage involves stealing trade secrets or other information that will provide commercial benefit.[146] The Commission on the Theft of American Intellectual Property estimates that, taken together, the theft of trade secrets, counterfeit goods, and pirated software costs America between $225 billion and $600 billion.[147] There is a distinction between economic espionage (i.e. stealing information to sell a product or service) and intellectual property theft to support national security objectives (i.e. stealing information to develop a national security capability), but that distinction can be hard to tease out in these indictments.[148] This is further complicated when groups one might naturally think of as conducting traditional espionage are also tasked with economic espionage responsibilities, like the

141. Russia (2017), *supra* note 100, at 10; *see also* Iran (2019), *supra* note 108, at 19.

142. DPRK (2018), *supra* note 104, at 105.

143. *Id.* at 4.

144. China (2020) – 2, *supra* note 105, at 3.

145. China (2020) – 1, *supra* note 98, at 2.

146. 18 U.S.C. § 1831.

147. CYBER REPORT, *supra* note 12, at 28.

148. Erica D. Borghard & Shawn W. Lonergan, *Public-Private Partnerships in Cyberspace in an Era of Great-Power Competition*, *in* TEN YEARS IN: IMPLEMENTING STRATEGIC APPROACHES TO CYBERSPACE 113 (Jacquelyn G. Schneider et al. eds., 2020).

IRGC.[149] Because the same information can be targeted for either purpose, this analysis errs on the side of classifying any theft of information with potential commercial utility as economic espionage.

Cyber economic espionage operations have targeted many sectors, including technology, manufacturing, aerospace, and financial services companies.[150] China has been the biggest offender, described as having stolen "hundreds of millions of dollars' worth of trade secrets, intellectual property, and other valuable business information" in one indictment alone.[151] Iran has also targeted academic research from universities that might have commercial implications.[152]

3. Direct Financial Gain

Distinct from economic espionage is the goal of direct financial gain either for the hacker or for the State-sponsor, through digital theft, extortion, or other digital exploitation. In a creative pursuit of personal enrichment, the experienced cybercriminal that aided the FSB in the Yahoo hacks used the operation to steal credit card and gift card information and sell millions of contact lists to spam marketers.[153] Russian government hackers do not appear to seek personal enrichment from their operations—perhaps to disincentivize Russian State hackers from personally enriching themselves through their operations, Russia decided to ban Russian government officials as well as their spouses and minor children from owning "cryptocurrencies and any digital assets issued outside the country."[154] However, the North Korean government hackers were described as pursuing private financial gain alongside their theft for the State.[155] Chinese government hackers seem to avoid personal enrichment, although Chinese criminal hackers have benefited personally from extortion and the sale of commercial information.[156]

North Korea is by far the most prolific in cyber theft for the enrichment of the State. The 2018 indictment described two major theft attempts: one from the central bank of Bangladesh that resulted in $81 million in losses (although the hackers tried to steal up to $1 billion)

149. Iran (2020), *supra* note 99, at 3.
150. Russia (2017), *supra* note 100, at 2.
151. China (2020) – 2, *supra* note 105, at 3.
152. Iran (2018), *supra* note 107, at 2–3.
153. Russia (2017), *supra* note 100, at 3.
154. Anna Baydakova, *Russian Public Officials Banned from Holding Cryptocurrency*, COINDESK (Jan. 25, 2021, 6:02 AM), https://www.coindesk.com/russian-public-officials-banned-crypto-holdings.
155. DPRK (2020), *supra* note 103, at 2.
156. China (2020) – 2, *supra* note 105, at 3.

and one from a bank in Africa that initially resulted in a $100 million loss, although the funds were ultimately recovered.[157] They also benefited from ransomware attacks, although the exact proceeds are uncertain.[158] The 2020 indictment described $1.3 billion in attempted cyber theft and extortion. The operations varied from cyber intrusions of banks and cryptocurrency companies to ATM cash-outs to a fake cryptocurrency offering known as the "Marine Chain Token."[159]

4. Election Interference

Russia is the only country thus far to be indicted for election interference efforts. Although there is no specific crime of "election interference," the Justice Department breaks interference efforts into five distinct categories: (1) cyber operations targeting election infrastructure; (2) cyber operations targeting political parties, campaigns, and public officials; (3) covert influence operations to assist or harm political organizations, campaigns and public officials; (4) covert influence operations to influence public opinion and sow division; (5) overt influence efforts to influence policymakers and the public.[160] Charged Russian activities fit mostly into the second and third categories.

In 2016, GRU hackers accessed the emails of volunteers and employees of the Clinton Campaign and accessed the networks of the Democratic Congressional Campaign Committee and the Democratic National Committee. They "staged and released tens of thousands of the stolen emails and documents" to harm those entities.[161] In 2017, the GRU targeted over 100 individuals from French President Emmanuel Macron's political party, seemingly hoping to replicate the 2016 U.S. efforts.[162]

5. Other Disruptive Activities

Russia, Iran, and North Korea have all conducted operations that fall under the umbrella of "other disruptive activities," including distributed denial of service (DDoS) attacks, data destruction, exploitation of critical infrastructure, operations in support of disinformation, and operations seeking public embarrassment. Again, it is unclear whether the Justice Department has not indicted Chinese State actors

157. DPRK (2018), *supra* note 104, at 56; *id.* at 85.
158. *Id.* at 106–07.
159. DPRK (2020), *supra* note 103, at 24–25.
160. CYBER REPORT, *supra* note 12, at 9.
161. Russia (2018) – 1, *supra* note 94, at 2–3.
162. Russia (2020), *supra* note 96, at 15.

for these types of activities because: (a) the Chinese rarely conduct these operations; (b) their operational security is good enough to not get caught; or (c) they have not been indicted even when detected, perhaps because other U.S. government equities weigh against an indictment.

A DDoS attack is the "intentional paralyzing of a computer network by flooding it with data sent simultaneously from many individual computers."[163] Iran conducted a large-scale campaign of DDoS attacks against U.S. financial institutions that lasted at least 176 days and caused hundreds of thousands of customers to be unable to access their bank accounts online.[164] The intent was seemingly just to undermine American businesses.[165]

Data destruction is the use of malicious software to erase information on a computer or to render a computer inoperable.[166] North Korea is a frequent destroyer of data, either for revenge—as in its hacks of Sony Pictures for a comedic movie disparaging North Korea—or for financial gain via ransomware or to cover its tracks.[167] Russia has also pursued data destruction, either out of spite—for example in its disruption of the Olympic Games in South Korea after a World Anti-Doping Agency report about Russian athletes doping—or out of recklessness—in the case of the NotPetya malware that rendered inoperable the computer systems of banks, newspapers, electricity companies, and health centers.[168]

The NotPetya indictment also detailed Russian exploitation of critical infrastructure, including the disruption of electricity to more than 225,000 Ukrainian residents and the disruption of approximately 150,000 financial transactions by Ukraine's Ministry of Finance and State Treasury Service.[169] On a much smaller scale, Iran has also been indicted for exploiting critical infrastructure, specifically the Bowman Dam in Rye, New York.[170]

Russia in particular has a penchant for disinformation. Russian GRU operatives were indicted for a series of cyber operations targeting anti-doping agencies and sporting federations to support a disinformation campaign to counter allegations of doping by Russian

163. *Cyber Operations Tracker*, *supra* note 9, at 19.
164. Iran (2016), *supra* note 106, at 4.
165. *Id.*
166. *Cyber Operations Tracker*, *supra* note 9, at 20.
167. DPRK (2018), *supra* note 104, at 3; DPRK (2020), *supra* note 103, at 4.
168. Russia (2020), *supra* note 96, at 34; *id.* at 16–22.
169. Russia (2020), *supra* note 96, at 10–11.
170. Iran (2016), *supra* note 106, at 14.

athletes.[171] The officers hoped to: "undermine, retaliate against and otherwise delegitimize the efforts of international anti-doping organizations and officials who had publicly exposed Russian government-sponsored doping by Russian athletes"; "publicize and expose individual sensitive medical information and drug testing results of athletes"; and "damage the reputations of clean athletes from various countries by falsely claiming that such athletes were using banned or performance-enhancing drugs."[172] The operatives similarly targeted the Organisation for the Prohibition of Chemical Weapons to inform other disinformation campaigns related to the GRU assassination attempt of Sergei Skripal.[173]

Both North Korea and Russia have undertaken cyber operations for the sake of publicly embarrassing others. North Korea stole movies and confidential email correspondence from Sony Pictures that they then released presumably to embarrass the company.[174] Russia defaced approximately 15,000 government and non-government websites in the country of Georgia as part of an extended campaign.[175]

Overall, Russia appears to be the most disruptive State in cyberspace, followed by North Korea and Iran, with China avoiding disruptive behavior and mostly sticking to traditional and economic espionage.

6. Counterintelligence & Internal Security

Russia, China, and Iran all appear to use their global hacking campaigns for counterintelligence and "internal security" purposes—an autocratic euphemism for crushing dissent—although the Justice Department has only detailed Russian and Chinese efforts. Presumably, this is less necessary for North Korea because most ordinary North Korean citizens do not have regular access to the internet.[176] As part of the Yahoo hacks, the FSB, which has an internal security func-

171. Russia (2018) – 2, *supra* note 95, at 2.
172. Russia (2018) – 2, *supra* note 95, at 5.
173. Russia (2018) – 2, *supra* note 95, at 3–4. The indictment mentions a former GRU officer poisoned in the United Kingdom, which is presumably Sergei Skripal. *See* Richard Pérez-Peña & Ellen Barry, *U.K. Charges 2 Men in Novichok Poisoning, Saying They're Russian Agents*, N.Y. Times (Sept. 5, 2018), https://www.nytimes.com/2018/09/05/world/europe/russia-uk-novichok-skripal.html.
174. DPRK (2018), *supra* note 104, at 3; *see also* Alex Altman & Alex Fitzpatrick, *Everything We Know About Sony, The Interview and North Korea*, Time (Dec. 17, 2014), https://time.com/3639275/the-interview-sony-hack-north-korea/.
175. Russia (2020), *supra* note 96, at 42.
176. Robert R. King, *North Koreans Want External Information, But Kim Jong-Un Seeks to Limit Access*, CSIS (May 15, 2019), https://www.csis.org/analysis/north-koreans-want-external-information-kim-jong-un-seeks-limit-access.

tion, sought access to the communications of Russian journalists, Russian government officials, Russian politicians critical of the Russian government, employees of Russian companies, and employees of a Russian investment banking firm.[177]

China's efforts have been similar. One of the 2020 indictments of Chinese hackers described the collection of personal email accounts belonging to Chinese dissidents, emails between dissidents and the office of the Dalai Lama, emails belonging to a Chinese Christian pastor in Chengdu, and emails from a U.S. professor and two Canadian residents, "who advocated for freedom and democracy in Hong Kong."[178]

Information security researchers have discovered Iranian hacking operations targeting dissidents and perceived domestic threat actors as well, but this has not yet been outlined in an indictment.[179]

D. Identity of the Target

A third major variable to analyze is the identity of the target of the computer network operation. This variable is ripe for extreme granularity, but this analysis divides target identities into four broad categories: (1) U.S. government entities; (2) U.S. non-government entities; (3) non-U.S. government entities; and (4) non-U.S. non-government entities. The categorization is based on the targeted network or accounts, not the target of the intelligence sought—for example, a U.S. defense contractor is considered a "U.S. non-government entity" even though the hacker may target it seeking information about U.S. military capabilities.

177. Russia (2017), *supra* note 100, at 2, 10.
178. China (2020) – 2, *supra* note 105, at 3–4.
179. *Domestic Kitten – An Inside Look at the Iranian Surveillance Operations*, CHECK POINT RSCH. (Feb. 8, 2021), https://research.checkpoint.com/2021/domestic-kitten-an-inside-look-at-the-iranian-surveillance-operations/.

TABLE 3. INDICTMENTS BY IDENTITY OF TARGET

Identity of Target(s)	Indictments With Indicated Identity of Target(s)
Government Entity (U.S.)	China (2020) – 2; China (2021) Iran (2018); Iran (2019); Iran (2020) DPRK (2020)
Non-Government Entity (U.S.) [* = "Critical Infrastructure Sector" Targeted]	Russia (2017)*; Russia (2018) – 1; Russia (2018) – 2*; Russia (2020)* China (2014)*; China (2018)*; China (2020) – 1*; China (2020) – 2*; China (2021)* Iran (2016)*; Iran (2018)*; Iran (2020)* DPRK (2018)*; DPRK (2020)*
Government Entity (Non-U.S.)	Russia (2020) China (2021) DPRK (2018); DPRK (2020)
Non-Government Entity (Non-U.S.)	Russia (2018) – 2; Russia (2020) China (2018); China (2020) – 2; China (2021) Iran (2018); Iran (2020) DPRK (2018); DPRK (2020)

1. Government Entity (U.S.)

Whether for reasons of great prolificacy, poor operational security, or Justice Department policy, the Justice Department indicts Iran most frequently among State actors for targeting government networks, both federal and state. Iran has pursued federal targets like the Department of Labor, the Federal Energy Regulatory Commission, the National Aeronautics and Space Administration, and individual federal government employees, as well as state targets like Hawaii and the Indiana Department of Education.[180] North Korea is alleged to have targeted individual federal employees, as well, primarily of the State Department and Department of Defense.[181] Federal prosecutors from the Eastern District of Washington identified Chinese hackers targeting a Department of Energy facility in their district, but the activity outlined in the indictment appears to be very minor reconnaissance likely included as a jurisdictional hook.[182] The 2021 indictment

180. Iran (2018), *supra* note 107, at 8–9; Iran (2019), *supra* note 108, at 19; Iran (2020), *supra* note 99, at 14.
181. DPRK (2020), *supra* note 103, at 23.
182. China (2020) – 2, *supra* note 105, at 12.

of Chinese intelligence officers describes an operation targeting the National Institutes of Health, especially information from the Office of Biodefense Research Affairs.[183]

2. Non-Government Entity (U.S.)

The indictments most frequently showcase operations against non-government entities in the United States. Of the indictments describing operations against those entities, all but one detail targets from designated "critical infrastructure" sectors. The Cybersecurity and Infrastructure Security Agency (CISA) helps coordinate the security of sixteen critical infrastructure sectors "whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[184] The sectors are: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater.[185] The only indictment that does not feature a critical infrastructure target is the indictment for the 2016 election-related DNC hacks.[186]

Non-government domestic targets of foreign State actor hackers run the gamut, but some categories are more common. Iran, China, and North Korea have all targeted defense contractors and technology companies.[187] Iran, North Korea, and China have targeted universities and academics.[188] China and Russia have even targeted the exact same nuclear energy company.[189]

Other targets are more idiosyncratic. North Korea is unique in its targeting of cryptocurrency websites and entertainment companies that

183. China (2021), *supra* note 102, at 13.
184. U.S. CYBERSECURITY & INFO. SEC. AGENCY, CRITICAL INFRASTRUCTURE SECTORS (2020), https://www.cisa.gov/critical-infrastructure-sectors.
185. *Id.*
186. *See generally* Russia (2018) – 1, *supra* note 94.
187. Iran (2020), *supra* note 99, at 4; DPRK (2018), *supra* note 104, at 4; DPRK (2020), *supra* note 103, at 23; China (2018), *supra* note 101, at 5–6; China (2020) – 2, *supra* note 105, at 11–14.
188. Iran (2018), *supra* note 107, at 2; DPRK (2018), *supra* note 104, at 4; China (2021), *supra* note 102, at 5–6. Universities are considered critical infrastructure as part of the "Education Facilities" subsector within the "Government Facilities" sector. U.S. CYBERSECURITY & INFO. SEC. AGENCY, *supra* note 184.
189. Russia (2018) – 2, *supra* note 95, at 2–3; China (2014), *supra* note 97, at 4.

produce content perceived as mocking North Korea.[190] Russia has a penchant for targeting political entities it perceives as enemies, such as the DNC and anti-doping organizations, in support of disinformation campaigns.[191] China targets the widest variety of companies as part of its intellectual property theft campaign, as well as repositories of personal information such as Equifax.[192]

3. Government Entity (Non-U.S.)

Several indictments also detail computer network operations against non-U.S. government entities. In North Korea's case, these have primarily been foreign State-run banks targeted for cyber-theft.[193] However, one indictment also details operations targeting South Korean government entities and ransomware targeting the U.K.'s National Health Service.[194] While only one indictment details Russian cyber operations against non-U.S. government entities, the actions appear quite widespread. Russia has targeted Ukrainian government entities, local governments in France, South Korean government agencies during the 2018 Winter Olympics, British agencies investigating Russian chemical weapons use, and many government websites in the country of Georgia.[195] The 2021 indictment of Chinese intelligence officers reveals a successful operation to infiltrate a Cambodian government ministry to steal documents about ongoing diplomatic negotiations.[196]

4. Non-Government Entity (Non-U.S.)

Similar to the breakdown of U.S. targets, more indictments detail non-government targets abroad than government targets abroad. The types of non-government targets abroad are also very similar to the types of non-government targets in the U.S. Iran targeted 176 foreign universities in 21 different countries and some international organizations.[197] North Korea has focused primarily on financial institutions, cryptocurrency companies, and entertainment companies.[198] Russia

190. DPRK (2018), *supra* note 104, at 4; DPRK (2020), *supra* note 103, at 19; *id.* at 4–5.
191. Russia (2018) – 1, *supra* note 94, at 2–3; Russia (2018) – 2, *supra* note 95, at 2–3.
192. China (2018), *supra* note 101, at 5.
193. DPRK (2018), *supra* note 104, at 3–4; DPRK (2020), *supra* note 103, at 5–6.
194. DPRK (2018), *supra* note 104, at 105–07.
195. Russia (2020), *supra* note 96, at 3–4; *id.* at 11; *id.* at 40–42.
196. China (2021), *supra* note 102, at 26.
197. Iran (2018), *supra* note 107, at 2; *id.* at 8–9.
198. DPRK (2018), *supra* note 104, at 4–6.

has gone after political adversaries and non-governmental organizations investigating nefarious Russian activities.[199] And China has targeted companies with commercially valuable intellectual property.[200]

E. Crimes Charged

Looking at the breakdown of the crimes charged in indictments of foreign State-directed hackers provides insight into the behavior of those hackers, but also into the access and evidence-gathering capabilities of U.S. investigators. The most common crimes charged can generally be sorted into computer fraud and abuse crimes, economic espionage crimes, and other crimes not specific to computer hacking.

199. Russia (2018) – 2, *supra* note 95, at 2–4; Russia (2020), *supra* note 96, at 3–4; *id.* at 39.

200. China (2018), *supra* note 101, at 5–6; China (2020) – 2, *supra* note 105, at 2.

TABLE 4. INDICTMENTS BY CRIMES CHARGED

Crime(s) Charged	Indictments With Indicated Crime(s) Charged
Unlawful Computer Access 18 U.S.C. § 1030(a)(2)	Russia (2017)*; Russia (2018) – 1**; Russia (2018) – 2**; Russia (2020)** China (2014)*; China (2018)**; China (2020) – 1*; China (2020) – 2*; China (2021)** Iran (2018)*; Iran (2019)*; Iran (2020)* DPRK (2018)**; DPRK (2020)**
Accessing a Computer to Defraud or Obtain Value 18 U.S.C. § 1030(a)(4)	DPRK (2018)**; DPRK (2020)**
Damaging a Computer 18 U.S.C. § 1030(a)(5)	Russia (2017)*; Russia (2018) – 1**; Russia (2018) – 2**; Russia (2020)* China (2014)*; China (2018)*; China (2020) – 1*; China (2020) – 2**; China (2021)** Iran (2016)*; Iran (2019)*; Iran (2020)* DPRK (2018)**; DPRK (2020)**
Trafficking in Passwords 18 U.S.C. § 1030(a)(6)	Iran (2018)**
Threatening to Damage a Computer 18 U.S.C. § 1030(a)(7)	DPRK (2020)**
Wire Fraud 18 U.S.C. § 1343	Russia (2017)**; Russia (2018) – 2*; Russia (2020)* China (2020) – 1*; China (2020) – 2** Iran (2018)*; Iran (2020)** DPRK (2018)**; DPRK (2020)**
Bank Fraud 18 U.S.C. § 1344	DPRK (2020)**
Access Device Fraud 18 U.S.C. § 1029	Russia (2017)*
Economic Espionage & Theft of Trade Secrets 18 U.S.C. §§ 1831, 1832	Russia (2017)* China (2014); China (2020) – 1*; China (2020) – 2**; China (2021)**
Identity Theft 18 U.S.C. §§ 1028, 1028A	Russia (2017); Russia (2018) – 1; Russia (2018) – 2; Russia (2020) China (2014); China (2020) – 2 Iran (2018); Iran (2019); Iran (2020)
Money Laundering 18 U.S.C. §§ 1956, 1957	Russia (2018) – 1**; Russia (2018) – 2**
* = Indicted for crime *and* conspiracy to commit crime; ** = Indicted for conspiracy *only*	

1. Charges Related to Computer Fraud and Abuse

Federal prosecutors most often charge foreign State-directed hackers with unlawful computer access and damaging a computer under the Computer Fraud and Abuse Act (CFAA) or conspiracy to commit those crimes.[201] North Korean hackers have only been charged with conspiracy to commit these crimes, while Iranian hackers have consistently been charged with conspiracy and the commission of the crimes themselves. This may illustrate the relative difficulty of fully infiltrating North Korean operations and the relative ease of infiltrating Iranian ones. Russia and China fall somewhere in between.

While the vast majority of computer charges come under 18 U.S.C. § 1030, one Russian indictment also featured a charge for "access device" fraud and trafficking, which prohibits the use or trafficking of means to access accounts that can be used to obtain something of value.[202] It is unclear why this crime, which seems to prohibit most phishing activities, has only been charged one time. There has also only been one use of 18 U.S.C. 3559(g)(1), which increases the maximum allowable sentence when someone falsely registers a domain in the commission of a felony.[203]

2. Charges Related to Economic Espionage and Trade Secret Theft

China is the most frequent offender of economic espionage and theft of trade secrets, although Russian hackers have been charged one time. 18 U.S.C. §§ 1831–32 prohibit the theft of trade secrets for the benefit of a foreign government (§ 1831) or someone other than the owner (§ 1832). It is unclear why prosecutors have only charged these crimes on four occasions, when ten indictments describe economic espionage activities.[204] This might signal a lack of capacity by U.S. investigators or a decision that proving such charges would require an undesirable revelation of sources and methods.

3. Other Crimes Charged

Several other charged crimes include wire fraud, identity theft, and money laundering. Wire fraud, 18 U.S.C. § 1343, is the most frequently charged crime outside of computer fraud and abuse crimes.

---

201. 18 U.S.C. §§ 1030(a)(2), 1030(a)(5), 1030(b).
202. 18 U.S.C. § 1029.
203. Russia (2020), *supra* note 96, at 1.
204. *See supra* Section II.C.

While wire fraud is similar to several computer fraud charges, wire fraud authorizes more punitive penalties and can serve as a predicate for racketeering and money laundering charges, unlike most CFAA violations.[205] North Korean hackers are the only ones thus far to also be charged with conspiracy to commit bank fraud, 18 U.S.C. § 1344, for their cyber-theft campaign targeting banks. Identity theft is another common charge, as false identities are frequently used in computer crimes.[206] Only Russian State hackers have been charged with conspiracy to commit money laundering, 18 U.S.C. §§ 1956–57, but private individuals from multiple countries have been indicted separately for money laundering in connection with these State-directed cybercrimes.[207] While not reflected in Table 4, prosecutors have also frequently used aiding and abetting charges, 18 U.S.C. § 2,[208] and pursued forfeiture in relation to the charged crimes.[209]

F. Characterization of Operations

While it is difficult to characterize all the indicted operations in a table according to the techniques used, an overview of the various techniques is useful in understanding how different indicators of computer network operations might prompt different U.S. government responses. The vast majority of these operations involved spear phishing and malware or vulnerability exploitations. There were also a few instances of ransomware, one DDoS attack, and other creative methods.

"Spear phishing" is when an individual sends an email to a target that is "not only designed to appear legitimate, but is also tailored and

---

205. CYBER REPORT, *supra* note 12, at 64. As shown in the chart, money laundering has been charged on two occasions, but racketeering has not been charged so far.

206. 18 U.S.C. § 1028(a)(7), 1028A.

207. *See, e.g.*, Press Release, U.S. Dep't of Just., Two Chinese Nationals Charged with Laundering Over $100 Million in Cryptocurrency from Exchange Hack (Mar. 2, 2020), https://www.justice.gov/opa/pr/two-chinese-nationals-charged-laundering-over-100-million-cryptocurrency-exchange-hack [https://perma.cc/7X6Q-KFKM]; *see also* Press Release, U.S. Dep't of Just., Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe (Feb. 17, 2021), https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and [https://perma.cc/JJ5P-S7P4].

208. *See, e.g.,* Russia (2017), *supra* note 100; Russia (2018) – 1, *supra* note 94; Russia (2018) – 2, *supra* note 95; Russia (2020), *supra* note 96; China (2014), *supra* note 97; China (2020) – 1, *supra* note 98; China (2020) – 2, *supra* note 105; Iran (2016), *supra* note 106; Iran (2018), *supra* note 107; Iran (2019), *supra* note 108; Iran (2020), *supra* note 99.

209. *See, e.g.,* Russia (2017), *supra* note 100; Russia (2018) – 1, *supra* note 94; Russia (2020), *supra* note 96; China (2018), *supra* note 101; China (2020) – 1, *supra* note 98; China (2020) – 2, *supra* note 105; Iran (2016), *supra* note 106; Iran (2018), *supra* note 107; Iran (2020), *supra* note 99; DPRK (2020), *supra* note 103.

personalized" for the target.[210] Generally, the email seeks to induce the target to click a link or download an attachment that contains malware, a tactic used by Russia, China, Iran, and North Korea.[211] Another common tactic across the indictments is the use of internet infrastructure in other countries, including the United States, sometimes paid for with cryptocurrency, in an attempt to avoid detection and mask the true identity of the hackers.[212]

Some other techniques were noticeably different among the four malicious States. Russian and Chinese hackers were more likely than their Iranian and North Korean counterparts to exploit software vulnerabilities, which may reflect greater sophistication or resources.[213] North Korean hackers were the only ones described as attempting social engineering, which they have continued to try according to security researchers.[214] North Korea was also unique in its widespread efforts to steal cryptocurrency, both through malware and the marketing of fake cryptocurrency software and enterprises.[215] At one point, North Korean hackers even used malware to make ATM's dispense cash to co-conspirators in Pakistan.[216] Russian GRU hackers were the only ones caught attempting a "false flag" operation, mimicking the techniques of North Korean hackers to hide their true affiliation.[217] Russian hackers were also the only ones described as traveling to other countries to try to access networks from close proximity, which they attempted in Brazil, Switzerland, and The Hague.[218]

---

210. DPRK (2018), *supra* note 104, at 12.

211. *See, e.g.,* Russia (2018) – 1, *supra* note 94, at 4; China (2014), *supra* note 97, at 9–10; China (2018), *supra* note 101, at 8–9; Iran (2018), *supra* note 107, at 3; Iran (2019), *supra* note 108, at 19–20; Iran (2020), *supra* note 99, at 8–9; DPRK (2018), *supra* note 104, at 105.

212. *See, e.g.,* Russia (2018) – 1, *supra* note 94, at 3; Russia (2018) – 2, *supra* note 95, at 8; Russia (2020), *supra* note 96, at 7; China (2020) – 1, *supra* note 98, at 6–7; Iran (2020), *supra* note 99, at 8.

213. Russia (2018) – 1, *supra* note 94, at 8, 25, and 26; China (2020) – 1, *supra* note 98, at 5; China (2020) – 2, *supra* note 105, at 8; China (2021), *supra* note 102, at 7.

214. DPRK (2018), *supra* note 104 at 105; Adam Weidemann, *New Campaign Targeting Security Researchers*, GOOGLE THREAT ANALYSIS GROUP (Jan. 25, 2021), https://blog.google/threat-analysis-group/new-campaign-targeting-security-researchers/.

215. DPRK (2020), *supra* note 103, at 14–15; *id.* at 19.

216. *Id.* at 15; Press Release, U.S. Dep't of Just., International Money Launderer Sentenced to Over 11 Years in Federal Prison for Laundering Millions from Cyber Crime Schemes (Sept. 8, 2021), https://www.justice.gov/usao-cdca/pr/international-money-launderer-sentenced-over-11-years-federal-prison-laundering.

217. Russia (2020), *supra* note 96, at 9.

218. Russia (2018) – 2, *supra* note 95, at 4; Russia (2018) – 2, *supra* note 93, at 16; Russia (2018) – 2, *supra* note 93, at 21–22; Russia (2018) – 2, *supra* note 93, at 28–29.

Russia and North Korea were the only two States whose hackers were indicted for releasing self-propagating worms, known as "NotPetya" and "WannaCry Version 2," respectively.[219] NotPetya appeared to be—and WannaCry Version 2 was—ransomware, "a type of malware that infects a computer and encrypts some or all of the data or files on the computer, and then demands that the user of the computer pay a ransom in order to decrypt and recover the files, or in order to prevent the malicious actors from distributing the data."[220] In reality, NotPetya's ransom messages were "only a ruse"—the worm simply rendered computer systems inoperable, reportedly causing $10 billion in total damages globally.[221] WannaCry really was ransomware, but it similarly rendered hundreds of thousands of computers inoperable, causing an estimated $4 billion in damages.[222] Iran also launched a disruptive operation, but it was a distributed denial of service (DDoS) attack, "a type of cyberattack in which a malicious actor seeks to overwhelm and thereby disable the victim's Internet-accessible computer servers."[223] At least based on the indictments, China has avoided using similarly disruptive techniques in its cyber operations.

***

A comprehensive analysis of the U.S. policy of indicting foreign State actor hackers reveals certain trends about how the offending countries conduct cyber operations and how federal prosecutors choose to charge the perpetrators. What does not emerge, however, is a clearly identifiable Justice Department policy for who to charge and for what behavior when State actors are involved.

III.
RECOMMENDATIONS FOR U.S. POLICY VIS-À-VIS MALICIOUS STATE AND STATE-SPONSORED CYBER ACTORS

The lack of a clear policy thus far for dealing with malicious State and State-sponsored cyber actors does not mean that the trends

219. Russia (2020), *supra* note 96, at 16; DPRK (2018), *supra* note 104, at 108.
220. DPRK (2018), *supra* note 104, at 11.
221. Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, WIRED (Aug. 22, 2018), https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.
222. Andy Greenberg, *Feds Indict North Korean Hackers for Years of Heists and Scams*, WIRED (Feb. 17, 2021), https://www.wired.com/story/north-korea-hackers-indictment-cryptocurrency-sony-swift/.
223. Iran (2016), *supra* note 106, at 2.

identified from the previous indictments cannot inform a more clearly-defined policy going forward. However, this begs the threshold question: would a more clearly-defined policy be beneficial? As U.S. historical practice relating to intelligence activities and State-sponsored terrorism illustrates, the U.S. government might favor inconsistency and flexibility rather than predictability.[224] This lack of line-drawing lets the government respond to each malicious act in its unique context and keeps every option on the table. While there are benefits and downsides to the State actor indictment policy writ-large, the best approach would be a more nuanced one that confines indictments to State-sponsored actors and to State actors conducting operations that do not constitute legitimate State activity and that harm U.S. individuals or non-government entities.

A. Benefits of Current Indictment Policy Writ-Large

The positive aspects of the current practice of indicting State cyber actors generally revolve around notions of justice and the rule of law. The U.S. government investigates all cyber incidents with rigor and seeks to identify the perpetrator(s) in the same legally rigorous way and hold them accountable, whether State actor or private cybercriminal.

The biggest benefit of the current U.S. policy of indicting State actor hackers just like cybercriminals is that the Justice Department can approach every cyber incident in roughly the same way. Typically, cybercrimes are investigated primarily by the FBI Cyber Division, often in conjunction with the FBI Counterintelligence Division in the case of a State-nexus.[225] Having these go-to set of investigators regardless of the perpetrator makes sense because the perpetrator will likely be unknown for at least the first stages of the investigation.

Additionally, if an incident looks like cybercrime, one could argue that the bad actor should not get to avoid indictment just because they are employed by another government. A U.N. report found that North Korea's total haul from cyber operations against banks and cryptocurrency exchanges is estimated to be over $2 billion.[226] If a group of cybercriminals acted the same way, there would be no doubt that the Justice Department should prosecute. In cases of cyber-theft

224. *See generally supra* Part I.

225. Carlin, *supra* note 18, at 414.

226. Michelle Nichols & Raphael Satter, *U.N. Experts Point Finger at North Korea for $281 Million Cyber Theft, KuCoin Likely Victim*, REUTERS (Feb. 9, 2021), https://www.reuters.com/article/us-northkorea-sanctions-cyber/un-experts-point-finger-at-north-korea-for-281-million-cyber-theft-kucoin-likely-victim-idUSKBN2AA00Q.

like that conducted by North Korea, the legal process is also important to obtain "civil forfeiture orders, seizure warrants, and search warrants" to try to recover the stolen money.[227] Monetary recovery aside, there are also no real alternatives to seek justice for the victims of these cyber incidents. And leaving the decision in the hands of the Justice Department alone aligns with traditional notions of prosecutorial independence.[228]

In a time of notable public distrust of the media, indictments are also "legally rigorous" and "uniquely credible forms of attribution[.]"[229] While critics might point out that at the time of the October 2020 GRU indictment, each of the major cyber campaigns outlined had already been attributed to the GRU, the indictments show that the Justice Department could prove the allegations "beyond a reasonable doubt" with "only unclassified, admissible evidence."[230] This might deter actors by broadcasting U.S. detection capabilities.[231]

Another benefit is that, while rare, sometimes the U.S. will apprehend one of the charged hackers. The Canadian hacker-for-hire from the Russia (2017) indictment was arrested in Canada immediately after the indictment was unsealed, extradited to the United States five months later, sentenced to 5 years in prison, and fined up to $2,250,000.[232] While the indictment of cybercriminals from the FIN7 hacking group did not involve State actors, it did involve overseas hackers similarly thought to be outside the reach of law enforcement

227. CYBER REPORT, *supra* note 12, at 53.

228. "Prosecutorial independence" generally refers to the idea that while the President manages the executive branch, the White House should not be involved in the Justice Department's individual criminal cases and investigations. Todd David Peterson, *Federal Prosecutorial Independence*, 15 DUKE J. CONST. L. & PUB. POL'Y 217, 261–62 (2020).

229. Hechler, *supra* note 22; Press Release, U.S. Dep't of Just., Assistant Attorney General John C. Demers Delivers Remarks on the National Security Cyber Investigation into North Korean Operatives (Feb. 17, 2021), https://www.justice.gov/opa/pr/assistant-attorney-general-john-c-demers-delivers-remarks-national-security-cyber [https://perma.cc/2RHN-H4YW].

230. Peter Machtiger, *The Latest GRU Indictment: A Failed Exercise in Deterrence*, JUST SECURITY (Oct. 29, 2020), https://www.justsecurity.org/73071/the-latest-gru-indictment-a-failed-exercise-in-deterrence/; Press Release, U.S. Dep't of Just., *supra* note 229. This paper explicitly does not analyze the implications of Justice Department attribution for cyber insurance claims, but that would be a worthwhile avenue for further research.

231. Chimène I. Keitner, *Attribution by Indictment*, 113 AJIL UNBOUND 207, 210 (2019).

232. Press Release, U.S. Dep't of Just., International Hacker-For-Hire Who Conspired With and Aided Russian FSB Officers Sentenced to 60 Months in Prison (May 29, 2018), https://www.justice.gov/opa/pr/international-hacker-hire-who-conspired-and-aided-russian-fsb-officers-sentenced-60-months [https://perma.cc/9AW8-7B4A].

until it led to several arrests.[233] The United States has extradition treaties with over 100 countries, so a public U.S. indictment hanging over someone's head does restrict their travel options unless they want to risk ending up in a U.S. courtroom.[234]

Finally, the policy of seeking individual accountability for State hacking mirrors another Justice Department policy that emerged at roughly the same time: the "Yates Memo" which emphasizes individual criminal indictments for corporate misconduct.[235] A full comparative analysis of the Justice Department's policies vis-à-vis individual accountability in the contexts of corporate malfeasance and State malicious activity is beyond the scope of this paper but could be an interesting avenue for further research.

B. Downsides of Current Indictment Policy Writ-Large

The arguments against the State actor indictment policy writ-large are typically resource-driven, emphasizing the time and effort it takes to generate the indictments, which risk adversary reciprocity and the revelation of sources and methods while having very little deterrent effect. As the sheer volume of cyber incidents increases to an almost unmanageable level, the U.S. government will need to make tough decisions about how to allocate resources. It might make sense to devote federal prosecutors to more traditional cybercrimes and to have military, intelligence, and diplomatic personnel respond to State action in cyberspace. Unfortunately, the United States does not lack for malicious cyber activity to prosecute, like cyber operations on behalf of ISIS[236] and cybercrime exploiting the COVID-19 pandemic.[237]

---

233. Press Release, U.S. Dep't of Just., Three Members of Notorious International Cybercrime Group "Fin7" In Custody for Role in Attacking Over 100 U.S. companies (Aug. 1, 2018), https://www.justice.gov/opa/pr/three-members-notorious-international-cybercrime-group-fin7-custody-role-attacking-over-100 [https://perma.cc/LL28-JDX7].

234. CYBER REPORT, *supra* note 12, at 58.

235. Katrice Bridges Copeland, The Yates Memo: Looking for "Individual Accountability" in All the Wrong Places, 102 IOWA L. REV. 1897, 1901 (2017). Credit to Ryan Nees for flagging this connection.

236. Hackers supportive of ISIS reportedly stole the personally identifiable information of 1,300 American military and government personnel and passed along that information to a Syria-based ISIS member. Press Release, U.S. Dep't of Just., Acting Assistant Attorney General Mary B. McCord for National Security Delivers Keynote Remarks at Second Annual Billington International Cybersecurity Summit Dinner (Mar. 29, 2017), https://www.justice.gov/opa/speech/acting-assistant-attorney-general-mary-b-mccord-national-security-delivers-keynot [https://perma.cc/2UE2-JGWL].

237. For example, the FBI has reported that fraudulent websites claimed to facilitate Paycheck Protection Program loans in order to steal personally identifiable informa-

The Center for Strategic and International Studies has estimated that the global cost of cybercrime is over $1 trillion.[238] One estimate indicates that less than 1% of malicious cyber incidents lead to an enforcement action against the perpetrators.[239] Against those odds, one might support the full devotion of prosecutorial resources to run-of-the-mill cybercriminals, leaving State actors to be addressed by other levers of government.

A norm of prosecuting State actor hackers also risks reciprocal indictments of U.S. government employees by foreign States.[240] While most countries would likely not extradite a U.S. citizen to, for example, China or Russia, both countries have been accused of abusing Interpol's Red Notice system, which can lead to visa cancellations, financial issues, and hefty legal fees to expose the corrupt motives.[241] Given the number of cyber operations conducted by the United States, cementing this norm of indictments might be very harmful for U.S. government cyber operators.[242]

Another risk of the indictments is the potential revelation of the sources and methods that made the indictment possible. Observing adversary activity when they believe it to be secret can be a very effective way of learning the tactics, techniques, and procedures of bad actors.[243] For example, in the case of the Russian "Illegals" program

---

tion for malicious purposes. Press Release, Fed. Bureau of Investigation, COVID-19 Fraud: Law Enforcement's Response to Those Exploiting the Pandemic (June 9, 2020), https://www.fbi.gov/news/testimony/covid-19-fraud-law-enforcements-response-to-those-exploiting-the-pandemic [https://perma.cc/3E2P-GSRH]; *see also* Press Release, U.S. Dep't of Just., Department of Justice Announces Disruption of Hundreds of Online COVID-19 Related Scams (Apr. 22, 2020), https://www.justice.gov/opa/pr/department-justice-announces-disruption-hundreds-online-covid-19-related-scams [https://perma.cc/XQ88-BY28].

238. Zhanna Malekos Smith & Eugenia Lostri, *The Hidden Costs of Cybercrime*, CSIS (Dec. 9, 2020), https://www.csis.org/analysis/hidden-costs-cybercrime.

239. Mieke Eoyang, Allison Peters, Ishan Mehta & Brandon Gaskew, *To Catch a Hacker: Toward a Comprehensive Strategy to Identify, Pursue, and Punish Malicious Cyber Actors*, THIRD WAY (Oct. 29, 2018), https://www.thirdway.org/report/to-catch-a-hacker-toward-a-comprehensive-strategy-to-identify-pursue-and-punish-malicious-cyber-actors.

240. Hink & Maurer, *supra* note 14, at 537–38.

241. Amy Mackinnon, *The Scourge of the Red Notice*, Foreign POL'Y (Dec. 3, 2018, 12:45 PM), https://foreignpolicy.com/2018/12/03/the-scourge-of-the-red-notice-interpol-uae-russia-china/; Kathy Gilsinan, *How Russia Tries to Catch Its 'Criminals' by Abusing Interpol*, ATLANTIC (May 30, 2018), https://www.theatlantic.com/international/archive/2018/05/russia-interpol-abuse/561539/.

242. Kolbe, *supra* note 11, at 1.

243. *See* JOHN LE CARRÉ, A MOST WANTED MAN 246 (1st ed. 2008) ("We are not policemen, we are spies. We do not arrest our targets. We develop them and redirect them at bigger targets. When we identify a network, we watch it, we listen to it, we penetrate it and by degrees we control it. Arrests are of negative value. They destroy a

in the United States, the FBI investigated, tracked, and surveilled the "Illegals" for more than a decade before arresting them.[244] The co-founder of a prominent cybersecurity company has compared Russian cyber activities targeting software supply chains to the "Illegals" program and believes Russian intelligence actors to be quite skilled at learning from past mistakes to improve their tradecraft.[245] While government officials thoroughly review these indictments to protect classified sources and methods, small revelations can sneak through. For example, one investigative journalist was able to determine that the "Wanted" poster photos that accompanied the October 2020 GRU indictment likely came from the Russian facial recognition site FindClone, which can take an uploaded photo (e.g., from an exploited webcam) and find the individual's social media profile.[246] Knowing this investigative method, the GRU might tighten its operational security by removing photos of operatives from Russian websites, thus making future U.S. investigations more difficult. Further, if foreign actors pull off operations without being indicted, the lack of indictment might signal a lack of capability by the United States in figuring out a certain technique.[247]

Finally, the continued amount of malicious State activity in cyberspace is signaling that the indictments (or any policy) probably have minimal deterrent effect. Experts are finding that deterrence theory is mismatched with cyberspace, which is characterized by interconnectedness, constant contact, and persistent action below the level of armed conflict.[248] In 2015, the members of the G20 (which includes China and Russia) agreed that no country should conduct or support cyber-enabled economic espionage "with the intent of providing competitive advantages to companies or commercial sectors" in their re-

---

precious acquisition. They send you scrabbling back to the drawing board, looking for another network half as good as the one you've just screwed up.").

244. *Operation Ghost Stories: Inside the Russia Spy Case*, *News*, FBI (Oct. 31, 2011), https://www.fbi.gov/news/stories/operation-ghost-stories-inside-the-russian-spy-case.

245. Homeland Cybersecurity: Assessing Cyber Threats and Building Resilience: *Hearing Before the H. Comm. on Homeland Sec.*, 117th Cong. 2 (2021), https://homeland.house.gov/imo/media/doc/Testimony-Alperovitch.pdf (statement of Dmitri Alperovitch, Executive Chairman, Silverado Policy Accelerator).

246. Machtiger, *supra* note 230.

247. *See* Dave Aitel, *The Folly of "Naming and Shaming" Iran*, LAWFARE (Apr. 19, 2016, 2:00 PM), https://www.lawfareblog.com/folly-naming-and-shaming-iran.

248. Emily O. Goldman, *The Cyber Paradigm Shift*, *in* TEN YEARS IN: IMPLEMENTING STRATEGIC APPROACHES TO CYBERSPACE 31, 38 (Jacquelyn G. Schneider, et al., eds.,) (U.S. Naval War Coll., Newport Papers Ser. No. 45, 2020).

spective countries."[249] And yet, based on evidence from these indictments alone, widespread cyber-enabled economic espionage has continued.[250] Overall, the limited effect of the indictments might not be worth the expenditure of time and resources that they require.

C. A More Nuanced Approach to State Actor Indictments and Other Policy Recommendations to Address Malicious State Cyber Activity

1. A Framework for U.S. Indictments of Malicious State and State-Sponsored Cyber Actors

Given the above considerations, the United States should pursue a more nuanced policy that confines indictments (1) to any State-sponsored actors and (2) to State actors conducting operations that do not constitute legitimate State activity and that harm U.S. individuals or non-government entities. This would conserve overall resources relative to the current policy while reinforcing responsible norms in cyberspace.

In an announcement of sanctions against Russia for, among other things, malicious cyber activity including the SolarWinds incident, the U.S. government identified, impliedly rather than explicitly, some variables to consider when assessing the validity of State behavior in cyberspace. These variables included: the "scope and scale" of the operations; the actor's "history of carrying out reckless and disruptive cyber operations[;]" the risk to the global technology supply chain; the fact that the financial sector, critical infrastructure, and government networks were targeted; the cost of remediation; and the actor's theft of offensive cyber tools.[251] It is unclear how the U.S. government weighs these variables when determining what behavior crosses a "redline" in cyberspace.[252]

---

249. Ellen Nakashima, *World's Richest Nations Agree Hacking for Commercial Benefit is Off-Limits*, WASH. POST (Nov. 16, 2015), https://www.washingtonpost.com/world/national-security/worlds-richest-nations-agree-hacking-for-commercial-benefit-is-off-limits/2015/11/16/40bd0800-8ca9-11e5-acff-673ae92ddd2b_story.html.

250. *See* Russia (2017), *supra* note 100; Russia (2018) – 2, *supra* note 95; China (2014), *supra* note 97; China (2018), *supra* note 101; China (2020) – 1, *supra* note 98; China (2020) – 2, *supra* note 105; Iran (2018), *supra* note 107; Iran (2020), *supra* note 99; DPRK (2018), *supra* note 104; DPRK (2020), *supra* note 103.

251. Press Release, Dep't of Treasury, Treasury Sanctions Russian with Sweeping New Sanctions Authority (Apr. 15, 2021), https://home.treasury.gov/news/press-releases/jy0127[https://perma.cc/FXL8-6K54].

252. Robert Chesney, *Sanctioning Russia for SolarWinds: What Normative Line Did Russia Cross?*, LAWFARE (Apr. 15, 2021, 2:17 PM), https://www.lawfareblog.com/sanctioning-russia-solarwinds-what-normative-line-did-russia-cross.

A more clearly-defined indictment policy would help establish what the United States considers acceptable cyber norms. *First*, the United States should announce that it will always indict "State-sponsored" hackers—individuals that do not serve in a country's military or intelligence services—if they break U.S. laws. This might even encourage countries to use government hackers for malicious State activity, centralizing that activity and making it easier for U.S. intelligence services to track.

Next, the United States should announce that it will also indict State hackers if they conduct operations that do not constitute legitimate State activity and that harm U.S. individuals or non-government entities. Determining what constitutes a "legitimate State activity" in cyberspace would require an international legal analysis of State practice, *opinio juris*, and international agreements beyond the scope of this paper, but scholars and practitioners have analyzed several of the behaviors discussed here. State practice provides a particularly persuasive measure of legitimacy because it inherently illustrates international legal principles as filtered through State interests and perceived needs.[253] In addition, State practice provides a better proxy for "legitimacy" than international agreements in a domain like cyberspace, where novel State activity will outpace any treaty or convention negotiations. While not comprehensive, here is a brief list of activities contained in various indictments and an assessment of their "legitimacy":

- Espionage: Espionage is a "legitimate function of a nation-state."[254]
- Economic Espionage: The G20 agreement against cyber-enabled economic espionage suggests that economic espionage and theft for direct financial gain are not legitimate or at least that consensus is moving in that direction.[255]
- Election Interference: Election interference is likely also not a legitimate State activity.[256] As laid out by a collection of public international lawyers and scholars, international law re-

253. Ryan Goodman & Derek Jinks, *Toward an Institutional Theory of Sovereignty*, 55 STAN. L. REV. 1749, 1766 (2003).

254. Williams, *supra* note 135, at 1174.

255. For a more robust analysis of economic espionage under international law, *see generally* Catherine Lotrionte, *Countering State-Sponsored Cyber Economic Espionage Under International Law*, 40 N.C. J. INT'L L.443 (2015).

256. Dapo Akande, Antonio Coco, Talita de Souza Dias, Duncan B. Hollis, Harold Hongju Koh, James C. O'Brien & Tsvetelina van Benthem, *Oxford Statement on International Law Protections Against Foreign Electoral Interference through Digital Means*, JUST SECURITY (Oct. 28, 2020), https://www.justsecurity.org/73097/oxford-statement-on-international-law-protections-against-foreign-electoral-interference-through-digital-means/.

quires States to refrain from "conducting, authorizing or endorsing cyber operations that have adverse consequences for electoral processes in other states."[257] What constitutes "election interference" is a more difficult question—the dissemination of truthful information as part of a foreign influence campaign might not be sufficiently coercive to violate international legal principles, but disinformation in pursuit of a specific electoral result might count.[258]

- Data Destruction or Disruption: Operations that destroy data are typically not legitimate, although consensus on DDoS attacks is less well-formed and more fact-dependent.[259] DDoS attacks temporarily render websites or computer networks inoperable, which can be benign—for example, a five second DDoS attack against a photo of a cat on a blogger's personal website—or inexcusably harmful—for example, a week-long DDoS attack on a hospital's computer network that interferes with the hospital's ability to provide care, leading to patient deaths. International legal experts involved in the drafting of the TALLINN MANUAL have not yet agreed on what factors should determine the international legal characterization of a DDoS attack, although "reversibility" is one potential variable.[260]
- Surveillance of Dissidents: The legitimacy of surveilling dissidents for purposes of "internal security" is also up for debate in international law, but the Justice Department should not include it in indictments of foreign State actor hackers because it does not directly harm U.S. individuals or non-government entities.[261]

---

257. *Id.*

258. *See generally* Michael Schmitt, *Foreign Cyber Interference in Elections: An International Law Primer, Part I*, EJIL: TALK! (Oct. 16, 2020), https://www.ejiltalk.org/foreign-cyber-interference-in-elections-an-international-law-primer-part-i/; Jens David Ohlin, *Did Russian Cyber Interference in the 2016 Election Violate International Law?*, 95 TEX. L. REV. 1570 (2017).

259. *See* TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 118–19 (Michael N. Schmitt ed., 2017) (explaining that DDoS operations are typically reversible and data destruction is not, but that there might be occasions where DDoS operations have irreversible effects, such as the 2012 to 2013 DDoS operations against U.S. banks).

260. *Id.*

261. *See* Julie Bloch et al., *CTRL+HALT+Defeat: State-Sponsored Surveillance and the Suppression of Dissent*, JUST SECURITY (May 15, 2019), https://www.justsecurity.org/64095/ctrlhaltdefeat-state-sponsored-surveillance-and-the-suppression-of-dissent/ (discussing the international legal implications of surveilling dissidents).

- Operations Targeting Critical Infrastructure: Of the operations outlined in the indictments, access to critical infrastructure presents the most difficult case. While access alone to critical infrastructure networks does not cause harm, the potential for inadvertent or purposeful harm might militate against considering it a legitimate activity, meaning it should be indictable when the targets are in the United States. However, the U.S. government might disfavor establishing this norm, as unconfirmed reporting has indicated that U.S. Cyber Command has accessed foreign critical infrastructure networks, like electric power grids.[262]

Restricting indictments to activities against U.S. persons or non-government entities and no longer including non-U.S. targets would be a change in narrative more than a change in legal theory. In the existing indictments, actions against non-U.S. targets are always included in "conspiracy" sections, as part of descriptions of the "manner and means" or "overt acts."[263] While the descriptions of actions against non-U.S. targets *are* valid evidence of a conspiracy, these indictments would similarly be able to show a conspiracy while sticking to U.S. targets.[264] If the U.S. has evidence of foreign State cyber activity against non-U.S. targets, it should share that evidence with the victim countries so that they might pursue their own indictments or countermeasures. In instances where the United States has a strategic reason for wanting to publicly attribute non-U.S. on non-U.S. cyber operations, it can do so through considered press releases by foreign policy or national security officials rather than in domestic criminal indictments. This would keep federal prosecutorial focus on protecting U.S. victims of criminal activity rather than on complex foreign policy calculations.

Finally, the United States should not indict for activity where foreign State actor hackers targeted U.S. government computer networks. State-on-State activity should be dealt with via diplomacy and other policy realms, not within the domestic criminal justice system.

Overall, the beginning of every investigation would look similar to current practice, with FBI investigators taking the lead. Only once

---

262. David E. Sanger & Nicole Perlroth, *U.S. Escalates Online Attacks on Russia's Power Grid*, N.Y. TIMES (June 15, 2019), https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html.

263. *See* Russia (2018) – 2, *supra* note 95; Russia (2020), *supra* note 96; China (2018), *supra* note 101; China (2020) – 2, *supra* note 105; Iran (2018), *supra* note 107; Iran (2020), *supra* note 99; DPRK (2020), *supra* note 103.

264. Russia (2018) – 2, *supra* note 95.

the investigators have reasonable confidence that they have identified the perpetrators, goals, and targets of the operation would the following framework kick in:

Step 1: Is the perpetrator an employee of a foreign State or not?

If 'Yes': continue to Step 2.

If 'No': proceed with indictment.

Step 2: Was the goal of the operation a 'legitimate State activity'?

If 'Yes': continue with counterintelligence investigation; do not indict.

If 'No': continue to Step 3.

Step 3: Did the operation harm U.S. persons or non-government entities?

If 'Yes': proceed with indictment.

If 'No': continue with investigation as desired; do not indict

This framework would provide the right balance of resource-conservation and norm-reinforcement in a consistent policy.

2. *Other Policy Recommendations to Address Malicious State Cyber Activity*

There have been numerous policy proposals published to improve U.S. cyber policy.[265] This section seeks to highlight just a few proposals that would help address malicious State cyber activity in light of the proposed framework for criminal indictments.

First, the United States should more heavily regulate and pursue enforcement actions against cryptocurrency exchanges, especially with regards to "Know Your Customer" (KYC) requirements.[266] The United States should also seek to take down cryptocurrency "tumblers" that primarily enable the money laundering of cybercrime pro-

265. *See, e.g.*, Allison Peters & Michael Garcia, *A Roadmap to Strengthen US Cyber Enforcement: Where Do We Go From Here?*, THIRD WAY (Nov. 12, 2020), https://www.thirdway.org/report/a-roadmap-to-strengthen-us-cyber-enforcement-where-do-we-go-from-here (providing an extensive list of recommendations to guide a response to growing cybercrime); *see also* U.S. CYBERSPACE SOLARIUM COMM'N, FINAL REPORT (2020), https://www.solarium.gov/report.

266. Krebs Statement, *supra* note 15, at 8; *see, e.g.,* Press Release, U.S. Dep't of the Treasury, The Financial Crimes Enforcement Network Proposes Rule Aimed at Closing Anti-Money Laundering Regulatory Gaps for Certain Convertible Virtual Currency and Digital Asset Transactions (Dec. 18, 2020), https://home.treasury.gov/news/press-releases/sm1216 [https://perma.cc/VSB3-EEW3].

ceeds.[267] This would help to combat ransomware generally, whether or not conducted by State actors.

Second, the United States should increase its emphasis on cyber defense in both the public and private sectors. While intelligence agencies like the National Security Agency surveil adversary cyber activity abroad, they do not surveil private sector networks in the United States.[268] Efforts like a proposed rule to impose KYC requirements on infrastructure-as-a-service providers in the United States might help push bad actors off of U.S. networks to overseas servers where they can be surveilled, but such a rule alone will not be a panacea.[269] In the public sector, Congress should build on legal authorities granted to CISA to hunt for threats in federal government networks and move towards a model where CISA leads information security for the entire civilian federal government.[270] In the private sector, Congress should consider a federal breach notification law, while expanding liability protections for information sharing between the private sector and the government.[271] This would encourage continued collaboration between government, private cybersecurity companies, and victims, as detailed in the latest GRU and DPRK indictments.[272] The establishment of a joint cyber planning office within CISA to develop coordinated plans between public and private sector for defense against cybersecurity risk is another positive development along this line of effort.[273] Action in this space should also progress past improved private enterprise defense to improved individual defense encouraged by public education campaigns.

---

267. Timothy G. Massad, *It's Time to Strengthen the Regulation of Crypto-Assets*, BROOKINGS ECON. STUD. 27–28 (Mar. 2019), https://www.brookings.edu/wp-content/uploads/2019/03/Economis-Studies-Timothy-Massad-Cryptocurrency-Paper.pdf.

268. Bill Whitaker, *Solarwinds: How Russian Spies Hacked the Justice, State, Treasury, Energy and Commerce Departments*, 60 MINUTES (Feb. 14, 2021), https://www.cbsnews.com/news/solarwinds-hack-russia-cyberattack-60-minutes-2021-02-14/ (statement of Chris Inglis).

269. Peter Machtiger, *An Analysis of the Trump Administration's Final Cyber-Focused Executive Order*, NYU WAGNER REV. ONLINE (Jan. 20, 2021), https://www.thewagnerreview.org/2021/01/an-analysis-of-the-trump-administrations-final-cyber-focused-executive-order/.

270. *See* William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, § 1705, 134 Stat. 4082 [hereinafter 2021 NDAA] (giving CISA legal authorities to hunt for threats in federal government networks); Alperovitch, *supra* note 245 at 2.

271. Alperovitch, *supra* note 245, at 2; Borghard & Lonergan, *supra* note 148, at 121.

272. Dugas, *supra* note 122.

273. 2021 NDAA, *supra* note 270, § 1715.

Third, the United States should continue and expand its multi-pronged disruption campaign against foreign State cyber activity, the total extent of which is unknown given the classified nature of some components. One component of this involves the traditional collection of human and signals intelligence to monitor adversary activity.[274] Another component of disruption is the dual "persistent engagement" and "defend forward" campaign adopted by USCYBERCOM. USCYBERCOM commander General Paul Nakasone has described persistent engagement as "the concept that states are in constant contact with adversaries in cyberspace, with success determined by how cyber forces *enable* partners and how they *act* while in contact with cyber adversaries."[275] Members of the Cyberspace Solarium Commission have described "defend forward" as the idea that "to disrupt and defeat malicious adversary cyber campaigns, the United States should proactively observe, pursue, and counter adversary operations in day-to-day competition."[276] This includes examples like USCYBERCOM disrupting the internet access of the Internet Research Agency, a Russian troll farm, during the 2018 U.S. midterm elections and U.S. officials revealing that U.S. cyber operatives have exploited Russia's electric power grid.[277] There is a risk to these activities, as unintended consequences can have wide-ranging effects and some disruptive actions may constitute violations of international law or norms that the United States should discourage, like accessing other countries' power grids.[278] As part of the persistent engagement and "defend forward" campaigns, the United States should publicly encourage responsible standard operating procedures for offensive cyber operations, such as stricter targeting due diligence, tighter scoping of targets, data collection limitations, and efforts to limit unpredictable harm.[279] A developing component of disruption is the coordinated global takedown of

274. Kolbe, *supra* note 11, at 1.

275. Lt. Gen. Timothy D. Haugh, et al., *Agile Collaboration in Defense of the Nation*, *in* TEN YEARS IN: IMPLEMENTING STRATEGIC APPROACHES TO CYBERSPACE 97, 101 (Jacquelyn G. Schneider, et al., eds.,) (U.S. Naval War Coll., Newport Papers Ser. No. 45, 2020)

276. Borghard & Lonergan, *supra* note 148, at 113.

277. Ellen Nakashima, *U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms*, WASH. POST (Feb. 27, 2019), https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html.; Sanger, *supra* note 262.

278. Ashley Deeks, *Defend Forward and Cyber Countermeasures*, *Aegies Series Paper, No. 2004*, HOOVER WORKING GR. ON NAT'L SEC., TECH., & L. (Aug. 4, 2020), https://www.hoover.org/research/defend-forward-and-cyber-countermeasures.

279. Aitel, *supra* note 139.

malicious botnets.[280] While those efforts have focused on private cybercriminals, the exercise of global coordination among government cyber investigators and private sector technology companies may prove useful for combatting future State actor cyber actions. A final component of disruption would be the continued use of sanctions to put economic pressure on foreign entities and officials.[281] These would be particularly effective targeted against high-ranking policy-makers and leaders, who may care more about their own access to wealth than the economic struggles of their citizenry.[282]

The above proposals will help improve U.S. resiliency in the face of malicious State cyber activity, but no one should expect to be completely safe. Unfortunately, time and money are finite—it is not possible to check every single line of code that has ever been written to ensure complete protection and human error would likely still lead to exploitations even if all the code was perfect. In addition, some level of computer network exploitation is probably undeterrable, just like traditional espionage. The United States should consider policies that will provide the greatest protection for U.S. persons and entities while encouraging responsible international behavior.

CONCLUSION

The world is still in the relatively early days of malicious activity in cyberspace, and the issues identified in this paper are just a small component of that complex issue. While the "Holiday Bear" software supply chain incident that leveraged SolarWinds and several other attack vectors to exploit government and private sector networks seems massive, the reality is that the average enterprise network likely runs dozens of products with similarly vulnerable supply chains.[283] The U.S. government response to incidents like these will have to scale up

280. Danny Palmer, *Emotet: The World's Most Dangerous Malware Botnet Was Just Disrupted By A Major Police Operation*, ZDNET (Jan. 27, 2021), https://www.zdnet.com/article/emotet-worlds-most-dangerous-malware-botnet-disrupted-by-international-police-operation/.

281. Press Release, Dep't of the Treasury, *supra* note 85, 15.

282. Garry Kasparov, *How Biden and the West Could Help Russians by Reining in Putin*, WASH. POST (Feb. 4, 2021), https://www.washingtonpost.com/opinions/2021/02/04/navalnys-jailing-was-groundhog-day-russian-democracy/ ("The traditional recipes of international diplomacy are worthless against a mafia dictatorship that cares nothing for ideology or national interests. Hurting the Russian people doesn't bother Putin, so sanctions must target him and his gang directly. Putin doesn't care about left or right; he cares about money.").

283. Haroon Meer, *Supply Chain Security is Actually Worse Than We Think*, ZDNET (Feb. 10, 2021), https://www.zdnet.com/article/supply-chain-security-is-actually-worse-than-we-think/.

massively in the coming years. In a world of limited resources, the U.S. government will need to have clear policies in place and dedicate resources to the elements of the response that have the biggest chance of disrupting the threat. Those most likely to disrupt the threat are security and intelligence professionals, not prosecutors. Prosecutors specializing in cyber activity will not lack for work as run-of-the-mill cybercrime continues to explode. Confining indictments of State actor hackers to a more limited set of circumstances is a policy change that makes sense as the United States continues to face malicious State cyber activity.