An Examination of U.S. Jurisdiction and Enforcement of U.S. Judgments Abroad in the Context of North Korean Cyberattacks

Carol Kim*

Abstract

Despite being one of the poorest nations in the world, North Korea has established a reputation as a major player in international cybercrime. In 2017, the Korea Institute of Liberal Democracy in Seoul estimated that North Korea's hackers generate approximately $860 million a year through cybercriminal activities, a number that has continued to rise. Cybercrime is an especially salient issue because it poses grave implications for not only military and financial security, but also public health. During the COVID-19 pandemic, North Korean hackers—along with Chinese and Russian hackers—have allegedly attempted to steal from pharmaceutical companies and other countries' national COVID-19 relief funds. The question isn't if cybercriminals will attack public health targets, but when.

To better illustrate this risk and its legal implications, this Essay presents a hypothetical case in which North Korean operatives, aided by operatives from Russia and China, have stolen $500 million in COVID-19 relief funds from the U.S. Treasury through hacking, all while residing in their respective countries. The purpose of this hypothetical is to explore the legal bases that the United States may use to prosecute cybercrimes and obtain judgments against foreign cybercriminals. This Essay also examines the current legal infrastructure for the enforcement of restitution and civil damages judgements, as well as legal and political obstacles to enforcement. It concludes that current legal infrastructure is insufficient to support the international enforcement of judgments against cybercriminals located outside the U.S. and provides suggestions for how to maximize current enforcement mechanisms, as well as cultivate a new forum for coordinating international cybercrime judgments.

* J.D. Candidate 2022, The University of Chicago Law School. This paper is dedicated to the memory of Dr. Charn-kiu Kim, who was a preeminent scholar and professor of international law and a loving grandfather who inspired the author to pursue international law and carry on his legacy.

Table of Contents

I. INTRODUCTION

"Cyber warfare, along with nuclear weapons and missiles, is an 'all-purpose sword' that guarantees our military's capability to strike."[1] These were the words of Kim Jong-un, leader of the Democratic People's Republic of Korea—also known as North Korea—when he equated his nation's cyber warfare capabilities with that of its infamous nuclear missiles program. Immediately after his ascension to the role of supreme leader of North Korea in 2011, Kim Jong-un established a cyber development and research institute in North Korea with a separate Cyber Command Department.[2] Under its auspices, he authorized the formation of various hacking groups, manned by thousands of hackers, that were tasked with developing software for use in cyberattacks against other nations.[3] In response, South Korea's National Intelligence Service (NIS) has been developing preventative measures against cyberattacks, and even cyber war, with North Korea.[4]

Because North Korea's hackers do not always claim responsibility for their cyberattacks, it is difficult to precisely quantify the success of North Korea's forays into cybercrime.[5] Nonetheless, over the course of the twenty-first century, North Korea has become a mainstay in international cybercrime news. In 2017, North Korean ransomware called "WannaCry" infected more than 300,000 computers in 150 countries,[6] disrupting the U.K. National Health Service's computer systems and rail systems in Germany, as well as institutions in various other countries.[7] That year, senior intelligence officials in the U.S. "assessed that North Korea was one of the top four cyber threats capable of launching 'disruptive or destructive cyberattacks'" against the U.S.[8] The *New York Times* mused, "The world once laughed at North Korea's cyberpower. No more."[9] The following year, the *Wall*

---

1 Jason Bartlett, *Why Is North Korea So Good at Cybercrime?*, THE DIPLOMAT (Nov. 1, 2020), https://perma.cc/UN28-7Z65.

2 *See* JoongAng Ilbo, *Kim Jong-un Says that "Cyber Warfare Is an All-purpose Sword" and One of Three Major Means of War*, JOONGANG ILBO (Nov. 5, 2013), https://perma.cc/P2TH-N88E.

3 *Id.*

4 *Id. See also* So Jeong Kim & Sunha Bae, *Korean Policies of Cybersecurity and Data Resilience*, *in* THE KOREAN WAY WITH DATA: HOW THE WORLD'S MOST WIRED COUNTRY IS FORGING A THIRD WAY (Aug. 17, 2021), https://perma.cc/Z455-C3XM.

5 *See* Ed Caesar, *The Incredible Rise of North Korea's Hacking Army*, NEW YORKER (Apr. 19, 2021).

6 Bartlett, *supra* note 1.

7 *See* Dan Bilefsky, *Britain Says North Korea Was Behind Cyberattack on Health Service*, N.Y. TIMES (Oct. 27, 2017), https://perma.cc/C2JQ-CBUQ.

8 Bruce Klingner, *North Korean Cyberattacks: A Dangerous and Evolving Threat*, THE HERITAGE FOUND. (Sept. 2, 2021), https://perma.cc/EQL6-5V3S (citing Chang Jae-soon, *U.S. Intelligence Chiefs Pick N. Korea as Major Cyber Threat*, YONHAP NEWS AGENCY (Jan. 6, 2017), https://perma.cc/B57B-BELC).

9 David E. Sanger, David D. Kirkpatrick & Nicole Perlroth, *The World Once Laughed at North Korean Cyberpower. No More*, N.Y. TIMES (Oct. 15, 2017), https://perma.cc/SS5U-ULRL.

Street Journal declared that North Korea's hackers had become "dangerously good."[10] And in 2021, North Korea's hackers earned the dubious honor of being "the world's leading 21st century nation-state bank robbers," pulling off their heists "using keyboards rather than guns," in the words of John Demers, the former assistant attorney general for national security.[11] Therefore, it comes as no surprise that North Korea, together with its ally China, has invested greatly in research and development in this area by signing the China–North Korea Education Exchange and Cooperation Agreement (2020–2030).[12]

Financial and military institutions are not the only targets of cybercriminals. The NotPetya malware attack initiated by Russia in 2017 was a harsh wakeup call to the medical community: that attack "compromised computer systems at two hospitals, 60 physician offices, and 18 community satellite facilities belonging to the Heritage Valley Health System . . . in Sewickley, Pennsylvania, and Beaver, Pennsylvania," highlighting the potentially catastrophic threat that cybercrime poses to public health.[13] More recently, during the COVID-19 pandemic, North Korean hackers—along with Chinese and Russian hackers—have allegedly attempted to steal funds from pharmaceutical companies and other countries' national COVID-19 relief funds.[14] As evidenced by these examples, cybercrime can endanger some of the most vulnerable populations—those who are sick or elderly—that rely on medical resources. The question isn't *if* cybercriminals will attack public health targets, but *when*.

To better illustrate this risk and its legal implications, this Essay presents a hypothetical case in which North Korean operatives, aided by respective operatives from Russia and China, have stolen $500 million in COVID-19 relief funds from the U.S. Treasury through hacking, all while residing in their respective countries. More specifically, in this hypothetical case, the hackers have obtained U.S. COVID-19 relief funds by stealing the Social Security numbers of relief recipients and setting up numerous bank accounts internationally. Under the guise of a health care consulting firm, these operatives targeted pharmaceutical company Johnson & Johnson by holding the company's research funds and data hostage, effectively freezing Johnson & Johnson's operations. The North Korean operatives' new ransomware, called "GiveMeMoney," demanded $100 million

---

10 Timothy W. Martin, *How North Korea's Hackers Became Dangerously Good*, WALL ST. J. (Apr. 19, 2018), https://perma.cc/N2X8-T6FP.

11 Eric Geller, *North Korean Hackers Are 'The World's Leading Bank Robbers,' U.S. Charges*, POLITICO (Feb. 17, 2021), https://perma.cc/B8Z9-CYNB.

12 *See* Press Release, Ministry of Education of the People's Republic of China, Chen Baosheng Meets Chairman of the Education Commission of North Korea (Nov. 7, 2019), https://perma.cc/M6P5-PF8M.

13 Indictment at 16, United States v. Andrienko, et al., Criminal No. 20-316 (W.D. Pa. Oct. 15, 2020), available at https://perma.cc/5NC4-G7Z6.

14 *See* Bartlett, *supra* note 1.

from Johnson & Johnson. Half of this ransom has already been paid—in Bitcoin, as stipulated by the hackers—so that some of Johnson & Johnson's data could be urgently released to further COVID-19 research and distribute vaccines. However, because of the delay caused by the ransomware attack, a scheduled batch of vaccines—intended for those in most critical need, namely elderly individuals in nursing homes and hospices—could not be delivered in a timely manner. Consequently, death tolls of these populations due to COVID-19 have spiked and continue to rise. Fortunately, the U.S. government was successful in tracing the whereabouts of some of the ransom money in various countries. In this scenario, what legal measures could the U.S. government take in response to this cyberattack?

The purpose of this hypothetical is to explore the legal bases that the U.S. could use to prosecute cybercrimes and obtain judgments against foreign cybercriminals. Using this hypothetical scenario, Section II addresses whether the U.S. could assert jurisdiction over the foreign nationals who have committed cyberattacks and other violations of U.S. statutes, while Section III applies the relevant principles of jurisdiction to the hypothetical cyberattack, particularly with regard to North Korean nationals. Section IV explores whether an alternative forum may be sought to bring operatives from Russia and China to trial. Section V discusses enforcement mechanisms after obtaining criminal judgments against cybercriminals and the enforcement of restitution or related civil judgments. Finally, Section VI concludes that the current legal infrastructure is insufficient to support the prosecution of cybercrimes committed by cybercriminals located outside the U.S. and international enforcement of judgments against these cybercriminals. It provides suggestions on how to maximize current enforcement mechanisms as well as cultivate a new forum for coordinating international cybercrime judgments.

II. U.S. JURISDICTION OVER FOREIGN CYBERCRIMINALS

Because the hypothetical Johnson & Johnson cyberattack was conducted by non-U.S. citizens on foreign soil, one first must examine whether U.S. courts have jurisdiction over both the person and subject-matter, especially since neither North Korea, Russia, nor China has extradition treaties with the U.S.[15] This

15 *See Countries Without Extradition 2021*, WORLDPOPULATIONREVIEW.COM, https://perma.cc/PP92-6LZ6. *See also* Daniel S. Goldman, *Russian Indictment and Probe*, AM. CONST. SOC'Y BLOGS, EXPERT F. (Feb. 28, 2018), https://perma.cc/T9KL-5NUC ("Perhaps not surprisingly given the tenor of diplomatic relations between the two countries, the United States and Russia do not have an extradition treaty. In addition, Russia . . . will not extradite its own citizens."); *China Blasts US Charges Against Agents Seeking Man's Return*, AP NEWS (Oct. 29, 2020), https://apnews.com/article/beijing-crime-china-fugitives-asia-pacific-5efbc060a190a13568617ac13f83d7c7 ("China has no extradition treaty with the U.S."); *U.S. Relations with the Democratic People's Republic of Korea*, U.S. DEP'T ST. (Aug.

Section concludes that although precedent is limited, one can argue that the U.S. does have extraterritorial jurisdiction in this hypothetical scenario.

In the U.S., there is a general presumption against extraterritorial jurisdiction. The Supreme Court has stated that "United States law governs domestically but does not rule the world."[16] Differences in the enforcement of foreign laws and foreign judgments "arise from a deep-rooted distrust in the administration of justice in other countries, and the fear arising therefrom that irreparable injury may be done to an individual," and there is "a striking similarity in the rules governing the conflict of laws in [ ] various countries."[17] Aside from the issue of conflict of laws, which may govern the subject matter in the foreign nation, it is advisable from a foreign diplomacy perspective that the U.S. maintains friendly relations with other nations.

However, in *RJR Nabisco, Inc. v. European Community*,[18] the Court carved out exceptions to this general presumption against extraterritorial jurisdiction by allowing the U.S. government to prosecute not only U.S. citizens, but also foreign nationals who have committed criminal acts outside U.S. territory. Although it is not a criminal case, *RJR Nabisco* is relevant because it involves allegations of money laundering by international drug traffickers in the sale of narcotics and other contraband, including RJR cigarettes in Europe. In the case, the Court used a two-prong test to determine whether extraterritorial jurisdiction is warranted by the Racketeer Influenced and Corrupt Organizations Act (RICO).[19] The first prong asks whether Congress expressly stated that the extraterritorial law applies outside U.S. territory without violating due process or constitutional rights. The second prong asks, even if Congress is silent about the extraterritorial jurisdiction of the law, whether U.S. laws could still apply to acts committed overseas when the conduct relevant to the statute's primary objective occurred in U.S. territory. In *RJR Nabisco*, the Court unanimously concluded that the RICO statute had extraterritorial applicability to criminal conduct outside U.S. territory.[20]

However, this is not to say that implied intent of Congress for extraterritorial jurisdiction has been broadened since an earlier standard set by *Morrison v. National Australia Bank, Ltd.*[21] In *Morrison*, the Court held that extraterritorial jurisdiction did not apply in failed private investment actions for securities fraud that occurred outside the U.S. territories, even when the fraud had effects within U.S. territory.

23, 2021), https://perma.cc/CS36-V5UG (stating that "[t]he United States and the DPRK do not have diplomatic relations," much less an extradition treaty).

16 Microsoft Corp. v. AT&T Corp., 550 U.S. 437, 454 (2007).

17 Ernest G. Lorenzen, *The Enforcement of American Judgments Abroad*, 29 YALE L. J. 188, 188 (1919).

18 136 S. Ct. 2090 (2016).

19 18 U.S.C. §§ 1961–68.

20 *See id.* at 2101–04.

21 130 S. Ct. 2869 (2010).

In *RJR Nabisco*, however, the Court held that Congress, by incorporating extraterritorial predicates into RICO, gave "a clear, affirmative indication" of RICO's applicability to foreign racketeering activity "to the extent that the predicate [acts] alleged in a particular case themselves apply extraterritorially," or in other words, when "a pattern of racketeering activity [ ] include[s] or consist[s] of offenses committed abroad in violation of a predicate statute for which the presumption against extraterritoriality has been overcome."[22] In effect, the Court "endorse[d] implied extraterritoriality" of U.S. courts over accessories or piggyback offenses, such as conspiracy, attempt, and aiding and abetting, that are predicated upon a U.S. criminal activity—even when such piggyback offenses occurred on foreign soil.[23] As RICO cases show, even foreigners living outside of the U.S. can face prosecution in the U.S.

Following the limited prescription set out in this precedent, one could argue that the hypothetical cyberattacks on the U.S. Treasury and Johnson & Johnson would be in violation of various sections of U.S. statutes that can be applied extraterritorially. Such statutes could include RICO;[24] Conspiracy to Defraud the United States;[25] Fraud and Related Activity in Connection with Computers;[26] Fraud by Wire, Radio, or Television; Fraud and Related Activity in Connection with Identification Documents, Authentication Features and Information;[27] Identity Theft;[28] and Money Laundering.[29]

III. APPLYING THE RELEVANT PRINCIPLES OF JURISDICTION TO THE HYPOTHETICAL CYBERATTACKS

This Section will apply relevant principles of jurisdiction to the hypothetical scenario, concluding that the U.S. can assert extraterritorial jurisdiction and counter potential allegations of violating a foreigner's procedural due process rights. Suppose that one of the North Korean operatives responsible for the Johnson & Johnson cyberattack has a fiancée, a South Korean citizen, whom he secretly visits in Seoul. With the help of the Korean Central Intelligence Agency, U.S. agents capture and detain the North Korean operative. A warrantless search-and-seizure is conducted in his fiancée's apartment, where he has been

22 *RJR Nabisco*, 136 S. Ct. at 2102.

23 CHARLES DOYLE, CONG. RSCH. SERV., RL94166, EXTRATERRITORIAL APPLICATION OF AMERICAN CRIMINAL LAW 20 (2016).

24 18 U.S.C. §§ 1961–68.

25 18 U.S.C. § 371.

26 18 U.S.C. § 1030.

27 18 U.S.C. § 1028.

28 18 U.S.C. § 1028A.

29 18 U.S.C. § 1956.

staying. In response, the North Korean operative protests that (1) neither the U.S. nor South Korea have any jurisdiction over him; (2) he was never served notice regarding the U.S. indictments; and (3) his fiancée's apartment was searched without a warrant. In this scenario, could the assertion of extraterritorial jurisdiction be squared with this alleged violation of a foreigner's due process rights?

Regarding concerns over jurisdiction, Section II established that, due to the specific type of criminal indictments lodged against the foreigner in question, extraterritorial jurisdiction could be applicable in this case. Thus, this Essay will not analyze the appropriateness of the subject matter and personal jurisdiction. To enforce U.S. laws in a foreign country, the U.S. would need to have a treaty with that country, observe international laws or conventions, and/or observe the laws of the foreign country regarding enforcement of foreign actions.[30] Noting that extraterritorial jurisdiction and the application of certain U.S. constitutional rights to an alien in a foreign country is an area that is extremely narrow in scope, the U.S. would have little choice but to turn to South Korea, a country with which the U.S. has an extradition treaty.[31] As an ally, South Korea would be more cooperative in this matter, especially since the U.S. and South Korea have a mutual interest in North Korea's cyberattacks, which have detrimentally affected not only the U.S., but also South Korea. For instance, South Korea's NIS has recorded multiple North Korean cyberattacks against private and public institutions in South Korea, including the Korea Atomic Energy Research Institute.[32] Furthermore, during the COVID-19 pandemic, NIS reportedly thwarted North Korea's attempts to hack into South Korean firms developing coronavirus vaccines.[33]

Regarding the hypothetical operative's protests over alleged deprivation of due process rights, in *United States v. Verdugo-Urquidez*,[34] the Supreme Court held that the Fourth Amendment protection against unjustified search-and-seizure is not "intended to restrain the actions of the Federal Government against aliens outside of the United States territory."[35] Additionally, the Court concluded that

---

30 *See Enforcement of Judgments*, U.S. DEP'T ST., https://perma.cc/6A4C-KSQR.

31 *See* Extradition Treaty Between the United States of America and Korea, U.S.–S. Korea, June 9, 1998, S. Treaty Doc. No. 106-2.

32 *See* Mitch Shin, *South Korea's Intelligence Agency Confirms North Korean Cyberattacks*, DIPLOMAT (July 9, 2021), https://perma.cc/9RVK-7V5Y.

33 *See* Sangmi Cha & Hyonhee Shin, *North Korean Hackers Tried to Steal Pfizer Vaccine Know-How, Lawmaker Says*, REUTERS (Feb. 16, 2021), https://perma.cc/C9Q9-D3AU. Experts have speculated that the hackers may have been "more interested in selling the stolen data than using it to develop a homegrown vaccine," as North Korea is "often accused of turning to an army of hackers to fill its cash-strapped coffers amid international sanctions that ban most international trade with it." *Id.*

34 494 U.S. 259 (1990).

35 *Id.* at 265–66.

the Fourth Amendment was intended to protect the "class of persons who are part of a national community or who have otherwise developed sufficient connection with this country to be considered part of that community."[36] The North Korean operative in this hypothetical does not belong to this class of persons because not only was his crime committed outside U.S. territory, but he also did not have "sufficient connection" with or in the U.S. to qualify as "part of that community."[37]

The North Korean operative's fiancée, a South Korean citizen, also might protest because she was not charged with any crime and her apartment was subjected to an unlawful search-and-seizure. In this instance, too, the U.S. could use the same argument as above in U.S. courts because some of the charges in the indictment are piggyback crimes, such as conspiracy and aiding and abetting in the crimes by hiding the North Korean operative. Additionally, the South Korean government could indict her with similar charges under South Korea's laws.[38] Furthermore, the government could also argue that exigent circumstances—namely, that the operative may flee any minute back to North Korea—as well as the overall clandestine nature of the U.S. federal agents' operation justify the absence of a warrant.[39]

In *Verdugo-Urquidez*, however, the Court left open the possibility that in certain instances, foreigners may be afforded some constitutional rights regarding the conduct of U.S. agents outside U.S. soil.[40] Acknowledging that some Bill of Rights protections may be available to foreigners for acts by U.S. agents on foreign soil, the Fifth Circuit in *Hernandez v. United States*[41] found that U.S. agents, by using "excessive force" in Mexico against Mexican teenager Jesús C. Hernández, violated the alien's clearly established substantive due process rights under the

---

36 *Id.* at 265.

37 *Id.* ("While this textual exegesis is by no means conclusive, it suggests that 'the people' protected by the Fourth Amendment, and by the First and Second Amendments, and to whom rights and powers are reserved in the Ninth and Tenth Amendments, refers to a class of persons who are part of a national community or who have otherwise developed sufficient connection with this country to be considered part of that community.").

38 *See* Criminal Act, Act No. 11731, Apr. 5, 2013 (S. Kor.), *translated in* KOREA LEGISLATION RESEARCH INSTITUTE: KOREA LAW TRANSLATION CENTER, https://perma.cc/R3AJ-8AMT.

39 Kuk Cho, *Unfinished "Criminal Procedure Revolution" of Post Democratization South Korea*, 30 DENV. J. INT'L L. & POL'Y 377, 385 (1997) ("The [Criminal Procedure Act of South Korea] requires a judicial warrant for search-and-seizure and inspection. The exceptions to the warrant requirement are: search-and-seizure and inspection incident to arrest on warrant, emergency arrest, arrest of flagrant offenders, detention on warrant, emergency search-and-seizure, and inspection on the spot of committed crimes." (citing the Criminal Procedure Act, arts. 215, 216 (1)-(3))).

40 *Verdugo-Urquidez*, 494 U.S. at 274.

41 757 F.3d 249, 272 (5th Cir. 2014). *Hernández* went for review to the U.S. Supreme Court twice, once in 2017 and 2019. The case was remanded back to the Fifth Circuit, which affirmed the trial court's decision that Mesa had qualified immunity and dismissed Hernández's lawsuit. On February 24, 2020, the Supreme Court upheld the Fifth Circuit decision once again in a narrow 5–4 decision.

Fifth Amendment. Following these precedents, this Essay now examines whether the Due Process Clause of the Fifth Amendment[42] applies to the North Korean operative in this hypothetical search-and-seizure outside of U.S. soil.

Unlike *Hernandez*, which concerned the violation of substantive due process rights in regard to the use of excessive force, the hypothetical case concerns procedural due process rights. Procedural due process under the Fifth Amendment requires that the federal government follow certain fair processes to protect innocent people from unlawful criminal prosecution. Procedural due process, in this case, is applicable to the actions of not only U.S. federal agents, but also South Korean agents, requiring this Essay to examine both country's laws.

As far as the U.S. is concerned, it could be argued that procedural due process is met by an arrest warrant in lieu of a service of summons with a notice to appear in court, since the government has probable cause to establish that the North Korean operative committed a cybercrime and poses a flight risk.[43] In the event that the U.S. tries to bring criminals to trial, there must be cooperation with the country where the extraterritorial jurisdiction is in effect.[44] In the case of enforcement for restitution or related civil judgments in South Korea, service of process must be made with an eye toward South Korean law—if the U.S. process violates South Korean law, then the service of process may not be recognized by South Korea.[45] As the most wired nation in the world,[46] South Korea would be a savvy partner in the enforcement of transnational cybercrimes. After proper service of indictment papers, the U.S. could request the extradition of the North Korean defendant to face trial in the U.S., since the cyberattacks are considered serious crimes in both countries and a prima facie case has been made against the North Korean operative.

---

42 It is important to note that Fourteenth Amendment also contains the Due Process Clause. Because the Due Process Clause of the Fifth Amendment applies specifically to the federal government, this Essay limits discussion to the Fifth Amendment.

43 Procedural due process under the Fifth Amendment requires that the federal government follow certain fair processes to protect innocent people from unlawful criminal prosecution. Under Rule 4 of the Federal Rules of Criminal Procedure (Arrest Warrant or Summons on a Complaint), if a complaint or affidavit is filed establishing probable cause, a warrant can be issued by the judge as in this case to make an immediate arrest; this would eliminate the need for the government attorney asking the judge to issue a summons, which would require notice to the defendant to appear in court for a hearing. Of course, the court can issue both a warrant and a summons on the same day, but in this case, due to the flight risk of the defendant and the difficulty of tracking him down at a place where U.S. agents can exert physical custody, the rest of the procedural due process requirements of service of process, notice of hearing, and other requirements can be overcome by a warrant for immediate arrest.

44 *See* DOYLE, *supra* note 23, at 30.

45 *See generally* Sung Hoon Lee, *Foreign Judgment Recognition and Enforcement System of Korea*, 6 J. KOREAN L. 110 (2006).

46 *See South Korea: The Most Wired Place on Earth*, PBS, https://perma.cc/9UZT-4FMP.

IV. WOULD THERE BE AN ALTERNATIVE FORUM TO BRING THE OPERATIVES FROM RUSSIA AND CHINA TO TRIAL?

Having previously discussed jurisdiction and due process, this Essay now considers whether there is a potential forum for trying the cybercriminals charged in the Johnson & Johnson cyberattack. Currently, the U.S. does not have extradition treaties with either China or Russia, although it does have an extradition treaty with South Korea. In addition, when considering international tribunals as a potential option, a major hurdle is that both nations must be member states or must consent to the court's jurisdiction. Neither Russia nor China would agree to the jurisdiction of the International Court of Justice (ICJ) in this case, and neither of the countries is a member of the International Criminal Court (ICC), although South Korea is.[47]

Absent an international cybercrime tribunal, however, the U.S. could accept jurisdiction of the ICC with respect to the cybercrimes committed within U.S. territory and request investigation by the court's prosecutor.[48] The U.S. could also request that the U.N. Security Council refer the case to the ICC.[49] The ICC has subject matter jurisdiction for crimes again humanity, genocide, war crimes, and crimes of aggression.[50] Additionally, although some controversy surrounds the ICC's application of adjudicatory jurisdiction to nationals of non-party states under Article 12 of the Rome Statute, the Statute "empowers the ICC to compel the nationals of non-parties to comply with its orders to provide evidence or surrender indicted persons"[51] and generally, "international law . . . places far fewer limits on the exercise of adjudicatory than prescriptive jurisdiction [sic], perhaps because the exercise of adjudicatory jurisdiction over extraterritorial activities is not viewed as infringing to the same degree on the sovereignty or domestic jurisdiction of the state where the activity at issue occurred."[52]

The problem, though, is whether a cyberattack can rise to the elements required for any of the listed crimes.[53] However, considering that none of the hackers' countries would agree to arbitrate or prosecute these hackers and that the

---

47 *See* The State Parties to the Rome Statute, ICC, https://perma.cc/HL59-ZZHX.

48 *See* Rome Statute of the International Criminal Court art. 5(1), July 17, 1998, 2187 U.N.T.S. 90 [hereinafter Rome Statute].

49 *See id.*

50 *See id.* arts. 5–8.

51 Michael P. Scharf, *The ICC's Jurisdiction Over the Nationals of Non-Party States: A Critique of the U.S. Position Critique of the U.S. Position*, 64 L. & CONTEMP. PROBS. 67, 71, 72, n. 23 (2001).

52 *Id.* (quoting Daniel Bodansky, *Human Rights and Universal Jurisdiction*, *in* WORLD JUSTICE: COURTS AND INTERNATIONAL HUMAN RIGHTS 6 (Mark Gibney ed., 1991)).

53 *See* Alexander Perloff-Giles, *Transnational Cyber Offenses: Overcoming Jurisdictional Challenges*, 43 YALE J. INT'L L. 191, 220 (2018). *See also* Rome Statute, *supra* note 48, at art. 9 (describing elements of crimes).

U.S. would have a difficult time moving beyond indictments on its own, the ICC forum could give the U.S. an opportunity to begin prosecuting these cybercrimes.

Although it would be a stretch, it could be alleged that this cyberattack on Johnson & Johnson—and, by extension, on the U.S. COVID-19 relief fund—could rise to the level of a war crime under Article 8 of the Rome Statute, considering that "a cyberattack destroys, rather than simply interferes with, civilian data and communications" and also results in a "breach of international humanitarian law."[54] In addition, the U.S. could contend that the cyberattack caused massive deaths of the elderly and hospice populations due to preventing Johnson & Johnson from delivering vaccines in a timely manner to those populations. This framing of events could also fall under the elements of genocide under Article 6—in particular, Articles 6(b) ("Genocide by causing seriously bodily or mental harm") or 6(c) ("Genocide by deliberately inflicting conditions of life calculated to bring about physical destruction").[55] Furthermore, the U.S. could argue that the increase in COVID-19 deaths and sharp rise in sickness in the population as a whole due to the prevention of vaccines from being delivered in a timely manner could be classified as a crime against humanity under Article 7, including Articles 7(1)(a) ("Crimes against humanity of murder") and 7(1)(b) ("Crimes against humanity of extermination").[56]

V. POSSIBLE ENFORCEMENT MECHANISMS

This Section explores the enforcement mechanisms that may be available to the U.S. after obtaining criminal judgments, whether from the ICC or a U.S. court. Victims of the cyberattacks may feel entitled to monetary damages that restitution under the criminal judgments does not adequately compensate. Thus, victims may decide to institute a separate civil proceeding for damages. However, enforcement of judgments abroad remains difficult under the current legal infrastructure.

China has recognized commercial and civil judgments from the U.S. and South Korea even without bilateral treaties on recognition or enforcement of foreign judgments.[57] Whether a bilateral treaty would make enforcement of U.S.

---

54 Perloff-Giles, *supra* note 53, at 222. *See also* Rome Statute, *supra* note 48, at art. 8(2)(iii) ("Willfully causing great suffering, or serious injury to body or health").

55 Rome Statute, *supra* note 48, at arts. 6, 6(b), 6(c).

56 *Id.* arts. 7(1)(a)–(b).

57 *See Recognition and Enforcement of Foreign Judgments in China*, CHINA JUST. OBSERVER, https://perma.cc/55TR-MBTD. *See also* Vassily Rudomino & Vladimir Kanashevskiy, *Enforcing Foreign Judgments and Arbitral Awards in Russia*, WORLD SERVICES GRP. (2009), https://perma.cc/9MZU-XEAA. The judgments referenced are commercial and civil judgments. Furthermore, note that except for North Korea, all countries mentioned are members of the Hague Conference on Private International Law (HCCH), but none have signed on to the Convention on the Recognition and Enforcement of Foreign Judgments in Civil and Commercial Matters. *See HCCH Members*, HCCH, https://perma.cc/Z8ZJ-2TJY.

judgments more likely is difficult to ascertain, considering the total absence of such treaties to which the U.S. is a party.[58] Regardless, commercial and civil judgments rendered in the U.S. and South Korea have been recognized in China based on reciprocity.[59] Also, regarding the enforcement of commercial and civil judgments, one might look to the Hague Choice of Court Convention. Under this Convention, signatory countries must recognize and enforce each other's judgments that follow "choice of court agreements," though it should be noted that this Convention is specifically for matters of international trade and investment.[60] The U.S. and China have both signed, though not yet ratified, the Convention, and no other countries concerned in this hypothetical scenario are even signatories.[61] Furthermore, under Article 11 of the Convention, signatory countries can refuse to enforce foreign judgments for excessive punitive damages.[62]

One should also consider the possibility that political considerations may affect a foreign country's attitude toward U.S. judgments. For example, even though China has demonstrated willingness to enforce foreign judgments, relations between China and the U.S. became frostier with the escalation of the trade war,[63] which may raise concerns about how amenable China would be to enforcing a U.S. judgment. Nonetheless, the *China Business Review* reported in 2019 that "[d]espite the heightened China–US frictions under the Trump administration, recent court decisions in China suggest an increase in deference and reciprocity between Chinese and US courts."[64]

Additionally, enforcing U.S. judgments has historically been difficult because it requires clearing the hurdles of the foreign country's "domestic law . . . but also

---

58 *See* U.S. DEP'T ST., *supra* note 30 ("There is no bilateral treaty or multilateral convention in force between the United States and any other country on reciprocal recognition and enforcement of judgments. Although there are many reasons for the absence of such agreements, a principal stumbling block appears to be the perception of many foreign states that U.S. money judgments are excessive according to their notions of liability. Moreover, foreign countries have objected to the extraterritorial jurisdiction asserted by courts in the United States. In consequence, absent a treaty, whether the courts of a foreign country would enforce a judgment issued by a court in the United States depends upon the internal laws of the foreign country and international comity.").

59 *See* CHINA JUST. OBSERVER, *supra* note 57.

60 Convention on Choice of Court Agreements (HCCH 2005 Choice of Court Convention), June 30, 2005, https://perma.cc/PS9S-R8D2 [hereinafter Hague Choice of Court Convention].

61 *See id.*

62 Hague Choice of Court Convention, *supra* note 60, at art. 11 (noting that "recognition or enforcement of a judgment may be refused if, and to the extent that, the judgment awards damages, including exemplary and punitive damages, that do not compensate a party for actual loss or harm suffered").

63 *See* Yukon Huang, *The U.S.–China Trade War Has Become a Cold War*, CARNEGIE ENDOWMENT FOR NAT'L PEACE (Sept. 16, 2021), https://perma.cc/SF3C-FZXT.

64 Qing Di & Karen King, *Trending Toward Reciprocity: Enforcement of US Judgments in China*, CHINA BUS. REV. (Sept. 6, 2019), https://perma.cc/3DNS-68R9.

[depends] on the principles of comity, reciprocity, and res judicata."[65] Moreover, "[f]oreign courts generally do not recognize U.S. money judgments unless: (1) the U.S. court had jurisdiction; (2) the defendant was properly served; (3) the proceedings were not vitiated by fraud; and (4) the judgment is not contrary to the public policy of the foreign country."[66] This means that from the inception of the litigation, the U.S. must have an eye toward the foreign country where the judgment is to be enforced so that the U.S. judgment is not obtained in contravention of the foreign country's law, which could prevent enforcement.

Similar to the enforcement process of U.S. civil and commercial judgments abroad, U.S. criminal judgments and restitution, as well as related civil and monetary judgments, most likely must follow the same path, meaning, the judgment cannot be enforced without cooperation from the foreign country where it needs to be enforced.[67] The ICC likewise does not have a separate, independent capacity to enforce its judgments. Thus, the ICC would also need the cooperation of the foreign country.[68] Taken together, this means that a U.S. criminal proceeding would need to be mindful of laws of the foreign jurisdiction where the judgment is to be enforced. In addition, one should account for the fact that there are a variety of cybercrimes. Therefore, the cooperating countries, either by treaty or convention, should agree to make their cybercrime laws consistent, resulting in automatic "dual criminality" that eliminates safe havens for cybercriminals.[69] Consider, for example, the case of the 2000 Love Bug virus, the creator and distributor of which could not be prosecuted because the Philippines did not consider his acts a crime.[70]

It is worth noting, however, that there are currently some international conventions that do not require dual criminality, and under these conventions, cybercrime can also be prosecuted.[71] For instance, Article 29(3) of the Budapest

---

65 Nadja Vietz, *Will Your U.S. Judgment Be Enforced Abroad?*, 40 THE ADVOC. 1, 14 (2010), https://perma.cc/6XTL-4TVP.

66 *Id. See also* U.S. DEP'T ST., *supra* note 30.

67 *See id. See generally* Samuel P. Baumgartner, *Understanding the Obstacles to the Recognition and Enforcement of U.S. Judgments Abroad*, 44 N.Y.U. J. INT'L L. & POL. 1 (2013).

68 *See* Maryam Jamshidi, *The Enforcement Gap: How the International Criminal Court Failed in Darfur*, AL JAZEERA (Mar. 25, 2013), https://perma.cc/D6VD-W8TS (explaining that "[i]ssues of enforcement have plagued the ICC since it first opened its doors in July 2002," in part because it lacks robust mechanisms to enforce its judgments and because states and inter-governmental organizations such as the U.N. are frequently unwilling to enforce its judgments).

69 *Formal International Cooperation Mechanisms*, UNODC, https://perma.cc/E2BA-NWUR.

70 *See id. See also* Robert Frank, *Philippine Prosecutors Drop Charge in "Love Bug" Case*, WALL ST. J. (Aug. 22, 2020), https://perma.cc/7H6B-34XF.

71 *See id.* (stating that: whenever dual criminality is considered a requirement, it shall be deemed fulfilled irrespective of whether the laws of the requested State Party place the offence within the same category of offence or denominate the offence by the same terminology as the requesting State Party, if the conduct underlying the offence for which assistance is sought is a criminal offence

Convention on Cybercrime of 2001, to which the U.S. is a signatory, does not require dual criminality for expedited data gathering from computers to substantiate the charges of a crime.[72] But under another provision, Article 29(4), a country can also deny the cooperation toward data gathering.[73]

VI. CONCLUSION

The hypothetical analysis above demonstrates that, at this time, prosecuting cybercrimes, obtaining judgments, and enforcing those judgments against foreign cybercriminals—especially if those cybercriminals are located outside U.S. territory—is a logistically challenging endeavor that is unlikely to succeed without further development of legal infrastructure that specifically addresses cyber issues. Due to the increasing sophistication of technology and the cybercriminals who exploit it, the present state of legal remedies is inadequate. To improve this state of affairs, this Essay argues that countries need to cooperate via bilateral treaties and by signing onto international conventions to advance the goal of consistently and uniformly criminalizing types of cybercrime.

Accordingly, many legal scholars and practitioners have proposed a separate cybercrime tribunal within the ICC; this may be the first place to start.[74] Because cybercrime observes no true physical borders, it is easier than ever for a state actor, armed with a computer, to wreak havoc on other nation-states on the other side of the world—and the attendant legal questions challenge legal regimes that, currently, may be too limited in scope to contend with increasingly cross-border issues. Individual responses by affected nations, even those as strong as the U.S., can only be a temporary measure at best as technology continues to advance and cyber infrastructure becomes more global. The creation of a designated, international forum for cybercrime cases would bolster the development of universal norms pertaining to cybersecurity and cybercrime, helping foster a unified front rather than piecemeal responses.

---

under the laws of both States Parties (citing United Nations Convention Against Corruption, Oct. 31, 2003, 2349 U.N.T.S. 41 at art. 43(2))).

72 *Id.*

73 *Id.* (explaining that a country can "refuse data preservation requests if they require dual criminality for mutual assistance for offences other than those included in the Convention").

74 *See generally* Stein Schjolberg, J., *Recommendations for Potential New Global Legal Mechanisms against Global Cyberattacks and Other Global Cybercrimes*, EASTWEST INST. CYBERCRIME LEGAL WORKING GRP. (Mar. 2012), https://perma.cc/XVM9-MR4L.