

A Call to Congress: The Urgent Need for Cyberattack Amendments to the Foreign Sovereign Immunities Act

Matthew A. Powell*

ABSTRACT

The United States must prioritize its battle against the exponential growth in foreign state-sponsored cyberattacks (e.g., ransomware attacks grew by 250% in early 2017, with the United States being the hardest hit). The Foreign Sovereign Immunities Act (FSIA), enacted in 1976, was drafted prior to the exceptional advancements in internet technology and as a result, the Act is woefully out of date. Congress should promptly amend the FSIA to hold foreign nation-state hackers and their agents liable in U.S. courts. Case law interpreting the applicable provision requires a cyberattack occur entirely within U.S. territory (from its inception to execution) in order for U.S. courts to exercise jurisdiction, which yields absurd results and nearly nonexistent remedies, given hackers seldomly travel to the United States to initiate attacks against U.S. persons or businesses. This Comment argues that nation-state actors must be held financially liable in U.S. courts for their tortious conduct, and that any liability would serve as a deterrent to future cyberattacks. Numerous proposals are examined to help curb such conduct, including draft proposals of amendments to the FSIA, financial rewards for hackers who prevent attacks, cryptocurrency tracing, and bilateral cybersecurity agreements.

* J.D. Candidate, 2019, Emory University School of Law; M.B.A. Candidate, 2019, Emory University Goizueta School of Business; B.S.B.A. 2015, Business Management and Entrepreneurship, University of Arizona. Special thanks to Professor Joanna Shepherd for her valuable insight and advice provided in researching and writing this Comment.

INTRODUCTION

A. Defining the Problem

A foreign government currently has absolute immunity in the U.S. courts pursuant to the Foreign Sovereign Immunities Act of 1976 (FSIA) unless there is an express exception to sovereign immunity provided in the FSIA.¹ The express exception to sovereign immunity focused on throughout this Comment is the noncommercial tort exception to the FSIA, which essentially provides that a foreign government shall not be immune from U.S. jurisdiction in any claim seeking money damages for “personal injury or death, or damage to or loss of property, occurring in the United States and caused by the tortious act or omission of [a] foreign state or of any official or employee of that foreign state while acting within the scope of his office or employment.”² The majority of decisions in federal court have adopted what is known as the entire tort doctrine, which means the foregoing noncommercial tort exception to FSIA immunity can only be met when the entire tort, from inception to injury, occurs in U.S. territory.³

Doe a/k/a Kidane v. Ethiopia,⁴ decided on March 14, 2017, is the leading precedent on the issue of whether a noncommercial tort claim can be brought against a foreign government or its agents when that government intentionally conducts a cyberattack against a U.S. person or entity’s computer or computer system in the United States.⁵ The rapid growth in transnational threats has resulted in U.S. law, particularly the FSIA, being rendered woefully inadequate by the

¹ 28 U.S.C. § 1604 (2018) (enacted Oct. 21, 1976; effective Jan. 19, 1977).

² 28 U.S.C. § 1605(a)(5) (2018).

³ SEAN D. MURPHY, PRINCIPLES OF INTERNATIONAL LAW 304, 317 (2d ed. 2012).

⁴ *Doe v. Federal Democratic Republic of Ethiopia (Kidane II)*, 851 F.3d 7, 7 (D.C. Cir. 2017), *reh’g denied*, 2017 U.S. App. LEXIS 10084 (D.C. Cir. June 6, 2017).

⁵ *Id.* at 7–9 (“Plaintiff John Doe—proceeding pseudonymously as ‘Kidane’—claims he was tricked into downloading a computer program. The program allegedly enabled [Ethiopia] to spy on him from abroad. He wants to sue the Republic of Ethiopia.”).

developing case law when it comes to foreign state-sponsored cyberattacks on U.S. companies and individuals.⁶

The increasing rate of digitalization of individuals' lives has resulted in the projected costs of cyberattacks reaching \$2.1 trillion by 2019.⁷ The economic costs of cybercrime quadrupled to approximately \$500 billion from 2013 to 2015, and the expected costs are projected to quadruple again by 2019.⁸ The cybersecurity sector is projected to see large increases in product sales.⁹ In short, cybercrime is swelling the demand for cybersecurity products and services, which is anticipated to increase from \$75 billion in 2015 to \$175 billion in 2020.¹⁰ The cyber insurance market is also projected to grow from \$2.5 billion in 2015 to \$7.5 billion in 2020 because of the increasing prevalence and public awareness of cybercrime.¹¹

The *Kidane* court held that the noncommercial tort exception to the FSIA did not apply to a civil action by a U.S. citizen against Ethiopia, "alleging that Ethiopia . . . committed [the] tort of intrusion upon seclusion [invasion of privacy] in violation of Maryland law" by tricking Mr. Kidane into downloading a computer program that enabled Ethiopia "to spy on him from abroad" without his knowledge.¹² The court found "the tortious intent aimed at Kidane plainly lay abroad and the tortious acts of computer programming likewise occurred abroad. . . . Ethiopia's placement of the virus on Kidane's computer, although completed in the United States when Kidane opened the infected email attachment, [also] began outside the United States."¹³ Thus, the court held "it cannot be said that the entire tort occurred in United States."¹⁴

⁶ Paige C. Anderson, *Cyber Attack Exception to the Foreign Sovereign Immunities Act*, 102 CORNELL L. REV. 1087, 1094–95 (2017).

⁷ Steve Morgan, *Cyber Crime Costs Projected to Reach \$2 Trillion by 2019*, FORBES (Jan. 17, 2016, 11:01 AM), <https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#7df7c4fa3a91>.

⁸ *Id.*

⁹ *Id.*

¹⁰ *Id.*

¹¹ *Id.*

¹² *Kidane II*, 851 F.3d 7, 7–8 (D.C. Cir. 2017), *reh'g denied*, 2017 U.S. App. LEXIS 10084 (D.C. Cir. June 6, 2017).

¹³ *Id.* at 10.

¹⁴ *Id.*

Other FSIA exceptions, such as the commercial tort exception or the waiver of immunity, are certainly significant in the context of cyberattacks. Cyberattack victims “face a major potential problem in proving that an attack is commercial activity at all.”¹⁵ Recent data breaches often result in angry consumers suing large corporations, such as the 2013 attack on Target’s point-of-sale system that affected nearly forty million customers.¹⁶ There is no adequate relief provided by the commercial tort exception, as illustrated by the North Korean hack of Sony Pictures prior to the release of *The Interview*, a controversial comedy film it produced making fun of the North Korean Regime.¹⁷ Nonetheless, the topic of the commercial tort exception is outside of the scope of this Comment, which will focus solely on the FSIA’s noncommercial tort exception.

B. Why Kidane Is Unique

The holding in *Kidane* is the first instance where a U.S. court has held that the FSIA entire tort exception did not apply simply because the internet was used as a medium to transcend national boundaries instead of using a physical actor to execute a cyberattack against an U.S. citizen.¹⁸ Over ninety percent of cyberespionage breaches in 2017 “were attributed to [foreign] state-affiliated groups The tactics used have remained consistent, with phishing remaining a favorite technique of attackers.”¹⁹ In this setting, cyberattacks often involve malicious emails with an attachment sent from a state-affiliated group to its victim.²⁰ When the victim opens the attachment, malware will gain and maintain control and/or surveillance over the victim’s electronic device, usually without the victim’s knowledge.²¹

¹⁵ Anderson, *supra* note 6, at 1091.

¹⁶ Ahiza Garcia, *Target Settles for \$39 Million Over Data Breach*, CNN MONEY (Dec. 2, 2015, 5:48 PM), <http://money.cnn.com/2015/12/02/news/companies/target-data-breach-settlement/index.html>.

¹⁷ Anderson, *supra* note 6, at 1088.

¹⁸ *Kidane II*, 851 F.3d at 9.

¹⁹ VERIZON ENTER. SOLS., 2017 DATA BREACH INVESTIGATIONS REPORT 43 (2017) https://www.verizonenterprise.com/resources/reports/2017_dbir_en_xg.pdf.

²⁰ *Id.*

²¹ *Id.*

The U.S. Court of Appeals for the D.C. Circuit, in *Kidane*, relied on dated cases as precedent and did not address the effect that the internet might have on the entire tort doctrine.²² Even the district court decision in *Kidane* noted “the question is a close one” as to where the tort occurred.²³ The Court of Appeal’s decision only further encourages an increase in the frequency of new attacks knowing that foreign states and their agents “are free to spy on, injure, or even kill Americans in their own homes—so long as they do so by remote control.”²⁴

The FSIA was enacted in 1976 and long before cyberattacks were a daily concern for Americans.²⁵ On the other hand, Congress “would have been aware that foreign states can engage in activities on U.S. territory through a variety of instrumentalities, including remote controlled devices.”²⁶ For example, “unmanned aerial vehicles (i.e., drones) were already in extensive use during the Vietnam War.”²⁷

Thus, when drafting the FSIA, Congress clearly did not contemplate the full extent of potential future cyber threats, even if drones did exist.²⁸ The rapid advancement and increasing affordability of cyber technology would have been nearly impossible to predict, especially with precision.²⁹ In short, Congress must amend or supplement the FSIA to afford proper relief to noncommercial cyber tort victims in American courts.

²² *Kidane II*, 851 F.3d at 7.

²³ *Doe v. Federal Democratic Republic of Ethiopia (Kidane I)*, 189 F. Supp. 3d 6, 21 (D.D.C. 2016), *aff’d*, 851 F.3d 7 (D.C. Cir. 2017).

²⁴ Nate Cardozo, *D.C. Circuit Court Issues Dangerous Decision for Cybersecurity: Ethiopia Is Free to Spy on Americans in Their Own Homes*, ELEC. FRONTIER FOUND. (Mar. 14, 2017), <https://www EFF.ORG/deeplinks/2017/03/dc-circuit-court-issues-dangerous-decision-cybersecurity-ethiopia-free-spy>.

²⁵ 28 U.S.C. § 1604 (2018).

²⁶ Final Opening Brief for Appellant John Doe at 38, *Kidane II*, 851 F.3d 7 (D.C. Cir. 2017) (No. 16-7081).

²⁷ *Id.* at 38–39.

²⁸ *Id.*

²⁹ Reuven Cohen, *The Age of Surprise: Predicting the Future of Technology*, FORBES (Dec. 18, 2013, 2:04 PM), <https://www.FORBES.COM/sites/reuvencohen/2013/12/18/the-age-of-surprise-predicting-the-future-of-technology/#4d77916b6570>.

C. Proposal

The FSIA's entire tort exception has been interpreted in a manner that does not account for modern cybertechnology, leaving foreign states virtually immune from suit in the United States for cyberattacks.³⁰ Thus, U.S. citizens and businesses, such as Mr. Kidane, will often be left without recourse against foreign nations that carry out cyberattacks.³¹ Essentially, victims are faced with the nearly impossible task of having to prove that the entire tort occurred in the United States and that it resulted in "damage to or loss of [the victim's] property."³²

Congress should adopt the International Criminal Tribunal's (ICT) "overall control" standard.³³ This standard, if adopted, would not only allow for increased state accountability, but also deter foreign states from engaging in clandestine state-sponsored cybercrimes.³⁴ The ICT's overall control standard holds a state liable where a state has a "role in organizing and coordinating, in addition to providing support for a [civilian] group, [and] it has sufficient overall control such that the group's acts are attributable to the State."³⁵

Another course of action Congress could take is to draft and adopt a cybersecurity exception to FSIA immunity. However, such a provision would need to be explicitly clear that the exception applies to cyberattacks and that another FSIA provision could not supersede it. Alexis Haller, an experienced trial and appellate attorney whose work concentrates on FSIA matters, has recommended specific language for amendments to the FSIA to be considered by Congress.³⁶ Another

³⁰ *Kidane II*, 851 F.3d 7, 10 (D.C. Cir. 2017), *reh'g denied*, 2017 U.S. App. LEXIS 10084 (D.C. Cir. June 6, 2017).

³¹ *Id.*

³² H.R. REP. NO. 94-1487, at 20–21 (1976).

³³ Scott J. Shackelford & Richard B. Andres, *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem*, 42 GEO. J. INT'L L. 971, 972–73 (2011).

³⁴ *Id.*

³⁵ *Id.* at 975.

³⁶ Alexis Haller, *The Cyberattack Exception to the Foreign Sovereign Immunities Act*, FSIA LAW (Feb. 19, 2017), <https://fsialaw.com/2017/02/19/the-cyberattack-exception-to-the-foreign-sovereign-immunities-act-a-proposal-to-strip-sovereign-immunity-when-foreign-states-engage-in-cyberattacks-against-individuals-and->

recommendation which could lead to increased tort relief for victims would be for the United States to negotiate specialty bilateral cybersecurity agreements.³⁷ The first joint U.S.-China bilateral cybersecurity treaty has been relatively turbulent,³⁸ especially following the indictment of five Chinese military members.³⁹ However, the United States should still actively seek out other, potentially more receptive, nations with the idea that joint cybersecurity cooperation could benefit both countries economically and establish the basis for developing new customary international law.⁴⁰ U.S. government security agencies should also follow private sector best practices, akin to those used by Tesla and Netscape, by hosting additional “bug bounty” programs (also referred to as “big bounty” programs).⁴¹ This would reward hackers for notifying the United States of cyberattacks before they occur.⁴²

Finally, Congress should consider investing more in the Department of Homeland Security’s (DHS) Computer Emergency Readiness Team (CERT) program,⁴³ as well as in the research and development of cryptocurrency detection technologies. Additional CERT funding is important because it would allow the DHS the ability

entities-in-the-united-stat; Alexis Haller, *The D.C. Circuit’s Recent Decision Reinforces the Urgent Need for a Cyberattack Exception to the FSIA*, FSIA LAW (Mar. 16, 2017), <https://fsialaw.com/2017/03/16/the-d-c-circuits-recent-decision-reinforces-the-urgent-need-for-a-cyberattack-exception-to-the-fsia>.

³⁷ Anderson, *supra* note 6, at 1109.

³⁸ Greg Austin, *China-US Cyber Agreements: Has Beijing Outmaneuvered Washington?*, DIPLOMAT (Sept. 28, 2015), <http://thediplomat.com/2015/09/china-us-cyber-agreements-has-beijing-outmaneuvered-washington>.

³⁹ Press Release No. 14-528, U.S. Dep’t of Justice, U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage (May 19, 2014), <https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor>.

⁴⁰ *Id.*

⁴¹ Angelo Young, *An Increasingly Connected World Needs Hackers More than Ever Before*, SALON (Mar. 14, 2017, 4:00 PM), <http://www.salon.com/2017/03/14/an-increasingly-connected-world-needs-hackers-more-than-ever-before>.

⁴² *Id.*

⁴³ OFFICE OF THE INSPECTOR GEN., U.S. DEP’T OF HOMELAND SEC., OIG-10-111, DHS NEEDS TO IMPROVE THE SECURITY POSTURE OF ITS CYBERSECURITY PROGRAM 1–5 (2010), https://www.oig.dhs.gov/assets/Mgmt/OIG_10-111_Aug10.pdf.

to update CERT's "outdated continuity of operations (COOP) plan."⁴⁴ Thus, CERT could better "restore [its] mission-essential functions in the event of an emergency."⁴⁵ This research, although an extremely challenging task, would likely allow investigators to better discern if a state is funding a state actor, or if the state itself is carrying out cyberattacks and trying to cover its tracks via payment in cryptocurrency such as bitcoin.⁴⁶

The United States simply does not have cybersecurity legislative protection for government systems⁴⁷ and Congress has failed to provide a solution.⁴⁸ A related problem is that, if the United States were to have sophisticated cryptocurrency (i.e., virtual assets that exist only in digital form used to purchase goods or services)⁴⁹ detection technology, it would most likely complement the ICT's overall control standard very well.⁵⁰ This symbiotic relationship can be realized by waiving the foreign state's immunity as long as "it has sufficient overall control such that the group's acts are attributable to the State."⁵¹

D. Results of Ineffective Remedies

Often, criminal proceedings are simply not worth the potential risks within an economic and geopolitical context. The indictment of

⁴⁴ SEN. TOM COBURN, S. COMM. ON HOMELAND SEC. & GOV'T AFFAIRS, 113TH CONG., A REVIEW OF THE DEPARTMENT OF HOMELAND SECURITY'S MISSIONS & PERFORMANCE 1, 92 (2015).

⁴⁵ *Id.*

⁴⁶ Kit Chellel, *British Cyber Cops Face Biggest Test After Worldwide Cyberattack*, BLOOMBERG (May 17, 2017, 7:30 AM), <https://www.bloomberg.com/news/articles/2017-05-17/british-cyber-cops-face-biggest-test-after-worldwide-cyberattack>.

⁴⁷ Chelsea C. Smith, *Hacking Federal Cybersecurity Legislation: Reforming Legislation to Promote the Effective Security of Federal Information Systems*, 4 NAT'L SEC. L.J. 345, 348 (2016).

⁴⁸ *Id.*

⁴⁹ Nicky Woolf, *Why the US Government Wants to Bring Cryptocurrency Out of the Shadows*, THE GUARDIAN, (Nov. 27, 2016, 10:00 AM), <https://www.theguardian.com/technology/2016/nov/27/coinbase-bitcoin-irs-government-summons-data-cryptocurrency>.

⁵⁰ Shackelford & Andres, *supra* note 33, at 975.

⁵¹ *Id.*

the five Chinese state-sponsored actors helped to place the first U.S. bilateral cybersecurity treaty⁵² on shaky grounds.⁵³ Likewise, economically, the resources required to support an investigation and subsequent prosecution are both costly and time consuming.⁵⁴

Any proposals should place additional attention on the scope and capabilities of foreign state-sponsored actors, while signaling to Congress the FSIA's urgent need for a cybersecurity exception and an incorporation of the ICT's overall control standard into its language.⁵⁵ Currently, foreign states are almost guaranteed not to face liability in U.S. courts, given the FSIA's present form and the decision in *Kidane*.⁵⁶

Many of the strongest military countries in the world also engage in the most sophisticated cyberattacks.⁵⁷ Thus, it is a delicate geopolitical dance when nation states such as the People's Republic of China or the Russian Federation are carrying out the most complex and damaging cyberattacks.⁵⁸ For example, the indictment of Chinese hackers under the Obama administration tested the United States' relationship with one of its largest trading partners⁵⁹ and a very capable nuclear counterpart.⁶⁰

State-sponsored cyberattacks will only get more difficult to trace as hackers increasingly demand cryptocurrencies (e.g., bitcoin, an

⁵² Anderson, *supra* note 6, at 1109.

⁵³ Cameron S.D. Brown, *Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice*, 9 INT'L J. CYBER CRIMINOLOGY 55, 88 (2015).

⁵⁴ *Id.* at 60.

⁵⁵ Shackelford & Andres, *supra* note 33, at 972–73.

⁵⁶ Anderson, *supra* note 6, at 1109.

⁵⁷ John E Dunn, *The World's 10 Most Dangerous Cyberwarfare Attacks*, TECHWORLD (Mar. 13, 2015), <https://www.techworld.com/security/worlds-10-most-dangerous-cyberwarfare-attacks-3601660>.

⁵⁸ Bill Gertz, *Pentagon: Russia, China Able to Launch Catastrophic Cyber Attacks on U.S. Infrastructure for Next 10 Years*, WASH. FREE BEACON (Mar. 10, 2017, 5:00 AM), <http://freebeacon.com/national-security/pentagon-russia-china-able-launch-catastrophic-cyber-attacks-u-s-infrastructure-next-10-years>.

⁵⁹ US-CHINA BUS. COUNCIL, 2018 STATE EXPORT REPORT (Apr. 2018), https://www.uschina.org/sites/default/files/final_uscbc_state_report_2018_1.pdf.

⁶⁰ Alex Lockie, *How the US's Nuclear Weapons Compare to Russia's*, BUS. INSIDER (Sept. 28, 2016, 9:45 AM), <http://www.businessinsider.com/us-vs-russia-nuclear-weapons-2016-9>.

online currency that is extremely difficult to track) as ransomware payment.⁶¹ More recently, cyberattacks following the *Kidane* case (e.g., WannaCry) have required prompt ransom payment in the form of bitcoin before the malicious file will spread from computer to computer automatically.⁶² Foreign state-sponsored hacking is assessed by experts today as both commonplace and constant, causing billions of dollars in damages and threatening national security because key U.S. infrastructure is at risk.⁶³ Future indictments of foreign nation-state actors could also potentially cause massive geopolitical instability, as the world has recently seen in the Democratic People's Republic of Korea (DPRK) following the imposition of sanctions by the U.N. Security Council in September 2017.⁶⁴

This Comment proceeds as follows. Section I commences with a description of the legal landscape of sovereign immunity and nation states as defendants in U.S. courts before and after the enactment of the FSIA. Section I focuses on the history and development of the FSIA, and particularly on how the entire tort doctrine developed and how it was applied by the D.C. Circuit in its decision in *Kidane*. It also contains an overview of the controlling case law that U.S. courts use to determine whether the FSIA's noncommercial tort exception applies. Section II examines the economic and geopolitical consequences of the FSIA's entire tort requirement and proposes that, under the current economic model, the doctrine provides virtually guaranteed immunity and profitability for foreign state-sponsored hackers. Section III offers numerous proposals to disincentivize state-sponsored cyberattacks and to afford their victims with relief, such as encouraging Congress to implement a narrowly tailored cyberattack exception and to incorporate an overall control standard into the FSIA. This Comment also advocates for the United States to join bilateral and multilateral treaties with receptive nation states in an effort to establish customary

⁶¹ Chellel, *supra* note 46 and accompanying text.

⁶² *Id.*

⁶³ Christopher Bodeen, *Cyber Attacks a Growing Irritant in US-China Ties*, SYDNEY MORNING HERALD (May 9, 2013, 11:30 AM), <http://www.smh.com.au/it-pro/security-it/cyber-attacks-a-growing-irritant-in-uschina-ties-20130509-2j951.html>.

⁶⁴ Zachary Cohen & Richard Roth, *UN Passes Fresh Sanctions on North Korea*, CNN (Sept. 12, 2017, 9:31 AM), <https://www.cnn.com/2017/09/11/politics/north-korea-un-security-council-vote/index.html>.

international law in the cybersecurity sector and argues that increased funding of the DHS' CERT program will help improve the United States readiness for future threats, as well as reduce the potential likelihood of successful cyberattacks.

I. BACKGROUND

Before a discussion is had on the consequences of cyberattacks and related proposals to reduce their likelihood, it helps to grasp the history and scope of sovereign immunity as it existed prior to the 1976 congressional enactment of the FSIA.

A. *Sovereign Immunity Before the FSIA*

The “doctrine of ‘absolute immunity,’ which had its basis in principles of state sovereignty, was for centuries deemed to reflect customary international law, and remains the approach taken in many countries, such as Brazil, China, and Russia.”⁶⁵ Early on in U.S. history, the Supreme Court fully embraced the doctrine of absolute immunity,⁶⁶ as indicated by its decision in *The Schooner Exchange v. McFaddon*.⁶⁷ In the *The Schooner Exchange*, the doctrine of sovereign immunity was clearly accepted and explained throughout Chief Justice John Marshall’s opinion.⁶⁸ Allegedly, persons acting for Napoleon, the Emperor of France, forcibly took a ship named the Schooner Exchange that was sailing in the Atlantic from Baltimore to Spain on December 30, 1810.⁶⁹ The alleged captors then sailed the ship to the port of Philadelphia.⁷⁰ On August 24, 1811, the American owners of the ship, John McFaddon and William Greetham brought suit against France and Napoleon, as Emperor, to attach the ship and to require that the appellants return the ship to its asserted American owners.⁷¹

⁶⁵ MURPHY, *supra* note 3, at 304.

⁶⁶ *Id.*

⁶⁷ *The Schooner Exch. v. McFaddon*, 11 U.S. 116, 138 (1812).

⁶⁸ MARK WESTON JANIS & JOHN E. NOYES, *INTERNATIONAL LAW CASES & COMMENTARY* 1020, 1020–23 (American Casebook Series, 5th ed. 2014).

⁶⁹ *The Schooner Exch.*, 11 U.S. at 117.

⁷⁰ *Id.*

⁷¹ *Id.*

Chief Justice John Marshall concluded that “no foreign sovereign would subject itself to the absolute and exclusive power of another [sovereign] without an implied understanding that entry into foreign territory included a grant of immunity from the territorial sovereign’s power.”⁷² The Supreme Court held in favor of the Country of France, relying on the doctrine of absolute immunity to find no jurisdiction over the matter for U.S. courts.⁷³ Other courts of the United States followed this doctrine closely up until shortly after World War I.⁷⁴ For example, the Supreme Court decided that the United States did not have jurisdiction in *Berizzi Bros. Co. v. S.S. Pesaro*⁷⁵ based on the doctrine of absolute immunity.⁷⁶ In *Pesaro*, the plaintiff claimed that a ship owned by the Country of Italy allegedly failed to deliver certain artificial silk, taken aboard in Italy, to the ship’s destination in the port of New York.⁷⁷ The Supreme Court addressed only the issue of whether a foreign government (Italy), which owned and operated a ship failing to deliver goods, was immune from the jurisdiction of a U.S. district court exercising its admiralty jurisdiction.⁷⁸ Again, the Supreme Court answered in the affirmative based on the absolute immunity doctrine.⁷⁹

However, in the 1940s, United States and European courts started considering circumstances in which restricted foreign sovereign immunity should apply.⁸⁰ To ascertain the cases in which sovereign immunity should be applied, U.S. courts started seeking recommendations from the U.S. Department of State (State Department); and, when they did not receive a timely recommendation, the court made its decision based on past State Department practice.⁸¹

⁷² MURPHY, *supra* note 3, at 304 (citing *The Schooner Exch.*, 11 U.S. at 146–47) (summarizing Justice Marshall’s rationale).

⁷³ *The Schooner Exch.*, 11 U.S. at 146–47.

⁷⁴ Daniel T. Murphy, *The American Doctrine of Sovereign Immunity: An Historical Analysis*, 13 VILL. L. REV. 583, 590–91 (1968).

⁷⁵ *Berizzi Bros. Co. v. The Pesaro*, 271 U.S. 562, 562 (1926).

⁷⁶ *Id.* at 576.

⁷⁷ *Id.* at 569–70.

⁷⁸ *Id.* at 570.

⁷⁹ *Id.* at 576.

⁸⁰ MURPHY, *supra* note 3, at 305.

⁸¹ *Id.*

Experience under this approach showed that the State Department's positions were often nebulous or contradictory.⁸²

The results, such as those from the Supreme Court's decision in *Mexico v. Hoffman*, demonstrate the unpredictable outcome under this procedure involving the State Department.⁸³ In *Hoffman*, a merchant ship owned by the Mexican government, but in the possession and operation of a private party, collided with and caused damage to a fishing ship owned by U.S. citizens.⁸⁴ The U.S. citizens subsequently brought suit in federal district court.⁸⁵ The Supreme Court held that the Mexican government was not immune from suit under the doctrine of sovereign immunity because "the State Department has certified such ownership, but it has refrained from certifying that it allows the immunity or recognizes ownership of the vessel without possession by the Mexican government as a ground for immunity."⁸⁶

In an effort to bring consistency to the State Department's positions on foreign sovereign immunity, the Department's legal advisor sent a letter in 1952 (the Tate letter) notifying the Department of Justice that, effective immediately, the State Department would endorse a theory of "restrictive" foreign sovereign immunity.⁸⁷ Under this theory, the State Department "would recommend immunity only when a case involved the public acts of a foreign government . . . ; it would not recommend immunity when a case involved the commercial acts of a foreign government, acts which could have been carried on by private parties" and if no recommendation was made "the characterization of an act as 'governmental' or 'commercial' was to be determined by the courts."⁸⁸ An application of the theory is found in *Victory Transport, Inc. v. Comisaria General*,⁸⁹ where the Second

⁸² *Id.*

⁸³ *Republic of Mexico v. Hoffman*, 324 U.S. 30, 30 (1945).

⁸⁴ *Id.* at 31.

⁸⁵ *Id.*

⁸⁶ *Id.* at 36.

⁸⁷ MURPHY, *supra* note 3, at 305; Letter from Jack B. Tate, Acting Legal Advisor of the United States Dep't of State, to Phillip B. Perlman, Acting Attorney Gen. of the United States (May 19, 1952), *reprinted in* 26 Dep't State Bull. 678 at 984 (June 27, 1952).

⁸⁸ *Id.*

⁸⁹ *Victory Transp., Inc. v. Comisaria Gen. de Abastecimientos y Transportes*, 336 F.2d 354, 360–62 (2d Cir. 1964).

Circuit held that an arm of the Spanish government chartering a ship to transport grain was an act precisely like a private commercial act.⁹⁰ Accordingly, the Second Circuit denied immunity to the arm of the Spanish government.⁹¹

The theory of restrictive foreign immunity did not eliminate the pressure the State Department faced from foreign diplomats requesting foreign governmental immunity, and international political friction often arose when a recommendation was not obtained.⁹² The State Department found that it was nearly impossible to evenly apply the theory and to keep international relationships intact when deciding whether to recommend immunity in individual cases.⁹³ The struggle of performing its conflicting responsibilities would continue for twenty years until the enactment of the FSIA in 1976, which was intended to eliminate the State Department's burdensome role in sovereign immunity cases and to place the burden on the judicial branch to determine sovereign immunity based on the FSIA's statutory scheme.

B. The History & Development of the FSIA

It has been reckoned that questions relating to the jurisdictional immunities of foreign sovereigns figure more before national courts than do any other questions of international law.⁹⁴

Enacted in 1976, the FSIA governs “all litigation in both state and federal courts against foreign states and governments, including their ‘agencies and instrumentalities.’”⁹⁵ “It provides the exclusive basis for obtaining jurisdiction over these entities in U.S. courts.”⁹⁶

⁹⁰ *Id.*; see MURPHY, *supra* note 3, at 305 (summarizing the court's holding and rationale in *Victory Transport, Inc.*).

⁹¹ *Victory Transp., Inc.*, 336 F.2d at 360–62.

⁹² MURPHY, *supra* note 3, at 305–06.

⁹³ *Id.* at 306.

⁹⁴ JANIS & NOYES, *supra* note 68, at 692 (quoting Leo J. Bouchez, *The Nature and Scope of State Immunity from Jurisdiction and Execution*, 10 NETH. Y.B. INT'L L. 3, 4 (1979)).

⁹⁵ David P. Stewart, *The Foreign Sovereign Immunities Act: A Guide for Judges*, FED. JUD. CTR. INT'L LITIG. GUIDE 1 (2013), <https://www.fjc.gov/sites/default/files/2014/FSIAGuide2013.pdf>.

⁹⁶ *Id.*

Furthermore, “[t]he number of FSIA cases has been rising dramatically. In the ten years ending in 2008, “the number of reported decisions . . . increased by nearly seventy percent.”⁹⁷ Sovereign immunity was absolute until the “restrictive theory” was adopted by U.S. courts in 1952 via the Tate letter.⁹⁸ All FSIA cases therefore require the following questions to be answered by a U.S. court at the outset of any FSIA case:

1. Is the defendant a “foreign state or government” within the meaning of the statute?
2. Has valid service been made as provided by the statute?
3. Does a statutory exception to immunity apply?⁹⁹

The *Kidane* court found the legislative history of the FSIA to show that the noncommercial tort exception was first “implemented to eliminate a foreign state’s immunity for traffic accidents and other torts committed in the United States,”¹⁰⁰ and “[i]t is thus unsurprising that transnational cyberespionage should lie beyond section 1605(a)(5)’s reach.”¹⁰¹ However, the *Kidane* court fails to mention the House Report describing the exception “in general terms as applying to all tort actions for money damages.”¹⁰²

C. *Kidane*: Basic Facts

The facts of the case read as if lifted from a cybersecurity spy novel. Mr. Kidane, born in Ethiopia, was a U.S. citizen living in Silver Spring, Maryland, at the time that his lawsuit was filed.¹⁰³ He was

⁹⁷ JANIS & NOYES, *supra* note 68, at 692 (quoting Aryeh S. Portney et al., *The Foreign Sovereign Immunities Act: 2008 Year in Review* 16 LAW & BUS. REV. AM. 179, 180 (2010)).

⁹⁸ Kevin P. Simmons, *The Foreign Sovereign Immunities Act of 1976: Giving the Plaintiff His Day in Court*, 46 FORDHAM L. REV. 543 (1977).

⁹⁹ Stewart, *supra* note 95, at 2.

¹⁰⁰ H.R. REP. NO. 94-1487, at 20–21 (1976).

¹⁰¹ *Kidane II*, 851 F.3d 7, 11 (D.C. Cir. 2017), *reh’g denied*, 2017 U.S. App. LEXIS 10084 (D.C. Cir. June 6, 2017).

¹⁰² H.R. REP. NO. 94-1487, at 20–21 (1976).

¹⁰³ *Kidane II*, 851 F.3d at 7–10.

granted asylum by the United States in the early 1990s.¹⁰⁴ He also remained active in the Ethiopian community to raise awareness of Ethiopian corruption and human rights issues.¹⁰⁵ Around 2012, Ethiopia or its agents used the internet to send Mr. Kidane an innocent looking email attachment from Ethiopia to his computer in his Maryland home which he opened, read, and then ignored.¹⁰⁶ Upon opening the attachment, Mr. Kidane unknowingly installed “FinSpy” on his computer, which allegedly recorded and sent to Ethiopia via the internet nearly all of the activities by the users of the computer.¹⁰⁷

D. FSIA Summary: How the Entire Tort Doctrine Developed

The noncommercial tort exception to the FSIA essentially provides that a foreign government shall not have immunity in a claim concerning “personal injury or death, or damage to or loss of property, occurring in the United States and caused by the tortious act or omission of [a] foreign state or of any official or employee of that foreign state while acting within the scope of his office or employment.”¹⁰⁸ The noncommercial tort exception or section 1605(a)(5) exception shall be used interchangeably throughout this Comment. The Supreme Court,¹⁰⁹ D.C. Circuit,¹¹⁰ Second Circuit,¹¹¹ and Sixth Circuit¹¹² have all adopted the entire tort doctrine, which means that the foregoing exception can only be met when the entire tort, from inception to injury, occurs in U.S. territory.¹¹³

¹⁰⁴ *Id.*

¹⁰⁵ *Id.*

¹⁰⁶ *Id.*

¹⁰⁷ *Id.*

¹⁰⁸ 28 U.S.C. § 1604(a)(5) (2018).

¹⁰⁹ See *Argentine Republic v. Amerada Hess Shipping Corp.*, 488 U.S. 428, 428 (1989).

¹¹⁰ See *Kidane II*, 851 F.3d at 7.

¹¹¹ See *De Letelier v. Republic of Chile*, 748 F.2d 790, 792 (2d Cir. 1984).

¹¹² See Final Brief for Appellee at 18, *Kidane II*, 851 F.3d 7 (D.C. Cir. 2017) (No. 16-7081), (citing *O’Bryan v. Holy See*, 556 F.3d 361, 385 (6th Cir. 2009)).

¹¹³ See *De Letelier*, 748 F.2d at 792.

E. Controlling Case Law Determining Whether the Noncommercial Tort Exception Applies

One of the earliest cases to determine whether the section 1605(a)(5) exception applied was the 1980 case of *De Letelier v. Republic of Chile*.¹¹⁴ The plaintiffs brought noncommercial tort claims against the country of Chile and a Chilean intelligence agency for allegedly ordering and aiding agents in the United States in successfully completing a Washington, D.C. car bombing that resulted in the death of the former Chilean ambassador.¹¹⁵ The court remarked that the alleged acts of ordering and aiding the assassins “may well have been carried out entirely within [Chile],” but refused to grant immunity to Chile because to do so would “totally emasculate the purpose and effectiveness of the Foreign Sovereign Immunities Act.”¹¹⁶

The first mention of the whole tort or the entire tort doctrine as it relates to the section 1605(a)(5) exception is found in a 1982 Southern District of Texas case, *In re Sedco, Inc.*¹¹⁷ An oil company owned by the country of Mexico created an oil spill while drilling in Mexican waters, and the spill had a damaging effect on the Texas coastline.¹¹⁸ The case was not even close for section 1605(a)(5) purposes because all alleged tortious acts occurred in Mexico, and the court found that Mexico retained its immunity.¹¹⁹ The court based its rationale on its reading of section 1605(a)(5)’s legislative history showing congressional intent that “the tort, in whole, must occur in the United States.”¹²⁰

In *Asociacion de Reclamantes v. United Mexican States*, decided in 1984,¹²¹ then appellate court Judge Antonin Scalia authored the opinion of the Court, which held that appellants’ tort claims must

¹¹⁴ *Id.*

¹¹⁵ *Id.* at 791.

¹¹⁶ *Letelier v. Republic of Chile*, 488 F. Supp. 665, 674 (D.D.C. 1980).

¹¹⁷ *In re Sedco, Inc.*, 543 F. Supp. 561 (S.D. Tex. 1982), *vacated in part*, 610 F. Supp. 306 (S.D. Tex. 1984).

¹¹⁸ *Id.* at 568.

¹¹⁹ *Id.* at 572.

¹²⁰ *Id.* at 567.

¹²¹ *Asociacion de Reclamantes v. United Mexican States*, 735 F.2d 1517, 1525 (D.C. Cir. 1984).

be dismissed because at least part of the alleged entire tort did not occur on U.S. soil.¹²² The court discussed *Sedco* approvingly in making its decision.¹²³ This case was not a difficult decision because the acts in question all took place within Mexico and outside of the United States. Further, the appellants alleged that Mexico, acting through its officials in Mexico, wrongfully took their private land, conveyed it to Texas and the United States, and failed to compensate them for the taking.¹²⁴

The first, and only ruling to date, of the Supreme Court concerning the entire tort doctrine came in its 1989 case, *Argentine Republic v. Amerada Hess Shipping Corp.*,¹²⁵ where a Liberian company alleged that Argentinian military jets attacked and damaged its oil tanker in international waters. Amerada raised a novel argument that the FSIA defines the “United States” as including all “territory and waters . . . subject to the jurisdiction of the United States,” that the tort occurred in international waters, and that such waters are within the admiralty jurisdiction of the United States.¹²⁶ The Supreme Court rejected Amerada’s argument and found that, for the section 1605(a)(5) exception, “United States” means the United States or its possessions, and does not include international waters.¹²⁷ Following the *Amerada* decision, the lower federal courts have significantly impacted the FSIA’s interpretation.

Remarkably, the 1989 Ninth Circuit decision in *Liu v. Republic of China*¹²⁸ does not follow the Supreme Court precedent set in *Amerada*, even though the Ninth Circuit decided *Liu* after the *Amerada* decision was issued. An official of the Chinese government, Mr. Wong, did not enter the United States personally, but in his official capacity, he hired gang members who successfully completed the assassination of Mr. Liu by shooting him to death in Daly City, California.¹²⁹ The court cited *Amerada* for the proposition that the FSIA is “the sole basis

¹²² *Id.*

¹²³ *Id.*

¹²⁴ *Id.* at 1524.

¹²⁵ *Argentine Republic v. Amerada Hess Shipping Corp.*, 488 U.S. 428, 441 (1989).

¹²⁶ *Id.* at 440.

¹²⁷ *Id.*

¹²⁸ *Liu v. Republic of China*, 892 F.2d 1419, 1419 (9th Cir. 1989).

¹²⁹ *Id.*

for obtaining [subject matter] jurisdiction over a foreign state in . . . [U.S.] courts,” and the court makes no mention of the entire or whole tort doctrine.¹³⁰ This case is significant because the Ninth Circuit ignored the Supreme Court’s *Amerada* decision and did not address the entire tort requirement, finding that all requirements of the Section 1605(a)(5) exception were met even though part of the acts occurred in China and part of the acts occurred in California.¹³¹ The Ninth Circuit ruled that the noncommercial tort claims against China could proceed.¹³²

In 1989, the Second Circuit first commented on the entire tort doctrine in *Cabiri v. Government Republic of Ghana*¹³³ where the court based its decision on another subsection of the FSIA. However, in a footnote, the Second Circuit cited the Supreme Court decision in *Amerada* to note that the noncommercial tort exception only covers torts “occurring [entirely] in the territorial jurisdiction of the United States.”¹³⁴

In a decision by the Sixth Circuit in 1989, *O’Bryan v. Holy See*,¹³⁵ there was no dispute among the parties that the Holy See (State of the Vatican) is a foreign state within the meaning of the FSIA.¹³⁶ The appellees alleged in their complaint that separate groups of Vatican personnel, both inside and outside of the United States, committed an extensive number of noncommercial torts by failing to properly supervise Roman Catholic priests.¹³⁷ These clergymen allegedly engaged in acts of sexual abuse in the United States that resulted in vicarious liability for their employer, the Vatican.¹³⁸ The court embraced the entire tort theory as a requirement for the section 1605(a)(5) exception, citing the Supreme Court’s decision in *Amerada* as well as similar previous holdings in both the D.C. and Second

¹³⁰ *Id.* at 1424.

¹³¹ *Id.*

¹³² *Id.* at 1421.

¹³³ *Cabiri v. Government of Republic of Ghana*, 165 F.3d 193 (2d Cir. 1999).

¹³⁴ *Id.* at 200.

¹³⁵ *O’Bryan v. Holy See*, 556 F.3d 361 (6th Cir. 2009).

¹³⁶ *Id.* at 372.

¹³⁷ *Id.* at 386.

¹³⁸ *Id.*

Circuits.¹³⁹ However, the court then found that the entire tort doctrine was satisfied with respect to all claims of tortious acts where Vatican personnel located inside the United States allegedly failed to properly supervise priests, making the Vatican liable.¹⁴⁰ The decision did not squarely address how the entire tort doctrine was affected by the factual allegation that some or all of the same tortious acts were also based on inadequate supervision by Vatican personnel located outside the United States.¹⁴¹

In 2014, the D.C. Circuit again examined the requirements to meet the noncommercial tort exception to the FSIA in *Jerez v. Republic of Cuba*,¹⁴² and the court again applied the entire tort doctrine.¹⁴³ Jerez alleged that he was intentionally infected with hepatitis C by a Cuban official while he was held in a prison in Cuba, and that after he was allowed to return to the U.S., a new tort occurred every time the virus replicated itself in his body.¹⁴⁴ The court dismissed the case, and held that the section 1605(a)(5) exception was not met because the “law is clear that ‘the entire tort’—including not only the injury but also the act precipitating that injury—must occur in the United States.”¹⁴⁵

II. ECONOMIC AND GEOPOLITICAL CONSEQUENCES OF THE FSIA’S ENTIRE TORT REQUIREMENT

Thus, the *Kidane* court’s failure to engage in judicial activism leaves Americans without sufficient legal recourse if a state-sponsored cyberattack targets a U.S. individual or entity. The FSIA’s entire tort requirement creates an economic model that is favorable to cybersecurity hackers and does immense harm to their victims. Although there have been measures put in place to prevent these attacks, this section addresses how the entire tort doctrine leaves victims without recourse in U.S. courts if a foreign sovereign conducts the cyberattack. With state-sponsored cyberattacks becoming more

¹³⁹ *Id.* at 382.

¹⁴⁰ *Id.* at 386.

¹⁴¹ *Id.*

¹⁴² *Jerez v. Republic of Cuba*, 775 F.3d 419 (D.C. Cir. 2014).

¹⁴³ *Id.* at 424.

¹⁴⁴ *Id.* at 421–22, 424.

¹⁴⁵ *Id.* at 424.

common, it seems clear that the court missed an opportunity in *Kidane* to help establish customary international law to better address growing cybersecurity concerns worldwide.

A. State Sponsorship: A Deadly Economic Model

Crimes in cyberspace will cost the global economy \$455 billion in 2016—more than the market cap of Microsoft (\$411 billion), Facebook (\$314 billion) or ExxonMobil (\$332 billion)—according to an estimate from the World Economic Forum’s 2016 Global Risk Report.¹⁴⁶

Given the types of hackers faced, recent cyberattacks “which paralyzed the websites of Amazon, Buy.com, and eBay” demonstrate that “there are brilliant but unscrupulous hackers out there who have developed technologies that the average person can’t even dream of.”¹⁴⁷ As another example, Hidden Lynx is a Chinese-affiliated group of approximately fifty to a hundred highly skilled, state-sponsored cyber hackers who also do private hacking for profit.¹⁴⁸ Computer expert Arnold Yabenson, President of the Washington-based consumer group National CyberCrime Prevention Foundation (NCPF), warns that even an seemingly innocent email attachment, akin to the attachment sent in the *Kidane* case, can turn a home computer into a “large hand grenade” by manipulating electrical currents.¹⁴⁹ The state-sponsored model that China is likely utilizing allows groups such as Hidden Lynx to operate in the private sector to make additional profits uninterrupted.¹⁵⁰ Essentially, Hidden Lynx is a group of “professional hackers for hire”

¹⁴⁶ Harriet Taylor, *An Inside Look at What’s Driving the Hacking Economy*, CNBC (Feb. 5, 2016, 10:02 AM), <https://www.cnbc.com/2016/02/05/an-inside-look-at-whats-driving-the-hacking-economy.html>.

¹⁴⁷ Team Register, *Hackers Can Make Your PC Explode*, REGISTER (July 4, 2000, 2:47 PM), https://www.theregister.co.uk/2000/07/04/hackers_can_make_your_pc.

¹⁴⁸ Kim Zetter, *State-Sponsored Hacker Gang Has a Side Gig in Fraud*, WIRED (Sept. 17, 2013, 9:00 AM), <https://www.wired.com/2013/09/hidden-lynx>.

¹⁴⁹ Team Register, *supra* note 147 and accompanying text; *Kidane II*, 851 F.3d 7, 8–9 (D.C. Cir. 2017), *reh’g denied*, 2017 U.S. App. LEXIS 10084 (D.C. Cir. June 6, 2017).

¹⁵⁰ Zetter, *supra* note 148 and accompanying text.

that will work for the highest bidder, both in the private and public sector.¹⁵¹

Former FBI Director James B. Comey stated, “[f]or too long, the Chinese government has blatantly sought to use cyber espionage to obtain economic advantage for its state-owned industries.”¹⁵² This state-sponsored meddling is only likely to reoccur as large nation states such as the People’s Republic of China and the Russian Federation are not only working internally, but are now contracting externally with groups who act as “pa[id] freelancers” when those respective groups have access to systems that the nation state determines are beneficial to their governmental interest.¹⁵³ The business model is the reverse of what victims of cyberattacks would desire because it is much more lucrative to be on the “offensive side” as opposed to the “defensive side” of a sophisticated cyberattack.¹⁵⁴ The following metrics reinforce how costly to victims and profitable to hackers the current economic model is. Cyber modelers are predicting that the recent WannaCry cyberattack could cost \$4 billion.¹⁵⁵ This makes 2017 the worst year in history for ransomware attacks.¹⁵⁶ Profits for state-sponsored cyberattacks are only attracting more hackers in countries such as the Russian Federation.¹⁵⁷ For example, the Russian Defense Ministry purchased recruiting advertising on Vkontakte, the most popular Russian social network.¹⁵⁸ “One video shows a man clanging a military rifle on a table beside a laptop computer, then starting to type.”¹⁵⁹

¹⁵¹ *Id.*

¹⁵² Press Release No. 14-528, *supra* note 39 and accompanying text.

¹⁵³ Kim Zetter, *We’re at Cyberwar: A Global Guide to Nation-State Digital Attacks*, WIRED (Sept. 1, 2015, 7:00 AM), <https://www.wired.com/2015/09/cyberwar-global-guide-nation-state-digital-attacks>.

¹⁵⁴ Dana Rubenstein, *Nation State Cyber Espionage and its Impacts*, at 8 (Dec. 15, 2014), http://www.cse.wustl.edu/~jain/cse571-14/ftp/cyber_espionage.pdf.

¹⁵⁵ Jonathan Berr, “WannaCry” Ransomware Attack Losses Could Reach \$4 Billion, CBS NEWS (May 16, 2017, 5:00 AM), <https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses>.

¹⁵⁶ *Id.*

¹⁵⁷ *Id.*

¹⁵⁸ Andrew E. Kramer, *How Russia Recruited Elite Hackers for Its Cyberwar*, N.Y. TIMES (Dec. 29, 2016), <https://www.nytimes.com/2016/12/29/world/europe/how-russia-recruited-elite-hackers-for-its-cyberwar.html>.

¹⁵⁹ *Id.*

Basic economic principles such as the assumption “that criminals behave rationally and weigh the costs and benefits of criminal activity before turning to crime”¹⁶⁰ explain why more hackers are entering this clandestine cybersecurity sector. Hackers can make more than \$80,000 a month and cyberattack “exploit kits” can cost as little as \$30 to rent and \$500 to buy.¹⁶¹ These “exploit kits” typically provide the hacker with the necessary electronic hardware and software to carry out a cyberattack against an individual or organization.¹⁶² Even more concerning for individuals and business entities is that “new and better exploit kits [are] being made, and the success rate has risen to as much as 40%.”¹⁶³ A cybersecurity firm called Trustwave found that one hacker’s bitcoin “wallet” made \$60,000 in one week.¹⁶⁴

B. Foreign States and Their Agents are Virtually Guaranteed Immunity and Profit

Although the [FSIA’s noncommercial tort] exception was “directed primarily at the problem of traffic accidents” [the House Report] “cast [it] in general terms as applying to *all tort actions* for money damages, not otherwise encompassed by section 1605(a)(2), relating to commercial activities.”¹⁶⁵

“Despite this broad legislative grant, courts often follow the influential D.C. Circuit’s practice and construe the exception narrowly “so as not to encompass the farthest reaches of common law.”¹⁶⁶ This leads to mixed signals among other U.S. courts.¹⁶⁷ International

¹⁶⁰ HENRY N. BUTLER ET AL., *ECONOMIC ANALYSIS FOR LAWYERS* 383, 393 (3d ed. 2014).

¹⁶¹ Cale Guthrie Weissman, *Some Hackers Make More than \$80,000 a Month — Here's How*, BUS. INSIDER (July 14, 2015, 12:16 PM), <http://www.businessinsider.com/we-found-out-how-much-money-hackers-actually-make-2015-7/#ploit-kits-2>.

¹⁶² *Id.*

¹⁶³ *Id.*

¹⁶⁴ *Id.*

¹⁶⁵ Final Opening Brief for Appellant John Doe, *supra* note 26, at 37 (emphasis added) (quoting S. REP. NO. 94-1310, at 20 (1976)).

¹⁶⁶ Scott A. Gilmore, *Suing the Surveillance States: The (Cyber) Tort Exception to the Foreign Sovereign Immunities Act*, 46 COLUM. HUM. RTS. L. REV. 227, 253 (2015).

¹⁶⁷ *Id.*

cyberattacks are very costly to the United States economy, with cyberattack damage estimates ranging “between \$57 billion and \$109 billion in 2016.”¹⁶⁸ This does not align with the lack of action taken by U.S. courts. For example, following the United States indicting five Chinese Army hackers, China responded by stating that the facts of the case were “fabricated” and that the indictment “grossly violates the basic norms governing international relations and jeopardizes China-U.S. cooperation.”¹⁶⁹ The damage only continued, as China also cut off cooperation with a joint U.S.-China working group on preventing cyberattacks that the Obama administration stated “was evidence that the two countries were trying to resolve their differences” prior to the five indictments.¹⁷⁰ Moreover, the Chinese suggested that the cancelation of the working group “would be only the first step in its response to the Obama administration’s action.”¹⁷¹

The Chinese indictments were unfortunate, particularly given that the U.S.-China bilateral cybersecurity agreement, at one point, appeared to be an “alternative to domestic legislation.”¹⁷² Thus, it should have resulted in a solid foundation for the path to establishing customary international law on the subject. In the geopolitical context, impoverished states such as the Democratic People’s Republic of Korea (DPRK) have discovered that state-sponsored cyberattacks are revenue sources as well as a method to combat the September 2017 United Nations sanctions against the DPRK regime.¹⁷³ To further demonstrate how widespread state sponsored cyberattacks are, the Russian Federation used directed social media to attract hackers to

¹⁶⁸ *Cyberattacks Are Costly, and Things Could Get Worse: US Report*, SCIENCE X (Feb. 16, 2018), <https://phys.org/news/2018-02-cyberattacks-costly-worse.html>.

¹⁶⁹ Michael S. Schmidt & David E. Sanger, *5 in China Army Face U.S. Charges of Cyberattacks*, N.Y. TIMES (May 19, 2014), <https://www.nytimes.com/2014/05/20/us/us-to-charge-chinese-workers-with-cyberspying.html>.

¹⁷⁰ *Id.*

¹⁷¹ *Id.*

¹⁷² Anderson, *supra* note 6, at 1109.

¹⁷³ Cohen & Roth, *supra* note 64 and accompanying text; Andy Greenberg, *North Korea’s Sloppy, Chaotic Cyberattacks Also Make Perfect Sense*, WIRED (June 15, 2017, 2:08 PM), <https://www.wired.com/story/north-korea-cyberattacks>.

pursue the task of influencing the November 2016 U.S. presidential election.¹⁷⁴

Thus, the D.C. Circuit's reliance on dated precedent regarding the Circuit's entire tort doctrine means there is no noncommercial tort remedy for international cyberattacks with a U.S. target. The current judgment enforcement provisions of the FSIA also only further perpetuate the "likelihood of enforcing a judgment against elusive hackers in a foreign country [to] nil."¹⁷⁵

C. The United States Missed an Opportunity to Help Establish Customary International Law Regarding a Foreign State's Sovereign Immunity Within the Cybersecurity Sector

The D.C. Circuit had the opportunity to break away from the dated entire tort doctrine defined in *In re Sedco, Inc.*,¹⁷⁶ the first case that adopted the entire tort rule.¹⁷⁷ To put the entire tort ruling into perspective, when Congress enacted the FSIA in 1976,¹⁷⁸ the first Microsoft Windows software package would not ship for another nine years.¹⁷⁹

Paul Rosenzweig, a former senior DHS official and cyberwar expert, states "[w]e're entering an era of the democratization of destructive capability" and that "things that only governments could do are now being done by individuals."¹⁸⁰ This only helps to support the

¹⁷⁴ *A Survey of Nation State Sponsored Hackers*, DARKOWL, (Aug. 31, 2017), <https://www.darkowl.com/blog/2017/2/23/nation-state-sponsored-hackers>.

¹⁷⁵ Anderson, *supra* note 6, at 1089.

¹⁷⁶ *In re Sedco, Inc.*, 543 F. Supp. 561 (S.D. Tex. 1982), *vacated in part*, 610 F. Supp. 306 (S.D. Tex. 1984); *see* Anderson, *supra* note 6, at 1089.

¹⁷⁷ Gilmore, *supra* note 166, at 257 n.150 (citing JOEL BRENNER, GLASS HOUSES: PRIVACY, SECURITY, AND CYBER INSECURITY IN A TRANSPARENT WORLD 54 (2013)).

¹⁷⁸ 28 U.S.C. § 1330 (2018).

¹⁷⁹ Samuel Gibbs, *From Windows 1 to Windows 10: 29 Years of Windows Evolution*, GUARDIAN (Oct. 2, 2014, 10:30 AM), <https://www.theguardian.com/technology/2014/oct/02/from-windows-1-to-windows-10-29-years-of-windows-evolution>.

¹⁸⁰ Josh Meyer, *The Future of Terrorism According to VICE*, VICE (Jan. 14, 2015, 9:30 AM), https://www.vice.com/en_us/article/nnqpkg/the-future-of-terrorism-114.

argument that “liability for these (cyberattack) incidents should fall on the most culpable party: the perpetrator of the attack,” (i.e., the foreign state actor).¹⁸¹ In *Kidane*, the appellee’s brief shows that “[t]he FSIA’s requirement that the act of the foreign state must occur within the state asserting jurisdiction is also present in the national law on sovereign immunity in several other countries.”¹⁸² This is troubling because it means that not only is the United States unprepared to combat cyberattacks, but so are many other developed nations as well. For example:

Australian Foreign Sovereign Immunities Act 1985, section 13 (“A foreign State is not immune in a proceeding in so far as the proceeding concerns: (a) the death of, or personal injury to, a person; or (b) loss of or damage to tangible property; *caused by an act or omission done or omitted to be done in Australia.*”); U.K. State Immunity Act 1978, section 5 (“A State is not immune as respects proceedings in respect of - (a) death or personal injury; or (b) damage to or loss of tangible property, *caused by an act or omission in the United Kingdom.*”); Singapore State Immunity Act of 1979, section 7 (“A State is not immune as respects proceedings in respect of - (a) death or personal injury; or (b) damage to or loss of tangible property, *caused by an act or omission in Singapore*”).¹⁸³

The United States “dominates the world’s-worst [cybersecurity] rankings in two categories.”¹⁸⁴ The first category being cyberespionage attacks and the latter category being the percentage of web app hacks.¹⁸⁵ “In 2013, more than half (54%) of the world’s cyberespionage attacks took place in the” United States.¹⁸⁶ In addition, “66% of [web app attacks] take place in the [United States], far outstripping any other country.”¹⁸⁷ Thus, America must be among the

¹⁸¹ Anderson, *supra* note 6, at 1094.

¹⁸² Final Brief for Appellee, *supra* note 112, at 25.

¹⁸³ *Id.*

¹⁸⁴ Kevin Murnane, *Cyber Security: The World’s Best and Worst Presented with a Well-Designed Infographic*, FORBES (May 4, 2017, 3:06 AM), <https://www.forbes.com/sites/kevinmurnane/2017/05/04/cyber-security-the-worlds-best-and-worst-presented-with-a-well-designed-infographic/#7deb100e4416>.

¹⁸⁵ *Id.*

¹⁸⁶ *Id.*

¹⁸⁷ *Id.*

most involved in setting up effective policies and workable solutions to protect against cyberattacks and to provide effective laws for victims seeking relief.

In addition, the United States needs to make it a top priority to combat the exponential cyberattack growth made possible by foreign state actors (e.g., ransomware attacks rose two hundred and fifty percent in early 2017, with the United States being the hardest hit).¹⁸⁸ Other international tribunals, legal organizations such as the American Bar Association (ABA), and seasoned practicing attorneys have proposed solutions that would help combat the ever-increasing threat of state-sponsored cyberattacks.¹⁸⁹ Some of the solutions presented in Section IV of this Comment are among those that are necessary for the United States to protect itself from future attacks and to set a precedent for other nation states to follow.

III. PROPOSALS TO DISINCENTIVIZE STATE-SPONSORED CYBERSECURITY ATTACKS AND AFFORD RELIEF TO VICTIMS

Current law does not address the increasing number of cyberattacks on Americans, nor do the necessary funds or treaty protections exist to help mitigate the likelihood of successful attacks occurring. This section begins by presenting several key legislative proposals which Congress should enact to combat state-sponsored cyberattacks, followed by a discussion of treaty proposals and additional funding initiatives to better support DHS' CERT Big Bounty program. This section concludes by advocating for the United States to play a key role in establishing customary international law by entering into bilateral and multilateral treaties with other nation states to combat cyberattacks on a global scale.

¹⁸⁸ Anthony Cuthbertson, *Ransomware Attacks Rise 250 Percent in 2017, Hitting U.S. Hardest*, NEWSWEEK (May 23, 2017, 1:37 PM), <http://www.newsweek.com/ransomware-attacks-rise-250-2017-us-wannacry-614034>.

¹⁸⁹ Allison Grande, *ABA Approves Resolution to Encourage Cybersecurity Plans*, LAW360 (Aug. 12, 2014, 1:40 PM), <https://www.law360.com/articles/566485/aba-approves-resolution-to-encourage-cybersecurity-plans>.

A. Legislative Amendment Proposals

1. Congress Should Incorporate the Overall Control Standard Implemented by the ICT

A key recommendation is to adopt the ICT's Overall Control Standard¹⁹⁰ to the FSIA, which would allow U.S. courts to afford relief to cyberattack victims and hold nations accountable for state-sponsored cyberattacks.¹⁹¹ An overall control standard would hold a nation state liable for a cyberattack where the state has a "role in organization and coordinating, in addition to providing support for a group, [and the state] has sufficient overall control such that the group's acts are attributable to the [s]tate."¹⁹² As previously mentioned, this would be an effective tool for cyberattack plaintiffs because it "may be difficult even to know . . . who the attacker is," and collect on a judgment.¹⁹³ This new provision would be particularly helpful in going after a more sophisticated nation-state actor and its agents belonging to groups such as Hidden Lynx, a state-sponsored hacker-for-hire group.¹⁹⁴

2. Congress Should Implement a Narrowly-Tailored Cyberattack Exception

The second recommendation for holding states accountable for their clandestine cyber activities is to adopt the American Bar Association's (ABA) 2002 blackline for the FSIA's section 5 waivers of immunity.¹⁹⁵ In 2002, an ABA working group found that the FSIA's entire tort requirement was unduly restrictive and proposed replacing the tort location language of "in the United States" with "a substantial

¹⁹⁰ Shackelford & Andres, *supra* note 33, at 975.

¹⁹¹ *Id.* at 1016.

¹⁹² *Id.* at 986.

¹⁹³ *Id.* at 985 (quoting COMM. ON OFFENSIVE INFO. WARFARE, NAT'L RESEARCH COUNCIL, TECHNOLOGY, POLICY, LAW AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 275 (William Owens et al. eds., 2010)).

¹⁹⁴ Zetter, *supra* note 153 and accompanying text.

¹⁹⁵ Working Group of the American Bar Association, *Reforming the Foreign Sovereign Immunities Act*, 40 COLUM. J. TRANSNAT'L L. 489, 601 (2002).

portion of which act or omission occurs in the United States.”¹⁹⁶ An additional amendment of the FSIA suggested by Alexis Haller, “a trial and appellate attorney with over thirteen years of FSIA litigation experience,”¹⁹⁷ suggests the following changes, which would give the current FSIA collection of judgments provision “teeth.”¹⁹⁸ Haller’s proposed wording is as follows: “[Any person or entity obtaining a judgment shall have] the ability to collect on judgments against [a] foreign state[] from the state’s instrumentalities and agencies, even if such entities were not involved in the cyberattack at issue.”¹⁹⁹ Nearly the entire statutory language of the noncommercial tort exception to the FSIA is set out below in order to better explain some of the numerous amendments required for an effective cyberattack exception:

- (5) [For a noncommercial tort] in which money damages are sought against a foreign state for personal injury or death, or damage to or loss of property, occurring *in the United States* and caused by the tortious act or omission of that foreign state or of any official or employee of that foreign state while acting within the scope of his office or employment; except this paragraph shall not apply to—
- (A) any claim based upon the exercise or performance or the failure to exercise or perform a *discretionary* function regardless of whether the discretion be abused, or
- (B) any claim arising out of malicious prosecution, abuse of process, libel, slander, *misrepresentation*, *deceit*, or interference with contract rights.²⁰⁰

For an effective cyberattack exception to the FSIA, there must be additional amendments to eliminate the discretionary, misrepresentation, and deceit defenses to jurisdiction shown in the statutory language above.²⁰¹ No specific wording is proposed for such amendments; however, one can easily see how these defenses might be

¹⁹⁶ *Id.*

¹⁹⁷ *The D.C. Circuit’s Recent Decision Reinforces the Urgent Need for a Cyberattack Exception to the FSIA*, *supra* note 36 and accompanying text.

¹⁹⁸ *Id.*

¹⁹⁹ *Id.*

²⁰⁰ 28 U.S.C. § 1605(a)(5) (2018) (emphasis added).

²⁰¹ *See The Cyberattack Exception to the Foreign Sovereign Immunities Act*, *supra* note 36.

raised by a defendant unless they are eliminated for cyberattacks.²⁰² The holding in *Kidane* did not address such defenses since the entire tort defense was dispositive.²⁰³

B. Other Amendment Proposals

1. Congress Should Allocate Additional Funding for the Development of Cryptocurrency Detection Technologies and Implementation of CERT Big Bounty Programs

U.S. government security agencies should follow private sector best practices (e.g., akin to those of Tesla and Netscape) by hosting additional big bounty programs. The goals of these programs are to make it more expensive and time consuming for foreign states to conduct cyberattacks, to make it less profitable by paying hackers to identify ongoing cyber concerns, and to weed out potential attacks before they occur.²⁰⁴ The United States should ensure that DHS has sufficient funding to keep CERTs equipped to efficiently and effectively identify and resolve threats to America's cyber infrastructure.²⁰⁵ Congress should provide more funding to detect and trace clandestine bitcoin transactions. Admittedly, this would be an extremely challenging task²⁰⁶ and would very likely have multiple legal hurdles to clear. However, nation [s]tates will continue to turn to decentralized and largely unregulated cryptocurrencies to cover their tracks following cyberattacks.²⁰⁷

²⁰² *Id.*

²⁰³ See *Kidane II*, 851 F.3d 7, 7–12 (D.C. Cir. 2017), *reh'g denied*, 2017 U.S. App. LEXIS 10084 (D.C. Cir. June 6, 2017).

²⁰⁴ *Id.*

²⁰⁵ OFFICE OF THE INSPECTOR GEN., *supra* note 43, at 3.

²⁰⁶ Chellel, *supra* note 46 and accompanying text.

²⁰⁷ *Id.*

2. The United States Should Enter into More Bilateral Cyber Agreements with Receptive Nation States to Help Establish Customary International Law for Cyberattacks

While China may be outmaneuvering bilateral cybersecurity treaties,²⁰⁸ the United States should still actively seek other potential nations that are more receptive to the idea of joint cooperation to help increase confidence in bilateral cyber agreements in the future. Destructive hacking is also occurring in smaller nation states.²⁰⁹ Smaller groups and nation states “could also have an outsized impact online relative to their resources.”²¹⁰ Modeling such a cyber agreement with a more receptive state actor (e.g., a smaller nation state with less leverage than the People’s Republic of China or the Russian Federation) would likely be beneficial as “today many countries large and small invest in cyber warfare.”²¹¹ However, if nation states work together on issues surrounding cybersecurity policy, these practices “could, in time, crystallize into customary international law with enough state practice.”²¹²

The joint U.S.-China agreement indicated that the United States and China would not “conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors.”²¹³ Although the phrase “conduct or knowingly support” is not defined in the agreement, “the agreement indicates that China acquiesced to American pressure to desist its sponsorship of commercial

²⁰⁸ Austin, *supra* note 38 and accompanying text.

²⁰⁹ Simon Parker, *Understanding the Physical Damage of Cyber Attacks*, INFOSECURITY MAG. (Oct. 3, 2017), <https://www.infosecurity-magazine.com/opinions/physical-damage-cyber-attacks>.

²¹⁰ Peter Suci, *Why Cyber Warfare is so Attractive to Small Nations*, FORTUNE (Dec. 21, 2014), <http://fortune.com/2014/12/21/why-cyber-warfare-is-so-attractive-to-small-nations>.

²¹¹ *Id.*

²¹² Scott J. Shackelford et al., *Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors*, 17 CHI. J. INT’L L. 1, 24 (2016).

²¹³ Anderson, *supra* note 6, at 1110.

espionage.”²¹⁴ The above treaty language serves as a beneficial template for nations engaging in bilateral and multilateral treaty negotiations, which, in turn, will contribute to establishing customary international law on cybersecurity and cyber warfare.

IV. CONCLUSION

The current version of the FSIA, originally enacted in 1976, was drafted prior to exponential advancements in technology and is out of date. U.S. courts should be more judicially active in addressing the increasingly complex and sophisticated foreign state-sponsored cybersecurity attacks to better afford protection to their victims.

State-sponsored cyberattacks are extremely profitable and they are only becoming harder to trace, with foreign state hackers turning to cryptocurrencies as their newest economic advancement. Furthermore, when nation-state hackers are tracked down, their foreign state-sponsors are often uncooperative in assisting with a U.S. indictment (e.g., the Chinese military indictment). Thus, there is a compelling need for mechanisms by which to hold foreign state hackers liable for money damages as compensation to the victims and as a deterrent. The United States is one of the world's top three cyberattack targets. To combat what is almost sure to be an ever-increasing threat, and to hold foreign state hackers responsible, Congress should promptly amend the FSIA. Congress should adopt the ABA's 2002 blackline of the FSIA and also provide additional funding for CERT and approve bounty rewards for rooting out future cyberattacks. Further, the United States should negotiate more bilateral agreements to help curb state-sponsored cyberattacks.

Ultimately, cybersecurity will always be a substantial threat in modern everyday life as we know it at the time of this writing. However, the United States can and should make a significant impact by reducing available profits, making it harder to hide money in cryptocurrency form, and holding foreign nations accountable for cyberattacks they carry out or sponsor.

²¹⁴ *Id.*