Journal of Business & Technology Law

Volume 19 | Issue 1 Article 7

Hit Em' Where it Hurts: Private Suits as a Necessary Check on State-Sponsored Cyber Attacks

Katie Mandarano

HIT EM' WHERE IT HURTS: PRIVATE SUIT AS A NECESSARY CHECK ON STATE-SPONSORED CYBERATTACKS

KATIE MANDARANO*

TABLE OF CONTENTS

INTRODUCTION

In 2022, the United States lost over $10.2 billion to cybercrime, surpassing the previous year's losses by over $3 billion.[1] U.S. losses to cybercrime are only predicted to worsen in the coming years, and experts predict global losses will reach $10.5 trillion by the year 2025.[2] Moreover, the U.S. government (the "Government") has noted that foreign governments and third parties sponsored by foreign governments increasingly make up the cyber-threat landscape,[3] resulting in more sophisticated cyberattacks and increased difficulties with attribution.[4] State-sponsored cyberattacks have devastating economic consequences for many American businesses for the following reasons. First, hacked businesses face the economic burden of the breach, which includes everything from

* © J.D. Candidate 2024, University of Maryland Francis King Carey School of Law. I would like to thank Professor Yelin and the editors of the Journal and Business & Technology Law for their invaluable feedback and ideas.

1. FED. BUREAU OF INVESTIGATION, INTERNET CRIME REPORT 2022 3 (2022).

2. *See, e.g.*, Chuck Brooks, *Alarming Cyber Statistics for Mid-Year 2022 That You Need to Know*, FORBES (June 3, 2022, 3:57 PM), https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=27e12e4f7864 (holding that every year the costs to industry and government get worse); Steve Morgan, *Cybercrime to Cost the World $10.5 Trillion Annually by 2025*, CYBERSECURITY VENTURES (Nov. 13, 2020), https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/ (estimating that global cybercrime costs will grow by fifteen percent per year over the next five years).

3. CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY ET AL., RUSSIAN STATE-SPONSORED CYBER ACTORS TARGET CLEARED DEFENSE CONTRACTOR NETWORKS TO OBTAIN SENSITIVE U.S. DEFENSE INFORMATION TECHNOLOGY 1-2 (Feb. 16, 2022) [hereinafter CISA REPORT].

4. Alan Raul et al., *Nation-State-Sponsored Attacks: Not Your Grandfather's Cyber Attacks*, NEW YORK L.J. (May 6, 2022, 2:40 PM), https://www.law.com/newyorklawjournal/2022/05/06/%C2%AD%C2%AD%C2%AD%C2%AD%C2%AD%C2%AD%C2%AD%C2%AD%C2%AD%C2%AD%C2%AD%C2%ADnation-state-sponsored-attacks-not-your-grandfathers-cyber-attacks/?slreturn=20221114154711.

upgrading their cybersecurity systems to hiring cyber specialists.[5] Secondly, on top of the cost of the breach itself, employees or customers can sue businesses for potential negligence in the cyberattack.[6] Finally, the Government has started to fine businesses with poor cybersecurity practices, as well as prohibit ransomware payments,[7] which forces businesses to pay fines as well as pay for any data lost through ransomware attacks.[8]

As this problem grows, American businesses and citizens have largely been left to the mercy of the Government to provide attribution and consequence to these foreign-state actors.[9] The Government's cybersecurity strategy currently consists of a mixed-bag of criminal indictments, economic sanctions, and diplomatic action.[10] But these strategies have proven largely ineffective at providing victims of state-sponsored

5. *See* Marc Wilczek, *Cyberattack Costs for US Businesses up by 80%*, DARKREADING (Sept. 19, 2022), https://www.darkreading.com/attacks-breaches/cyberattack-costs-for-us-businesses-up-by-80- (showing that 40% of cyberattack victims in the U.S. incur costs of $25,000 or higher).

6. *See* In re Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F.Supp.2d 942, 953 (S.D. Cal. 2014) (hearing a class action law negligence lawsuit against Sony for its role in a data breach); Nate Raymond, *Sony to pay up to $8 million in 'Interview' hacking lawsuit*, REUTERS (Oct. 20, 2015, 2:35 PM), https://www.reuters.com/article/us-sony-cyberattack-lawsuit/sony-to-pay-up-to-8-million-in-interview-hacking-lawsuit-idUSKCN0SE2JI20151020 (reporting that Sony agreed to pay up to $8 million to resolve the lawsuit by its employees).

7. *See* Press Release, *SEC Announces Three Actions Charging Deficient Cybersecurity Procedures*, U.S. SECURITIES AND EXCHANGE COMMISSION, (Aug. 30, 2021), https://www.sec.gov/news/press-release/2021-169 (announcing SEC sanctions of eight firms for failures in their cybersecurity policies and procedures that resulted in data breaches); Press Release, *Treasury Continues to Counter Ransomware as Part of Whole-of-Government Effort: Sanctions Ransomware Operators and Virtual Currency Exchange*, U.S. DEP'T OF THE TREASURY (Nov. 8, 2021), https://home.treasury.gov/news/press-releases/jy0471 (announcing the Treasury's designation of certain ransomware operators, meaning U.S. persons are prohibited from engaging in transactions with them).

8. *See* SecureWorld News Team, *Baltimore, $18 Million Later: "This Is Why We Didn't Pay the Ransom"*, SECUREWORLD (Jun 12, 2019, 7:30 AM), https://www.secureworld.io/industry-news/baltimore-ransomware-attack-2019 (showing that the City of Baltimore paid $18 million in remediation, new hardware, and lost or deferred revenue because it refused to pay the initial $80,000 ransomware payment).

9. *See* Mark Montgomery & Erica Borghard, *Cyber Threats and Vulnerabilities to Conventional and Strategic Deterrence*, NAT'L DEF. UNIV. 79, 79 (July 1, 2021) (arguing that the U.S. has failed to create sufficient costs for adversaries engaged in cyberattacks); Paige C. Anderson, *Cyber Attack Exception to the Foreign Sovereign Immunities Act*, 102 CORNELL L. REV. 1087, 1089 (2017) (showing that when business and consumers are the victims of state-sponsored cyberattacks they often do not pursue recourse against the attackers themselves).

10. *See* Anderson *supra* note 9, at 1108-09 (showing that the U.S. government uses criminal indictments and bilateral cybersecurity agreements to address state-sponsored cyberattacks); CONG. RSCH. SERV., R47011, CYBERSECURITY: DETERRENCE POLICY 10 (2022) (noting that economic sanctions are an important tool for the U.S. government in addressing cyberattacks).

cyberattacks with adequate redress, and further, they have been shown to be minimally effective at deterring these types of cyberattacks.[11]

With the Government's strategy for state-sponsored cyberattacks lacking, multiple legal commentators have turned to private suits as a potential avenue for redress.[12] But private suits for state-sponsored cyberattacks pose challenges, as foreign governments have absolute immunity in U.S. courts pursuant to the Foreign Sovereign Immunities Act ("FSIA") unless an exception applies.[13] The existing FSIA exceptions with the potential to provide redress for state-sponsored cyberattacks include the commercial exception,[14] the noncommercial tortious exception,[15] and the terrorism exception.[16] As currently written, these exceptions are largely insufficient avenues for private parties who are victims of state-sponsored cyberattacks because they entail specific doctrinal hurdles, such as the "entire tort" doctrine, rendering them largely inapplicable to the cyber world.[17]

This Comment argues that Congress should create a cyber-specific exception to FSIA to better compensate victims of state-sponsored cyberattacks and hold foreign governments responsible for the role they play in these cyberattacks. Section I shows how the Government's current mechanisms to deter and hold foreign states accountable for their roles in cyberattacks against U.S. persons are inadequate.[18] Section II describes the legal landscape of sovereign immunity and the development of FISA.[19]

11. *See* Matthew A. Powell, *A Call to Congress: The Urgent Need for Cyberattack Amendments to the Foreign Sovereign Immunities Act*, 7 J.L. & CYBER WARFARE 117, 143 (2018) (arguing that current U.S. government protections do not help mitigate the likelihood of cyberattacks).

12. *See, e.g.*, Alexis Haller, *The Cyberattack Exception to the Foreign Sovereign Immunities Act: A Proposal to Strip Sovereign Immunity When Foreign States Conduct Cyberattacks Against Individuals and Entities in the United States*, FSIA LAW (Feb. 19, 2017), https://fsialaw.com/author/aihaller/ (arguing for a cyberattack exception to FSIA); Adam L. Silow, *Bubbles over Barriers: Amending the Foreign Sovereign Immunities Act for Cyber Accountability*, NAT'L SEC. L. & POL'Y 659, 660 (2022) (arguing for a specific cyber amendment to FSIA).

13. Foreign Sovereign Immunities Act, 28 U.S.C. §§ 1602-1611 (1976).

14. 28 U.S.C. § 1605(a)(2).

15. 28 U.S.C. § 1605(a)(5).

16. 28 U.S.C. § 1605(B).

17. *See, e.g.*, Powell, *supra* note 11, at 142-43 (arguing that current law, including the FSIA exceptions, do not address the increasing number of cyberattacks); Benjamin Kurland, *Sovereign Immunity in Cyberspace: Towards Defining a Cyber-Intrusion Exception to the Foreign Sovereign Immunities Act*, 10 J. NATL. SEC. L. & POLICY 225, 262 (2019) (arguing that under the current FSIA exceptions, a new exception would need to explicitly address cyber conduct perpetrated by a foreign government, regardless of where the conduct originated).

18. *See infra* Section I.

19. *See infra* Section II.

Section III examines the current FSIA exceptions and analyzes the potential problems with bringing a cyberattack claim under each exception.[20] Section IV advocates that a cyber-specific exception to FSIA is both the best way to provide relief to Americans and to deter foreign state actors.[21] Specifically, this Comment argues that proposed legislation, the Homeland and Cyber Threat Act ("HACT"),[22] can be further amended to include a statute of limitation of five years, a lower level of proof for attribution, the ability for U.S. courts to assign punitive damages and attach foreign-owned property as compensation, and a "cyber-intruder" executive designation.[23] Section V addresses potential criticisms of such an amendment, which include foreign diplomatic concerns, the feasibility of such a bill, and reciprocity concerns of such a bill.[24]

I. THE INADEQUACY OF CURRENT SOLUTIONS FOR STATE-SPONSORED CYBERATTACKS

The Government primarily uses criminal indictments, economic sanctions, and diplomatic action to deter cyberattacks and hold foreign states accountable for their roles in cyberattacks. This section will examine how each of these strategies inadequately serves victims of state-sponsored cyberattacks.

A. Criminal Indictments

Criminal indictments are one of the tools the Government currently uses to address state-sponsored cyberattacks. For example, in 2014 the Government indicted five members of the Chinese military under the Computer Fraud and Abuse Act ("CFAA")[25] for their alleged hacking of various U.S. companies.[26] At first glance, this strategy seemed promising, as the number of cyberattacks attributable to the Chinese military significantly dropped following the Government's indictment.[27] But, as detailed below,

20. *See infra* Section III.

21. *See infra* Section IV.

22. H.R. 1607, 117th Cong. (2021-2022).

23. *See infra* Section IV.

24. *See infra* Section V.

25. Computer Fraud and Abuse Act, 18 U.S.C. § 1030.

26. *U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage,* OFFICE OF PUB. AFF., U.S. DEP'T OF JUST. (May 19, 2014), https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

27. Ellen Nakashima, *Following U.S. Indictments, China Shifts Commercial Hacking Away from Military to Civilian Agency*, WASH. POST (Nov. 30, 2015),

there are many shortcomings that make criminal indictments inadequate for most victims of state-sponsored cyberattacks.[28]

First, the perpetrators of state-sponsored cyberattacks are unlikely to ever face prosecution because they are located abroad and any alleged foreign government would not extradite the perpetrators, as the perpetrators are foreign states themselves or third-parties sponsored by the foreign states.[29] Secondly, since foreign governments perpetuate some of the most sophisticated cyberattacks, attribution is difficult.[30] And if attribution is wrong, the Government runs the risk of disrupting foreign relations.[31] Thus, the Government has been hesitant to publicly attribute and indict perpetrators of these cyberattacks even when it is fairly certain the perpetrators were acting on behalf of a foreign government.[32] Further, criminal indictments are expensive and time consuming, so they are saved for exceptional cases, like when the Government wants to send a political message.[33] Finally, although criminal indictments may lead to fines on foreign states, those payments go directly to the Government, leaving the actual victims of these cyberattacks with no monetary relief.[34] An example of this trend was seen in the 2014 Sony Picture Entertainment hacks (the "Sony hacks"), where the Government indicted the North Korean government actors responsible,[35] but Sony was left with the full

https://www.washingtonpost.com/world/national-security/following-us-indictments-chinese-military-scaled-back-hacks-on-american-industry/2015/11/30/fcdb097a-9450-11e5-b5e4-279b4501e8a6_story.html.

28. *See, e.g.*, Scott A. Gilmore, *Suing the Surveillance States: The (Cyber) Tort Exception to the Foreign Sovereign Immunities Act*, 46 COLUM. HUM. RIGHTS L. REV. 227, 284 (2015) (finding flaws with the practicality of criminal indictments as a solution to state-sponsored cyberattacks); Anderson, *supra* note 9, at 1111 (finding problems with criminal indictments as a solution for victims of state-sponsored cyberattacks).

29. Gilmore, *supra* note 28, at 284.

30. *See id.* at 229-30 (noting the difficulty of attribution for cyberattacks and how responding with economic sanctions can easily escalate foreign relations).

31. *Id.* at 283-84.

32. Anderson, *supra* note 9, at 1104, 1111.

33. *See* Powell, *supra* note 11, at 124-25 (arguing that criminal indictments for state-sponsored cyberattacks are not usually worth the risk because they place foreign relations on shaky grounds and are often costly and time consuming).

34. Anderson, *supra* note 9, at 1111.

35. *See generally*, *North Korea Regime-Backed Programmer Charged with Conspiracy to Conduct Multiple Cyber Attacks and Intrusions*, OFFICE OF PUB. AFF., U.S. DEP'T OF JUST. (Sept. 6, 2018), https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and.

cost of the hack.[36] Accordingly, even if the Government decides to criminally indict these bad actors–which is unlikely–American businesses and individuals are not compensated for their injuries.[37]

B. Economic Sanctions

Economic sanctions are also used by the Government to address state-sponsored cyberattacks. The Government first started using economic sanctions as a part of its cybersecurity policy in 2012 as a result of Iran's role in various cyberattacks aimed at the U.S.[38] Though the Government has slowly increased its use of sanctions since 2012, illicit state-sponsored cybercriminals continue to perpetuate attacks at high rates.[39] Like criminal indictments, economic sanctions serve as a relatively weak deterrence method because of the logistical difficulty of attributing cyberattacks to specific actors and the high level of certainty required when accusing a foreign government of such an attack.[40] Further, a lot of these state-sponsored cybercriminals are located in jurisdictions with poor sanctions compliance, such as Russia or China, so even if the Government imposes a sanction, the perpetrators are unlikely to ever feel the intended consequences.[41] Moreover, like criminal indictments, economic sanctions leave individuals and companies without redress because economic sanctions typically take the form of trade embargoes or the Government blocking the foreign state's assets.[42]

Even worse than with criminal indictments, economic sanctions can serve as a motivation for nation-states to conduct cyberattacks. For example, North Korea continuously compensates for severe economic

36. *See Sony pays up to $8m over employees' hacked data*, BBC (Oct. 21, 2015), https://www.bbc.com/news/business-34589710 (showing that Sony agreed to pay $8 million for the data breach without any viable avenue to seek compensation for themselves).

37. Anderson, *supra* note 9, at 1111.

38. Jason Bartlett & Meghan Ophel, *Sanctions by the Numbers: Spotlight on Cyber Sanctions*, CNAS (May 4, 2021), https://www.cnas.org/publications/reports/sanctions-by-the-numbers-cyber.

39. *See id.* (showing that use of economic sanctions has steadily been increasing since 2012); Morgan, *supra* note 2 (showing that state-sponsored cyberattacks have continued to grow each year).

40. *See* Gilmore, *supra* note 28, at 229, 283-84 (noting the difficulty of attribution for cyberattacks and how responding with economic sanctions can easily escalate foreign relations).

41. Bartlett & Ophel, *supra* note 38.

42. Anderson, *supra* note 9, at 1089; *Basic Information on OFAC and Sanctions*, OFFICE OF FOREIGN ASSETS CONTROL U.S. DEP'T OF THE TREASURY (last updated June 14, 2023), https://ofac.treasury.gov/faqs/topic/1501#:~:text=OFAC%20administers%20a%20number%20of,target%20specific%20individuals%20and%20entities.

sanctions from the U.S. and the United Nations with funds it obtains through illicit cyber activity.[43] This behavior is not limited to North Korea: in March 2022, the White House issued a statement warning the private sector to prepare for potential retaliatory Russian cyberattacks in response to U.S.-imposed economic sanctions for Russia's actions in Ukraine.[44] Accordingly, economic sanctions face serious problems as an effective cybersecurity strategy: they provide no relief to victims, they are used sparingly and are often ignored, and they can instead serve as a motivation for state-sponsored cyberattacks.

C. Diplomatic Action

A third strategy is for the Government to enter into bilateral agreements that prohibit cyber-attacks between signatory countries. Like previously mentioned strategies, treaties often contain no provisions about compensation for victims, leaving victims of state-sponsored cyberattacks without redress.[45] Further, these types of agreements typically only include the intent of the signatories not to conduct cyberattacks against one another, with no real means of enforcement.[46] As such, many commentators typically view these treaties more as "an expression of hope" rather than a limitation on conduct.[47] Potentially the biggest hurdle with bilateral cybersecurity agreements is that the nation-states that perpetuate the most cyberattacks against the U.S. have fundamentally different values than the U.S.[48] For example, the U.S. and its allies promote a multistakeholder vision of Internet governance, where the government, the private sector, civil society, academia, and individuals all play a role in governance.[49] On the other side, states like China and Russia argue for a multilateral model where sovereigns exclusively regulate the content of the Internet and monitor and suppress any content they view as a security threat.[50] This

43. Jason Bartlett, *Exposing the Financial Footprints of North Korea's Hackers*, CNAS (Nov. 18, 2020), https://www.cnas.org/publications/reports/exposing-the-financial-footprints-of-north-koreas-hackers (showing that North Korean cyber actors have circumvented sanctions by stealing an estimated $2 billion from foreign banks, financial institutions, and cryptocurrency exchanges).

44. Presidential Statement on Cybersecurity, WEEKLY COMP. PRES. DOC. 1 (Mar. 21, 2022).

45. Anderson, *supra* note 9, at 1111.

46. *Id.*

47. Jack Goldsmith, *Don't Get Too Excited About a US-China Arms Control Agreement for Cyber*, LAWFARE (Sept. 21, 2015, 8:25 AM), https://www.lawfareblog.com/dont-get-too-excited-about-us-china-arms-control-agreement-cyber.

48. *See* Kristen E. Eichensehr, *The Cyber-Law of Nations*, 103 GEO. L.J. 317, 346 (2015) (showing that Russia and China endorse a different internet model than the U.S. and its allies).

49. Eichensehr, *supra* note 48, at 330.

50. *Id.* at 331.

clash of values has made it increasingly difficult for nation-states to agree on how the law should apply to cyberspace.[51] Accordingly, bilateral cybersecurity agreements are unlikely to be implemented on a widespread basis and there is no real guarantee that nation-states will abide by such agreements.

II. PRIVATE SUIT AS A POTENTIAL SOLUTION TO STATE-SPONSORED CYBERATTACKS

Private suits plays an important role in society first because they force wrongdoers to account for any damages they inflicted or injuries they have caused through compensation, and secondly because it expresses society's values and norms about what behavior it considers wrong.[52] Therefore, as technology has developed and societal expectations have shifted, nation states all over the world have created new cyber-specific private rights of action,[53] so that private suits can continue to play their "traditional social control role" in the digital age.[54] Since cyber-intrusions by state-actors remain a prevalent threat, many commentors and scholars have looked towards private suits as a potential avenue to redress injuries these cyberattacks cause and to reflect the international norm that state-sponsored cyberattacks should not be tolerated by the international community.[55] In the U.S., for victims of state-sponsored cyberattacks to bring private suit, their claim must fall under one of the FSIA exceptions, or the foreign government accused will enjoy sovereign immunity in all U.S. courts.[56] First, this section will lay out the doctrine of absolute sovereignty, discussing how the concept has shrunk over the years into a

51. *Id.* at 357.

52. Michael L. Rustad, *Smoke Signals from Private Attorneys General in Mega Social Policy Cases*, 51 DEPAUL L. REV. 511, 527 (2001); Elizabeth D. De Armond, *A Dearth of Remedies*, 113 PENN ST. L. REV. 1, 37 (2008).

53. *See, e.g.*, Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. K 119/1 (providing a range of private rights of action against controllers and processors for breaches of the data protection law); Cal. Civ. Code § 1798.150 (2020) (creating a private right of action related to certain data breaches when a business fails to implement certain security procedures).

54. De Armond, *supra* note 52, at 39.

55. *See, e.g.*, Sam Kleiner & Ambassador (ret.) Lee Wolosky, *Time for a Cyber-Attack Exception to the Foreign Sovereign Immunities Act*, JUST SECURITY (Aug. 14, 2019), https://www.justsecurity.org/65809/time-for-a-cyber-attack-exception-to-the-foreign-sovereign-immunities-act/; Stephen J. Schultze, *Hacking Immunity: Computer Attacks on the United States Territory by Foreign Sovereigns*, 53 AM. CRIM. L. REV. 861, 881 (2016).

56. Schultze, *supra* note 55, at 866.

more restrictive approach and how this restrictive approach was codified in FSIA.[57] Finally, this section details what FSIA looks like today and the various exceptions relevant to state-sponsored cyberattacks.[58]

A. Absolute Sovereign Immunity

The concept of foreign sovereign immunity started in the Middle Ages when kings were considered to be on equal standing with each other, and thus "one monarch could not be subject to the jurisdiction of another sovereign monarch."[59] The U.S. embraced the doctrine of absolute immunity as early as 1811, as indicated in the Supreme Court's decision in *Schooner Exchange v. McFaddon*.[60] In *Schooner Exchange*, American ship owners brought suit against France for allegedly directing persons to forcibly take an American ship while it was en route to Spain.[61] The Court ruled that U.S. courts had no jurisdiction over the matter, as France enjoyed absolute immunity from private suit.[62] The U.S. continued to follow this theory until the mid-twentieth century, providing foreign governments with broad immunity in U.S. courts.[63]

B. Restrictive Approach

During the mid-twentieth century, the U.S. and the rest of the world generally began to transition away from the absolute theory of foreign sovereign immunity and towards a more restrictive approach.[64] U.S. courts originally sought recommendations from the U.S. Department of State ("State Department") on how to apply restrictive foreign sovereign immunity.[65] When the State Department provided no official recommendation, U.S. courts applied past State Department practice, leading to

57. *See infra* Section II.A-B.

58. *See infra* Section II.C.

59. Samantha N. Sergent, *Extinguishing the Firewall: Addressing the Jurisdictional Challenges to Bringing Cyber Tort Suits Against Foreign Sovereigns*, 72 VAND. L. REV. 391, 397 (2019).

60. Schooner Exchange v. McFaddon, 11 U.S. 116, 137, 145-46 (1812) (holding that it was "a principle of public law, that national ships of war, entering the port of a friendly power open for their reception, are to be considered as exempted by the consent of that power from its jurisdiction.").

61. *Id.* at 117.

62. *Id.* at 147.

63. Ilana Arnowitz Drescher, *Seeking Justice for America's Forgotten Victims: Reforming Sovereign Immunities Act Terrorism Exception*, 15 N.Y.U. J. LEGIS. & PUB. POL'Y 791, 798 (2012).

64. Sergent, *supra* note 59, at 397-98.

65. Powell, *supra* note 11, at 128.

inconsistent results throughout U.S. jurisdictions.[66] Then, in 1952, the State Department's legal advisor sent a letter to the Attorney General stating that absolute immunity was no longer appropriate and that the State Department would officially follow the restrictive theory going forward.[67] This letter, known as the "Tate Letter," specifically recommended that the U.S. grant immunity to foreign states when they were acting in their official capacity as a state, but not "for the state's private or commercial acts."[68] After the State Department provided its official recommendation, it faced considerable pressure from foreign governments to grant them sovereign immunity in pending private suits, threatening that foreign relations would break down if the State Department did not.[69]

In 1976 the U.S. passed FSIA, codifying the restrictive approach.[70] Congress ultimately passed FSIA because it wanted to promote consistency in litigation brought against foreign states in U.S. courts[71] and to shift decisions about sovereign immunity away from the State Department and onto the politically isolated judicial branch.[72]

C. FSIA Today

FSIA broadly grants foreign sovereign immunity to foreign states and their instrumentalities from the jurisdiction of U.S. courts unless a statutory exception applies.[73] The current exceptions to FSIA include (1) waiver of immunity by the foreign state, (2) noncommercial tortious activity, (3) commercial activity, and (4) expropriations in violation of international law.[74] Additionally in 1996, in response to public outrage over Libya's role in the bombing of Pan Am Flight 103, Congress passed the "Anti-Terrorism and Effective Death Penalty Act" ("AEDPA"), which added a private right of action to FSIA for victims of terrorist attacks.[75]

66. *Id.* at 128-29.

67. Drescher, *supra* note 63, at 798.

68. *Id.*

69. Powell, *supra* note 11, at 130.

70. *See generally*, 28 U.S.C. §§ 1602-1611 (1976).

71. John J. Martin, *Hacks Dangerous to Human Life: Using JASTA to Overcome Foreign Sovereign Immunity State-Sponsored Cyberattack Cases*, 121 COLUM. L. REV. 119, 125 (2021).

72. Powell, *supra* note 11, at 130.

73. 28 U.S.C. § 1604.

74. 28 U.S.C. § 1605.

75. Drescher, *supra* note 63, at 800-801.

The AEDPA[76] was amended further in 2016 when Congress passed the Justice Against Sponsors of Terrorism Act ("JASTA")[77] in response to Saudi Arabia's role in the September, 11 terrorist attacks.[78] JASTA broadened the scope of the original terrorism exception, adding another private right of action for tortious acts of "international terrorism."[79] Under FSIA, if the actions of a foreign state fall within one of these specific exceptions, FSIA confers both subject matter and personal jurisdiction over the foreign state and U.S. citizens can bring private suit against the foreign state or its instrumentalities.[80]

III. THE INADEQUACY OF THE CURRENT FSIA EXCEPTIONS

Under current law, whether an alleged state-sponsor of a cyberattack is subject to liability in U.S. courts depends on whether the alleged state action falls within one of FSIA's exceptions. Bringing a claim under the first exception to FSIA would be incredibly rare as foreign governments are unlikely to waive their immunity in suits against them for committing or sponsoring a cyberattack.[81] Moreover, the fourth exception to FSIA – expropriations of property–is also likely to be a long shot in the cyber context because it is unclear whether a government can physically seize electronic property under the takings law.[82] As such, this Comment will analyze the remaining three exceptions (the commercial activity exception, the noncommercial tortious exception, and the terrorism exception) and assess the likelihood of success for plaintiffs bringing suits against foreign governments for their role in cyberattacks under each.[83] The analysis

76. Antiterrorism and Effective Death Penalty Act of 1996, Pub. L. No. 104-132 § 221, 110 Stat. 1214, 1241 (codified at 28 U.S.C. § 1605(a)(7) (1996)).

77. Justice Against Sponsors of Terrorism Act, Pub. L. No. 114-222, 130 Stat. 852 (2016) (codified as amendment at 28 U.S.C. § 1605B).

78. Glenn M. Spitler III, *Foreign State-Sponsored Terrorism A History and Legislative Analysis*, SOUTH CAROLINA LAWYER (2017), http://www.onlineissues.wherewhenhow.com/publication/?i=422606&article_id=2829727&view=articleBrowser.

79. *Id.*

80. *See generally*, 28 U.S.C. § 1605.

81. *See, e.g.*, Anderson, *supra* note 9, at 1091 (assuming foreign governments will not waive their immunity in suits against them); Martin, *supra* note 71, at 125-26 (showing that the waiver exception to sovereign immunity rarely occurs as courts construe the waiver narrowly in favor of the foreign state).

82. *See, e.g.*, Sergent, *supra* note 59, at 401 (finding it unclear whether electronic property can be taken); Anderson, *supra* note 9, at 1090-91 (acknowledging the lack of scholarship on expropriations in the cyber context).

83. *See infra* Section III.

shows that the likelihood of success for victims of state-sponsored cyberattacks is doubtful under each exception.[84]

A. The Commercial Activity Exception

The commercial activity exception requires a foreign state's action to be "commercial in nature" in order for the act to fall outside the state's immunity.[85] U.S. courts interpret "commercial in nature" to mean conduct that is the type in which private parties usually engage for "trade and traffic or commerce" purposes.[86] The Supreme Court applied this test in *Republic of Argentina v. Weltover, Inc.*,[87] where it held Argentina could be held liable under FSIA for refinancing debt through bond issuances because it had participated in the bond market just like a private player would.[88]

As a result, the commercial activity exception creates problems for plaintiffs seeking redress for state-sponsored cyberattacks intended to steal and leak private information or damage the functionality of computer systems, as they would probably not be considered acts in furtherance of trade or commerce.[89] Commentator Paige Anderson notes that claimants could be successful if U.S. courts interpreted the term "cyberattack" more liberally.[90] Anderson argues that under a more liberal definition of cyberattack, such as merely gaining unauthorized access to a U.S. computer system, foreign governments would be acting analogous to private actors.[91] But courts are unlikely to adopt this interpretation because hacking has so many different objectives, some commercial, and many not.[92] Moreover, judges will be cognizant that this interpretation would

84. *See infra* Section III.

85. Grant H. Frazier & Mark B. Frazier, *Taming the Paper Tiger: Deterring Chinese Economic Cyber-Espionage and Remediating Damage to U.S. Interests Caused by Such Attacks*, 30 S. CAL. INTERDISC. L.J. 1, 20 (2021).

86. *Id.*

87. 504 U.S. 607 (1992).

88. *Id.* at 614, 620. In this case Argentina was specifically held liable for refinancing debt through bond issuances. *Id.*

89. *See* Sergent, *supra* note 59, at 401 (arguing because cyber torts are usually employed to steal information or impair the functionality of electronic systems, they will not likely be considered commercial activity); Martin, *supra* note 71, at 125 (stating that cyberattack such as infecting a political dissident's computer with spyware is not commercial activity).

90. Anderson, *supra* note 9, at 1091-92.

91. *Id.*

92. *Id.* at 1092.

open foreign governments up to broad liability, which has the potential for serious ramifications on the international stage.[93]

Even if a claimant were able to overcome these hurdles, hacking is a crime under U.S. federal law,[94] and U.S. courts have consistently held that crimes like murder, kidnapping, and assassination are not considered commercial under FSIA.[95] The only statutorily defined criminal activity that is considered commercial under FSIA is illegal contracts because contracts are considered the default method for "private parties operating in the market."[96] Because cybercrimes are not the conventional way that private parties operate in the market, a state-sponsored cyberattack would likely not qualify as this type of commercial criminal activity.[97] For these reasons, it is highly unlikely that victims of state-sponsored cyberattacks will successfully bring claims under the FSIA commercial activity exception.

B. The Noncommercial Tortious Exception

The noncommercial tortious exception to FSIA is probably the most popular existing avenue for victims seeking relief from state-sponsored cyberattacks.[98] A foreign state loses immunity under this exception when there is a "(1) noncommercial tortious act or omission (2) committed by a state or its agents that (3) causes personal injury or property damage and (4) occurs in the United States."[99] The first two elements are relatively unproblematic for state-sponsored cyberattacks as a cyberattack will largely be considered a noncommercial tortious act and it will allegedly be committed by a foreign state or its agents.[100] But many victims of state-sponsored cyberattacks may run into issues with the third element because cyberattacks do not typically cause "damage to or loss of property" in the traditional sense.[101] Although some cyberattacks would likely meet this prong, such as the Stuxnet attack that caused substantial physical

93. *Id.*

94. 18 U.S.C. § 1030.

95. Anderson, *supra* note 9, at 1092.

96. *Id.* at 1092-93.

97. *Id.* at 1093.

98. *See, e.g.*, Schultze, *supra* note 55, at 893 (arguing that the noncommercial tort exception should be used to hold foreign governments accountable for their roles in cyberattacks); Gilmore, *supra* note 28, at 259 (arguing that state-sponsored cyberattacks should be analyzed like other cross-border torts executed in the U.S.).

99. Sergent, *supra* note 59, at 402-03.

100. *Id.* at 403.

101. *Id.*

damage to Iran's nuclear program, most cyberattacks do not cause such significant physical damage.[102] Victims of state-sponsored cyberattacks have a better chance of obtaining jurisdiction if victims argue that a foreign state has caused them "personal injury," as FSIA notably does not define "personal injury" leaving room for courts to apply a more liberal interpretation that includes invasions of privacy and reputational harm.[103] But again, claimants may run into issues here as the traditional understanding of personal injury in U.S. courts requires a physical effect that would not include cyberattacks that merely steal, leak, or erase data.[104]

On top of the previously mentioned problems, the fourth element–occurs in the U.S.–will be difficult to overcome for victims of state-sponsored cyberattacks.[105] In 2016, an Ethiopian political dissident sued Ethiopia under the noncommercial tortious exception for allegedly infecting his computer with spyware and monitoring his online activity.[106] The D.C. Circuit Court held that because the spyware had been sent to the plaintiff from London the "entire tort" did not occur in the U.S. and thus the claim failed on the fourth element of the noncommercial tortious exception.[107] By "entire tort" the court held that in addition to the injury, all acts that "precipitate that injury" must take place in the U.S.[108] Because the tortious intent aimed at the plaintiff and the initial deployment of the spyware occurred abroad, the entire tort did not occur in the U.S.[109] Commentators were initially hopeful that the entire tort doctrine would not become a widespread requirement for this exception because cyberattacks are often transnational nature.[110] But, since *Doe v. Ethiopia*, district courts within the Second and Ninth Circuits have adopted the entire tort doctrine for state-sponsored cyberattacks.[111] Further, the Second, Sixth,

102. James Andrew Lewis, *Cyber Attacks, Real or Imagined, and Cyber War*, CTR. FOR STRATEGIC & INT'L STUD. (July 11, 2011), https://www.csis.org/analysis/cyber-attacks-real-or-imagined-and-cyber-war.

103. Sergent, *supra* note 59, at 404.

104. *See* Mullen Coughlin, *Can Cyber Cause "Bodily" or "Personal" Injury? Maybe in the Not-So-Far Future*, MULLEN COUGHLIN (Mar. 4, 2021), https://www.mullen.law/can-a-cyber-crime-cause-bodily-or-personal-injury/ (showing that a cyberattack must have physical damage to be considered a tort).

105. Martin, *supra* note 71, at 126.

106. Doe v. Federal Democratic Republic of Ethiopia, 851 F.3d 7, 8 (D.C. Cir. 2017).

107. *Id.* at 10.

108. *Id.* at 11.

109. *Id.*

110. Martin, *supra* note 71, at 139-40.

111. *Id.*

and Ninth Circuits have adopted the entire tort doctrine in other cases dealing with the noncommercial tortious exception, indicating that they would apply the doctrine if faced with a state-sponsored cyberattack claim.[112] Consequently, it is likely that the entire tort doctrine will become the norm in U.S. jurisdictions, leaving little hope for victims of state-sponsored cyberattacks wishing to bring claims under the noncommercial tortious exception.

Even if the entire tort doctrine does not become the norm, there is yet another aspect of the noncommercial tortious exception that poses problems for victims of state-sponsored cyberattacks: the discretionary exception.[113] This exception restores immunity to States under the noncommercial tortious exception for "any claim based upon the exercise or performance or the failure to exercise or perform a discretionary function."[114] FSIA does not define what constitutes a "discretionary function,"[115] and thus U.S. courts have generally applied the jurisprudence surrounding the U.S. Federal Tort Claims Act ("FTCA") to the concept of discretion under FSIA.[116] Under FTCA jurisprudence the discretionary function protects government officials from liability for actions or decisions they make in implementing a state social, economic, or political policy.[117] With this understanding, a foreign government could potentially avoid FSIA liability by claiming that a cyberattack was in furtherance of a state policy.[118] For example, China could argue its repeated commercial espionage and intellectual property theft is an official part of its economic policy[119] and that Russia's interference in the 2016 U.S. presidential election stood as a part of its official political policy.[120]

Commentator Scott Gilmore argues that the discretion exception would not apply to state-sponsored cyberattacks because foreign states are committing "illegal acts."[121] Commentators point to longstanding

112. *Id.*

113. 28 U.S.C. § 1605(a)(5)(A).

114. Schultze, *supra* note 55, at 879 (quoting 28 U.S.C. § 1605(a)(5)(A)).

115. *Id.*

116. *Id.* at 880.

117. Anderson, *supra* note 9, at 1097.

118. *Id.*

119. *Id.*

120. INTELLIGENCE COMMUNITY ASSESSMENT, ASSESSING RUSSIAN ACTIVITIES AND INTENTIONS IN RECENT US ELECTIONS 1 (Jan. 6, 2017) (showing that Russia's 2016 election interference was a part of Russia's continued effort to under the U.S. led liberal democratic order because it views this political ideology as a threat to
Vladimir Putin's regime).

121. Gilmore, *supra* note 28, at 267.

FTCA precedent, which shows that unlawful government surveillance and trespass generally do not qualify as discretionary under the FTCA.[122] Thus, foreign states would not have the discretion to commit these cyberattacks in the U.S.—even if they advance the country's official policy—because they would violate U.S. computer misuse laws.[123]

In sum, victims of state-sponsored cyberattacks likely face a difficult road to success under the noncommercial tortious exception because the nature of the harm is usually not physical, the tort is often partially committed abroad, and states may claim their role in cyberattacks are in furtherance of an official state policy, protected under the discretionary exception.

C. The Terrorism Exception

Under the original terrorism exception to FSIA, sovereign immunity could only be pierced for those foreign states officially designated by the U.S. government as "sponsors of terrorism."[124] Following the September, 11 terrorist attacks there was a strong call for legislative reform of FSIA because although Saudi Arabia was credited with financing the attacks, it was not a designated state sponsor of terrorism at the time of the attacks, and thus victims could not sue Saudi Arabia under FSIA.[125] In 2016, Congress passed JASTA, which expanded the original terrorism exception to include "'any act of international terrorism in the United States that causes 'physical injury to person or property or death occurring in the United States,' so long as the international terrorism is accompanied by a tortious act of a foreign state or actor of said state."[126]

At first, JASTA appears to be a more promising avenue of redress for state-sponsored cyberattack claimants than the noncommercial tortious exception, as it merely requires a foreign state to commit a tort regardless of where the tort occurred.[127] Moreover, the JASTA exception does not define what acts are to be considered tortious, "beyond stating that omissions or acts of 'mere negligence' are not enough."[128] Theoretically, this means that JASTA could apply to a range of cyber state actions depending on how liberally courts interpret tortious acts.[129] But upon closer

122. *Id.* at 269.
123. *Id.*
124. Martin, *supra* note 71, at 129.
125. *Id.* at 129-30.
126. *Id.* at 131 (quoting 28 U.S.C. § 1605B (2018)).
127. *Id.*
128. *Id.*
129. *Id.*

inspection, there are multiple hurdles to bringing a state-sponsored cyberattack claim under the JASTA exception to FSIA.

First, the terrorism exception's requirement that an act result in "physical injury" or "death" to persons or property rules out a vast number of state-sponsored cyberattacks.[130] Again, state-sponsored cyberattacks could take this form: in the Stuxnet cyberattacks, the U.S. and Israel directed a cyberattack against Iranian nuclear facilities physically damaging the centrifuges.[131] However, a majority of identified state-sponsored cyberattacks take an "informational" form, where a foreign state attempts to erase or leak data or to mislead a victim by inserting false information.[132] Accordingly, JASTA currently does not provide an adequate avenue of redress for the majority of state-sponsored attacks because they result in more of intangible harms.

Further, state-sponsored cyberattack victims will likely face a great challenge in demonstrating that the alleged cyberattack is an act of "international terrorism."[133] In order for a tortious act to be considered an act of international terrorism it must be considered a "(1) violent act or [an] 'act dangerous to human life,' (2) which appears to have proper intent, and (3) either occurs outside the United States or 'transcends national boundaries.'"[134]

The first element of international terrorism provides victims of state-sponsored cyberattacks with the greatest hurdle, as a majority of state-sponsored cyberattacks are simply not violent acts.[135] But, U.S. courts could adopt a more liberal interpretation of "violent acts," where the cyberattack would only need to create circumstances in which there could be danger to a person's well-being.[136] However, even under this more liberal interpretation a state-sponsored cyberattack—like the Sony hacks,

130. *Id.* at 147.

131. *Stuxnet*, BRITANNICA.COM, https://www.britannica.com/technology/Stuxnet (last visited Dec. 16, 2022).

132. *See* Lewis, *supra* note 102 (showing that most state-sponsored cyberattacks take this informational form because they are deliberately trying to stay below the threshold of use of force or an act of war under international law).

133. Martin, *supra* note 71, at 149.

134. *Id.* at 149-50 (quoting 18 U.S.C. § 2331(1) (2018)).

135. *Id.* at 150; CYFIRMA Research, *Cyber Threat Landscape Expands with Collaboration Between State-Sponsored Groups*, CYFIRMA DECODING THREATS (Feb. 19, 2022), https://www.cyfirma.com/blogs/cyber-threat-landscape-expands-with-state-sponsored-cyber-attackers/.

136. Martin, *supra* note 71, at 150. For example, a state-sponsored cyberattack that turns off the power at a hospital may not be violent itself but could result in circumstances in which there is a danger to a person's well-being.

where North Korea allegedly breached Sony's database and leaked personal customer information, would not rise to the level of creating physical danger for the victims' well-being. Further, applying a liberal interpretation to the elements of international terrorism carries potential problems, as critics of JASTA have argued that an overly broad definition of international terrorism could provide an avenue to prosecute protest groups or activist organizations.[137]

Finally, the legislative intent underlying JASTA does not indicate that it is applicable to state-sponsored cyberattacks.[138] JASTA was passed with the sole intention of allowing September 11 victims and their families to sue Saudi Arabia for its role in the terrorist attacks.[139] Thus, using JASTA to allow state-sponsored cyberattack victims to overcome sovereign immunity may seem inconsistent with JASTA's original legislative purpose, as most cyberattacks take a very different form than the September 11 attacks.[140] Between the physical injury and death requirements, the challenges inherent in defining international terrorism, and the legislative intent of JASTA, FSIA's terrorism exception currently provides limited potential for victims of state-sponsored cyberattacks even under its most liberal application.

IV. PROPOSAL FOR A CYBERATTACK EXCEPTION TO FSIA

As detailed above, FSIA has limited exceptions which courts have interpreted quite narrowly, minimizing their potential to hold foreign governments accountable for their roles in cyberattacks.[141] Accordingly, it is time for Congress to fix the law. A pending bipartisan piece of legislation, the Homeland and Cyber Threat Act ("HACT"), seeks to do just that.[142] This section examines the proposed HACT Act and addresses areas for potential additions and clarifications.

The HACT Act confers jurisdiction to U.S. courts to hear claims concerning the following state-sponsored activities, as long as the activities result in "personal injury, harm to reputation, or damage to or loss of property" affecting U.S. nationals:

137. *Id.* at 155.
138. *Id.*
139. *Id.* at 155-56.
140. *Id.* at 156.
141. *See supra* Section III.A.-C.
142. H.R. 1607, 117th Cong. (2021-2022).

(1) Unauthorized access to or access exceeding authorization to a computer located in the United States.[143]
(2) Unauthorized access to confidential, electronic stored information located in the United States.[144]
(3) The transmission of a program, information, code, or command to a computer located in the United States, which, as a result of such conduct, causes damage without authorization.[145]
(4) The use, dissemination, or disclosure, without consent, of any information obtained by means of any activity described in paragraph (1), (2), or (3).[146]
(5) The provision of material support or resources for any activity described in (1) (2) (3), or (4) including by an official, employee, or agent of such foreign state.[147]

The proposed bill's language does much to address the most pressing issues with the other FSIA exceptions. First, the bill explicitly adds "harm to reputation" as an element instead of just covering personal injuries or property damage, which would bring most data breaches and privacy violations within the scope of the amendment.[148] This is exemplified by applying the amendment's language to the Sony hacks, where North Korea's role in leaking customers' personal data and emails would certainly rise to the level of reputational harm.[149]

Second, the bill addresses the problem that the entire tort doctrine poses to plaintiffs alleging state-sponsored cyberattacks by including the language "a foreign state shall not be immune ... from any of the following activities, whether occurring in the U.S. or a foreign state."[150] Accordingly, U.S. courts would still have jurisdiction even if a cyberattack is planned or initiated in a foreign country if it is ultimately directed at a computer or network within the U.S. Finally, the bill contains no requirements that a cyberattack be an act of "international terrorism" or

143. H.R. 1607 § 1605(C)(1).
144. H.R. 1607 § 1605(C)(2).
145. H.R. 1607 § 1605(C)(3).
146. H.R. 1607 § 1605(C)(4).
147. H.R. 1607 § 1605(C)(5).
148. H.R. 1607 § 1605.
149. *See generally* In re Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942 (S.D. Cal. 2014) (showing a lawsuit filed by former Sony employees claiming Sony's negligence in the cyberattack caused them economic harm).
150. H.R. 1607 § 1605(C).

"commercial in nature" as seen in JASTA or the commercial activity exceptions to FSIA.[151]

While this bill as drafted is a good first step towards holding foreign governments accountable and providing those harmed with means of redress, there are several key components that should be added to the legislation to make it as effective as possible. Specifically, Section IV.A proposes the HACT Act add a statute of limitations of five years.[152] Section IV.B recommends the HACT Act implement a lower standard for attribution due to difficulties specific to state-sponsored cyberattacks, such as the sophistication of the technology used and the sensitivity of foreign relations.[153] Section IV.C argues that the HACT Act should allow courts to impose punitive damages due to the potential severity of state-sponsored cyberattacks.[154] Section IV.D argues that the HACT Act should allow courts to attach and execute foreign states' property located in the U.S., due to potential difficulties with satisfying judgments against uncooperative foreign states.[155] Lastly, Section IV.E proposes the HACT Act include a "cyber-intruder" designation, allowing the Government to maintain a level of control over potentially risky litigation.[156]

A. The HACT Act Should Add a Five-Year Statute of Limitations

The HACT Act should contain a statute of limitations of five years that is triggered once a potential plaintiff becomes aware of the alleged state-sponsored cyberattack.[157] Anderson argues that the legislation's statute of limitations should be significantly less than JASTA's ten years because cyberattacks generally cause less grave harm than terrorist attacks.[158] Proponents of a shorter statute of limitations note that the statute of limitations should only start once a potential claimant learns of the cyberattack,[159] acknowledging that many state-sponsored cyberattacks are among the most sophisticated and hardest to detect.[160] Others argue that the statute of limitations should be the same as JASTA to allow maximum

151. *See generally* H.R.1607, 117th Cong. (2021-2022) (showing the amendment as a whole contains no such specific language).

152. *See infra* Section IV.A.

153. *See infra* Section IV.B.

154. *See infra* Section IV.C.

155. *See infra* Section IV.D.

156. *See infra* Section IV.E.

157. Anderson, *supra* note 9, at 1103.

158. *Id.*

159. *Id.*

160. Raul, *supra* note 4.

compensation and opportunity for redress.[161] This Comment takes the position that the HACT Act should contain a statute of limitations somewhere in the middle: five years that is triggered at the filing of a complaint or once the claimant becomes aware of the state-sponsored cyberattack. A five-year statute of limitations takes into account the difficulties of attribution that plague state-sponsored cyberattacks, giving claimants enough time once they become aware of a cyberattack to gather relevant evidence.[162] Moreover, a five-year statute of limitations for state-sponsored cyberattacks recognizes that physical terrorist attacks are likely to be more severe, requiring a longer statute of limitations.[163] Lastly, a five-year statute of limitations is more consistent with the U.S.'s major cybersecurity statute, the Computer Fraud and Abuse Act, which has a two-year statute of limitations that runs from "the date of the act complained of or the date of the discovery of the damages."[164] Accordingly, a five-year statute of limitations would strike the best balance as it adequately accounts for the sophistication of state-sponsored cyberattacks and is more consistent with the federal legislation regulating cyberattacks.

B. The HACT Act Should Reduce the Level of Proof for Attribution Due to Circumstances Unique to State-Sponsored Cyberattacks

The HACT Act should contain a lower level of proof for attribution because of the difficulty of achieving attribution in the cyber context.[165] FSIA case law indicates that when foreign governments are sued, they will likely not appear in court or they will withdraw from participating in the litigation after an initial appearance.[166] When this happens, FSIA allows a court to enter a default judgment when "the claimant establishes his claim or right to relief by evidence satisfactory to the court."[167] Still, private parties seeking to bring suit under the HACT Act may struggle to prove their case depending on what a court deems "satisfactory."[168]

161. Kurland, *supra* note 17, at 263.

162. Anderson, *supra* note 9, at 1103.

163. *Id.*

164. 18 U.S.C. § 1030(g).

165. Gilmore, *supra* note 28, at 229-30.

166. *See, e.g.*, Calderon-Cardona v. Democratic People's Republic of Korea, 723 F. Supp. 2d 441, 444 (D.P.R. 2010) (showing North Korea's non-appearance in a FSIA action); Aguadas Chasidei Chabad of U.S. v. Russian Fed'n, 729 F. Supp. 2d 141, 144 (D.D.C. 2010) (showing that after years of participation in the litigation, Russia withdrew from the litigation).

167. 28 U.S.C. § 1608(e).

168. Haller, *supra* note 12.

Providing concrete evidence of a cyberattack is especially difficult when the perpetrator is a State, as they tend to have access to the most sophisticated technology.[169] Therefore, the HACT Act should incorporate Alexis Haller's provision for a cyberattack exception to FSIA:

> *If any federal law enforcement or intelligence agency certifies that there is probable cause that a foreign state, or an official, employee or official thereof, committed the act described in section * * *, there shall be a rebuttable presumption that the foreign state, or the official, employee or official thereof, has committed the act. If the foreign state does not appear in the action, that presumption shall be accepted by the district court and shall constitute sufficient evidence to satisfy the requirements of section 1608(e). If the foreign state appears in the action, the rebuttable presumption shall be rendered ineffective until such time, if any, that the foreign state no longer participates in the litigation.*[170]

Haller notes that if such provision were adopted, then federal law enforcement and intelligence agencies would need to set up specific procedures for certification.[171] This lesser standard of proof will help the HACT Act be more effective since intelligence agencies and the executive branch have been reluctant to publicly attribute cyberattacks to foreign countries due in part to the high level of certainty required.[172] A standard of probable cause on the other hand is lower, as it merely requires a fact to be somewhere between "less than evidence which would justify conviction" and "more than bare suspicion."[173] Further, this standard would allow the Government to maintain some level of control over potential proceedings: if it does not see the case as legitimate, it does not have to certify that there is probable cause that the accused foreign state was involved.[174]

169. Anderson, *supra* note 9, at 1103; Alan W. Ezekiel, *Hackers, Spies, and Stolen Secrets: Protecting Law Firms from Data Theft*, 26 HARV. J.L. & TECH. 649, 652 (2013).

170. Haller, *supra* note 12.

171. *Id.* at n.22.

172. Anderson, *supra* note 9, at 1107.

173. United States v. Prandy- Binett, 995 F.2d 1069, 1070 (D.C. Cir. 1993) (quoting Brinegar v. United States, 338 U.S. 160, 175 (1949)).

174. *See* Chimène Keitner & Allison Peters, *Private Lawsuits Against Nation-States Are Not the Way to Deal with America's Cyber Threats*, LAWFARE (June 15, 2020, 9:09 AM), https://www.lawfareblog.com/private-lawsuits-against-nation-states-are-not-way-deal-americas-cyber-threats (indicating that FSIA litigation pursuable only when the Government is willing to publicly attribute a foreign state would be largely unhelp for victims.)

Some commentators have argued that Haller's proposed provision would defeat the purpose of moving the problem of state-sponsored cyberattacks from the realm of foreign policy to private suit, and that a certification requirement would be ineffective because a majority of the evidence the intelligence community collects on state-sponsored cyberattacks would be classified.[175] Acknowledging this criticism, this Comment argues that plaintiffs and the intelligence community should have a choice as to the level of proof required: the Government can either certify probable cause that a foreign state conducted the cyberattack or the private party can provide the evidence themselves at a higher level of proof. Although attributing cyberattacks is difficult, private parties have proven to be just as adept at providing attribution as the Government.[176] For example, the private firm, CrowdStrike, collected intelligence and analyzed the Democratic National Committee's data breach in 2016, publicly attributing the attack to Russia before the intelligence community confirmed this designation.[177] Allowing plaintiffs a choice between providing attribution evidence themselves or through a lower government certification procedure takes into account the difficulty of attribution when the perpetrator is a state actor but also ensures that the litigation is not getting bogged down by foreign policy concerns.

C. The HACT Act Should Allow U.S. Courts to Assign Punitive Damages

The HACT Act should include a provision that allows courts to assign punitive damages. A court generally awards punitive damages when it deems a defendant's behavior to be especially harmful.[178] For example, in tort law, courts will sometimes assign punitive damages if the plaintiff can prove the defendant engaged in an "intentional tort" or engaged in "wanton and willful misconduct," as this additional monetary penalty is reasoned to provide added deterrence for conduct society deems unreasonable.[179] Most of the FSIA exceptions hold that foreign states shall not be liable for punitive damages,[180] because it adds a level of escalation to

175. Kurland, *supra* note 17, at 264.

176. Sasha Romanosky, *Private-Sector Attribution of Cyber Attacks: A Growing Concern for the U.S. Government*, LAWFARE (Dec. 21, 2017, 11:20 AM), https://www.lawfareblog.com/private-sector-attribution-cyber-attacks-growing-concern-us-government#.

177. Editorial Team, *CrowdStrike's work with the Democratic National Committee: Setting the record straight*, CROWDSTRIKE BLOG (June 5, 2020), https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/.

178. *Punitive Damages*, CORNELL L. SCH.: LEGAL INFO. INST., https://www.law.cornell.edu/wex/punitive_damages (last visited Dec. 19, 2022).

179. *Id.*

180. 28 U.S.C. § 1606.

foreign relations. Some commentators raise practical concerns with FSIA punitive damages: punitive damages often result in high monetary judgments, which are difficult for individuals to enforce, as any single State's foreign assets located in the U.S. are limited and often depleted before all victims can get their share.[181] Nonetheless, in 2008, Congress removed this hurdle for the terrorism exception and allowed punitive damages for victims of terrorism due to the severity of the harm that accompanies terrorist attacks.[182] As state-sponsored cyberattacks have become increasingly prevalent and harmful to American businesses and individuals,[183] the HACT Act should also provide for punitive damages.[184] First, punitive damages would result in larger judgments, allowing victims to receive meaningful compensation in cases where a cyberattack causes major damage or disruption.[185] More importantly, the threat of punitive damages is intended to add an extra level of deterrence for state-sponsored actors, hopefully resulting in fewer victims who are seeking a piece of the pie.[186] Accordingly, including punitive damages in the HACT Act provides the best chance for the legislation to have a real impact on claimants and foreign governments.

D. The HACT Act Should Allow U.S. Courts to Attach and Execute Foreign Property Located in the U.S. in Order to Satisfy Judgments

The HACT Act should include a provision that allows U.S. courts to attach and execute a foreign state's property located in the U.S. to satisfy potential FSIA judgments. Generally, FSIA provides strong protections against attachment and execution of the property of foreign governments.[187] In order for a U.S. court to attach and execute a foreign state's property, a plaintiff must be able to show one of the following:

(1) that the foreign state has waived its immunity;
(2) that "the property is or was used for the commercial activity upon which the claim is based";

181. Haim Abraham, *Awarding Punitive Damages Against Foreign States is Dangerous and Counterproductive*, LAWFARE (March 1, 2019, 8:00 AM), https://www.lawfaremedia.org/article/awarding-punitive-damages-against-foreign-states-dangerous-and-counterproductive.

182. 28 U.S.C. § 1605A(c).

183. Raul, *supra* note 4.

184. Kleiner & Wolosky, *supra* note 55.

185. *Id.*

186. *Punitive Damages*, CORNELL L. SCH.: LEGAL INFO. INST., https://www.law.cornell.edu/wex/punitive_damages (last visited Dec. 19, 2022).

187. 28 U.S.C. § 1609.

(3) that "the execution relates to a judgment establishing rights in property which has been taken in violation of international law or which has been exchanged for property taken in violation";
(4) that "the execution relates to a judgment establishing rights in property ... which is acquired by succession or gift, or ... which is immovable and situated in the United States";
(5) that "the judgment is based on an order confirming an arbitral award rendered against the foreign state, provided that attachment in aid of execution, or execution, would not be inconsistent with any provision in the arbitral agreement[;]" or
(6) that "the judgment relates to a claim for which the foreign state is not immune under previous sections."[188]

The specificity of these exceptions makes it very difficult for successful plaintiffs to attach foreign property under FSIA.[189] When the original terrorism exception was passed in 1996, Congress allowed courts to attach property owned by the state sponsors of terrorism when it was used for commercial activity in the U.S.[190] For example, in 2010, the Second Circuit ruled that $2 billion of frozen Iranian assets held in New York must be turned over to the families of victims of Iranian terrorism when Iran failed to participate in the litigation.[191]

The HACT Act should include a parallel provision to the terrorism exception, as plaintiffs seeking redress under a potential cyberattack exception will likely face the same types of challenges that those seeking to collect under FSIA faced.[192] Further, the HACT Act should also be subject to § 1610(g)(1).[193] Section 1610(g)(1) addresses the circumstances by which property owned by a foreign state sponsor of terrorism or their agents can be used to satisfy a FSIA judgment.[194] This additional language will ensure that victims of state-sponsored cyberattacks receive adequate relief as the foreign states involved in these civil suits will likely not be cooperative in any judgments.

188. 28 U.S.C. § 1610(a)(1)-(7).
189. Kurland, *supra* note 17, at 265.
190. 28 U.S.C. § 1610(g)(1).
191. Weinstein v. Islamic Republic of Iran, 609 F.3d 43, 46, 56 (2d Cir. 2010).
192. Kurland, *supra* note 17, at 266.
193. Haller, *supra* note 12.
194. CONG. RSCH. SERV., LSB10104, IT BELONGS IN A MUSEUM: SOVEREIGN IMMUNITY SHIELDS IRANIAN ANTIQUITIES EVEN WHEN IT DOES NOT PROTECT IRAN 2 (2018).

E. The HACT Act Should Add a "Cyber-Intruder" Designation

Lastly, the HACT Act should include a "cyber-intruder" designation element, so the executive branch can maintain some level of control over proceedings. The original terrorism exception contained a similar designation where the executive branch had to first designate a foreign state as a "sponsor of terrorism" before a private suit could be brought under the FSIA exception,[195] but JASTA eliminated this designation for tortious acts of international terrorism.[196] This type of executive designation would allow the executive government to play "gatekeeper" with respect to which foreign states can be held liable, which would partially alleviate foreign diplomacy concerns and make the bill more likely to pass.[197] Further, an executive designation may open the door for these private suits to become linked to Government sanctions programs, which could provide an extra level of deterrence to those countries designated as "cyber-intruders."[198] Finally, having government involvement in cyberattack cases may make finding and seizing foreign property located in the U.S. more effective.[199]

V. POTENTIAL CRITICISMS OF A CYBERATTACK EXCEPTION TO FSIA

Some argue that the HACT Act will create more problems than it solves.[200] Common criticisms of a cyberattack exception to FSIA concern international diplomacy, the feasibility of implementation, and reciprocity regarding the U.S.'s extraterritorial cyber activity. This section will address these concerns.

A. Diplomacy Concerns

Commentators Chimène Keitner and Allison Peters argue that opening up another avenue for foreign state liability through a cyberattack exception to FSIA would upset U.S. foreign relations.[201] As mentioned

195. 28 U.S.C. § 1605A(a)(2)(A)(i). The term "state sponsor of terrorism" refers to a country that the Secretary of State has determined to have "repeatedly provided support for acts of international terrorism." *28 U.S.C.* § 1605A(h)(6).

196. Sergent, *supra* note 59, at 410.

197. Kurland, *supra* note 17, at 267.

198. *Id.*

199. *Id.*

200. *See generally* Keitner & Peters, *supra* note 174 (arguing that this sort of amendment to FSIA will cause serious problems).

201. *Id.*

previously, the Government has been reluctant to confront foreign governments responsible for cyberattacks due to the difficulty of attribution for cyberattacks.[202] But as some commentators have correctly noted, a cyberattack exception to FSIA gives the executive branch an avenue to "quietly toughen its stance" against these foreign actors.[203] In comparison to criminal indictments, a private party bringing a civil suit "packs less of a normative punch" and in "the sensitive area of foreign affairs, that can be a virtue."[204] Further, the HACT Act only applies to "national[s] of the United States."[205] This means that common government actions like cyber espionage and intelligence-gathering methods would remain free from liability, as they often target the Government and its proxies, not U.S. nationals.[206] Further, the addition of a "cyber-intruder" requirement would ensure the executive branch can maintain some level of control over which assets are used, protecting potentially sensitive assets.[207]

B. Feasibility

A common critique of the cyberattack exception to the FSIA proposal is that it is unlikely to ever come to fruition due to a lack of political support.[208] Critics point out that the most recent exception to FSIA, JASTA, was only passed under extraordinary circumstances and unprecedented bipartisan support following the September 11 terrorist attacks.[209] It is also important to note that even after Congress passed the bill, President Obama vetoed the bill due to some of the diplomacy concerns mentioned above.[210] Further, critics argue that even if such a bill had enough bipartisan support to move forward, it would still take a long time for the bill to move through Congress, as JASTA was introduced in 2009 and was not passed until 2016.[211] But, as noted above, members of Congress on both sides of the aisle have already introduced a cyberattack exception and the bill has at least ten co-sponsors, with five supporters from the Democratic

202. *See* Anderson, *supra* note 9, at 1089, 1107 (showing that the nature of cyberattacks makes it near impossible to attribute an attack with complete certainty, and that state-sponsored cyberattacks are some of the most sophisticated cyberattacks).

203. *Id.* at 1107.

204. Gilmore, *supra* note 28, at 285.

205. H.R. 1607, 117th Cong. § 1605C (2021).

206. Anderson, *supra* note 9, at 1107.

207. Kurland, *supra* note 17, at 267.

208. Martin, *supra* note 71, at 143.

209. *Id.*

210. Keitner & Peters, *supra* note 174.

211. Martin, *supra* note 71, at 143.

Party and five supporters from the Republican Party.[212] Moreover, Congress has reintroduced this Bill for the 2023 session.[213] State-sponsored cyberattacks are already widespread and incredibly damaging to individuals and businesses, Democrats and Republicans alike, and the harms are only predicted to increase.[214] As such, it is fair to assume that holding foreign governments accountable for their roles in cyberattacks is likely to enjoy bipartisan support.

Critics also argue that even if such a bill were to pass, the compensation system would be ineffective at providing adequate relief to victims, providing a deterrent effect to its use.[215] But data shows that the foreign assets located in the U.S. are enough to satisfy victims' claims: "OFAC states that there are over $520 million in [state-sponsored terrorists'] assets located in the United States."[216] Lastly, there is the possibility that once these foreign nations realize they could soon be liable to victims of their cyberattacks, they may instead choose to negotiate with the U.S. to reach a more cost-effective solution.[217]

C. Reciprocity Concerns

Some critics argue that this type of amendment to FSIA would in turn open up the U.S. to increased litigation abroad.[218] The "if we do it to them, they will do it to us" objection has been around since the introduction of the original terrorism exception to FSIA.[219] But numerous other countries are analyzing their laws to determine how to best address cyberattacks, and thus the U.S. will soon be held accountable for their activities abroad

212. *Bipartisan Bill Seeks to Hold Foreign Governments Accountable for Hacking Americans*, CONGRESSMAN ANDY KIM NJ 03 (Oct. 29, 2019), https://kim.house.gov/media/in-the-news/bipartisan-bill-seeks-hold-foreign-governments-accountable-hacking-americans.

213. Press Release, ICYMI: Bergman Introduces Bipartisan Legislation to Hold Foreign Entities Responsible for Cyberattacks (May 9, 2023), https://bergman.house.gov/news/documentsingle.aspx?DocumentID=1078.

214. *See generally* Morgan, *supra* note 2 (showing that cybercrime is predicted to inflict damages totaling $10.5 trillion USD by 2025).

215. *See* Drescher, *supra* note 63, at 825 (showing that some have raised concerns that the Office of Foreign Assets Control will not be able to adequately compensate each victim under the Fund).

216. *Id.* (citing OFFICE OF FOREIGN ASSET CONTROL, TERRORIST ASSETS REPORT: CALENDAR YEAR 2011 TWENTIETH ANNUAL REPORT TO THE CONGRESS ON ASSETS IN THE UNITED STATES RELATING TO TERRORIST COUNTRIES AND INTERNATIONAL TERRORISM PROGRAM DESIGNEES (2011)).

217. *Id.* at 827.

218. Keitner & Peters, *supra* note 174.

219. Kurland, *supra* note 17, at 269.

anyway.[220] For example, Germany has publicly suggested that a foreign state would not be immune from suit for their role in cyberattacks following the 2013 Snowden leaks.[221] Further, the U.S. has publicly committed to creating and promoting international cyber norms against such cyberattacks and thus should be held accountable for its potential role in cyberattacks on private parties abroad.[222] Moreover, the Government's commitment is seemingly not empty promises: since 2006, the U.S. has only been accused of a handful of significant cyberattacks, while foreign governments such as Russia and China make up a large percentage of identified cyberattacks.[223] Finally, the proposed executive designation of a country as a "cyber-intruder" may limit this type of reciprocity risk because it would only expose those foreign states deemed worth the risk of reciprocity by the executive branch.

CONCLUSION

In the digital age, foreign governments or third parties sponsored by foreign governments increasingly make up the cyber-threat landscape.[224] As this Comment argues, current U.S. solutions to state-sponsored cyberattacks suffer from two primary issues: they do not adequately provide redress for the victims of cyberattacks, nor do they deter foreign governments. Accordingly, hostile foreign states currently enjoy almost complete freedom and immunity to target U.S. businesses and individuals with malicious cyberattacks. Congress intended for FSIA to protect individuals from foreign states causing harm in the U.S., and thus it is time for FSIA to reflect and account for the predominate threat that American businesses and individuals face from foreign states in the digital age. More specifically, Congress should pass the HACT Act to amend FSIA, with the following additions to ensure maximum efficacy: a statute of limitations of five years, a lower standard of proof that takes into account the difficulties of attribution with state-sponsored cyberattacks, the opportunity for claimants to receive punitive damages and courts to attach foreign

220. Sergent, *supra* note 59, at 410.

221. *Id.*

222. *See* U.N. Gen. Assembly, Open-ended working group on developments in the field of information and telecommunications in the context of international security (Mar. 10, 2021), https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf (showing that all UN members agreed on the need for greater accountability for malicious state behavior in cyberspace).

223. *Significant Cyber Incidents*, CTR. FOR STRATEGIC & INT'L STUD., https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents (last visited Dec. 18, 2022).

224. CISA REPORT, *supra* note 3, at 1-2.

property located in the U.S., and an executive designation requirement to better balance the sensitivity of foreign relations. With these changes, the HACT Act provides the best opportunity for private actors to hold foreign states financially accountable and express U.S. cyber norms moving forward.