HACKS DANGEROUS TO HUMAN LIFE: USING JASTA TO OVERCOME FOREIGN SOVEREIGN IMMUNITY IN STATE-SPONSORED CYBERATTACK CASES

*John J. Martin**

State-sponsored cyberattacks are on the rise. With the continually growing presence of automated and autonomous technologies in our lives, the ability to harm individuals from behind a keyboard is becoming an increasingly plausible and desirable option for foreign states seeking to target persons abroad. Those particularly vulnerable to such attacks include political dissidents, activists, and any individuals deemed to be an enemy of the regime employing such cyberattacks. In recent years, U.S. nationals victimized by foreign state-sponsored cyberattacks have attempted to sue their foreign-state cyberattackers in U.S. courts under the traditional exceptions to the Foreign Sovereign Immunities Act (FSIA), to no avail. Commentators have offered a few suggestions to help these victims overcome the barrier of sovereign immunity, including an alternative interpretation of the FSIA's noncommercial tort exception or a cyberattack exception amendment to the FSIA. This Note, however, presents a more concrete and accessible solution: the Justice Against Sponsors of Terrorism Act (JASTA). The recently passed JASTA creates the latest exception to the FSIA, which differs from the other exceptions in two important ways: (1) it does not require an alleged tort to have taken place in the United States, and (2) it does not require the foreign state being sued to have been officially designated a state sponsor of terrorism by the U.S. government. Thus, under JASTA, many U.S. victims of state-sponsored cyberattacks should be able to overcome sovereign immunity and attain justice against their foreign-state cyberattackers in U.S. courts.

* J.D. Candidate 2021, Columbia Law School. The author would like to thank Professor Lori Damrosch for her invaluable expertise and guidance, as well as Nick Argentieri for his support throughout this writing process. The author also extends special thanks to Adi Kamdar for giving him the initial spark of inspiration for this piece.

INTRODUCTION

Foreign state actors are increasingly using malware to target U.S. nationals.[1] In 2016, the U.S. court system saw its first attempt to sue a for-

1. "Malware" is short for "malicious software" and is used to "disrupt a computer's normal operations, gather sensitive information, or gain access to private computer systems." What Is Malware?, Univ. of Cent. Ark., https://uca.edu/it/knowledgebase/what-is-malware [https://perma.cc/P2MY-HH4L] (last visited Nov. 1, 2019). Malware is an

eign state for a cyberattack when an Ethiopian asylee and political dissident—going by the pseudonym "Kidane"—sued Ethiopia for installing and using spyware to monitor his online activity.[2] Kidane claimed jurisdiction under the noncommercial tort exception to the Foreign Sovereign Immunities Act (FSIA).[3] The D.C. Circuit rejected this argument, noting that a tort must occur entirely in the United States for the noncommercial tort exception to apply.[4] Therefore, because the spyware infecting Kidane's devices had been emailed to Kidane by somebody outside the United States, the D.C. Circuit deemed that the tort did not entirely occur in the United States.[5] Despite receiving heavy criticism,[6] the D.C. Circuit's narrow approach has now been adopted within two additional circuits.[7]

Doe v. Ethiopia raises a troubling question: What happens if a foreign state takes it one step further? What if, instead of simply spying on a U.S. national, a foreign state uses malware to cause that national's self-driving car to crash?[8] To cripple the computer system of the hospital where that national is admitted?[9] To remotely switch off that national's insulin pump or pacemaker?[10] Moreover, what if a foreign state uses information it

---

umbrella term and can be used to refer to "computer viruses, worms, trojan horses, spyware, or adware." Id.

2. Doe v. Federal Democratic Republic of Ethiopia (*Doe I*), 189 F. Supp. 3d 6, 8–11 (D.D.C. 2016), aff'd, 851 F.3d 7 (D.C. Cir. 2017). "Spyware" grants a hacker the ability to "capture information like Web browsing habits, e-mail messages, usernames and passwords, and credit card information." Spyware, TechTerms, https://techterms.com/definition/spyware [https://perma.cc/538L-WCVC] (last visited Nov. 2, 2019). Hackers infect their victims' computers or phones with spyware either by sending it through email attachment or by attaching it to the installation of another program. Id.

3. *Doe I*, 189 F. Supp. 3d at 16.

4. See Doe v. Federal Democratic Republic of Ethiopia (*Doe II*), 851 F.3d 7, 10 (D.C. Cir. 2017) (citing Jerez v. Republic of Cuba, 775 F.3d 419, 424 (D.C. Cir. 2014)).

5. See id. at 8, 10 (noting that the person who sent the email likely did so from London).

6. See, e.g., Recent Case, Doe v. Federal Democratic Republic of Ethiopia, 851 F.3d 7 (D.C. Cir. 2017), 131 Harv. L. Rev. 1179, 1184–85 (2018) ("The court's analysis of the acts that make up the tort has . . . problems.").

7. See DNC v. Russian Federation, 392 F. Supp. 3d 410, 428 (S.D.N.Y. 2019); Broidy Cap. Mgmt., LLC v. Qatar, No. CV 18-2421-JFW(Ex), 2018 WL 6074570, at *5 (C.D. Cal. Aug. 8, 2018).

8. See Saheli Roy Choudhury, Malicious Use of A.I. Could Turn Self-Driving Cars and Drones into Weapons, Top Researchers Warn, CNBC (Feb. 21, 2018), https://www.cnbc.com/2018/02/21/malicious-use-of-ai-by-hackers-could-pose-security-risksthreats.html [https://perma.cc/C5SD-ZVTZ] ("Self-driving cars . . . could be tricked into misinterpreting a stop sign that might cause road accidents . . . .").

9. See Alabama Hospital System Halts Admissions amid Malware Attack, Ala. Pub. Radio (Oct. 1, 2019), https://www.apr.org/post/alabama-hospital-system-halts-admissions-amid-malware-attack [https://perma.cc/PJC6-3M5B].

10. See Olivia Tambini, Life-Saving Pacemakers Could Be Hacked with Malware, TechRadar (Aug. 10, 2018), https://www.techradar.com/news/life-saving-pacemakers-

obtained with spyware to track down and directly kill a U.S. national?[11] The growth of automated and autonomous technologies presents foreign-state actors nowadays with a myriad of opportunities to harm political rivals and dissidents mostly, if not entirely, from abroad. In the aftermath of *Doe v. Ethiopia*, concerns arose questioning whether a U.S. national harmed by a state-sponsored cyberattack could ever obtain any redress against the sponsoring state. Nate Cardozo, Kidane's attorney, went so far as to issue a statement saying that "[u]nder [*Doe v. Ethiopia*], you have no recourse under law if a foreign government . . . targets you for a drone strike . . . as long as the government planned the attack on foreign soil."[12] Consequently, some have pushed to adopt a cyberattack exception to the FSIA,[13] while others have urged for courts to adopt a more lenient approach to the noncommercial tort exception.[14]

This Note argues, however, that there is already an existing alternative FSIA exception through which many future U.S. victims of malicious, state-sponsored cyberattacks can obtain jurisdiction over foreign-state sponsors: the Justice Against Sponsors of Terrorism Act (JASTA).[15] Before 2016, U.S. victims of terrorism could sue a state responsible for the attack only if the

---

could-be-hacked-with-malware [https://perma.cc/T5Q5-R8TS] (discussing a demonstration where researchers showed that they could "remotely switch[] off an insulin pump" and "tak[e] control of a pacemaker by hacking the program doctors use to monitor a patient's device").

11. Cf. David D. Kirkpatrick, Israeli Software Helped Saudis Spy on Khashoggi, Lawsuit Says, N.Y. Times (Dec. 2, 2018), https://www.nytimes.com/2018/12/02/world/middleeast/saudi-khashoggi-spyware-israel.html (on file with the *Columbia Law Review*). Saudi Crown Prince Mohammed bin Salman ordered Jamal Khashoggi, a Saudi national and dissident, to be killed in October 2018. Shane Harris, Greg Miller & Josh Dawsey, CIA Concludes Saudi Crown Prince Ordered Jamal Khashoggi's Assassination, Wash. Post (Nov. 16, 2018), https://www.washingtonpost.com/world/national-security/cia-concludes-saudi-crownprince-ordered-jamal-khashoggis-assassination/2018/11/16/98c89fe6-e9b2-11e8a9399469f1166f9d_story.html (on file with the *Columbia Law Review*).

12. 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 [https://perma.cc/KL5C-CGS6].

13. See, e.g., Paige C. Anderson, Note, Cyber Attack Exception to the Foreign Sovereign Immunities Act, 102 Cornell L. Rev. 1087, 1102–03 (2017); Matthew A. Powell, Comment, A Call to Congress: The Urgent Need for Cyberattack Amendments to the Foreign Sovereign Immunities Act, J.L. & Cyber Warfare, Fall 2018, at 117, 144–47; Sam Kleiner & Lee Wolosky, Time for a Cyber-Attack Exception to the Foreign Sovereign Immunities Act, Just Sec. (Aug. 14, 2019), https://www.justsecurity.org/65809/time-for-a-cyber-attack-exception-to-the-foreign-sovereign-immunities-act [https://perma.cc/7E6E-3ETQ].

14. See, e.g., Samantha N. Sergent, Note, Extinguishing the Firewall: Addressing the Jurisdictional Challenges to Bringing Cyber Tort Suits Against Foreign Sovereigns, 72 Vand. L. Rev. 391, 413–16 (2019).

15. Justice Against Sponsors of Terrorism Act, Pub. L. No. 114-222, 130 Stat. 852 (2016) (codified at 18 U.S.C. § 2333 (2018); 28 U.S.C. § 1605B (2018)).

state had been "designated as a state sponsor of terrorism."[16] But in 2016, Congress passed JASTA, which expanded the FSIA to allow U.S. nationals to sue *any* foreign state that physically injured them or their property through "an act of international terrorism in the United States; and a tortious act . . . regardless where [it] occurred."[17] Accordingly, this Note argues that many future instances of state-sponsored cyberattacks can be characterized within the JASTA exception's framework: A foreign state commits a tortious act of infecting a U.S. national's device with malware, resulting in a separate act of terrorism that physically harms said national or their property on U.S. soil.

Part I overviews the FSIA and its exceptions, including the noncommercial tort exception, the terrorism exception, and the JASTA exception. Part II demonstrates why the noncommercial tort exception and other pre-JASTA FSIA exceptions, as well as the proposed cyberattack exception, provide inadequate solutions for U.S. victims of state-sponsored cyberattacks. Part III then offers the JASTA exception as a practical, already-existing mechanism through which U.S. nationals harmed by state-sponsored cyberattacks could potentially obtain jurisdiction over the foreign state responsible for the attack, and further addresses arguments for why courts may still wish to refrain from using JASTA as a means to sue a foreign state.

I. THE FOREIGN SOVEREIGN IMMUNITIES ACT, ITS RELEVANT EXCEPTIONS, AND TREATMENT OF THOSE EXCEPTIONS

Any discussion of the ability to obtain jurisdiction over a foreign state in U.S. courts must inevitably revolve around the FSIA and its exceptions. For the purpose of this Note, the three most relevant exceptions are the noncommercial tort exception, the terrorism exception, and the JASTA exception. Section I.A briefly reviews the history of the FSIA and its current parameters. Section I.B overviews the FSIA exceptions that likely would not apply to state-sponsored cyberattack cases. Section I.C discusses the noncommercial tort exception and its application to state-sponsored cyberattack cases, including *Doe v. Ethiopia* and two other cases that adopted *Doe v. Ethiopia*'s approach. Section I.D discusses the JASTA exception, its differences from the terrorism exception, and how it has been substantively applied by courts since its passage.

16. 28 U.S.C. § 1605A(a)(2)(A)(i)(I).

17. Id. § 1605B(b).

A. *The Foreign Sovereign Immunities Act*

Congress passed the FSIA in 1976,[18] establishing statutory limitations on the ability to bring suit against foreign states in both federal and state courts in the United States. Under the FSIA, one may not sue a foreign state in U.S. court except under a limited array of ten enumerated exceptions.[19] A U.S. national, for example, may not sue a foreign state in U.S. court simply for abuse of process.[20] They may, however, sue said foreign state for personal injury or property damage occurring in the United States, which would fall under the noncommercial tort exception.[21] Today, the FSIA remains "the sole basis" for obtaining jurisdiction over a foreign state in U.S. courts,[22] meaning that if litigants hope to sue a foreign state in U.S. court, they must satisfy one of the FSIA exceptions.

Congress had three objectives when it passed the FSIA. First, it wanted to "depolitici[ze] sovereign immunity" by transferring determinations of immunity from the executive to the judiciary.[23] Prior to the FSIA, courts would defer to the U.S. Department of State to determine whether immunity applied in a suit against a foreign state.[24] Second, Congress wanted "to codify the restrictive theory of immunity" into the judicial system.[25] U.S. courts originally adhered to the absolute theory of sovereign immunity, under which foreign states were presumptively immune from suits in all circumstances, barring a state's waiver of immunity.[26] This began to change, however, in 1952 when the State Department adopted the restrictive theory of sovereign immunity, under which immunity is not

---

18. Foreign Sovereign Immunities Act of 1976, Pub. L. No. 94-583, 90 Stat. 2891 (codified at 28 U.S.C. §§ 1330, 1391(f), 1441(d), 1602–1611).

19. For an exhaustive list of the FSIA exceptions, see infra sections I.B–.D.

20. See Khochinsky v. Republic of Poland, No. 18-cv-1532 (DLF), 2019 WL 5789740, at *6 (D.D.C. Nov. 6, 2019) ("[The FSIA] makes clear that if the predicate conduct for the alleged tort is simply a foreign state's abuse of process, then the court lacks jurisdiction to hear the resulting claim.").

21. See id.

22. OBB Personenverkehr v. Sachs, 136 S. Ct. 390, 393 (2015) (quoting Argentine Republic v. Amerada Hess Shipping Corp., 488 U.S. 428, 443 (1989)).

23. Mark B. Feldman, The United States Foreign Sovereign Immunities Act of 1976 in Perspective: A Founder's View, 35 Int'l & Comp. L.Q. 302, 304–05 (1986).

24. See, e.g., Republic of Mexico v. Hoffman, 324 U.S. 30, 36–38 (1945) (refusing to grant sovereign immunity in a suit regarding a vessel owned, but not possessed, by the Mexican government because "[t]he State Department . . . has refrained from certifying that it allows the immunity").

25. Feldman, supra note 23, at 305.

26. See The Schooner Exchange v. McFaddon, 11 U.S. (7 Cranch) 116, 136 (1812) ("The jurisdiction of the nation within its own territory is necessarily exclusive and absolute . . . . All exceptions, therefore, to the full and complete power of a nation within its own territories, must be traced up to the consent of the nation itself.").

recognized "with respect to private acts,"[27] mainly covering commercial activity conducted by the foreign state.[28] Finally, Congress wanted to establish procedural uniformity for litigation brought against foreign states in the United States, and therefore viewed the FSIA as "a comprehensive and exclusive federal regime" meant to govern such litigation.[29]

B. *The FSIA Exceptions Less Applicable to Cyberattack Cases*

Before dissecting the FSIA's noncommercial tort, terrorism, and JASTA exceptions,[30] it is important to note that the FSIA has seven other exceptions: waiver, commercial activity, expropriations, rights on certain property, arbitration, maritime liens, and counterclaims.[31] Aside from waiver, these exceptions apply in very specific circumstances that would likely not arise in cyberattack cases. The commercial activity exception, for example, applies only when a foreign state engages in conduct that is based on commercial activity carried out in the United States;[32] infecting a political dissident's computer with spyware is not commercial activity.

The waiver exception, under which litigants can sue a foreign state that "has waived its immunity either explicitly or by implication," could occasionally apply.[33] Federal courts, however, find implied waiver in only three circumstances: "(1) a foreign state has agreed to arbitration in another country; (2) a foreign state has agreed that a contract is governed by the law of a particular country; and (3) a foreign state has filed a responsive pleading in a case without raising the defense of sovereign immunity."[34] Accordingly, a waiver of foreign sovereign immunity rarely

---

27. Letter from Jack B. Tate, Acting Legal Adviser, U.S. Dep't of State, to Philip B. Perlman, Acting Att'y Gen., DOJ (May 19, 1952), reprinted in 26 Dep't St. Bull. 984, 984–85 (1952).

28. Lucian C. Martinez, Jr., Sovereign Impunity: Does the Foreign Sovereign Immunities Act Bar Lawsuits Against the Holy See in Clerical Sexual Abuse Cases?, 44 Tex. Int'l L.J. 123, 128–29 (2008) ("When sovereigns engaged in commercial activities like any private actor, they could not claim immunity to suit.").

29. Feldman, supra note 23, at 305.

30. See infra sections I.C–.D.

31. See David P. Stewart, Fed. Jud. Ctr., The Foreign Sovereign Immunities Act: A Guide for Judges 47 (2d ed. 2018), https://www.fjc.gov/sites/default/files/materials/41/FSIA_Guide_2d_ed_2018.pdf [https://perma.cc/CE92-6JD3].

32. 28 U.S.C. § 1605(a)(2) (2018).

33. Id. § 1605(a)(1).

34. In re Republic of Philippines, 309 F.3d 1143, 1151 (9th Cir. 2002) (quoting Joseph v. Off. of the Consulate Gen. of Nigeria, 830 F.2d 1018, 1022 (9th Cir. 1987)). The circuit courts have also made it clear that a violation of international legal norms does not waive sovereign immunity. See, e.g., Matar v. Dichter, 563 F.3d 9, 14 (2d Cir. 2009) ("[T]here is no general *jus cogens* exception to FSIA immunity.").

occurs, and even if it does, courts will construe the waiver narrowly in favor of the foreign state.[35]

C. *The Noncommercial Tort Exception*

This section provides an overview of the FSIA's noncommercial tort exception, which has thus far been the exception of choice for U.S. victims of state-sponsored cyberattacks. Section I.C.1 discusses the general parameters of the noncommercial tort exception. Section I.C.2 discusses the application of the noncommercial tort exception to state-sponsored cyberattack cases.

1. *The Exception.* — One way to obtain jurisdiction over a foreign state is through the noncommercial tort exception.[36] Under this exception, one may sue a foreign state to seek 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 that foreign state or of any official or employee of that foreign state while acting within the scope of his office or employment."[37] Congress included the noncommercial tort exception primarily to eliminate sovereign immunity for traffic accidents and other torts covered under domestic tort law.[38]

Courts have emphasized that a tort must occur "in the United States" for the noncommercial tort exception to apply,[39] and many lower federal courts have interpreted this to mean that the *entire* tort must occur in the United States.[40] For example, a plaintiff would have a successful tort claim

---

35. Stewart, supra note 31, at 48, 50 (noting that both express and implied waivers are construed narrowly "in favor of the sovereign").

36. 28 U.S.C. § 1605(a)(5).

37. Id. (emphasis added).

38. See H.R. Rep. No. 94-1487, at 20–21 (1976), as reprinted in 1976 U.S.C.C.A.N. 6604, 6619–20 ("The purpose of section 1605(a)(5) is to permit the victim of a traffic accident or other noncommercial tort to maintain an action against the foreign state to the extent otherwise provided by law.").

39. See, e.g., Argentine Republic v. Amerada Hess Shipping Corp., 488 U.S. 428, 439 (1989) ("Section 1605(a)(5) is limited by its terms, however, to those cases in which the damage to or loss of property occurs *in the United States*.").

40. See, e.g., Jerez v. Republic of Cuba, 775 F.3d 419, 424 (D.C. Cir. 2014) ("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."); In re Terrorist Attacks on September 11, 2001, 714 F.3d 109, 115 (2d Cir. 2013) ("For [the noncommercial tort] exception to apply, however, the 'entire tort' must be committed in the United States."); O'Bryan v. Holy See, 556 F.3d 361, 382 (6th Cir. 2009) ("We join the Second and D.C. Circuits in concluding that in order to apply the tortious act exception, the 'entire tort' must occur in the United States."); Olsen v. Gov't of Mex., 729 F.2d 641, 646 (9th Cir. 1984) ("[W]e hold that if plaintiffs allege at least one entire tort occurring in the United States, they may claim under section 1605(a)(5)."), abrogated in part on other grounds by Joseph v. Off. of the Consulate Gen. of Nigeria, 830 F.2d 1018 (9th Cir. 1987); Coleman v. Alcolac, Inc., 888 F. Supp. 1388, 1403 (S.D. Tex. 1995) ("Plaintiffs have not pleaded facts indicating that the entire tort

against Singapore under the noncommercial tort exception if said plaintiff injured themselves by tripping over tables negligently placed near a stairwell at Singapore's embassy in Washington, D.C.[41] If said plaintiff, however, suffered the same accident at a Singaporean embassy in another country, and subsequently suffered further injuries while in the United States due to the initial accident abroad,[42] said plaintiff could not bring a successful tort claim against Singapore because the tort partially occurred outside the United States. For the purpose of the exception, the "United States" includes "all territory and waters, continental or insular, subject to the jurisdiction of the United States,"[43] which has been more narrowly construed as meaning only the United States' territorial jurisdiction.[44]

2. *Application of the Noncommercial Tort Exception to State-Sponsored Cyberattack Cases.* — Since 2016, U.S. courts have confronted three cases of plaintiffs suing foreign states under the noncommercial tort exception for alleged cyberattacks conducted against them. Section I.C.2.a discusses the first case—*Doe v. Ethiopia*—in which the D.C. Circuit applied the "entire tort" rule to the noncommercial tort exception.[45] Section I.C.2.b overviews the other two cases, both of which resulted in the adoption of the D.C. Circuit's approach.

a. Doe v. Ethiopia. — In 2016, Ethiopian asylee and political dissident Kidane sued Ethiopia for infecting his computer with spyware and using it to monitor his online activity.[46] Kidane alleged that Ethiopia used spyware called FinSpy—sold exclusively to government agencies—to record his Skype calls, emails, and online searches.[47] To overcome Ethiopia's sovereign immunity, Kidane invoked the noncommercial tort exception,[48] thus requiring him to prove that Ethiopia's alleged cybertort

---

occurred in the United States so as to bring them within the noncommercial tort exception, as is their burden once the defendant shows the potential entitlement to immunity.").

41. See Olson v. Republic of Singapore, 636 F. Supp. 885, 885–87 (D.D.C. 1986) (stating that to hold otherwise "would be inconsistent with the purpose of the FSIA in that it would improperly free foreign embassies from the same duties of care owed by private landowners as well as the United States government").

42. In U.S. tort law, additional injuries arising out of an initial injury can usually be factored into damages, provided that the additional injuries were not incurred through negligence. See Wagner v. Mittendorf, 232 N.Y. 481, 486 (1922) ("[A]dded injuries may be included in the damage provided they arose out of the first injury or would not have happened but for the first injury, and are not due to the neglect or carelessness of the injured party.").

43. 28 U.S.C. § 1603(c) (2018).

44. See *Amerada Hess*, 488 U.S. at 440 (finding that injuries that have occurred on the high seas cannot be deemed to have occurred in the United States based on the definition provided by 28 U.S.C. § 1603(c)).

45. See supra notes 40–42 and accompanying text.

46. *Doe I*, 189 F. Supp. 3d 6, 8–11 (D.D.C. 2016), aff'd, 851 F.3d 7 (D.C. Cir. 2017).

47. Id. at 9–11.

48. Id. at 16.

occurred "in the United States."[49] Kidane argued for an "essential locus" test, which would require only that "the injury and the act that proximately cause[d] [Kidane's] injury occur[red] in the United States."[50] Under this "essential locus" test, it would have been enough for Kidane to prove that the spyware infected his electronic devices in the United States. The District Court for the District of Columbia, however, applied the "entire tort" approach. Focusing on the physical location of the tortfeasor, the district court found that the "entire tort" did not occur in the United States because the spyware had been sent to Kidane from someone in London.[51] The district court thus held that even though Kidane's alleged injury occurred in the United States, the noncommercial tort exception could not apply.[52] The D.C. Circuit upheld the district court's reasoning, holding that "at least a portion of Ethiopia's alleged tort occurred abroad."[53]

b. *Cases Applying* Doe v. Ethiopia. — Since *Doe v. Ethiopia*, courts in two additional circuits have adopted the D.C. Circuit's reasoning and applied the "entire tort" rule to state-sponsored cyberattack cases in which the noncommercial tort exception had been invoked. First, the District Court for the Central District of California applied *Doe v. Ethiopia* in *Broidy Capital Management, LLC v. Qatar*, in which Qatar allegedly infiltrated Broidy Capital's computer systems and stole private documents, including trade secrets and business plans.[54] Broidy Capital argued that the district court had jurisdiction over Qatar under the noncommercial tort exception.[55] Applying *Doe v. Ethiopia*, the district court held that Broidy Capital could not raise the exception because "the actual location of a computer or computers accessing Plaintiff['s] . . . network" was in Qatar.[56] Similarly, the District Court for the Southern District of New York applied *Doe v. Ethiopia* in *DNC v. Russian Federation*, in which Russia allegedly hacked into the DNC's computers.[57] The DNC contended that Russia distributed the material it stole from DNC computers to publicly available websites such as WikiLeaks.[58] Responding to the DNC's noncommercial tort exception argument, the district court held that the exception could not apply because "the hack was executed from computers located outside of the

---

49. Id. at 18; see also *Amerada Hess*, 488 U.S. at 439.

50. *Doe I*, 189 F. Supp. 3d at 22 (internal quotation marks omitted).

51. Id. at 21–25.

52. Id. at 19, 25.

53. *Doe II*, 851 F.3d 7, 10, 12 (D.C. Cir. 2017).

54. Broidy Cap. Mgmt., LLC v. Qatar, No. CV 18-2421-JFW(Ex), 2018 WL 6074570, at *1 (C.D. Cal. Aug. 8, 2018).

55. See id. at *4.

56. Id. at *5.

57. DNC v. Russian Federation, 392 F. Supp. 3d 410, 418–19 (S.D.N.Y. 2019).

58. Id.

United States."[59] Overall, the "entire tort" rule has now been applied in state-sponsored cyberattack cases by courts within the Second, Ninth, and D.C. Circuits.

D. *The JASTA Exception*

This section provides an overview of the JASTA exception to the FSIA. Section I.D.1 overviews JASTA's text and legislative history. Section I.D.2 discusses how the JASTA exception differs from and expands upon the FSIA's terrorism exception[60] and noncommercial tort exception. Section I.D.3 discusses how the JASTA exception has been interpreted thus far by U.S. courts—particularly the District Court for the Southern District of New York.

1. *Text and Legislative History.* — In 2016, Congress passed JASTA, which created the latest exception to the FSIA.[61] The most substantial portion of the statute states that a foreign state will not have sovereign immunity in U.S. court in cases in which U.S. nationals seek money damages for physical injury or property damage occurring *in the United States* caused by (1) "an act of international terrorism *in the United States*,"[62] and (2) "a tortious act or acts of the foreign state, or of any official, employee, or agent of that foreign state while acting within the scope of his or her office, employment, or agency, *regardless where the tortious act or acts of the foreign state occurred*."[63] Prior to the JASTA exception, U.S. nationals injured by acts of terrorism could sue the responsible foreign state only under the FSIA's terrorism exception, which requires foreign states to be "designated as a state sponsor of terrorism" by the U.S. government for the exception to apply.[64]

Pressure built following the September 11th attacks to amend the FSIA so that September 11th victims' families could sue Saudi Arabia—

---

59. Id. at 428.

60. In this Note, the "JASTA exception" and the "terrorism exception" are treated as two independent exceptions to the FSIA, despite both dealing with terrorism. The JASTA exception is the exception that falls under 28 U.S.C. § 1605B (2018), and the terrorism exception is the older, more limited exception that falls under 28 U.S.C. § 1605A. See infra note 64 and accompanying text.

61. Justice Against Sponsors of Terrorism Act, Pub. L. No. 114-222, 130 Stat. 852 (2016). The Act is codified in 28 U.S.C. § 1605B. JASTA also amended 18 U.S.C. § 2333, which specifies the civil remedies available to U.S. nationals injured by acts of international terrorism, including treble damages and attorney's fees. 18 U.S.C. § 2333(a) (2018).

62. 28 U.S.C. § 1605B(b)(1) (emphasis added). JASTA defines "international terrorism" as any criminal activity that (1) involves violent acts or acts "dangerous to human life," (2) is intended to intimidate or coerce civilian populations, influence policy, or affect the conduct of governments, and (3) either occurs outside the United States or "transcends national boundaries." See id. § 1605B(a) (applying the three-pronged definition of "international terrorism" laid out in 18 U.S.C. § 2331).

63. Id. § 1605B(b)(2) (emphasis added).

64. Id. § 1605A(2)(A)(i)(I).

which is not a designated state sponsor of terrorism and thus cannot be sued under the terrorism exception[65]—for financing the attacks.[66] Accordingly, Senator Chuck Schumer introduced JASTA to the U.S. Senate,[67] which passed the bill by "unanimous voice vote" in May 2016.[68] The U.S. House of Representatives subsequently passed JASTA, also unanimously by voice vote, in September 2016.[69] President Barack Obama ultimately vetoed JASTA, arguing that "[it] would invite consequential decisions to be made [by courts] based upon incomplete information . . . about the culpability of individual foreign governments and their role in terrorist activities directed against the United States."[70] Congress nonetheless overrode the President's veto—the first override of his presidency—with overwhelming bipartisan support: 97-to-1 in the Senate and 348-to-77 in the House.[71]

2. *Distinguishing the JASTA Exception from the Terrorism Exception and the Noncommercial Tort Exception.* — The JASTA exception differs from the terrorism exception in two important ways. First, it does not contain a "designated state sponsor of terrorism" requirement, effectively opening up any foreign state to the possibility of being subject to the exception.[72]

---

65. See Cong. Rsch. Serv., R43835, State Sponsors of Acts of International Terrorism—Legislative Parameters: In Brief 1–2 (2018), https://fas.org/sgp/crs/terror/R43835.pdf [https://perma.cc/JWX2-NQMS] ("Current designees are the governments of Iran, North Korea, Sudan, and Syria.").

66. See Maria Alvarez, Schumer: JASTA Bill Would Allow Suits Against Foreign Countries for Financing Terrorism on American Soil, Newsday, https://www.newsday.com/911-anniversary/senate-judiciary-committee-to-consider-bill-to-allow-suits-against-foreign-countries-for-financing-terrorism-on-americansoil-1.9201412 [https://perma.cc/9R7L-LBSS] (last updated Sept. 1, 2014) ("Members of the 9/11 Families United for Justice Against Terrorism have pushed for the legislation. They have claimed Saudi Arabia and its rulers are legally responsible for the terror attacks. But lower courts dismissed much of their lawsuit . . . .").

67. See id.

68. Patricia Zengerle, Senate Passes Bill Allowing 9/11 Victims to Sue Saudi Arabia, Reuters (May 17, 2016), https://www.reuters.com/article/us-saudi-usa-congress-idUSKCN0Y8239 [https://perma.cc/QAL8-JN7P].

69. Katie Bo Williams, House Unanimously Passes Bill to Allow 9/11 Lawsuits Against Saudi Arabia, Hill (Sept. 9, 2016), https://thehill.com/policy/national-security/295157-house-unanimously-passes-bill-to-allow-9-11-lawsuits-against-saudi [https://perma.cc/8SU2-GCLT].

70. Seung Min Kim, Obama Vetoes Saudi 9/11 Bill, Politico (Sept. 23, 2016), https://www.politico.com/story/2016/09/obama-jasta-228548 [https://perma.cc/7DMY-9U7J].

71. Jennifer Steinhauer, Mark Mazzetti & Julie Hirschfeld Davis, Congress Votes to Override Obama Veto on 9/11 Victims Bill, N.Y. Times (Sept. 28, 2016), https://www.nytimes.com/2016/09/29/us/politics/senate-votes-to-override-obama-veto-on-9-11-victims-bill.html?_r=0 (on file with the *Columbia Law Review*).

72. See 162 Cong. Rec. S2140 (daily ed. Apr. 19, 2016) (statement of Sen. Cornyn) ("The only real change is allowing victims of terrorist attacks on the homeland to sue even if the defendant is not designated by the State Department as a state sponsor of terrorism.").

Second, while JASTA was clearly written with September 11th victims in mind,[73] Congress passed it with the express purpose to "provide civil litigants with the broadest possible basis" to sue any foreign state that materially supports terrorist activities against U.S. citizens.[74] The JASTA exception expands the coverage of the terrorism exception to 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.[75]

Moreover, the JASTA exception differs from the noncommercial tort exception in that its tortious act requirement does not require the tort to have occurred entirely within the United States. Rather, the JASTA exception simply requires the tortious acts to have been committed by a foreign state or actor of said state, "*regardless where the tortious act or acts of the foreign state occurred*."[76] The JASTA exception furthermore "does not itself define what acts are considered tortious"[77] beyond stating that omissions or acts of "mere negligence" will not be enough to invoke the exception.[78] Consequently, the JASTA exception could theoretically apply to a wide range of state actions.[79] So far, however, plaintiffs have not brought forward many claims against foreign states under JASTA, and so it remains unclear just how extensively courts will apply the exception.[80]

3. Terrorist Attacks XIII *and the Application of JASTA*. — The most substantive application of JASTA thus far has been the most recent judgment of *In re Terrorist Attacks on September 11, 2001* (*Terrorist Attacks XIII*), in which victims of the September 11th attacks sued Saudi Arabia,

---

73. See id. ("JASTA is also important because it would help the victims of the 9/11 attacks achieve closure from that horrific tragedy.").

74. See Justice Against Sponsors of Terrorism Act, Pub. L. No. 114-222, 130 Stat. 852, 853 (2016).

75. 28 U.S.C. § 1605B (2018).

76. Id. § 1605B(b)(2) (emphasis added).

77. In re Terrorist Attacks on September 11, 2001 (*Terrorist Attacks XIII*), 298 F. Supp. 3d 631, 643 (S.D.N.Y. 2018).

78. 28 U.S.C. § 1605B(d).

79. Cf. How the USA PATRIOT Act Redefines "Domestic Terrorism", ACLU, https://www.aclu.org/other/how-usa-patriot-act-redefines-domestic-terrorism [https://perma.cc/7DHG-HQ9X] (last visited Oct. 5, 2019) (arguing that the government's definition of "domestic terrorism"—which is practically identical to its definition of international terrorism—is "broad enough to encompass the activities of several prominent activist campaigns and organizations").

80. There have been only two cases thus far in which a plaintiff has attempted to use the JASTA exception to waive sovereign immunity. See Krua v. Sirleaf, No. 18-10574-DJC, 2019 WL 1936733, at *6 (D. Mass May 1, 2019) (noting that plaintiffs sued Liberian defendants under the JASTA exception despite defendants not acting under the authority of the Liberian government, consequently finding no cause of action under JASTA); *Terrorist Attacks XIII*, 298 F. Supp. 3d at 639. For discussion on how the District Court for the Southern District of New York interpreted and applied JASTA, see infra section I.D.3.

among other parties, for "assist[ing] the hijackers and plotters who carried out the attacks."[81] Plaintiffs had originally sued Saudi Arabia under the noncommercial tort exception.[82] Applying the "entire tort" approach, the district court held that the noncommercial tort exception did not strip Saudi Arabia of its sovereign immunity because its government's tortious activities occurred abroad.[83] Plaintiffs initially appealed to the Second Circuit,[84] but Congress soon after passed JASTA.[85] Accordingly, both parties filed a joint motion to vacate and remanded the case back to the district court, recognizing that "JASTA was intended to apply to this case."[86] The Second Circuit granted the motion.[87]

In *Terrorist Attacks XIII*, the district court recognized four discrete elements within the JASTA exception:

> (1) physical injury to a person or property or death occurring in the United States; (2) an act of international terrorism in the United States, *and* a tortious act or acts by a foreign state, or *any* official, employee, or agent of that state taken while acting within the scope of that person's office, employment, or agency; (3) causation; and (4) damages.[88]

The district court went into greater detail on only the second and third elements. Regarding the second element, the district court recognized that "JASTA does not itself define what acts are considered tortious."[89] The court found, however, that the tortfeasor must at least commit the tortious act knowingly or with deliberate indifference, rather than negligently.[90] Furthermore, the district court elaborated that an agent acts within the scope of their agency when they agree to act on another party's behalf and be subject to that party's control, whereas an agent acts outside the scope of their agency if they are "motivated solely by personal motives unrelated to the furtherance of the principal's business."[91]

---

81. 298 F. Supp. 3d at 632.

82. See In re Terrorist Attacks on September 11, 2001 (*Terrorist Attacks XI*), 134 F. Supp. 3d 774, 777–78 (S.D.N.Y. 2015).

83. Id. at 781, 788.

84. See Brief for Plaintiffs-Appellants at 2, In re Terrorist Attacks on September 11, 2001 (*Terrorist Attacks XII*), No. 15-3426 (L) (2d Cir. Feb. 7, 2017), 2016 WL 944407.

85. See supra notes 67–71 and accompanying text.

86. *Terrorist Attacks XIII*, 298 F. Supp. 3d at 639 (internal quotation marks omitted) (quoting Joint Motion to Vacate and Remand at 2, *Terrorist Attacks XII*, No. 15-3426 (L) (2d Cir. Feb. 7, 2017)).

87. *Terrorist Attacks XII*, 2017 WL 8776686, at *1.

88. *Terrorist Attacks XIII*, 298 F. Supp. 3d at 642.

89. Id. at 643.

90. See id.

91. Id. at 644 (internal quotation marks omitted) (quoting John St. Leasehold, LLC v. Capital Mgmt. Res., L.P., 154 F. Supp. 2d 527, 543 (S.D.N.Y. 2001)).

Regarding causation, the court refused to apply a strict "but for" causation standard,[92] instead applying a less strict two-factor standard under which (1) the defendant's conduct must have been a "substantial factor" leading to plaintiff's injury, and (2) the plaintiff's injury "'must have been reasonably foreseeable or anticipated as a natural consequence of' the defendant's actions."[93] Based on these principles, the district court denied Saudi Arabia's motion to dismiss.[94] The district court found the plaintiffs' alleged facts to sufficiently demonstrate that two of the defendants had assisted the September 11th hijackers under the instruction of senior Saudi officials.[95] Consequently, the district court found "a reasonable basis for Saudi Arabia to be held responsible for the conduct of [two of] its agents."[96]

The district court's somewhat broad interpretation of the JASTA exception in *Terrorist Attacks XIII* suggests that the exception could potentially be applicable in a variety of state-sponsored cyberattack cases. As Part II demonstrates, this could be crucial for state-sponsored cyberattack victims, who have largely been unable to obtain redress under current approaches.

II. THE RISING THREAT OF STATE-SPONSORED CYBERATTACKS AND THE INADEQUACY OF CURRENT APPROACHES TO OVERCOMING FOREIGN SOVEREIGN IMMUNITY IN CYBERATTACK CASES

Every new technological advancement affords states greater opportunity to employ malware to disrupt the lives of individuals they deem to be enemies.[97] For instance, in the months leading up to journalist and Saudi dissident Jamal Khashoggi's death, Saudi Arabia implanted spyware onto the phone of Omar Abdulaziz, another Saudi dissident.[98] The Saudi government used this spyware to monitor Khashoggi's communications with Abdulaziz, which some believe "contributed in a significant manner to the decision to murder Mr. Khashoggi."[99] Moreover, the rise in reliance

92. Under this standard, a defendant is held liable for a plaintiff's injuries only if said injuries would not have occurred "but for the defendant's negligent act." Proximate Cause, The Free Dictionary, https://legal-dictionary.thefreedictionary.com/But+for+causation [https://perma.cc/ME2L-3Y7B] (last visited Nov. 1, 2019).

93. *Terrorist Attacks XIII*, 298 F. Supp. 3d at 645–46 (quoting Owens v. Republic of Sudan, 864 F.3d 751, 794 (2017)).

94. Id. at 661.

95. Id. at 650.

96. Id. at 651, 661.

97. For a description of "malware," see supra note 1.

98. Kirkpatrick, supra note 11.

99. Id. (internal quotation marks omitted) (quoting court papers in Abdulaziz's lawsuit). Hatice Cengiz, Khashoggi's wife, raised similar concerns in the complaint filed in her lawsuit against Saudi Crown Prince Mohammed bin Salman. See Complaint at 28–29, Cengiz v. bin Salman, No. 1:20-cv-03009 (D.D.C. filed Oct. 20, 2020), 2020 WL 6152108

on automated and autonomous technologies presents states with creative ways to physically harm people by the stroke of a few keys.[100] In light of these growing threats, *Doe v. Ethiopia* has raised pressing questions about whether future victims of cyberattacks will be left without redress if their attacker happens to be a foreign state.[101]

This Part overviews how foreign states can currently use malware to harm individuals and illustrates the difficulty of obtaining jurisdiction over such foreign states pursuing the various solutions suggested in the wake of *Doe v. Ethiopia*. Section II.A details the growing threat and scale of state-sponsored cyberattacks, the potential methods foreign states could use to attack U.S. nationals, and the motivations foreign states have to increasingly resort to these attacks. Section II.B reviews the FSIA's noncommercial tort exception and its other pre-JASTA exceptions, as well as the proposed cyberattack exception, and demonstrates why these routes provide an inadequate solution for U.S. victims of state-sponsored cyberattacks seeking to overcome foreign sovereign immunity.

A. *The Growing Threat and Scale of Cyberattacks*

State-sponsored cyberattacks are on the rise.[102] This rise comes at a time when there is both a growing list of possible ways for hackers to

---

("[T]here is no question that after hacking Mr. Abdulaziz's mobile phone, Defendants were aware or became aware of Mr. Khashoggi's contractual relationship with DAWN and his intent to use it as a platform to advocate for human rights and democratic reform in the Kingdom.").

100. See Jeremy Straub, Hackers Could Kill More People than a Nuclear Weapon, Live Sci. (Aug. 27, 2019), https://www.livescience.com/cyberattacks-could-kill-more-than-nuclear-attacks.html (on file with the *Columbia Law Review*) ("Unlike a nuclear weapon . . . the death toll from most cyberattacks would be slower. People might die from a lack of food, power or gas for heat or from car crashes resulting from a corrupted traffic light system."); see also supra notes 8–11 and accompanying text.

101. See, e.g., Cardozo, supra note 12 ("[Y]ou have no recourse under law if a foreign government . . . hacks into your car and drives it off the road, targets you for a drone strike, or even sends a virus to your pacemaker, as long as the government planned the attack on foreign soil.").

102. See Christina Lam, Note, A Slap on the Wrist: Combatting Russia's Cyber Attack on the 2016 U.S. Presidential Election, 59 B.C. L. Rev. 2167, 2199–200 (2018) ("[S]tate-sponsored cyber attacks are wreaking havoc with increasing regularity . . . ."); Powell, supra note 13, at 143 (noting "the exponential cyberattack growth made possible by foreign state actors," including a 250% increase in ransomware attacks in early 2017); see also David Wallace & Mark Visger, Responding to the Call for a Digital Geneva Convention: An Open Letter to Brad Smith and the Technology Community, J.L. & Cyber Warfare, Winter 2018, at 3, 8–9 ("[T]here is an increasing threat of State cyber-attacks."); Alex Kimani, State-Sponsored Cyberattacks Are on the Rise, Nasdaq (Feb. 21, 2019), https://www.nasdaq.com/articles/state-sponsored-cyberattacks-are-rise-2019-02-21 [https://perma.cc/6LVV-UU2E] ("There has been a surge of attacks on businesses and government agencies in the United States from Chinese and Iranian hackers . . . . [E]vidence suggests that these are not the work of isolated felons but rather are state-sponsored hacks that the two governments could be using for political expediency."). Cyberattacks are generally increasing in frequency,

employ malware[103] and increasing motivation for foreign states to use such malware over more traditional methods to harm perceived enemies.[104] Accordingly, state-sponsored cyberattacks will increasingly become a very real threat for certain U.S. nationals—such as dissidents like Kidane—in the near future.[105] This section lays out some of the possibilities of state-sponsored cyberattacks that exist now or are on the horizon, and then discusses why foreign states are ever more likely to resort to such cyberattacks.

1. *Growing Possibilities.* — Currently, the most frequent and well-known type of state-sponsored cyberattack involves foreign states simply stealing data or information.[106] The most famous example of this—at least in recent times—is probably the 2016 hacking of the DNC's network by Russian intelligence officers.[107] While such incidents are troubling, the harm that results from them is difficult to quantify; some may even laud such incidents as a step toward greater transparency, depending on the "victim."[108] Khashoggi's recent death shows, nevertheless, that states are willing to use stolen information to achieve far more tangible results—that

---

regardless of the culprit. See Nick Ismail, Worldwide, Targeted Cyber Attacks Are on the Rise—SonicWall, Info. Age (Mar. 26, 2019), https://www.information-age.com/targeted-cyber-attacks-rise-sonicwall-123481185 [https://perma.cc/A67R-NEUP] (detailing a study that found both "an escalation in the volume of cyber attacks" and "new, targeted cyber attacks and threat tactics used by cybercriminals").

103. See supra notes 8–11 and accompanying text; infra section II.A.1.

104. See infra section II.A.2.

105. As we have seen in *Doe v. Ethiopia*, this threat is already very real for some U.S. nationals. See supra section I.C.2.a.

106. See Straub, supra note 100 ("[M]ost of the well-known hacking incidents . . . have done little more than steal data.").

107. For a detailed account of this incident, see 1 Robert S. Mueller, III, DOJ, Report on the Investigation into Russian Interference in the 2016 Presidential Election 38–49 (2019), https://www.justice.gov/storage/report.pdf [https://perma.cc/J2UU-2479] [hereinafter Mueller Report] (finding that Russian intelligence officers "stole thousands of documents from the DCCC and DNC networks, including significant amounts of data pertaining to the 2016 U.S. federal elections"); Alvin Chang, How Russian Hackers Stole Information from Democrats, in 3 Simple Diagrams, Vox (July 16, 2018), https://www.vox.com/policy-and-politics/2018/7/16/17575940/russian-election-hack-democrats-trump-putin-diagram [https://perma.cc/G6V5-CFFR]. For information on the court case that resulted from this incident, see supra notes 57–59 and accompanying text. Malware was also used to disrupt the 2020 presidential election. See Samuel Haig, First Ransomware Attack in 2020 Election Hits Voting Infrastructure in Georgia, Cointelegraph (Oct. 23, 2020), https://cointelegraph.com/news/first-ransomware-attack-in-2020-election-hits-voting-infrastructure-in-georgia [https://perma.cc/UUD2-MQN9] ("According to Hall County spokesperson Katie Crumley, the county's voter signature database and voting precinct map were heavily impacted by [a ransomware attack].").

108. See, e.g., John J. Martin, Can Election Hacking Be Good for Democracy?, Fair Observer (June 13, 2017), https://www.fairobserver.com/region/north_america/russia-election-hacking-us-election-france-election-democracy-news-98156 [https://perma.cc/XUR5-L9NM] ("A more transparent electoral process creates more informed voters and deters corruption in political institutions, and the Russian leaks have actually achieved this.").

is, the physical harm or death of a targeted individual.[109] And the Khashoggi incident is far from unique.[110] If anything, it is merely a preview of a future where states will increasingly use spyware[111] to keeps tabs on dissidents, acquiring the necessary knowledge to determine whether, when, and where to strike them.

Perhaps more startling, foreign states are beginning to use malware to harm people by exploiting society's growing dependency on automated and autonomous technologies.[112] For instance, during heightened Russian–Ukrainian tensions in December 2015, a group of pro-Russian hackers managed to successfully disrupt energy company BlackEnergy's systems with malware, which left 225,000 Ukrainians without power.[113] This blackout occurred on a night with nearly subzero temperatures, resulting in "slowly sinking temperatures in thousands of homes, and [a] countdown until dead water pumps led to frozen pipes."[114] While this particular blackout only lasted a few hours,[115] a longer blackout in similar circumstances could easily result in deaths due to a lack of power or heat.[116] Such large-scale cyberattacks may very well become a common

---

109. See supra notes 98–99 and accompanying text.

110. See, e.g., Ravie Lakshmanan, iPhone Spyware Campaign Reportedly Targeted Uyghur Muslims for 2 Years, TNW (Sept. 2, 2019), https://thenextweb.com/security/2019/09/02/iphone-spyware-campaign-reportedly-targeted-uyghur-muslims-for-2-years [https://perma.cc/2JGK-MTXB] (detailing how the Chinese government allegedly used spyware to infect the phones of Uyghur Muslims, a minority ethnic group subject to persecution).

111. For a definition of spyware, see supra note 2.

112. It should be noted that there is technically a difference between "autonomous" technology and "automated" technology. "Autonomous" implies "acting alone or independently," whereas "automated" implies "control or operation by a machine." Stephen P. Wood, Jesse Chang, Thomas Healy & John Wood, The Potential Regulatory Challenges of Increasingly Autonomous Motor Vehicles, 52 Santa Clara L. Rev. 1423, 1425 n.2 (2012). Some argue that "automated" is a better descriptor for technology like self-driving cars, because some control over the technology is still exerted by a human (e.g., choosing the destination). See id. For the purposes of this Note, the catch-all phrase "automated and autonomous technology" is used to avoid such a debate, and should be interpreted as covering all technology that can function somewhat independently of human control.

113. See Ukraine Blackout—The Future of War, Cyber Sec. Intel. (Mar. 23, 2016), https://www.cybersecurityintelligence.com/blog/ukraine-blackout–the-future-of-war-1136.html [https://perma.cc/CVG7-C6EZ].

114. Andy Greenberg, How an Entire Nation Became Russia's Test Lab for Cyberwar, WIRED (June 20, 2017), https://www.wired.com/story/russian-hackers-attack-ukraine (on file with the *Columbia Law Review*).

115. See id.

116. See Straub, supra note 100 ("[T]he death toll from most cyberattacks would be slower. People might die from a lack of . . . power or gas for heat . . . .").

tactic of foreign states seeking to make a statement against opposing states or peoples.[117]

On a more individualized level, states can get even more creative. Hackers are now able to, for example, remotely target insulin pumps to withhold insulin from its user or dispense a lethal dose.[118] Hackers can also disrupt hospital computer systems to the point where a hospital has to halt the admission of new patients,[119] a predicament that can naturally lead to fatal consequences. And with the inevitable onset of commercially available self-driving cars,[120] hackers will be presented with new opportunities to directly harm individuals on the road. One report finds that hackers could very plausibly exploit the vulnerabilities of self-driving cars' systems in the future, causing them to, for instance, fail to recognize stop signs and run through them.[121] Thus, a state could, within a few decades, have the ability to remotely target and threaten the lives of individuals who are simply on their daily commute to work.

2. *Growing Motivation.* — In addition to growing methods to commit cyberattacks, states also have growing motivations to resort to the use of

---

117. But see Indra Overland, The Geopolitics of Renewable Energy: Debunking Four Emerging Myths, 49 Energy Rsch. & Soc. Sci. 36, 38 (2019) (arguing that the 2015 Ukrainian blackout was unique because of "unusually dilapidated infrastructure, a high level of corruption, a military conflict with Russia, and exceptional possibilities for Russian infiltration due to the historical linkages between the two countries").

118. Lily Hay Newman, These Hackers Made an App That Kills to Prove a Point, WIRED (July 16, 2019), https://www.wired.com/story/medtronic-insulin-pump-hack-app (on file with the *Columbia Law Review*); see also Tambini, supra note 10 (discussing the possibilities of "remotely switching off an insulin pump"). While such an attack currently "can't be executed from miles away," this tactic could very well progress to the point where such a remote attack is possible in the future. See Newman, supra.

119. See, e.g., Alabama Hospital System Halts Admissions Amid Malware Attack, supra note 9.

120. Even conservative estimates predict that it will take about "a decade or more to develop driverless cars that could travel anywhere, any time." Neal E. Boudette, Despite High Hopes, Self-Driving Cars Are 'Way in the Future', N.Y. Times (July 17, 2019), https://www.nytimes.com/2019/07/17/business/self-driving-autonomous-cars.html (on file with the *Columbia Law Review*).

121. See Miles Brundage, Shahar Avin, Jack Clark, Helen Toner, Peter Eckersley, Ben Garfinkel, Allan Dafoe, Paul Scharre, Thomas Zeitzoff, Bobby Filar, Hyrum Anderson, Heather Roff, Gregory C. Allen, Jacob Steinhardt, Carrick Flynn, Seán Ó hÉigeartaigh, Simon Beard, Haydn Belfield, Sebastian Farquhar, Clare Lyle, Rebecca Crootof, Owain Evans, Michael Page, Joanna Bryson, Roman Yampolskiy & Dario Amodei, The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation 20 (2018), https://img1.wsimg.com/blobby/go/3d82daa4-97fe-4096-9c6b-376b92c619de/downloads/1c6q2kc4v_50335.pdf [https://perma.cc/9G9U-BN4Q]. A self-driving car will have an image of a stop sign programmed into its system, and will be assigned a command corresponding with this image to stop upon seeing a stop sign. However, if a hacker alters the corresponding image of the stop sign, even with just "a few pixels," the self-driving car then runs the risk of not recognizing actual stop signs. See id. Such exploits could cause one's self-driving car to ignore basic traffic signals, creating a risk of immense harm to the passenger.

malware if they wish to threaten or harm an individual, rather than using more traditional methods to accomplish the same goal.[122] While traditional methods of attack are still used,[123] cybermethods offer three advantages that may explain their increasing usage by states:[124] lower cost, less accountability, and unparalleled opportunity. First, infecting a device with malware will typically cost less than engaging in actions that require a more physical presence[125]—the cost of infecting someone's phone with spyware is cheaper than physically locating their home and sending a state agent to break in to find documents containing similar information.

Second, it is far more difficult to hold a state accountable for its actions when said state attacks an individual through cybermethods rather than through traditional methods. As evidenced in *Doe v. Ethiopia*, courts—at least U.S. courts—present a high jurisdictional barrier that often prevents individuals from suing foreign states for torts that involve a cyber element.[126] Moreover, the nature of cyberattacks itself creates a high evidentiary barrier for plaintiffs. State-sponsored cyberattacks often involve third parties, which makes it difficult for victims to know whom to fully blame for the cyberattack against them.[127] In the case of Omar Abdulaziz,[128] for instance, Abdulaziz ultimately sued the NSO Group, a private company that supplied Saudi Arabia with the spyware used to track his conversations with Khashoggi, rather than Saudi Arabia directly.[129]

---

122. For the purpose of this Note, "traditional methods" refers to methods that do not employ malware, but instead require a more physical element to accomplish the desired goal.

123. See, e.g., Alexander Litvinenko: Profile of Murdered Russian Spy, BBC News (Jan. 21, 2016), https://www.bbc.com/news/uk-19647226 [https://perma.cc/5QTB-KZ7K] (detailing how Alexander Litvinenko, a fierce Russian dissident, was killed by poison administered in a cup of tea, likely at the request and approval of Russian President Vladimir Putin).

124. See supra note 102 and accompanying text.

125. See Danny Palmer, How Cybercriminals Are Still Snaring Victims Using Seven-Year-Old Malware, ZDNet (July 24, 2019), https://www.zdnet.com/article/how-cyber-criminals-are-still-snaring-victims-using-seven-year-old-malware [https://perma.cc/6TK4-EYM3] (detailing how "[s]ome of the most popular forms of malware" are cheap); cf. Alan Daley, Cyber Warfare Is Cheaper than Conventional Warfare, Am. Consumer Inst. Ctr. for Citizen Rsch. (Feb. 15, 2018), https://www.theamericanconsumer.org/2018/02/cyber-warfare-cheaper-conventional-warfare [https://perma.cc/3FDJ-UB4D] ("Today[,] [c]yber warfare provides Russia with a sharp edge at far less cost than armed forces equipped with missiles, tanks, fighter planes, and battleships.").

126. See supra section I.C.2.a.

127. See, e.g., *Doe I*, 189 F. Supp. 3d 6, 9–10 (D.D.C. 2016) (emphasizing that the Ethiopian government did not directly send Kidane the email that infected his phone with spyware; rather, the email was sent by a third party allegedly in London), aff'd, 851 F.3d 7 (D.C. Cir. 2017).

128. For background information on Omar Abdulaziz, see supra notes 98–99 and accompanying text.

129. See Kirkpatrick, supra note 11.

States like Saudi Arabia can hide behind third parties like the NSO Group, thus turning the third party into a scapegoat for the state's actions.

Finally, cybermethods present states with many opportunities that are unavailable when using traditional methods. The Chinese government, for instance, would not be able to spy on thousands of Uyghur Muslims in such a comprehensive manner without the use of spyware.[130] Furthermore, cybermethods grant states the ability to conduct attacks from the comfort of their own soil, which lessens both the potential of casualties and the likelihood of blowback should a particular attack fail.[131] The expansive scope and nonconfrontational nature of cyberattacks make them an attractive option for foreign states. Overall, foreign states these days have a variety of incentives to conduct cyberattacks in place of more traditional methods of attacks.

B. *Current Approaches Are Inadequate*

Post–*Doe v. Ethiopia*, U.S. nationals are left with few viable options to obtain redress in court should they become the victim of a state-sponsored cyberattack. Some argue, however, that the FSIA's noncommercial tort exception still provides a workable approach to bypassing state sovereign immunity in instances of cyberattacks, suggesting that other U.S. courts simply could adopt a less strict standard than that adopted by the D.C. Circuit.[132] Others advocate for the adoption of a cyberattack exception to the FSIA, which would automatically provide victims of state-sponsored cyberattacks with the ability to overcome foreign sovereign immunity.[133] Sections II.B.1 and II.B.2 respectively explain why the noncommercial tort exception and the other pre-JASTA FSIA exceptions do not present a feasible path for state-sponsored cyberattack victims seeking to hold the attacking state accountable. Furthermore, section II.B.3 discusses why the proposed cyberattack exception is not a viable solution.

1. *The Noncommercial Tort Exception Is a Lost Cause.* — Recent case developments suggest that cyberattack victims should not expect the "entire tort" rule to go away any time soon.[134] In *Doe v. Ethiopia*, for instance, Kidane argued that the court should apply an "essential locus"

---

130. See Lakshmanan, supra note 110.

131. Cf. Ian Thresher, Note, Can Armed Drones Halt the Trend of Increasing Police Militarization?, 31 Notre Dame J.L. Ethics & Pub. Pol'y 455, 459 (2017) (arguing that use of drones by police officers would "reduce the risk to officers by reducing the instances of confrontation").

132. See, e.g., Sergent, supra note 14, at 413–16; see also *Doe I*, 189 F. Supp. 3d at 22 (noting that Kidane argued that the district court should apply an "essential locus" test, which requires only that "'the injury and the act that proximately causes that injury' occur in the United States," treating the actions of hackers abroad as merely "collateral").

133. See supra note 13 and accompanying text.

134. For an explanation of the "entire tort" rule, see supra notes 40–44 and accompanying text.

test, under which a victim of a state-sponsored cyberattack would only need to prove that their injuries and the act that proximately caused them occurred in the United States.[135] As reasonable as this test may seem, the D.C. Circuit rejected it and applied the "entire tort" rule.[136] Some commentators, nevertheless, still believe that the noncommercial tort exception approach to state-sponsored cyberattacks is a salvageable approach.[137] However, as one commentator states, "If widely accepted by other circuits, the reasoning employed by the D.C. Circuit in *Doe* would make it practically impossible to bring cyber tort claims against foreign states."[138] Unfortunately, this fear is becoming a reality. Since *Doe v. Ethiopia*, district courts within both the Second and Ninth Circuits have adopted the D.C. Circuit's application of the "entire tort" rule to state-sponsored cyberattacks.[139] Moreover, the Second, Sixth, and Ninth Circuits and district courts within the Fifth Circuit have also adopted the "entire tort" rule in the application of the noncommercial tort exception to other types of cases.[140] This wide-spread adoption of the "entire tort" rule suggests that the D.C. Circuit's approach to the noncommercial tort exception in the context of cyberattack cases will soon become the norm, rather than an exception. Consequently, if a cyberattack victim wants to obtain redress against a foreign-state sponsor in a U.S. court, they should not expect to do so through the noncommercial tort exception.

2. *Other FSIA Exceptions Will Not Work for Cyberattack Victims.* — The FSIA continues to be the sole basis for obtaining jurisdiction over foreign states in U.S. courts.[141] Accordingly, if state-sponsored cyberattack victims want to sue the sponsoring state, they will have to do so under one of the FSIA's enumerated exceptions. Aside from the noncommercial tort exception, the traditional terrorism exception, and the JASTA exception,

---

135. See *Doe I*, 189 F. Supp. 3d at 22.

136. See *Doe II*, 851 F.3d 7, 12 (D.C. Cir. 2017).

137. One recent piece in particular argued that the D.C. Circuit's approach should be treated as an outlier, and that other circuits should adopt a more lenient standard under which the noncommercial tort exception's "occurring in the United States" language is read to simply mean that a foreign state "knew or should have known that the brunt of the injury would be felt in the United States." Sergent, supra note 14, at 416. Under this standard, a victim of state-sponsored cyberattacks would have jurisdiction so long as the sponsoring state (1) acted intentionally, (2) expressly aimed its cyberattack at the victim, and (3) knew or should have known that the victim's injuries would be felt in the United States. See id. (basing the standard on the effects tests employed by the Supreme Court in Calder v. Jones, 465 U.S. 783, 789–90 (1984)).

138. Id. at 413.

139. See DNC v. Russian Federation, 392 F. Supp. 3d 410, 427–28 (S.D.N.Y. 2019); Broidy Cap. Mgmt., LLC v. Qatar, No. CV 18-2421-JFW(Ex), 2018 WL 6074570, at *5 (C.D. Cal. Aug. 8, 2018).

140. See supra note 40.

141. OBB Personenverkehr AG v. Sachs, 136 S. Ct. 390, 393 (2015) (quoting Argentine Republic v. Amerada Hess Shipping Corp., 488 U.S. 428, 443 (1989)).

the FSIA has seven other exceptions.[142] This section provides a brief overview explaining why none of these exceptions will help a victim of a state-sponsored cyberattack find relief in U.S. court.

First, regarding the waiver exception, cyberattack victims would be able to sue a foreign-state sponsor only if the state waives its immunity explicitly or by implication.[143] Hence, in the unlikely circumstances that a foreign state that sponsored a cyberattack explicitly waives its immunity, the cyberattack's victims would be able to sue it. Assuming this is not the case though, the victims would need to find that the foreign state implicitly waived its sovereign immunity,[144] meaning they would essentially need to hope for the state to file a responsive pleading in their lawsuit without raising the defense of sovereign immunity.[145] While this certainly is a possibility,[146] such a circumstance occurs as a matter of luck; state-sponsored cyberattack victims should not rely on the sponsoring state making an error in its responsive pleading to be able to get redress. Overall, the waiver exception will likely not result in state-sponsored cyberattack victims obtaining jurisdiction over a foreign-state sponsor in a U.S. court.

The remaining exceptions are even less likely to help. The act of infecting a computer system or phone with malware is not "a commercial activity carried on in the United States,"[147] nor does it involve the exchange or acquisition of property.[148] A foreign-state sponsor of a cyberattack likely would not have entered into an agreement with the cyberattack victims to submit to arbitration to settle claims between them.[149] Cyberattack victims typically are not trying to "enforce a maritime

142. Stewart, supra note 31, at 47. For greater detail on these exceptions (particularly the waiver exception), see supra section I.B.

143. 28 U.S.C. § 1605(a)(1) (2018).

144. See id.

145. See In re Republic of Philippines, 309 F.3d 1143, 1151 (9th Cir. 2002) (quoting Joseph v. Off. of the Consulate Gen. of Nigeria, 830 F.2d 1018, 1022 (9th Cir. 1987)); see also supra note 34 and accompanying text. The other two circumstances of implied waiver mentioned in *In re Republic of Philippines*—a foreign state agreeing to arbitration in another country or a foreign state agreeing that a contract is governed by U.S. law—would not be applicable to a case involving a cyberattack. See 309 F.3d at 1151.

146. See, e.g., BAE Sys. Tech. Sol. & Servs., Inc. v. Republic of Korea's Def. Acquisition Program Admin., 884 F.3d 463, 473–74 (4th Cir. 2018) ("Korea participated in the litigation for over a year, including by filing a motion to dismiss and a responsive pleading, without giving any indication it asserted sovereign immunity. For that reason, it waived its immunity defense . . . .").

147. 28 U.S.C. § 1605(a)(2) (commercial activity exception).

148. See id. § 1605(a)(3)–(4) (expropriations and rights on certain property exceptions).

149. See id. § 1605(a)(6) (arbitration exception).

lien against a vessel or cargo of" a foreign-state sponsor.[150] Lastly, a sponsoring state would probably have no reason to sue victims of their cyberattack in a U.S. court, and therefore said victims would be afforded no opportunity to raise a counterclaim against said state.[151] Thus, if state-sponsored cyberattack victims hope to rely on the FSIA's exceptions to overcome a sponsoring state's sovereign immunity, their only chance now will be either the JASTA exception or a future amendment to the FSIA creating a cyberattack exception. As the next section demonstrates, the latter option is not a viable one.

3. *A Cyberattack Exception Will Not Happen Anytime Soon.* — Multiple critics of *Doe v. Ethiopia* have called for Congress to adopt an amendment to the FSIA that would strip sovereign immunity from foreign states in instances of state-sponsored cyberattacks.[152] These pushes for a cyberattack amendment, while laudable, will not provide any real solution for state-sponsored cyberattack victims, at least in the near future. First, one must appreciate the fact that Congress has become remarkably partisan in recent history.[153] This partisanship "has had negative effects on Congressional productivity."[154] Relying on Congress to provide any statutory relief for cyberattack victims is therefore already more likely than not to result in no relief whatsoever.

Despite the recent gridlock, proponents of the cyberattack exception hold up JASTA as evidence of Congress's willingness to expand the FSIA's exceptions. Sam Kleiner and Ambassador Lee Wolosky, for instance, assert that a cyberattack exception would apply the "same principles" that JASTA applies: holding foreign states accountable for attacking U.S. citizens.[155] Accordingly, proponents of the cyberattack exception may feel that

---

150. Id. § 1605(b) (maritime lien exception).

151. See id. § 1607 (counterclaim exception).

152. See supra note 13 and accompanying text.

153. See Clio Andris, David Lee, Marcus J. Hamilton, Mauro Martino, Christian E. Gunning & John Armistead Selden, The Rise of Partisanship and Super-Cooperators in the U.S. House of Representatives 3–12 (2015), https://journals.plos.org/plosone/article/file?id=10.1371/journal.pone.0123507&type=printable [https://perma.cc/939F-UVN9] (presenting evidence that "Congressional partisanship has been increasing exponentially for over 60 years"); Yvonne Wingett Sanchez & Ronald J. Hansen, Congress Declares Biden President After Mob Violence, Battles over AZ, PA Electors, AZ Central (Jan. 6, 2021), https://www.azcentral.com/story/news/politics/elections/2021/01/06/congress-accepts-arizona-presidential-electors-biden/6577024002 [https://perma.cc/A7NK-RHGB] (last updated Jan. 7, 2021) (noting that over one hundred Republican members of Congress objected to the certification of Arizona's and Pennsylvania's electors for Democratic President-elect Joe Biden and Vice President elect Kamala Harris).

154. Andris et al., supra note 153, at 10; see also Jeffrey D. Grynaviski, Congress Used to Pass Bipartisan Legislation—Will It Ever Again?, Conversation (Jan. 4, 2019), http://theconversation.com/congress-used-to-pass-bipartisan-legislation-will-it-ever-again-107134 [https://perma.cc/4AJZ-969N] ("[T]he 283 laws passed by the 112th were the fewest enacted by any Congress going back at least until the Korean War.").

155. See Kleiner & Wolosky, supra note 13.

because JASTA passed with overwhelming bipartisan support,[156] a cyberattack exception amendment should be able to acquire bipartisan support as well. JASTA was passed, however, under extraordinary circumstances, where the bill's fate determined whether the victims of the greatest terrorist attack on U.S. soil could sue Saudi Arabia for its contributions to said attacks.[157] JASTA was so intertwined with the September 11th attacks that some media outlets began to refer to it simply as the "Saudi 9/11 Bill."[158] In comparison, there has not been any major or universally mourned cyberattack against U.S. nationals that could garner a similarly large amount of support in Congress to pass a cyberattack exception amendment to the FSIA. If anything, the most famous state-sponsored cyberattack in recent times against a U.S. national/entity has been the 2016 DNC cyberattacks.[159] Given the partisan nature of that cyberattack,[160] an introduction of a bill calling for a cyberattack exception to the FSIA will likely be perceived as a Democratic Party ploy rather than a true attempt at justice for cyberattack victims.[161]

Even if a cyberattack exception amendment did get introduced as a bill to Congress with moderate bipartisan support, there is no telling how long the bill could take to pass. It took Congress seven years to pass JASTA despite its tremendous support, introducing the bill in 2009[162] and passing it in 2016.[163] State-sponsored cyberattack victims would thus be forced to potentially wait years before they could properly sue and obtain relief from the responsible country. This should not be regarded as an adequate solution.

---

156. See Steinhauer et al., supra note 71 (highlighting that JASTA passed 97-1 in the Senate and 348-77 in the House).

157. See 162 Cong. Rec. S2140 (daily ed. Apr. 19, 2016) (statement of Sen. Cornyn) ("JASTA is also important because it would help the victims of the 9/11 attacks achieve closure from that horrific tragedy.").

158. See, e.g., Jordan Fabian & Katie Bo Williams, How the White House Got Rolled on the Saudi-9/11 Bill, Hill (Sept. 30, 2016), https://thehill.com/homenews/administration/298635-how-the-white-house-got-rolled-on-the-saudi-bill [https://perma.cc/JVX2-AKQ3]; David A. Graham, Obama's Veto Threat on the Saudi 9/11 Bill, Atlantic (Sept. 12, 2016), https://www.theatlantic.com/politics/archive/2016/09/the-white-houses-veto-threat-on-the-saudi-911-bill/499694 (on file with the *Columbia Law Review*); Kim, supra note 70.

159. See supra note 107 and accompanying text.

160. See, e.g., Natasha Bertrand, The Trump Campaign Says Exploiting Hacked Emails Is Free Speech, Atlantic (Oct. 10, 2018), https://www.theatlantic.com/politics/archive/2018/10/trump-campaign-defends-wikileaks-use-hacked-dnc-emails/572587 (on file with the *Columbia Law Review*).

161. The recent dismissal of the DNC's lawsuit against Russia would only further support such a narrative. See DNC v. Russian Federation, 392 F. Supp. 3d 410, 428 (S.D.N.Y. 2019). A cyberattack exception amendment would likely be seen as a tool for Democrats to undo the district court's decision.

162. See 155 Cong. Rec. 33,162 (2009) (statement of Sen. Specter).

163. See supra section I.D.1.

III. JASTA AND THE PATH TO JURISDICTION

Part II details the growing threat of foreign states using cyberattacks to harm U.S. nationals, especially political dissidents like Kidane.[164] Part II also explains why such U.S. nationals likely cannot overcome foreign sovereign immunity under any of the FSIA exceptions that existed before JASTA—in particular, the noncommercial tort exception will not provide relief to future cyberattack victims given the increasing adoption of the D.C. Circuit's "entire tort" rule. Finally, Part II explores the possibility of future amendments to the FSIA that would create a cyberattack exception to foreign sovereign immunity, and ultimately concludes that such an amendment would not be a viable option in the current U.S. political climate. Consequently, this Part argues that the recently passed JASTA exception provides the best—and perhaps only[165]—opportunity for U.S. victims of state-sponsored cyberattacks to overcome sovereign immunity and obtain redress against their foreign-state cyberattackers in a U.S. court.

Section III.A discusses how the JASTA exception could be applied in cases of state-sponsored cyberattacks, particularly through the application of the four-element test adopted by the District Court for the Southern District of New York in *Terrorist Attacks XIII*.[166] Section III.B then addresses concerns that may arise when encouraging the use of the JASTA exception in cyberattack cases, including the separation of powers implications, the use of an expansive definition of "international terrorism," and the potential deviation from JASTA's legislative purpose.

A. *The JASTA Exception and State-Sponsored Cyberattack Cases*

The JASTA exception provides state-sponsored cyberattack victims with an unprecedented opportunity to sue their foreign-state cyberattackers in U.S. courts. This section overviews how the JASTA exception can and should be applied to state-sponsored cyberattack cases to allow these victims to overcome foreign sovereign immunity.[167] Section III.A.1 demonstrates how the differences between the JASTA exception and the terrorism exception and noncommercial tort exception allow cyberattack victims to circumvent challenges previously faced in a pre-JASTA world, such as the designated-sponsor-of-terrorism requirement and the "entire tort" rule. Section III.A.2 argues that many future incidents of state-

164. For an overview of Kidane's case in *Doe v. Ethiopia*, see supra section I.C.2.a.

165. The FSIA's exceptions provide the sole basis for obtaining jurisdiction over a foreign state in a U.S. court. OBB Personenverkehr v. Sachs, 136 S. Ct. 390, 393 (2015) (quoting Argentine Republic v. Amerada Hess Shipping Corp., 488 U.S. 428, 443 (1989)).

166. See supra notes 88–93 and accompanying text.

167. For an overview of the JASTA exception's components and requirements, see supra section I.D.

sponsored cyberattacks could satisfy the elements of the JASTA exception as put forth in *Terrorist Attacks XIII*.

1. *Distinguishing the JASTA Exception in the Cyberattack Context.* — The JASTA exception differs from both the terrorism exception and the noncommercial tort exception in two important respects;[168] these differences allow cyberattack victims to overcome two specific barriers previously faced when attempting to sue a foreign state. First, whereas the terrorism exception requires the foreign state being sued to be designated as a state sponsor of terrorism by the U.S. federal government,[169] the JASTA exception has no such limitation. If the DNC, therefore, viewed Russia's hacking into its computer network as a form of cyberterrorism,[170] the JASTA exception affords the DNC an actual opportunity to sue Russia, regardless of Russia's lack of designated-sponsor-of-terrorism status.[171] Overall, the JASTA exception permits U.S. nationals to potentially sue any foreign state, irrespective of how the federal government classifies them.

More importantly, the tortious act component of the JASTA exception does not require a tortious act committed by a foreign state to have taken place entirely in the United States, as is required under the noncommercial tort exception in many federal circuit and district courts.[172] Instead, the JASTA exception explicitly states that the physical

---

168. For greater detail on these differences, see supra section I.D.2.

169. See 28 U.S.C. § 1605A(a)(2)(A)(i)(I) (2018).

170. See Shelly A. Sanford & Meredith Drukker Stratigopoulos, Democrats and Republicans Seek Federal Jurisdiction over Cybercrimes by Foreign Actors in *DNC v. Russian Federation* and *Broidy Capital Mgmt. v. State of Qatar*, J.L. & Cyber Warfare, Fall 2019, at 1, 26–27. Admittedly, the DNC likely did not view Russia's hacking as an act of terrorism, given that the DNC did not mention "JASTA" or "terrorism" in its court filings in DNC v. Russian Federation, 392 F. Supp. 3d 410, 428 (S.D.N.Y. 2019). Cf. Final Reply Brief of Appellant at 8, *Doe II*, 851 F.3d 7 (D.C. Cir. 2017) (No. 16-7081), 2016 WL 7449231 (stating that for JASTA to apply, a tort must "involv[e] terrorism, which of course is not the case here"). This Note does not disagree that certain forms of state-sponsored cyberattacks do not rise to the level of an act of terrorism, perhaps including the data breach that occurred in the DNC case and the act of monitoring Kidane's internet activities that occurred in *Doe v. Ethiopia*. See supra section I.C.2. Naturally, such cases might be precluded from the JASTA exception given that the exception requires an "act of international terrorism in the United States." 28 U.S.C. § 1605B(b)(1). This, however, is a matter that would be disputed based on the facts on a case-by-case basis through the application of the definition of "international terrorism" as stated in 18 U.S.C. § 2331 (2018). Consequently, this Note is not concerned with whether specific past incidents of cyberattacks would qualify as an act of terrorism. Rather, it argues simply that JASTA at the very least affords future state-sponsored cyberattack victims the opportunity to plead that the cyberattack conducted against them was an act of terrorism, rather than being immediately precluded by a designated-sponsor-of-terrorism requirement, which gives such victims a greater opportunity to overcome foreign sovereign immunity than previously afforded.

171. See Cong. Rsch. Serv., supra note 65, at 1–2 (excluding Russia from the list of designated state sponsors of terrorism).

172. See supra note 40. While the Supreme Court has never officially commented on the "entire tort" rule, more federal circuit and district courts will likely continue to adopt

location of the tortious act does not matter.[173] In fact, the only two JASTA components that must occur domestically appear to be the act of international terrorism and the plaintiff's physical injury or property damage.[174] This distinction is crucial for state-sponsored cyberattack victims, given the transboundary nature of the distribution of malware.[175] Under the JASTA exception, cyberattack victims will no longer face an "entire tort" barrier.

If Kidane attempted to sue Ethiopia under the JASTA exception,[176] for example, he could have argued that the initial act of sending FinSpy spyware to his electronic device constituted the tortious act required by JASTA, making it irrelevant that the spyware had likely been sent from London.[177] He could then have argued that the actual act of the spyware monitoring his electronic activity constituted the "act of international terrorism" in the United States required by JASTA. This argument, of course, is not guaranteed to win, and would turn heavily on the facts, as section III.A.2 discusses. The JASTA exception, however, provides at the very least a plausible opportunity for state-sponsored cyberattack victims to overcome foreign sovereign immunity, whereas the terrorism and noncommercial tort exceptions leave such victims with an insurmountable barrier. This gives U.S. nationals—particularly political dissidents now

---

the rule if confronted with a noncommercial tort case. See supra notes 138–140 and accompanying text (noting how, at least in the cyberattack context, federal courts are increasingly adopting the "entire tort" approach to the noncommercial tort exception).

173. 28 U.S.C. § 1605B(b) ("A foreign state shall not be immune from the jurisdiction of the courts of the United States . . . for physical injury to person or property or death occurring in the United States and caused by . . . a tortious act . . . *regardless where the tortious act or acts of the foreign state occurred*." (emphasis added)).

174. Id. Although the statute only states that the act of international terrorism must occur "in the United States," rather than entirely in the United States, it seems safe to presume that courts will restrict their interpretation of the JASTA exception to require the entire act to have occurred in the United States. Though the *Terrorist Attacks XIII* court did not interpret this statutory language, the noncommercial tort exception contains the exact same "in the United States" language. Id. § 1605(a)(5). Accordingly, courts will likely adopt an "entire act" rule for the JASTA exception similar to how many have adopted the "entire tort" rule for the noncommercial tort exception. See supra note 40.

175. See *Doe II*, 851 F.3d at 10 ("Ethiopia's placement of the FinSpy virus on Kidane's computer . . . began outside the United States. It thus cannot be said that the entire tort occurred in the United States.").

176. Kidane's final reply brief in *Doe II* suggests that this would be an unlikely scenario. See Final Reply Brief of Appellant, supra note 170, at 8 (stating that for JASTA to apply, a tort must "involv[e] terrorism, which of course is not the case here"). This Note does not entirely disagree that the JASTA exception would be difficult to employ in a case such as Kidane's where no physical injury or property damage seemingly occurred. There is, nevertheless, at least an argument to be made that the JASTA exception could have been used to obtain jurisdiction in *Doe v. Ethiopia* if it were determined that the FinSpy spyware internally damaged Kidane's electronic devices. See infra section III.A.2.a; see also Sanford & Stratigopoulos, supra note 170, at 26–27.

177. For an overview of the facts in *Doe v. Ethiopia*, see supra section I.C.2.a.

living in the United States seeking protection from certain regimes—a fighting chance to hold foreign states accountable for conducting cyberattacks against them, as foreign states under JASTA can no longer shield themselves behind a lack of a designated-sponsor-of-terrorism status or the physical location of their hackers.

2. *Applying the* Terrorist Attacks XIII *Elements to State-Sponsored Cyberattacks*. — This section now analyzes the application of the four elements of the JASTA exception, as presented in *Terrorist Attacks XIII*, to state-sponsored cyberattack cases.[178] These elements include (1) physical injury to person or property, (2) an act of international terrorism in the United States and a tortious act by a foreign state or state actor, (3) causation, and (4) damages.[179] While not every state-sponsored cyberattack will meet all four elements, this section makes the case that many instances can do so, especially those that result in physical injury to the victim.

a. *Physical Injury to Person or Property*. — To successfully invoke the FSIA's JASTA exception, a U.S. victim of a state-sponsored cyberattack must first demonstrate "physical injury to a person or property or death occurring in the United States."[180] The easiest way to satisfy this element would be through a showing of concrete injury to oneself or one's property. If a plaintiff, for instance, became injured by a tornado strike in Texas because a cyberattack shut off the plaintiff's local emergency sirens,[181] this would be an obvious case of physical injury that occurred in the United States. While such extreme and clear-cut cases are currently rare in the cyberattack context, they could very well become increasingly common with the rise of automated and autonomous technologies.[182]

As of now, though, the majority of state-sponsored cyberattacks likely result in more intangible injuries, caused either through data breaches or spyware usage.[183] The 2015–2016 DNC data breach, for instance, did not result in physical injury to any individuals, nor did it cause any concrete

178. This Note specifically focuses on the four-element test developed by the *Terrorist Attacks XIII* court because *Terrorist Attacks XIII* is the only case thus far that has substantively analyzed the JASTA exception. The court's four-element test is therefore likely to influence how other federal courts interpret JASTA in the future.

179. *Terrorist Attacks XIII*, 298 F. Supp. 3d 631, 642 (S.D.N.Y. 2018); see also supra section I.D.3.

180. *Terrorist Attacks XIII*, 298 F. Supp. 3d at 642.

181. See Catalin Cimpanu, Hacked Tornado Sirens Taken Offline in Two Texas Cities Ahead of Major Storm, ZDNet (Mar. 18, 2019), https://www.zdnet.com/article/hacked-tornado-sirens-taken-offline-in-two-texas-cities-ahead-of-major-storm [https://perma.cc/XSJ7-FL8C].

182. See supra notes 112–121 and accompanying text.

183. See Kayla Matthews, Spookier Than Ghosts: 5 of the Biggest Cyberattacks We Saw in 2019, vXchnge (Oct. 31, 2019), https://www.vxchnge.com/blog/biggest-cyberattacks-2019 [https://perma.cc/2W7E-8BN7] (noting that all five of the "biggest" cyberattacks of 2019 were data breaches).

injury to DNC property.[184] Such cases may have a difficult time satisfying the first element of the JASTA exception. Some cybersecurity legal experts have, however, emphasized that "[c]omputers, phones, and storage mechanisms can . . . be physically damaged through hacking, requiring significant repairs."[185] This physical damage can be caused by, among other things, overheating hardware.[186] The DNC itself complained in its lawsuit against Russia that it incurred "over a million dollars in physical damage" to its electronic equipment due to the data breach.[187] Consequently, state-sponsored cyberattack victims such as the DNC or Kidane may still be able to prove physical property damage, and thus satisfy the first element of the JASTA exception, if they can demonstrate internal hardware damage to their electronic devices that were targeted by malware.[188]

b. *Tortious Act and Act of International Terrorism.* — The next element—and perhaps the most crucial element—that a state-sponsored cyberattack victim must satisfy under the JASTA exception can be separated into two parts: (1) "an act of international terrorism in the United States," and (2) a tortious act by a foreign state or actor of said state committed while acting within the scope of their office, employment, or agency, regardless of where the act occurred.[189] The tortious act requirement should not present a high barrier for cyberattack victims, as cyberattacks often involve some form of intentional tort.[190] Some courts,

---

184. See Mueller Report, supra note 107, at 38–49 (mentioning no incident of physical damage or injury).

185. Sanford & Stratigopoulos, supra note 170, at 26.

186. Alan Zeichick, Malware Can Damage Hardware—Intentionally and Accidentally, Zonic (Dec. 26, 2017), https://www.zonicgroup.com/malware-can-damage-hardware-intentionally-accidentally [https://perma.cc/C858-MD4G] ("It's possible that malware could somehow damage the device inadvertently, perhaps by messing up the firmware and bricking the machine, or by overloading the processor and memory to the point where it overwhelms on-board cooling mechanisms."). But see Kevin Williams, Can Malware Physically Damage a Computer?, Smarter MSP (Dec. 19, 2018), https://smartermsp.com/can-malware-physically-damage-a-computer [https://perma.cc/E7HR-7TY9] (quoting one homeland security expert as saying that there are only a few foreign states that would be interested in spending enough money to physically harm hardware through the usage of malware).

187. Sanford & Stratigopoulos, supra note 170, at 26.

188. But cf. Intel Corp. v. Hamidi, 71 P.3d 296, 308 (Cal. 2003) (rejecting the argument that spamming Intel's servers with emails qualified as trespass to chattels because spamming did not constitute physical property damage).

189. 28 U.S.C. § 1605B(b) (2018); *Terrorist Attacks XIII*, 298 F. Supp. 3d 631, 642 (S.D.N.Y. 2018).

190. See Jay P. Kesan & Carol M. Hayes, Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace, 25 Harv. J.L. & Tech. 429, 496 (2012) ("It is most likely that an action against [a cyberattacker] would fall under some intentional tort theory."); see also Meiring de Villiers, Free Radicals in Cyberspace: Complex Liability Issues in Information Warfare, 4 Nw. J. Tech. & Intell. Prop. 13, 59 (2005) ("An intervening crime or intentional tort, as is often the case in a cyber attack, normally cuts off the liability of the first tortfeasor.").

for example, have decided cyberattack cases on a trespass-to-chattels theory.[191] In *Doe v. Ethiopia*, Kidane raised an intrusion-upon-seclusion tort claim, which covers "[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns."[192] State-sponsored cyberattack victims overall should not face too much difficulty demonstrating that the sending or installation of malware onto their electronic devices constitutes some form of tortious behavior. And while the JASTA exception also requires any tortious act committed by a foreign state official, employee, or agent to have been committed "within the scope of his or her office, employment, or agency,"[193] *Terrorist Attacks XIII* suggests that this may also be easily satisfied. In *Terrorist Attacks XIII*, the district court found that two defendants acted within the scope of their agency simply because they "follow[ed] instructions from more senior officials."[194] While the district court was specifically applying New York state law, some other states have adopted similarly broad definitions of "scope of employment" or "scope of agency."[195] Other states, however, do not have any clear definitions of such terms for civil cases,[196] which could present hurdles for those looking to sue a foreign state under the JASTA exception in those states' jurisdictions. Largely though, state-sponsored cyberattack victims should not have too much trouble establishing that their cyberattack constitutes a tortious act under the JASTA exception.

State-sponsored cyberattack victims will face a somewhat more challenging task demonstrating that the domestic portion of their cyberattack constitutes an "act of international terrorism in the United States."[197] To do this, they must satisfy the three elements of international terrorism as defined in 18 U.S.C. § 2331(1), covering any criminal activity

---

191. See, e.g., eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1071–72 (N.D. Cal. 2000) (finding that eBay was likely to prevail on the merits of its trespass-to-chattels claim when bots had exceeded the scope of eBay's consent by downloading large quantities of auction information); CompuServe Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1027 (S.D. Ohio 1997) (finding that defendant's trespass-to-chattels cause of action applied to spam).

192. *Doe II*, 851 F.3d 7, 10 (D.C. Cir. 2017) (alteration in original) (internal quotation marks omitted) (quoting Bailer v. Erie Ins. Exch., 687 A.2d 1735, 1380–81 (Md. 1997)).

193. 28 U.S.C. § 1605B(b)(2).

194. *Terrorist Attacks XIII*, 298 F. Supp. 3d at 650.

195. See, e.g., Mary M. v. City of Los Angeles, 814 P.2d 1341, 1344 (Cal. 1991) ("Tortious conduct that violates an employee's official duties or disregards the employer's express orders may nonetheless be within the scope of employment.").

196. See, e.g., Crystal M. Ovsak, Case Comment, Master and Servant—Incompetency of Servant: North Dakota Adopts the Restatement's "Scope of Employment" Test and Explores the Phenomenon of "Transference"—*Nelson v. Gillette*, 1997 N.D. 205, 571 N.W.2d 332, 75 N.D. L. Rev. 137, 140–41 (1999) (noting that North Dakota has not defined "scope of employment" for civil law purposes).

197. 28 U.S.C. § 1605B(b)(1).

that (1) involves violent acts or "acts dangerous to human life," (2) appears to have proper intent, and (3) either occurs outside the United States or "transcend[s] national boundaries."[198] This difficulty will not arise out of any limiting case law, but rather out of a lack of case law applying § 2331(1) to instances of cyberattacks.[199] Therefore, if state-sponsored cyberattack victims wish to characterize their cyberattack as international cyberterrorism, they will need to look to how the language of § 2331(1) has been applied in other contexts.[200]

First, while cyberattacks themselves may not be "violent acts," they certainly could qualify as "acts dangerous to human life."[201] Such acts need not directly threaten human life, but may instead simply "create circumstances in which there is real danger to [nationals'] safety and wellbeing."[202] Some courts have been willing to adopt a very liberal interpretation of this language, going so far as to include the provision of funds to militant organizations under the umbrella of "acts dangerous to human life."[203] Consequently, it is no stretch to imagine that many cyberattacks could also fall under this umbrella. Using malware to shut down a power plant in the dead of winter could endanger human lives by subjecting people to freezing temperatures.[204] On a more individual level, the act of distributing secret information after a data breach could endanger human life if it contains personal information about an individual that then

198. 18 U.S.C. § 2331(1) (2018). For an overview of which types of intent satisfy the second element, see infra notes 209–211 and accompanying text.

199. See Paul N. Stockton & Michele Golabek-Goldman, Prosecuting Cyberterrorists: Applying Traditional Jurisdictional Frameworks to a Modern Threat, 25 Stan. L. & Pol'y Rev. 211, 259 (2014) ("Given the international community's failure to achieve a consensus on the definition of terrorism, attempts to achieve universal agreement on a cyberterrorism definition may prove similarly futile.").

200. In many of these contexts, the definition of "domestic terrorism" might be the language being applied. Domestic terrorism's first two elements under § 2331, however, are nearly identical to the first two elements of international terrorism. See 18 U.S.C. § 2331(5). Therefore, the language should be interpreted the same either way.

201. 18 U.S.C. § 2331(1)(A).

202. Matthew James Enzweiler, Note, Swatting Political Discourse: A Domestic Terrorism Threat, 90 Notre Dame L. Rev. 2001, 2029 (2015) (asserting that swatting may be regarded as an act dangerous to human life).

203. See Boim v. Holy Land Found. for Relief & Dev., 549 F.3d 685, 690 (7th Cir. 2008) (en banc) ("Giving money to Hamas, like giving a loaded gun to a child (which also is not a violent act), is an 'act dangerous to human life.'"). But see Rothstein v. UBS AG, 708 F.3d 82, 87, 97 (2d Cir. 2013) (holding that defendant's aiding and abetting of Hezbollah and Hamas through its transfer of money to Iran did not proximately cause plaintiffs' injuries); Geoffrey Sant, So Banks Are Terrorists Now?: The Misuse of the Civil Suit Provision of the Anti-Terrorism Act, 45 Ariz. St. L.J. 533, 568–69 ("There is no logical link between giving a child a gun and donating funds other than the majority's simple assertion that these are the same thing.").

204. See Greenberg, supra note 114 (describing the 2015 BlackEnergy shutdown as resulting in "slowly sinking temperatures in thousands of homes, and [a] countdown until dead water pumps led to frozen pipes").

subjects them to potential targeting and harassment.[205] Even if these acts qualify as international terrorism though, questions may arise as to whether they occurred "in the United States."[206] This is, however, precisely why the JASTA exception is so conducive to allowing state-sponsored cyberattack victims to overcome foreign sovereign immunity. Because the initial act of sending malware from abroad can be regarded as a distinct tortious act under JASTA's framework,[207] the actual act of malware functioning on an electronic device in the United States can be separately regarded as the required act of international terrorism. The act of sending malware from abroad is akin to planning and developing a bomb in a foreign country, and the malware actually performing its functions on a device in the United States is akin to the bomb actually being set off in a U.S. city.[208]

Whether a state-sponsored cyberattack satisfies the second and third elements of international terrorism will be heavily fact dependent. The second element can be satisfied if the foreign state's cyberattack appears to have been intended to (1) intimidate or coerce a civilian population, (2) influence government policy by intimidation or coercion, or (3) affect government conduct by mass destruction, assassination, or kidnapping.[209] The objective nature of the "appear[s] to be intended"[210] language of this element reduces the hurdle for state-sponsored cyberattack victims, as they need not inquire into the foreign state's actual intent.[211] Consequently, one could imagine all three possible forms of intent appearing in different types of cyberattack cases. Using spyware to monitor political dissidents' activity could appear to be intended to intimidate a civilian population because doing so could be meant to "strike fear into [them] to deter them from exercising their rights."[212] Stealing a political party's information through a data breach to influence a U.S. election could appear to be

205. See Mueller Report, supra note 107, at 40 (describing the data captured in the DNC data breach to include "passwords, internal communications between employees, banking information, and sensitive personal information").

206. 28 U.S.C. § 1605B(b)(1) (2018).

207. See supra notes 190–196 and accompanying text.

208. Cf. Letelier v. Republic of Chile, 488 F. Supp. 665, 665, 674 (D.D.C. 1980) (holding that simply because the car bomb used to assassinate Orlando Letelier in Washington, D.C., was entirely planned in Chile did not completely absolve Chile of liability for the tortious injury sustained in the United States).

209. 18 U.S.C. § 2331(1)(B) (2018).

210. Id.

211. See, e.g., In re Chiquita Brands Int'l, Inc., 284 F. Supp. 3d 1284, 1307 (S.D. Fla. 2018) (describing the language "appears to be intended" as an objective intent requirement).

212. People v. Morales, 982 N.E.2d 580, 585 (N.Y. 2012) (quoting S. Rep. No. 95-701, at 30 (1978), as reprinted in 1978 U.S.C.C.A.N. 3973, 3999).

intended to coercively influence U.S. government policy.[213] Finally, in extreme circumstances, cyberattacks could appear to be intended to affect government conduct through, for example, mass destruction caused by tampering with U.S. infrastructure[214] or assassination caused by using malware to tamper with future automated and autonomous technologies.[215] Such possibilities demonstrate the broad leeway granted under the second element of § 2331(1) to state-sponsored cyberattack victims.[216]

The third element of international terrorism can be satisfied if the cyberattack either occurs "primarily outside the territorial jurisdiction of the United States" or "transcend[s] national boundaries."[217] For the purposes of the JASTA exception, only the "transcend national boundaries" route will be possible for cyberattack victims since the JASTA exception requires the act of international terrorism to have occurred "in the United States."[218] Under § 2331(1), a state-sponsored cyberattack can transcend national boundaries through either the means by which the foreign state accomplished it, the persons intended to be intimidated or coerced (if there are any) by the cyberattack, or the "locale" in which the cyberattack's perpetrator operates.[219] This element should be fairly straightforward for state-sponsored cyberattack victims to fulfill based on the high likelihood that a state-sponsored cyberattack will have been planned and implemented initially in a different country.[220] Moreover, the very fact that a cyberattack is sponsored by a foreign state should be enough to transcend

---

213. See, e.g., Mueller Report, supra note 107, at 44–49 ("In order to expand its interference in the 2016 U.S. presidential election, the GRU units transferred many of the documents they stole from the DNC . . . to WikiLeaks.").

214. See, e.g., supra notes 113–114 and accompanying text (describing a similar incident in Ukraine).

215. See, e.g., Brundage et al., supra note 121, at 20 (describing how self-driving cars' ability to obey traffic signs can be hindered through the manipulation of "a few pixels").

216. Some critics argue that this leeway may be too broad, thus putting innocent organizations at risk of being classified as terrorists. See, e.g., Erwin Chemerinsky, Losing Liberties: Applying a Foreign Intelligence Model to Domestic Law Enforcement, 51 UCLA L. Rev. 1619, 1624 (2004) ("This is an incredibly broad definition. Many lawful protests might be seen as trying to coerce or intimidate government or civilian populations."). For further discussion on such criticisms, see infra section III.B.2.

217. 18 U.S.C. § 2331(1)(C) (2018).

218. 28 U.S.C. § 1605B(b)(1) (2018). State-sponsored cyberattack victims could possibly still bring forth a claim against a foreign state under the JASTA exception for a cyberattack that occurred "primarily outside" the United States if courts interpret JASTA's "in the United States" language as meaning only partially in the United States. This seems unlikely, however, given how courts have applied the "entire tort" rule to the noncommercial tort exception, which has the same "in the United States" language. See supra note 174.

219. 18 U.S.C. § 2331(1)(C).

220. Otherwise, there would not be much reason to conduct the cyberattack in the first place. See supra note 131 and accompanying text (describing the remote nature of cyberattacks as one of their major benefits).

national boundaries.[221] Characterizing a cyberattack as an act of international terrorism under the JASTA exception will thus present a challenging, but attainable, task for many U.S. victims of state-sponsored cyberattacks.

c. *Causation and Damages.* — Should a state-sponsored cyberattack victim successfully satisfy the first two elements of the JASTA exception, they will still need to establish causation and damages.[222] These latter two elements, however, should not be too prohibitive for cyberattack victims. Regarding causation, cyberattack victims need not demonstrate "but for" causation under the *Terrorist Attacks XIII* approach; rather, they simply need to show that a foreign state's support of the cyberattack had "some reasonable connection" to the damages they suffered.[223] Under this approach, cyberattack victims need only show two factors to prove causation. First, the victim must show that the foreign state's sponsoring of the cyberattack was a "substantial factor" in the sequence of events that resulted in the victim's injury,[224] which should not be too difficult to prove when a foreign state is partially planning or funding the cyberattack. Second, the cyberattack victim's injury must have been "reasonably foreseeable or anticipated as a natural consequence" of the foreign state's actions.[225] Given that state-sponsored cyberattacks are by definition intentional,[226] satisfying this second factor should be simple. Regarding damages, so long as a U.S. victim of a state-sponsored cyberattack can demonstrate proper injury,[227] they will have a cause of action for damages.[228]

Overall, whether a U.S. victim of a state-sponsored cyberattack can satisfy the four elements of the JASTA exception, as established in *Terrorist Attacks XIII*, will turn largely on the facts. Many victims, however, could very

---

221. See 140 Cong. Rec. 4704 (1994) (describing activities that receive support or direction from foreign government as having enough of a "substantial international character" to transcend national boundaries).

222. *Terrorist Attacks XIII*, 298 F. Supp. 3d 631, 642 (S.D.N.Y. 2018).

223. Id. at 645 (quoting Owens v. Republic of Sudan, 864 F.3d 751, 794 (D.C. Cir. 2017)). The *Terrorist Attacks XIII* court's rejection of "but for" causation was influenced by JASTA's legislative history. See id.; see also 162 Cong. Rec. S2845 (daily ed. May 17, 2016) (statement of Sen. Cornyn) (stating that courts should look to the causation analyses of specific cases, such as *Owens*, that do not use "but for" causation when applying the causation element of the JASTA exception). This rejection of "but for" causation is further supported by the fact that the stated purpose of JASTA is to provide civil remedies against "indirect[]" material support of terrorist activities. See Justice Against Sponsors of Terrorism Act, Pub. L. No. 114-222, sec. 2(b), 130 Stat. 852, 853 (2016).

224. *Terrorist Attacks XIII*, 298 F. Supp. 3d at 646 (internal quotation marks omitted) (quoting *Owens*, 864 F.3d at 794).

225. Id.

226. See supra notes 190–192 and accompanying text.

227. See supra section III.A.2.a.

228. See 18 U.S.C. § 2333(a) (2018).

plausibly meet all four elements, and thus should be able to use JASTA to their advantage to hold their foreign-state attacker accountable in a U.S. court.

B. *Arguments Against the Use of JASTA*

This section addresses a variety of arguments that can be made against encouraging the use of the JASTA exception by state-sponsored cyberattack victims. Section III.B.1 addresses the concern that using JASTA will result in a violation of separation of powers. Section III.B.2 addresses the fear that relying on the JASTA exception indirectly supports its overly broad definition of "international terrorism." Section III.B.3 addresses the argument that using the JASTA exception in the cyberattack context runs counter to JASTA's original legislative purpose.

1. *Separation of Powers.* — After Congress passed JASTA, some critics claimed that the Act conflicted with constitutional separation of powers, arguing that the judiciary would end up intruding upon the executive's foreign affairs powers.[229] President Obama even vetoed JASTA under the belief that it would take matters of terrorism "out of the hands of national security and foreign policy professionals and plac[e] them in the hands of private litigants and courts."[230] Such criticisms, however, ignore two key factors. First, the FSIA itself was passed by Congress to "depolitici[ze] sovereign immunity" by transferring determinations of sovereign immunity from the executive to the judiciary.[231] JASTA, therefore, seems to fall straight in line with how determinations of foreign sovereign immunity have been separated between the two branches over the past four decades.[232] Second, U.S. courts have historically been hesitant to encroach upon the realm of foreign affairs. Courts will often deem cases as being

---

229. See, e.g., Katherine Holcombe, Note, JASTA Straw Man? How the Justice Against Sponsors of Terrorism Act Undermines Our Security and Its Stated Purpose, 25 Am. U. J. Gender Soc. Pol'y & L. 359, 380–87 (2017) ("Fighting terrorism and the exercise of diplomatic relations are traditionally within the purview of the executive branch . . . ."); Nawaf Obaid, This Congressional Act Threatens US National Security, CNN, https://www.cnn.com/2017/08/29/opinions/overturn-jasta-opinion-obaid/index.html [https://perma.cc/XC7H-F2J8] (last updated Aug. 29, 2017) ("JASTA intrudes on the President's exclusive foreign affairs powers . . . .").

230. Message to the Senate Returning Without Approval the Justice Against Sponsors of Terrorism Acts, 2016 Daily Comp. Pres. Doc. 1 (Sept. 23, 2016). Congress overrode President Obama's veto. See Steinhauer et al., supra note 71.

231. Feldman, supra note 23, at 304–05.

232. This naturally raises nondelegation concerns: Perhaps the FSIA unconstitutionally delegates executive powers to the judiciary. However, the nondelegation doctrine falls well outside the realm of this Note. For now, it seems sufficient to say that "the nondelegation . . . doctrine[] [is] rarely enforced by the judiciary." Edward T. Swaine, The Constitutionality of International Delegations, 104 Colum. L. Rev. 1492, 1500 (2004).

nonjusticiable if they involve foreign policy questions.[233] Accordingly, it seems highly unlikely that a court would decide a case under the JASTA exception if the questions raised in said case clearly fall within the executive's powers.

2. *Overly Broad Definition of International Terrorism.* — Another major concern with JASTA is that it employs a dangerously broad definition of "international terrorism."[234] Since the passage of the USA PATRIOT Act,[235] critics have expressed fears that 18 U.S.C. § 2331(5)'s broad definition of "domestic terrorism"[236]—a definition almost identical to that of "international terrorism"[237]—could be used to target protest groups or activist organizations.[238] These fears remain valid today, where newly proposed bills could potentially result in the prosecution of anti-fascist groups as domestic terrorists.[239] For this reason, critics may believe that litigants should not be encouraged to take advantage of the overly broad definition of "international terrorism" used by JASTA, as doing so would legitimize it. This definition, however, is not going away any time soon, as there remains bipartisan support for continued use of the current definitions of both domestic and international terrorism.[240] Consequently, the best means of countering these expansive definitions may be to use them in a manner that assists, rather than oppresses, political minorities. Given that some of the most vulnerable targets of state-sponsored cyberattacks include political dissidents,[241] using the JASTA exception to characterize state-sponsored cyberattacks as acts of terrorism could be, at the very least, a productive use of U.S. national security law that actually empowers civil liberties for a change.

3. *JASTA's Legislative Purpose.* — One final concern that may arise when encouraging state-sponsored cyberattack victims to invoke the JASTA exception is JASTA's legislative purpose. It is no secret that Congress passed JASTA for one specific purpose: to allow September 11th

233. See, e.g., Banco Nacional de Cuba v. Sabbatino, 376 U.S. 398, 439 (1964) (refusing to determine the validity of a foreign government's actions).

234. For an overview of the definition, see supra notes 197–221 and accompanying text.

235. USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272.

236. See 18 U.S.C. § 2331(5) (2018).

237. See supra note 200.

238. See, e.g., Chemerinsky, supra note 216, at 1624; ACLU, supra note 79.

239. See Harsha Panduranga & Faiza Patel, "Domestic Terrorism" Bills Create More Problems than They Solve, Just Sec. (Aug. 28, 2019), https://www.justsecurity.org/65998/domestic-terrorism-bills-create-more-problems-than-they-solve [https://perma.cc/NZ3N-4ZWC].

240. See id. (noting bipartisan support for a "domestic terrorism" prosecution bill); Steinhauer et al., supra note 71 (noting bipartisan support for JASTA).

241. See supra notes 46, 98 and accompanying text.

victims' families to sue Saudi Arabia.[242] Therefore, using JASTA to allow state-sponsored cyberattack victims to overcome foreign sovereign immunity may seem like a far cry from JASTA's original legislative purpose. However, despite being branded as the "Saudi 9/11 Bill,"[243] Congress's intent when passing JASTA is far from clear. The stated purpose of JASTA, for instance, is to "provide civil litigants with the broadest possible basis . . . to seek relief" when foreign states "provide[] material support" to terrorist activities.[244] Nothing in this stated purpose appears to preclude cyberterrorism from qualifying as "terrorist activities"; if anything, seeking to provide "the broadest possible basis" suggests that U.S. nationals should feel encouraged to bring forward unique claims of international terrorism to U.S. courts under the JASTA exception.

Moreover, there is no guarantee that courts will even look to legislative purpose when interpreting JASTA. While the *Terrorist Attacks XIII* court did look to JASTA's legislative history to determine whether to apply "but for" causation,[245] the Supreme Court has instructed courts to "not resort to legislative history to cloud a statutory text that is clear."[246] Rather, the Court "normally interprets a statute in accord with the ordinary public meaning of its terms at the time of its enactment."[247] And if courts were to rely simply on the plain meaning of JASTA's text, the JASTA exception appears perfectly applicable to instances of state-sponsored cyberattacks: For instance, the contemporary meaning of "acts of international terrorism" should at this point incorporate cyberactivities under its umbrella,[248] and "tortious acts" have long included cyberactivities in the U.S. legal system.[249] Consequently, JASTA's legislative purpose would likely present no barrier to applying JASTA in a cyberattack context.

CONCLUSION

Foreign states have greater power than ever to employ malware to target and harm political rivals, dissidents, and perceived enemies in the

---

242. See 164 Cong. Rec. S6316 (daily ed. Sept. 26, 2018) (statement of Sen. Blumenthal) (stating that the enactment of JASTA earned September 11th victims' families "the right to have their day in court").

243. See supra note 158 and accompanying text.

244. Justice Against Sponsors of Terrorism Act, Pub. L. No. 114-222, sec. 2(b), 130 Stat. 852, 853 (2016).

245. See *Terrorist Attacks XIII*, 298 F. Supp. 3d 631, 645 (S.D.N.Y. 2018).

246. Ratzlaf v. United States, 510 U.S. 135, 147–48 (1994).

247. Bostock v. Clayton County, 140 S. Ct. 1731, 1738 (2020).

248. See, e.g., DOJ, FBI, Terrorism: 2002–2005, at 46 (2005), https://www.fbi.gov/file-repository/stats-services-publications-terrorism-2002-2005-terror02_05.pdf (on file with the *Columbia Law Review*) (including cyberterrorism in an early-2000s report on terrorist activities in the United States); Cyberterrorism, Merriam-Webster, https://www.merriam-webster.com/dictionary/cyberterrorism [https://perma.cc/P476-ARVS] (last visited Sept. 4, 2020) (defining cyberterrorism as "terrorists activities").

249. See supra notes 190–192 and accompanying text.

United States. These foreign states, however, often escape justice in U.S. courts under the principle of sovereign immunity codified in the FSIA. Current approaches to overcoming sovereign immunity in cases of state-sponsored cyberattacks have proven to be futile. Accordingly, future victims of state-sponsored cyberattacks should look to the recently passed JASTA, which lacks many of the limitations found in other FSIA exceptions to sovereign immunity. If a victim is harmed by a state-sponsored cyberattack, the JASTA exception could very well provide them with jurisdiction over the sponsoring state. This would result in better accountability against foreign states that seek to harm U.S. nationals behind the comfort of a keyboard.