Catholic University Journal of Law and Technology

Volume 30
Issue 1 *Fall 2021*

Article 5

2021

The FSIA and Cyberspace: Could HACT be the Answer?

Ritika Malkani
Catholic University of America (Student)

THE FSIA AND CYBERSPACE: COULD HACT BE THE ANSWER?

Ritika Malkani[*]

What if another country could launch an attack against you while you were in the United States, and you could do nothing about it in an American court of law?

Imagine sitting in your living room opening an email from a friend, when suddenly, without your knowledge, malware embedded in the email installed a program that allowed the government of another country to spy on everything you do for years. A program that can extract private passwords from your computer and record every call and email you send. Then, you try to get justice for this tortious conduct in court, but because the command-and-control server where the malware originated is located abroad, the American justice system cannot help you.

Unfortunately, for one plaintiff who goes by the pseudonym Kidane, this was not merely a hypothetical, but his reality.[1] To add fuel to the fire, defense counsel in Kidane's case did not deny that he had been wiretapped, and claimed that the Defendant could not even be sued for more extreme conduct like "mailing a letter bomb into the United States to assassinate an opponent," or hacking a self-driving car, causing a horrific crash, simply because this conduct could be done from abroad.[2]

Despite the rapid advancement of internet related technologies, and the

[*] *Juris Doctor* Candidate, Columbus School of Law, 2022; *Comparative and International Law Institute Concentration* Candidate, 2022; *The Catholic University Journal of Law and Technology*, Note and Comment Editor, 2021-2022; Bachelor of Arts, University of Miami, 2017. Many thanks to my expert reader Professor Geoffrey Watson, to my fellow JLT Vol. 30 Executive Board members, and to my family, friends, and fiancé, who have supported me throughout my academic career.

1 Doe v. Fed. Democratic Republic of Eth., 189 F. Supp. 3d 6, 9 (D.D.C. 2016).

2 *U.S. Court Hears Appeal in Ethiopia's State-sponsored Illegal Spying Case*, AFRICA TIMES (Feb. 4, 2017), https://africatimes.com/2017/02/04/u-s-court-hears-appeal-in-ethiopia-state-sponsored-illegal-spying-case/.

proliferation of cybercrimes, a foreign state's tortious actions using these tools from afar do not currently result in legal consequences, as these cases are barred from being brought in American courts by jurisdictional considerations set out in the Foreign Sovereign Immunities Act ("FSIA" or the "Act").[3]

Existing law is insufficient in addressing several issues regarding cyberspace. The FSIA is an example of such existing law.[4] In summary, the Act immunizes foreign states from the jurisdiction of American courts, provided certain exceptions to immunity do not apply.[5] One such exception is the non-commercial tort exception,[6] which several courts have interpreted as referring to torts occurring 'wholly' within the United States.[7] This gives rise to a gap in the legal framework regarding cybercrime when a portion of the crime occurs abroad (i.e., a foreign state hacks into the electronic devices of U.S. citizens from abroad), since the victim in the United States is left with no avenue of redress in a U.S. court.[8] The Homeland and Cyber Threat Act ("HACT") purports to close this gap by amending Title 28 of the U.S. Code, "to allow claims against foreign states for unlawful computer intrusion and other purposes."[9] Is this sufficient to address the existing problem? Could a wholly new cyber convention be necessary?

Section II of this article will examine the existing framework: immunity from jurisdiction under international law and the FSIA. Section III will discuss the existing problems, including attribution of conduct and defenses to attribution of conduct, and Section IV considers potential solutions, namely: the HACT, expansion of the terrorism exception of the FSIA, and overruling the entire tort doctrine as applied to the FSIA's non-commercial tort exception.

I. THE EXISTING FRAMEWORK

A. Immunity From Jurisdiction Under International Law

Before the FSIA was enacted, the doctrine of foreign sovereign immunity was

---

3 Foreign Sovereign Immunities Act (FSIA), 28 U.S.C. § 1604 (2016).
4 *Id.*
5 *Id.*
6 § 1605(a)(5).
7 Doe v. Fed. Democratic Republic of Eth., 189 F. Supp. 3d 6, 19 (D.D.C. 2016).
8 John B. Bellinger, III et al., *Can You Be Sued Under the Foreign Sovereign Immunities Act?: A Primer for Foreign Governments and Their Agencies*, ARNOLD&PORTER (Jan. 26, 2021), https://www.arnoldporter.com/en/perspectives/publications/2021/01/can-you-be-sued-under-fsia.
9 H.R. 4189, 116th Cong. (2019).

developed through the common law.[10] States generally followed one of two theories of jurisdictional immunity of foreign states: (1) the absolute (classical) theory, whereby a sovereign could not, unless it consented, be made a respondent in a court of another sovereign, or (2) the restrictive theory, where the immunity of a sovereign was recognized with regard to its public acts, but not its private acts.[11]

The United States initially followed the absolute theory of immunity, according to foreign states immunity from suit unless the executive branch objected. [12] In 1812, in *Schooner Exchange v. McFaddon*, Chief Justice Marshall of the Supreme Court wrote:

> Jurisdiction of the nation within its own territory is necessarily exclusive and absolute. It is susceptible of no limitation not imposed by itself… this full and absolute territorial jurisdiction being alike the attribute of every sovereign would not seem to contemplate foreign sovereigns nor their sovereign rights as its objects.[13]

A definitive break in U.S. practice regarding immunity only came about in 1952, promulgated by a letter from the Department of State's[14] acting legal advisor, Jack B. Tate, to the Acting U.S. Attorney General Philip B. Perlman.[15] This would later become known as "the Tate letter."[16] The Tate letter purported to adopt the restrictive approach, abandoning the theory of absolute immunity, and allowing plaintiffs to sue foreign governments for their public (i.e., commercial) acts for the first time. In support of this decision, and upon examination of other state's practices, Tate wrote "little support has been found… for continued full acceptance of the absolute theory of sovereign immunity" and "for these reasons it will hereafter be the Department's policy to follow the restrictive theory of sovereign immunity in the consideration of requests of foreign governments for a grant of sovereign immunity."[17]

This had little effect at first in federal court, as the executive branch continued

---

10 James E. Berger & Charlene Sun, *Sovereign Immunity: A Venerable Concept in Transition?*, 27 INT'L LITIG. Q. at 1 (May 3, 2011), *as reproduced by* PAUL HASTINGS, https://webstorage.paulhastings.com/Documents/PDFs/1902.pdf.

11 *See generally* LORI FISLER DAMROSCH & SEAN D. MURPHY, INTERNATIONAL LAW CASES AND MATERIALS (7th ed. 2019) (describing both theories of jurisdictional immunity of foreign states and their backgrounds).

12 Berger & Sun, *supra* note 10.

13 Schooner Exch. v. McFaddon, 11 U.S. (7 Cranch) 116, 136–37 (1812).

14 The Department of State is "the agency responsible for interpreting immunities to be accorded under international law." DAMROSCH & MURPHY, *supra* note 11, at 807.

15 Berger & Sun, *supra* note 10. *See* DAMROSCH & MURPHY, *supra* note 11, at 807 (explaining that the Department of State is "the agency responsible for interpreting immunities to be accorded under international law").

16 Berger & Sun, *supra* note 10.

17 DAMROSCH & MURPHY, *supra* note 11, at 809–10.

to decide questions of sovereign immunity, and courts continued to abide by their suggestions of immunity.[18] However, this did "throw immunity determinations into some disarray, as foreign nations often placed diplomatic pressure on the State Department, and political considerations sometimes led the Department to file suggestions of immunity in cases where immunity would not have been available under the restrictive theory."[19]

After the Tate Letter, determinations of immunity started to involve two separate branches of government, the judicial branch and the executive branch, instead of just the executive branch, which made the entire process more difficult and less clear. Despite this dilution of power, the executive branch was frequently called upon to appear in court to give its opinion on determinations of grants of immunity, a burden which added to the pressure to "enact a statutory scheme that would provide legally defined standards for courts to apply rather than ad hoc interventions by the executive."[20]

The FSIA was born out of these challenges.

B. The United States' Adoption of the FSIA

Congress enacted the Foreign Sovereign Immunities Act in 1976, which codified the restrictive theory of immunity set out in the Tate letter. [21] It is a statute that prohibits U.S. courts from having jurisdiction over cases against foreign states, unless one of several enumerated exceptions apply.[22] Essentially, the Act presumes immunity, and an exception to it could rebut the presumption. It is important to note that the FSIA's application is required in every cause of action against a foreign sovereign, because subject-matter jurisdiction depends on it.[23]

1. Exclusivity

One of the first issues that U.S. courts grappled with after the FSIA was passed was whether the Act provided the exclusive basis for suing foreign states in U.S. courts.[24] The United States Supreme Court ruled on this issue in *Argentine Republic v. Amerada Hess Shipping Corp.*, holding in favor of FSIA's

---

18 Republic of Austria v. Altmann, 541 U.S. 677, 690 (2004).
19 *Id.*
20 DAMROSCH & MURPHY, *supra* note 11, at 812.
21 28 U.S.C. § 1604 (2016).
22 *See id.*
23 Argentine Republic v. Amerada Hess Shipping Corp., 488 U.S. 428, 434–35 (1989).
24 DAMROSCH & MURPHY, *supra* note 11, at 812.

exclusivity.[25] In the opinion, Chief Justice Rehnquist wrote "we think that the text and structure of the FSIA demonstrate Congress' intention that the FSIA be the sole basis for obtaining jurisdiction over a foreign state in our courts."[26]

This has been reaffirmed many times since then, and is no longer a contentious issue.[27] One such reaffirmation is the Second Circuit's decision in *Weinstein v. Islamic Republic of Iran*, stating that if applied, the FSIA "provides the exclusive basis for subject matter jurisdiction over all civil actions against foreign state defendants, and therefore for a court to exercise subject matter jurisdiction over a defendant the action must fall within one of the FSIA's exceptions to foreign sovereign immunity."[28]

2. Retroactivity

Another issue facing U.S. courts after the enactment of the FSIA was whether the Act applied retroactively to a foreign state's actions taken prior to the enactment. Three cases decided in the 1980s[29] established that prior to the Tate letter, the FSIA could not be retroactively applied.[30] However, after those decisions were handed down, there was still debate about whether the FSIA applied retroactively to the time period between the Tate letter and the enactment of the FSIA.

Before the FSIA was enacted, jurisdiction over foreign states was treated as diversity jurisdiction under the U.S. Code.[31] Congress eliminated that portion of the Code upon enactment of the FSIA, since the FSIA became the only basis for jurisdiction over foreign states.[32] This raised a problem, because "by removing foreign sovereign defendants from the diversity jurisdiction statute, a prospective FSIA would have the effect of preventing suits prior to 1976 from being heard in U.S. courts . . . [creating] 'a blank period' from 1952-1976 when

---

25 *Amerada Hess Shipping Corp.*, 488 U.S. at 443.

26 *Id.* at 434.

27 *Id.* at 434, 443 (1989); Weinstein v. Islamic Republic of Iran, 609 F.3d 43, 47 (2d Cir. 2010); Saudi Arabia v. Nelson, 507 U.S. 349, 355 (1963).

28 *Weinstein*, 609 F.3d at 47.

29 Carl Marks & Co. v. Union of Soviet Socialist Republic, 665 F. Supp. 323 (S.D.N.Y. 1987), *aff'd*, 841 F.2d 26 (2d Cir.), *cert. denied*, 108 S. Ct. 2874 (1988); Jackson v. China, 596 F. Supp. 386, *aff'd*, 74 F.2d 1490 (11th Cir. 1986), *cert. denied*, 480 U.S. 917 (1987); Slade v. Mex., 617 F. Supp. 351 (D.D.C. 1985), *aff'd*, 790 F.2d 163 (D.C. Cir. 1986), *cert denied*, 479 U.S. 1032, *reh'g denied*, 480 U.S. 912 (1987).

30 Michael E. Jansen, *FSIA Retroactivity Subsequent to the Issuance of the Tate Letter: A Proposed Solution to the Confusion*, 10 NW. J. INT'L L. & BUS. 333, 335 (1989).

31 Adam K. A. Mortara, *The Case Against Retroactive Application of the Foreign Sovereign Immunities Act of 1976*, U. CHI. L. REV. 253, 261 (2001).

32 *Id.* at 261–62.

the U.S. had adopted, but not codified, the restrictive theory of sovereign immunity."[33]

The Supreme Court discussed this issue in *Landgraf v. USI Film Products*, noting strong historical opposition toward and presumption against retroactive statutory application. [34] Commentary accompanying the *Landgraf* decision opines that:

> The presumption against statutory retroactivity is founded upon elementary considerations of fairness dictating that individuals should have an opportunity to know what the law is and to conform their conduct accordingly. It is deeply rooted in this Court's jurisprudence and finds expression in several constitutional provisions, including, in the criminal context, the *Ex Post Facto* Clause. In the civil context, prospectivity remains the appropriate default rule unless Congress has made clear its intent to disrupt settled expectations.[35]

Additionally, the *Landgraf* Court referenced the Constitution's prohibition on bills of attainder, the due process clause, and the Fifth Amendment as supporting this presumption, and to demonstrate concern surrounding retroactive statutes.[36]

After *Landgraf* was decided, the Supreme Court in *Austria v. Altmann* struggled with whether or not the FSIA applied to pre-enactment conduct, since "Landgraf's default rule does not definitively resolve this case."[37] The Court considered that the FSIA was not just a jurisdictional statute, but that it codified substantive standards of foreign sovereign immunity.[38] The Court also looked to the purpose of the presumption against retroactivity—"the aim of the presumption is to avoid unnecessary post hoc changes to legal rules on which parties relied in shaping their primary conduct", and the purpose of the FSIA, which has "never been to permit foreign states and their instrumentalities to shape their conduct in reliance on the promise of future immunity from suit in United States courts. Rather, such immunity "reflects current political realities and relationships . . ." acting to prevent the inconvenience of litigating suits abroad, as a matter of comity.[39]

The *Altmann* Court ultimately determined that the FSIA indeed applied to petitioner's 1948 actions, citing "clear" evidence of Congress' intent for the Act to apply to such actions, pointing to the preamble of the Act, which the Court

---

33 *Id.* at 262.
34 Landgraf v. USI Film Prods., 511 U.S. 244, 279 (1994).
35 *Id*. at 245.
36 *Id.* at 266.
37 Republic of Austria v. Altmann, 541 U.S. 677, 696 (2004).
38 *Id.* at 691.
39 *Id.* at 696.

interpreted as "Congress intended courts to resolve all such claims 'in conformity with the principles set forth' in the Act, regardless of when the underlying conduct occurred."[40]

Some scholars take the view that the FSIA should not be applied retroactively, since there is no express provision regarding retroactivity within it.[41] Others believe retroactivity is inappropriate as applied to substantive statutes (versus purely jurisdictional statutes, which the FSIA is not), and "that a pre-1952 application of FSIA would prejudice antecedent rights."[42] This, however, does not seem to be the view of the U.S. Supreme Court.

In May of 2020, the Supreme Court in *Opati v. Republic of Sudan* ruled for plaintiffs who sought compensation from Sudan for its participation in terrorist attacks bombing U.S. embassies in Tanzania and Kenya in 1998.[43] These acts occurred prior to the amendment of the FSIA's terrorism exception allowing punitive damages, however, the Court found *Altmann* compelling in deciding for the plaintiffs and allowed retroactive application of the statute; "because foreign sovereign immunity is a gesture of grace and comity, *Altmann* reasoned, it is also something that may be withdrawn retroactively without the same risk to due process and equal protection principles that other forms of backward-looking legislation can pose."[44] The Court determined that the new provisions both explicitly authorized punitive damages, and allowed the provision to be used to remedy past acts of terrorism.[45]

While the *Opati* and *Altmann* decisions are quite narrow, they are a step toward Congress' potential ability to pass future legislation that applies retroactively, therefore imposing liability on previously immune sovereigns.

3. Judicial Interpretation: What Is A 'Foreign State'?

In order for the FSIA to apply, a state must be considered a 'foreign state'. After the FSIA was enacted, courts struggled with what this meant. The FSIA section 1603(a) defines the term "foreign state" to include "a political subdivision of a foreign state or an agency or instrumentality of a foreign state."[46]

---

40 *Id.* at 697–98.
41 Mortara, *supra* note 31, at 260.
42 *Id.* at 254, 261.
43 Opati v. Republic of Sudan, 140 S. Ct. 1601, 1604 (2020).
44 *Id.* at 1608. *See Altmann*, 541 U.S. at 689.
45 *Opati*, 140 S. Ct. at 1609.
46 28 U.S.C. § 1603(a) (2016).

i. Agency or Instrumentality

FSIA Section 1603(b) provides that an "agency or instrumentality of a foreign state" is one:

> (1) which is a separate legal person, corporate or otherwise, and
>
> (2) which is an organ of a foreign state or political subdivision thereof, or a majority of whose shares or other ownership interest is owned by a foreign state or political subdivision thereof, and
>
> (3) which is neither a citizen of a State of the United States as defined in section 1332 (c) and (e) of this title, nor created under the laws of any third country.[47]

According to the FSIA's legislative history, generally, an entity that meets the definition of "agency or instrumentality of a foreign state could assume a variety of forms, organizations, such as a shipping line or an airline, a steel company, a central bank, an export association, a governmental procurement agency, or a department or ministry which acts and is su[e]able in its own name."[48]

There is some additional guidance regarding the definition of "agency or instrumentality of a foreign state" within case law. For example, in considering whether foreign officials acting in an official capacity are considered a "foreign state" within the FSIA, the United States Supreme Court in *Samantar v. Yousef* stated that:

> Petitioner argues that either 'foreign state,' . . . or 'agency or instrumentality,' . . . could be read to include a foreign official. Although we agree that petitioner's interpretation is literally possible, our analysis of the entire statutory text persuades us that petitioner's reading is not the meaning that Congress enacted.[49]

The Court reasoned that the terms used within the FSIA, specifically "organ," and "separate legal person" do not typically apply to natural persons or individuals.[50] The Court also reasoned that Congress could have, if it had wanted to, explicitly stated that the FSIA applies to foreign officials because "elsewhere in the FSIA Congress expressly mentioned officials when it wished to count their acts as equivalent to those of the foreign state, which suggests that officials are not included within the unadorned term 'foreign state.'"[51]

Other examples include *Singh v. Caribbean Airlines, Ltd*., a case in which the

---

47 § 1603(b).

48 *Foreign Sovereign Immunities Act*, U.S. DEP'T OF STATE, http://travel.state.gov/content/travel/en/legal/travel-legal-considerations/internl-judicial-asst/Service-of-Process/Foreign-Sovereign-Immunities-Act.html (last visited Nov. 4, 2021).

49 Samantar v. Yousuf, 560 U.S. 305, 314–15 (2010).

50 *Id.* at 315.

51 *Id.* at 317.

Eleventh Circuit found that an airline "qualifie[d] as an agency or instrumentality of Trinidad and Tobago,"[52] and *Dole Food Co. v. Patrickson*, where the Supreme Court upheld a lower court holding that "a subsidiary of an instrumentality is not itself entitled to instrumentality status" with regard to the FSIA.[53]

C. FSIA Exceptions

If a claim falls outside of the listed exceptions to the FSIA, a U.S. court lacks both subject-matter and personal jurisdiction, rendering the defendant immune.[54] When one of the exceptions applies, however, "the foreign state shall be liable in the same manner and to the same extent as a private individual under like circumstances."[55] The listed exceptions include: waiver,[56] commercial activities,[57] "property taken in violation of international law,"[58] "succession or gift or rights in immovable property situated in the United States,"[59] non-commercial torts,[60] maritime liens,[61] and terrorism.[62] Specifically with regard to cybercrime, relevant exceptions include the non-commercial tort exception, and the terrorism exception.[63]

1. FSIA: Non-Commercial Tort Exception

The non-commercial tort exception of the FSIA is laid out in section 1605, which states in pertinent part:

> (a) A foreign state shall not be immune from the jurisdiction of courts of the United States or of the States in any case—
> (5) …money damages are sought against a foreign state for personal injury or death, or damage to or loss of property, occurring in the United States and caused by the tortious act or omission of that foreign state or of any official or employee of that foreign state while

---

52 Singh v. Caribbean Airlines Ltd., 798 F.3d 1355, 1358 (11th Cir. 2015).
53 Dole Food Co. v. Patrickson, 538 U.S. 468, 473 (2003).
54 David P. Stewart, *The Foreign Sovereign Immunities Act: A Guide for Judges*, FED. JUD. CENTER (2013), https://www.fjc.gov/sites/default/files/2014/FSIAGuide2013.pdf.
55 28 U.S.C. § 1606 (2016).
56 § 1605(a)(1).
57 § 1605(a)(2).
58 § 1605(a)(3).
59 § 1605(a)(4).
60 § 1605(a)(5).
61 § 1605(b).
62 28 U.S.C. § 1605A(a)(1)–(2) (2008).
63 John J. Martin, *Hacks Dangerous to Human Life: Using Jasta to Overcome Foreign Sovereign Immunity in State-Sponsored Cyberattack Cases*, 121 COLUM. L. REV. 119, 122–23, 126 (2021).

> acting within the scope of his office or employment; except this paragraph shall not apply to— (A) any claim based upon the exercise or performance or the failure to exercise or perform a discretionary function regardless of whether the discretion be abused, or (B) any claim arising out of malicious prosecution, abuse of process, libel, slander, misrepresentation, deceit, or interference with contract rights.[64]

This provision allows American plaintiffs to sue and claim damages against foreign states in U.S. courts with regard to the foreign state's tortious actions against them.[65] The Supreme Court in *Amerada Hess*, explained that "Congress' primary purpose in enacting [section] 1605(a)(5) was to eliminate a foreign state's immunity for traffic accidents and other torts committed in the United States, for which liability is imposed under domestic tort law." [66] However, despite Congress' hope that enacting the FSIA would solve issues raised by common law, subsequent judicial interpretation of the Act has brought up new issues of its own.[67]

i. Judicial Interpretation: The Entire Tort Doctrine

An example of an issue raised by judicial interpretation of the FSIA appears in the context of the non-commercial tort exception, which the Supreme Court and "every federal court of appeals to have considered the question" considers to apply to only torts occurring entirely within the United States.[68] This has come to be known as 'the entire tort doctrine.'

In addressing what is meant by "entirely within the United States," the D.C. Circuit Court in *Schermerhorn v. State of Israel* "held recently that 'the United States' is 'limited to the geographic territories and waters of the United States' and does not include US-flagged ships on the high seas."[69] Additionally, the Supreme Court in *Amerada Hess* denied jurisdiction over a dispute occurring 5,000 miles off U.S. shores under the FSIA non-commercial tort exception, construing the phrase "continental and insular" in the statute "to restrict the definition of United States to the continental United States and those islands that are part of the United States or its possessions; any other reading would render

---

64 28 U.S.C. § 1605(a)(5)(A)–(B) (2016).
65 Bellinger, III et al., *supra* note 8.
66 Argentine Republic v. Amerada Hess Shipping Corp., 488 U.S. 428, 439–40 (1989).
67 Judi L. Abbott, The Noncommercial Torts Exception to the Foreign Sovereign Immunities Act, 9 FORDHAM INT'L L. J. 134, 141 (1985).
68 Bellinger, III et al., *supra* note 8.
69 Bellinger, III et al., *supra* note 8; Schermerhorn v. State of Israel, 876 F.3d 351, 355–56 (D.C. Cir. 2017).

this phrase nugatory."[70] The *Amerada Hess* Court went on to say that Congress could have, if it had intended to, placed the high seas within the statute, and thus applied the "the canon of construction which teaches that legislation of Congress, unless contrary intent appears, is meant to apply only within the territorial jurisdiction of the United States."[71]

ii. Judicial Interpretation: Direct Effects

The concept of 'direct effects' opines that a tort occurring abroad could have consequences that are felt within the United States. However, this concept does not apply to the non-commercial tort exception because "[a]lthough the statutory provision is susceptible of the interpretation that only the effect of the tortious action need occur here, where Congress intended such a result elsewhere in the FSIA it said so more explicitly."[72]

The Court in *Amerada Hess* explains this point, articulating that the case would not have come out differently even if the "petitioner's tort had had effects felt in the United States," and notes that Congress intentionally used explicit language in section 1605(a)(2) regarding "direct effects," yet chose not to include this phrase in section 1605(a)(5) (i.e. the non-commercial tort exception), indicating that section 1605(a)(5) "covers only torts occurring within the territorial jurisdiction of the United States."[73]

In a more recent case, *Doe v. Federal Democratic Republic of Ethiopia*, the D.C. District Court upheld the interpretation of "occurring in the United States" to mean occurring *wholly* within the United States, invoking the "entire tort" doctrine relied on by several other courts.[74] The Court reiterated that "the fact that the plaintiff incurred an *injury* in the United States, or that the 'alleged tort may have had *effects* in the United States,' is insufficient to waive sovereign immunity."[75]

The *Doe* case is a recent interpretation of the "entire tort" doctrine, and what this article's initial hypothetical is based on. The facts are as follows: Plaintiff "Kidane," a Maryland resident who was born in Ethiopia, and who sought asylum in the United States, fell victim to a computer program called FinSpy when he opened an email on his computer which had allegedly been sent from

---

70 *Amerada Hess Shipping Corp.*, 488 U.S. at 440.

71 *Id.* (quoting Foley Brothers v. Filardo, 336 U.S. 281, 285 (1949)).

72 Asociacion de Reclamantes v. United Mexican States, 735 F.2d 1517, 1524 (D.C. Cir. 1984).

73 *Amerada Hess Shipping Corp.*, 488 U.S. at 441; *see* 28 U.S.C. § 1605(a)(5) (2016).

74 Doe v. Fed. Democratic Republic of Eth., 189 F. Supp. 3d 6, 19 (D.D.C. 2016).

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

Ethiopia to a third party and forwarded to Kidane.[76] The email had an attachment that, once opened, caused a "clandestine client program to be surreptitiously downloaded onto his computer."[77] Kidane alleged that FinSpy intercepted and recorded some of his emails, web searches, and Skype calls.[78] He filed a two-claim complaint, one pursuant to the Wiretap Act, and the other under Maryland tort law. [79] Ethiopia moved to dismiss.[80] The Court concluded that the Wiretap Act did not create a cause of action against a foreign state for interceptions of certain communication and granted Ethiopia's motion to dismiss count one.[81]

Then the *Doe* Court considered the FSIA, and whether it barred Kidane from asserting the tort claim against Ethiopia.[82] In its discussion, the Court stated that:

> Although it is well-settled that the non-commercial tort exception "covers only torts occurring within the territorial jurisdiction of the United States," it is unclear how that rule applies to the instant case, in which the alleged intrusion involves the infiltration of Kidane's computer located at his home in Maryland, yet no agent or employee of Ethiopia is alleged to have ever set foot in the United States in connection with that tort.[83]

It then looked to committee reports and proponents of the legislation to aid them in concluding the legislative intent of Congress was to limit liability to torts carried out in the United States.[84] The fact that Congress' primary purpose in enacting the FSIA was to create liability for foreign states regarding torts like traffic accidents committed in the United States also supported their determination.[85]

The Court acknowledged that had Ethiopia sent a human to Kidane's house to install the same device, Kidane would have an avenue of remedy under FSIA,[86] however, the Court stated "technology has simply rendered the human agent obsolete."[87] Additionally, the Court conceded that Ethiopia's argument that the entire tort did not occur within the U.S. since the tortfeasors were located

---

76 *Id.* at 9.
77 *Id.* at 10.
78 *Id.*
79 *Id.* at 10–11.
80 *Id.*at 11.
81 *Id.* at 19–20.
82 *Id.* at 16–25.
83 *Id.* at 18.
84 *Id.* at 19.
85 *Id.*
86 *Id.* at 20.
87 *Id.*

overseas was incomplete because it "fails to grapple with the modern world in which the Internet breaks down traditional conceptions of physical presence."[88]

Despite this, the *Doe* Court concluded that Ethiopia's view was more compelling upon the consideration of three factors, including: (1) that where the tort occurred was not separate from the physical location of the tortfeasors, (2) the D.C. Circuit had previously cautioned against broadly applying the non-commercial tort exception for all torts that have some relationship to the U.S., and (3) the legislative history of the Act provided support for the view that a tort must be wholly occurring in the U.S.[89] Additionally, the Court noted that the FSIA can be amended by the legislature, if enough people disagree with their interpretation.[90] The Court ultimately held that Kidane's claim was barred, due to the entire tort doctrine, therefore rendering Ethiopia immune from jurisdiction in U.S. federal court under the FSIA.[91]

The "entire tort" test has been widely accepted and even incorporated into the Restatement (Fourth) of the Foreign Relations Law of the U.S.[92] However, criticism has been levied that this interpretation gives rise to "intuitive practical objections . . . [f]or one, it seems to reward gamesmanship on the part of foreign governments . . . [and] it isn't the easiest concept to apply with confidence. And however difficult locating a tort might be in an ordinary case, a tort involving the Internet immensely complicates the inquiry."[93]

iii. FSIA: Terrorism exception

The FSIA has been amended several times—perhaps most notably in 1996, "to deny immunity to foreign states that have been formally designated by the U.S. government as state sponsors of terrorism . . . "[94] It was amended again in 2008, recodifying the state sponsored terrorism exception and creating a new code section, section 1605A.[95]

The terrorism exception (section 1605A) states in pertinent part:

(a)IN GENERAL.—

(1)NO IMMUNITY.—

---

88 *Id.*

89 *Id.* at 21, 23, 24.

90 *Id.* at 25–25, *aff'd*, 851 F.3d 7 (D.C. Cir. 2017).

91 *Id.*

92 RESTATEMENT (FOURTH) OF FOREIGN RELATIONS LAW § 457, reporters' notes n.1 (AM. LAW INST. 2018).

93 Grayson Clary, *Under the Foreign Sovereign Immunities Act, Where Do Hacking Torts Happen?* LAWFARE (May 1, 2018) https://www.lawfareblog.com/under-foreign-sovereign-immunities-act-where-do-hacking-torts-happen.

94 DAMROSCH & MURPHY, *supra* note 11, at 817.

95 28 U.S.C.A. § 1605A (2008); *see also* DAMROSCH & MURPHY, *supra* note 11, at 817.

> A foreign state shall not be immune from the jurisdiction of courts of the United States or of the States in any case not otherwise covered by this chapter in which money damages are sought against a foreign state for personal injury or death that was caused by an act of torture, extrajudicial killing, aircraft sabotage, hostage taking, or the provision of material support or resources for such an act if such act or provision of material support or resources is engaged in by an official, employee, or agent of such foreign state while acting within the scope of his or her office, employment, or agency.[96]

In comparing the 2008 terrorism exception and the non-commercial tort exception, notable differences arise, including that the non-commercial tort exception only applies to torts occurring fully within the United States, whereas the terrorism exception in section 1605A applies to torts committed abroad, and that the non-commercial tort exception "presents a more limited jurisdictional framework than the one reflected in the state-sponsors-of-terrorism exception," because even torts committed outside the U.S. that have a direct effect within the U.S. are insufficient to invoke the exception.[97]

Additionally, section 1605A provides "that such plaintiffs could seek punitive damages," a departure from the FSIA's general bar of punitive damages in suits falling under one of the exceptions to the Act.[98] In *Opati*, the Supreme Court "declared without any ambiguity that . . . 'Congress was as clear as it could have been when it authorized plaintiffs to seek and win punitive damages for past conduct. . . .'"[99] This decision, however, does not prevent challenges to punitive damages sought retroactively under the FSIA.[100]

(i) JASTA

In 2016, the legislature overrode President Barack Obama's veto and passed the Justice

Against Sponsors of Terrorism Act ("JASTA").[101] This Act eliminated the "state sponsor of terrorism" designation requirement under the existing FSIA provision, abrogated the entire tort doctrine, and allowed for its retroactive

---

96 § 1605A (2008).

97 *Compare* 28 U.S.C. § 1605A, *with* 28 U.S.C. § 1605(a)(5); RESTATEMENT (FOURTH) OF FOREIGN RELATIONS LAW § 457.

98 Haley S. Anderson, *The Significant of the Supreme Court's Opati Decision for States and Companies Sued for Terrorism in U.S. Courts*, JUST SEC. (May 19, 2020), https://www.justsecurity.org/70260/the-significance-of-the-supreme-courts-opati-decision-for-states-and-companies-sued-for-terrorism-in-u-s-courts/. *See* § 1605A(c).

99 Anderson, *supra* note 98.

100 *Id.*

101 Justice Against Sponsors of Terrorism Act (JASTA), Pub. L. No. 114-222, sec. 3, § 1605B(b), 130 Stat. 852, 853 (2016) (codified at 28 U.S.C. § 1605B).

application.[102]

The purpose of JASTA was "to provide civil litigants with the broadest possible basis, consistent with the Constitution of the United States, to seek relief against persons, entities, and foreign countries…that have provided material support, directly or indirectly, to foreign organizations or persons that engage in terrorist activities against the United States."[103]

The Act provides in pertinent part:

> A foreign state shall not be immune from the jurisdiction of the courts of the United States in any case in which money damages are sought against a foreign state for physical injury to person or property or death occurring in the United States and caused by—
>
> (1) an act of international terrorism in the United States; 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.[104]

With regard to the FSIA, JASTA "further narrows sovereign immunity of foreign countries in giving the U.S. jurisdiction to respond in court to any act of international terrorism, including monetary support for terrorist groups."[105] Prior to JASTA's enactment, the FSIA's terrorism exception made it such that you could not sue a foreign state for international terrorism in U.S. courts unless the government first designated that state as a "state sponsor of terrorism."[106] JASTA eliminated this limitation, and "as a result, any foreign state may now be sued in US courts for acts of international terrorism that cause injury in the United States."[107]

By expanding the FSIA's non-commercial tort exception, JASTA abrogated the entire tort doctrine, providing for "jurisdiction 'regardless of where the tortious act or acts of the foreign state occurred' . . . a state can now be sued in U.S. courts for alleged tortious conduct committed anywhere in the world, as long as there is a nexus to an act of terrorism occurring within the United

---

102 Matthew H. Kirtland & Andrew James Lom, *Layperson's Guide- Justice Against Sponsors of Terrorism Act*, NORTON ROSE FULBRIGHT (Dec. 2016), https://www.nortonrosefulbright.com/en-zw/knowledge/publications/d1a384e4/laypersons-guide—-justice-against-sponsors-of-terrorism-act.

103 Pub. L. No. 114-222, sec. 2(b), 130 Stat. 852, 853.

104 Pub. L. No. 114-222, sec. 3, § 1605B(b), 130 Stat. 852, 853.

105 Lindsay Meyerson, *Should We Prioritize Sovereign States or American Victims? JASTA & FSIA*, COLUM. UNDERGRADUATE L. REV. (Oct. 31, 2016), https://blogs.cuit.columbia.edu/culr/2016/10/31/should-we-prioritize-sovereign-states-or-american-victims-jasta-fsia/.

106 Kirtland & Lom, *supra* note 102.

107 *Id.*

States."[108] Additionally, JASTA can be applied retroactively to "any civil lawsuit pending on, or commenced on or after, the date it was enacted (September 28, 2016) and arising out of an injury to a person, property, or business occurring on or after September 11, 2001."[109] This allowed for legislative abrogation of "judicial decisions that had dismissed such cases brought by victims of the September 11, 2011 attacks on the United States."[110]

II. THE EXISTING PROBLEMS

A. The Rise of Cyber Crime

1. Background

Cybercrime is "defined as a crime where a computer is the object of the crime or us used as a tool to commit an offense."[111] It is generally divided into two types: "crimes that target networks or devices [and] crimes using devices to participate in criminal activities."[112] There are also three general categories of cybercrime, organized by who or what the crime affects or who or what the criminal is: individual, property, or government.[113]

Cybercrime was born in the 1970s, when a group of technologically savvy individuals ("phreakers") targeted computerized phone systems.[114] Almost two decades later, in 1986, Congress enacted the Federal Computer Fraud and Abuse Act ("CFAA") as a direct legislative response to hacking.[115] The CFAA's purpose was to criminalize unauthorized access to protected computers, and has been amended several times to address new advances in cybercrime.[116] Its scope has also broadened over time—amendments in 1994 "added civil remedies and expanded the coverage of the statute to include unauthorized transmissions, and amendments in 1996 changed the phrase 'federal interest computer' to

---

108 James Berger & Charlene Sun, *JASTA Amendments to FSIA Become Law*, KING & SPALDING (Oct. 11, 2016), https://www.jdsupra.com/legalnews/jasta-amendments-to-fsia-become-law-81257/.

109 Kirtland & Lom, *supra* note 102.

110 Berger & Sun, *supra* note 108.

111 *Types of Cybercrime*, PANDA SEC. (Aug. 26, 2021), https://www.pandasecurity.com/en/mediacenter/panda-security/types-of-cybercrime [hereinafter PANDA SEC.].

112 *Id.*

113 *Id.*

114 Connor Madsen, *The Evolution of Cybercrime*, WEBROOT (Apr. 23, 2019), https://www.webroot.com/blog/2019/04/23/the-evolution-of-cybercrime.

115 *Computer Fraud and Abuse Act (CFAA)*, NACDL, https://www.nacdl.org/Landing/ComputerFraudandAbuseAct# (last visited Nov. 6, 2021) [hereinafter NACDL].

116 18 U.S.C. § 1030 (2020).

'protected computer,' thereby significantly broadening the Act's reach."[117] Along with these amendments came the question of extraterritorial application of the statute — whether you could prosecute perpetrators abroad who commit computer abuse affecting computers in the U.S.[118]

In *United States v. Ivanov*, where the defendant was physically in Russia but accessed computers in the U.S., the District Court of Connecticut found that it had subject matter jurisdiction "whether or not the statutes under which the substantive offenses are charged are intended by Congress to apply extraterritorially, because the intended and actual detrimental effects of the substantive offenses Ivanov is charged with in the indictment occurred within the United States."[119] In looking at the 1996 amendments to the CFAA and comments to the statute, the Court stated "Congress has clearly manifested its intent to apply § 1030 to computers used either in interstate or in foreign commerce. The legislative history of the CFAA supports this reading of the plain language of the statute."[120]

In less than half a century, federal computer crime laws went from being virtually non-existent to covering almost every aspect of computer activity in society.[121] Penalties for violating the CFAA are up to 10 years in prison, and double that for a second offense.[122] In 1989, Robert Morris became the first person to be prosecuted under the CFAA.[123] He released "the Morris worm" into the world — a self-replicating program which overwhelmed computers and servers, causing widespread damage.[124]

Since then, cybercrime has risen exponentially, and evolved extremely rapidly.[125] There are several new ways in which cybercriminals can wreak havoc, including: phishing (tricking users into giving up sensitive information), ransomware (malware that can gain access to a system and block users from their own data), and cryptojacking (stealing cryptocurrency by embedding a type of code into a website).[126] Other common methods of attack include, distributed denial of service attacks (which make an online service unavailable to users), botnets (externally controlled networks from compromised computers), identity

---

117 William K. Kane & Melissa M. Mikhail, *Extraterritorial Application of the Computer Fraud and Abuse Act*, NAT'L L. REV. (July 3, 2020), https://www.natlawreview.com /article/extraterritorial-application-computer-fraud-and-abuse-act.

118 *Id.*

119 United States v. Ivanov, 175 F. Supp. 2d 367, 373 (D. Conn. 2001).

120 *Id.* at 374.

121 NACDL, *supra* note 115.

122 *Id.*

123 Madsen, *supra* note 114.

124 *Id.*

125 *The Fascinating Decade in Cybercrime: 2010 to 2020*, ARCTIC WOLF BLOG (Feb. 21, 2020), https://arcticwolf.com/resources/blog/decade-of-cybercrime.

126 Madsen, *supra* note 114.

theft, cyberstalking, and exploit kits (tools criminals can buy online to gain control of a user's computer).[127]

In 2020, worldwide spending on cybersecurity was in the billions, and security breaches have increased from 2018 by 11% (up 67% since 2014).[128] Hackers attack approximately every 39 seconds, and the average cost of a data breach or malware attack is in the millions.[129] Even more troubling to note, cybercrime increased during the COVID-19 pandemic.[130]

2. COVID-19 and Cybercrime

Phishing websites increased by 350% during the first quarter of 2020, with many attacks targeting hospitals and health care systems causing delays and disruptions in their responses to the COVID-19 pandemic.[131] Hackers and terrorists are "exploiting the significant disruption and economic hardships caused by COVID-19 to spread fear, hate, and division and radicalize and recruit new followers."[132] An Interpol assessment on cybercrime and COVID-19 has shown a shift towards larger targets such as governments, critical infrastructure, and big corporations as opposed to individuals and small businesses.[133] With people working from home, increasing online dependency, cybercriminals are taking advantage of the increased vulnerabilities in computer systems.[134] Hackers are also taking advantage of human vulnerabilities — perpetuating uncertainty and fear in people by spreading misinformation and fake news, contributing to anxiety in communities.[135]

Before a COVID-19 vaccine was available, medical trials became a target for foreign computer hackers in an attempt to steal the formula for their country in order to disrupt the distribution.[136] Microsoft reported that "seven prominent

---

127 PANDA SEC., *supra* note 111.

128 *29 Must-know Cybersecurity Statistics for 2020*, CYBER OBSERVER, https://www.cyber-observer.com/cyber-news-29-statistics-for-2020-cyber-observer/ (last visited Sept. 30, 2021).

129 *Id.*

130 Edith M. Lederer, *UN Reports Sharp Increase in Cybercrime During Pandemic*, AP NEWS (Aug. 7, 2020), https://apnews.com/article/virus-outbreak-counterterrorism-health-crime-phishing-824b3e8cd5002fe238fb9cbd99115bca.

131 *Id.*

132 *Id.*

133 *INTERPOL Report Shows Alarming Rate of Cyberattacks During COVID-19*, INTERPOL (Aug. 4, 2020), https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19.

134 *Id.*

135 *Id.*

136 Gary Horcher, *Microsoft: Foreign Cyber Hackers Are Targeting COVID-19 Vaccine*

but unnamed biotech companies testing vaccines were targeted in Canada, France, India, South Korea, and the United States" by Strontium, a Russian actor, and by Zinc and Cerium, North Korean actors.[137] As the law stands, these foreign-state bad actors who deploy malware from abroad, despite attacking American citizens, hospitals, and corporations, are immune from prosecution in U.S. courts under the FSIA.[138]

The threat is here, immediate, and very real. In fact, in 2020, the U.S. Department of Justice charged, and a grand jury indicted, two Chinese hackers with attempting to steal coronavirus research.[139] The grand jury's indictment against the two men alleged that "in many cases they worked on behalf of China's Ministry of State Security and other government agencies."[140] However, proving this is the difficult part.

B. Attribution of Conduct and State Responsibility

In order for an exception to the FSIA's immunity to apply, a Plaintiff must attribute the tortious conduct at issue to a foreign state. A state must take responsibility for its actions. In international law, there are fundamental principles of state responsibility: (1) if a state breaches an international obligation, it incurs responsibility for it; (2) if the breach results in injury to another state, the breaching state must pay the injured State reparations; and (3) the injured state may, in certain circumstances, take actions of self-help and countermeasures.[141] These primary rules of state responsibility address the sources of responsibility, and secondary rules on state responsibility address the consequences of "failure[s] to fulfill obligations established by the primary rules."[142]

In *Gabcikovo-Nagymaros Project,* the International Court of Justice ("ICJ") discussed the distinction between the two types of rules, opining that while a determination of whether a convention is in force is made per the law of treaties, an "evaluation of the extent to which the suspension or denunciation of a

---

Companies, KIRO 7 (Nov. 24, 2020), https://www.kiro7.com/news/local/microsoft-foreign-cyber-hackers-are-targeting-covid-19-vaccine-companies/VVTSOVZ2NBDPLBW6FESIUN4UGA.

137 *Id.*

138 28 U.S.C. § 1604 (1976).

139 Sergei Klebnikov, *DOJ Charges Chinese Hackers with Trying to Steal Coronavirus Research As Part of Decade-Long Intrusion Campaign*, FORBES (July 21, 2020), https://www.forbes.com/sites/sergeiklebnikov/2020/07/21/doj-charges-chinese-hackers-with-trying-to-steal-coronavirus-research-as-part-of-decade-long-intrusion-campaign/?sh=f5a876a35a10.

140 *Id.*

141 DAMROSCH & MURPHY, *supra* note 11, at 479.

142 *Id.* at 481.

convention, seen as incompatible with the law of treaties, involves the responsibility of the state which proceeded to it, is to be made under the law of state responsibility."[143]

A persuasive, although not governing, source on the matter of state responsibility is the International Law Commission Articles on State Responsibility ("ILC Articles").[144] Adopted in 2001, the Articles are an influential instrument of the secondary rules of state responsibility and per the general commentary accompanying them, do not "attempt to define the content of the international obligations, the breach of which gives rise to responsibility."[145]

Article I of the ILC Articles provides "[e]very internationally wrongful act of a State entails the international responsibility of that State."[146] Article II defines "internationally wrongful act" as "conduct consisting of an action or omission: [that is] (a) attributable to the State under international law; and (b) constitutes a breach of an international obligation."[147]

1. Defenses to State Responsibility

Defenses to state responsibility, can be invoked when a state admits to wrongful conduct but contends they should not be responsible for it, or that there should not be consequences for it. These defenses include: necessity, distress, consent, and force majeure.[148] The occurrence of any of these is considered a circumstance that precludes wrongfulness, as does "two other categories of state conduct[:] . . . countermeasures, and self-defense."[149]

i. Force Majeure

Article 23 of the ILC Articles provides that:

> the wrongfulness of an act of a State not in conformity with an international obligation of that State is precluded if the act is due to force majeure, that is the occurrence of an irresistible force or of an unforeseen event, beyond the control of the State, making it

---

143 Gabcikovo-Nagymaros Project (Hung./Slovk.) 1997 I.C.J. 7, ¶ 47 (Sept. 25); DAMROSCH & MURPHY, *supra* note 11, at 481.

144 DAMROSCH & MURPHY, *supra* note 11, at 481.

145 Int'l Law Comm'n, Draft articles on Responsibility of States for Internationally Wrongful Acts, U.N. Doc. A/56/10, at 31 (2001).

146 *Id.* at 32.

147 *Id.* at 34.

148 DAMROSCH & MURPHY, *supra* note 11, at 502.

149 *Id.*

> materially impossible in the circumstances to perform the obligation.[150]

The commentary on this provision notes the difference between force majeure and distress or necessity is partly due to the fact that the conduct involved in invoking force majeure is "involuntary, or at least involves no element of free choice."[151]

Force majeure and distress are discussed in the *Rainbow Warrior* case (*New Zealand v. France*) as decided by the France-New Zealand Arbitration Tribunal in 1990.[152] In that case, French agents blew up a civilian vessel docked in New Zealand.[153] Two of the French agents involved were then transferred to an island in French-Polynesia for three years, and were not allowed to leave unless given permission by both the French and New Zealand governments.[154] Both agents, at different times, were moved off the island without consent of the New Zealand government—one for urgent medical treatment, and the other to see her father, who was dying of cancer.[155] In both cases, the French government argued circumstances precluding wrongfulness existed and it had therefore not breached its obligation.[156] New Zealand disagreed.[157] The tribunal ultimately found that France had breached its obligations, and none of the applicable defenses were sufficient to preclude the wrongfulness of their conduct.[158] The tribunal in *Rainbow Warrior* ruled in favor of New Zealand on this defense, explaining that "a circumstance rendering performance more difficult or burdensome does not constitute a case of force majeure."[159]

(i) Force Majeure and COVID-19

States have imposed measures to protect the health and safety of their populations and secure their economies during COVID-19 that could potentially breach international law but for the force majeure exception.[160] This exception has provided states some protection from otherwise wrongful conduct during the

---

150 Draft articles on Responsibility of States for Internationally Wrongful Acts, *supra* note 145, at 76.

151 *Id.*

152 Rainbow Warrior (N.Z. v. Fr.), France-New Zealand Arb. Trib., 20 R.I.A.A. 217 (2006).

153 *Id.* at 223.

154 *Id.* at 224–25.

155 *Id.* at 241–42.

156 *Id.* at 229–30, 240–41.

157 *Id.* at 230, 241.

158 *Id.* at 265–66.

159 *Id.* at 253.

160 Riddhi Joshi, *Force Majeure Under the ILC Draft Articles on State Responsibility: Assessing its Viability Against COVID-19 Claims*, AM. SOC'Y OF INT'L L. (Sept. 17, 2020), https://www.asil.org/insights/volume/24/issue/24/force-majeure-under-ilc-draft-articles-state-responsibility-assessing.

ongoing global health crisis.[161] However, COVID-19 doesn't always satisfy the elements of the defense of force majeure, "because force majeure is a matter of contract, the language in the parties' agreement determines when and to what extent force majeure will excuse performance in that particular contract."[162]

ii. Necessity

Article 25 of the ILC Articles provides that:

> necessity may not be invoked by a State as a ground for precluding the wrongfulness of an act not in conformity with an international obligation of that state unless the act (a) is the only way to safeguard an essential interest against a grave and imminent peril; and (b) does not seriously impair an essential interest of the State or States towards which the obligation exists, or of the international community as a whole.[163]

This provision further states that the doctrine may not be invoked if the international obligation at issue excludes the possibility of invocation of the doctrine, or if the state contributed in any way to the situation of necessity.[164]

Necessity is discussed in the International Court of Justice's ("ICJ") 1990 decision *Gabčíkovo-Nagymaros Project* (Hungary/Slovakia).[165] In that case, the ICJ considered whether necessity was a successful defense to Hungary's breach of international obligation when it suspended and abandoned works it committed to perform on a hydroelectric dam project pursuant to a treaty.[166] Hungary claimed Czechoslovakia appropriated the Danube River water in constructing a dam as their reason for stopping work, holding Hungary responsible for its breach.[167] The court ultimately decided that the elements of necessity were not satisfied, determining that "the state of necessity can only be invoked under certain strictly defined conditions which must be cumulatively satisfied, and the state concerned is not the sole judge of whether those conditions have been met."[168] One of these conditions is "peril." The court distinguishes material damage from peril by explaining that peril implies a risk of some kind, and

---

161 *Id.*

162 David A. Shargel, *Revisiting Force Majeure and Other Contractual Considerations Amid COVID-19*, NAT'L L. REV. (Nov. 6, 2020) https://www.natlawreview.com/article/revisiting-force-majeure-and-other-contractual-considerations-amid-covid-19.

163 Draft articles on Responsibility of States for Internationally Wrongful Acts, *supra* note 145, at 80.

164 *Id.*

165 Gabcikovo-Nagymaros Project (Hung./Slovk.) 1997 I.C.J. 7, ¶ 48.

166 *Id.* ¶ 49.

167 *Id.* ¶ 107.

168 *Id.* ¶ 51.

regarding the imminency of the peril, the "mere apprehension of a possible peril could not suffice in that respect."[169]

An important distinction between necessity and force majeure is that "the former involves a deliberate act not to conform to the obligation whereas the latter involves material impossibility to conform with the obligation or to realize the conduct is contrary to the obligation."[170]

iii. Distress

Article 24 of the ILC Articles provides that:

> The wrongfulness of an act of a State not in conformity with an international obligation of that State is precluded if the author of the act in question has no other reasonable way, in a situation of distress, of saving the author's life or the lives of other persons entrusted to the author's care.[171]

The comments to this provision provide that "Article 24 is limited to cases where human life is at stake."[172] Exceptions include where "(a) the situation of distress is due . . . to the conduct of the State invoking it; or (b) the act in question is likely to create a comparable or greater peril."[173] Examples provided in the commentary include vehicles entering another State's territory due to weather or technical failures.[174]

However, distress is not confined to such cases, as the comments to the Articles explain, and as *Rainbow Warrior* illustrates.[175] The tribunal in *Rainbow Warrior* accepted France's plea of "circumstances of distress in a case of extreme urgency involving elementary humanitarian considerations affecting the acting organs of the State," despite ultimately rejecting the defense.[176]

iv. Consent

Article 20 of the ILC Articles states that "valid consent by a State to the commission of a given act by another State precludes the wrongfulness of that

---

169 *Id.* ¶ 54.

170 DAMROSCH & MURPHY, *supra* note 11, at 511.

171 Draft articles on Responsibility of States for Internationally Wrongful Acts, *supra* note 145, at 78.

172 *Id.* at 79.

173 *Id.* at 78.

174 *Id.*

175 Rainbow Warrior (N.Z. v. Fr.), France-New Zealand Arb. Trib., 20 R.I.A.A. 215, 253 (2006).

176 Draft articles on Responsibility of States for Internationally Wrongful Acts, *supra* note 145, at 79.

act in relation to the former State to the extent that the act remains within the limits of that consent."[177] Commentary accompanying the provision provides that consent is common, and gives examples of consent such as "transit through the airspace or internal waters of a state, the location of facilities on its territory, or the conduct of official investigations or inquiries there."[178] Comment 3 opines that

> Consent to the commission of otherwise wrongful conduct may be given by a State in advance or even at the time it is occurring. By contrast, cases of consent given after the conduct has occurred are a form of waiver or acquiescence, leading to loss of the right to invoke responsibility.[179]

v. Countermeasures

When one state breaches an international obligation, "a state injured by . . . [that] violation . . . is entitled to take certain self-help measures against the offending state as a means of inducing that state's compliance."[180] However, one must first accurately attribute conduct to a state before countermeasures are appropriate.[181] Additionally, Article 51 of the ILC Articles establishes a proportionality requirement—"countermeasures must be commensurate with the injury suffered, taking into account the gravity of the internationally wrongful act and the rights in question."[182]

The above-mentioned factors must be considered in their totality in deciding whether, or how to respond to cyberattacks.

C. Attribution of Conduct and the FSIA

In order for a foreign state to be subject to jurisdiction in U.S. courts under the FSIA, there must be attribution of conduct to that state. Conduct can be attributed to a state when that conduct was either committed by an organ of the state, or if the conduct was committed by a person acting "under the direction, instigation or control of those organs, i.e., as agents of the State."[183] The

---

177 *Id.* at 72.

178 *Id.*

179 *Id.* at 73.

180 DAMROSCH & MURPHY, *supra* note 11, at 515.

181 *Id.*

182 Draft articles on Responsibility of States for Internationally Wrongful Acts, *supra* note 145, at 134.

183 DAMROSCH & MURPHY, *supra* note 11, at 481; *see* Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serbia & Montenegro), Judgement, 2007 I.C.J. 119 at 43, ¶ 179 (Feb. 26) ("[T]he Court affirms that

commentary to the ILC Articles also clarifies this point—"the general rule is that the only conduct attributed to the State at the international level is that of its organs of government, or of others who have acted under the direction, instigation, or control of those organs, i.e., as agents of the State."[184]

In sum, there is a two-step inquiry in determining whether conduct is attributable to a state: (1) was the conduct perpetrated by an organ of the state? If not, (2) was the conduct perpetrated by someone acting under state control or direction? If the answer to either question is yes, then the conduct is attributable to a state.[185] In order to complete this inquiry, one must clarify what constitutes an "organ of the state," and what "control" entails.

1. Organ

The ICJ in *Bosnia & Herzegovina v. Serbia & Montenegro* restated a customary rule of international law, reflected by the ILC Articles in Article 4, "that the conduct of any State organ is to be considered an act of the State . . . and therefore gives rise to the responsibility of the State if it constitutes a breach of an international obligation of the State."[186]

Article 4 of the ILC Articles states in pertinent part:

> 1. The conduct of any State organ shall be considered an act of that State under international law, whether the organ exercises legislative, executive, judicial or any other functions, whatever position it holds in the organization of the State, and whatever its character as an organ of the central government or of a territorial unit of the State.
>
> 2. An organ includes any person or entity which has that status in accordance with the internal law of the State.[187]

The accompanying commentary states that

> reference to a State organ . . . is intended in the most general sense . . . It extends to organs of government of whatever kind or classification, exercising whatever functions, and at whatever level in the hierarchy . . . No distinction is made for this purpose between legislative, executive, or judicial organs.[188]

---

the Contracting Parties are bound by the obligation under the Convention not to commit, through their organs or persons or groups whose conduct is attributable to them, genocide . . ..").

184 Draft articles on Responsibility of States for Internationally Wrongful Acts, *supra* note 145, at 38.

185 *Id.* at 72.

186 Bosn. & Herz. v. Serbia & Montenegro, 2007 I.C.J. 119 at 43, ¶ 385.

187 Draft articles on Responsibility of States for Internationally Wrongful Acts, *supra* note 145, at 40.

188 *Id.*

Additionally, the ICJ in *Bosnia & Herzegovina v. Serbia & Montenegro* emphasized that "persons, groups of persons or entities may . . . be equated with State organs even if that status does not follow from internal law, provided that in fact the persons, groups or entities act in 'complete dependence' on the State, of which they are ultimately merely the instrument."[189]

While there is no test within the FSIA to determine whether an entity is an "organ," some courts will consider certain factors.[190] The Court in *Hausler v. JP Morgan*, following the factors for consideration set forth by the Second Circuit, set out such factors for consideration:

> Factors relevant under balancing analysis used in determining whether entity is "organ of a foreign state," under definition of "agency or instrumentality" set forth by Foreign Sovereign Immunities Act (FSIA), include (1) whether the foreign state created the entity for a national purpose, (2) whether the foreign state actively supervises the entity, (3) whether the foreign state requires the hiring of public employees and pays their salaries, (4) whether the entity holds exclusive rights to some right in the foreign country, and (5) how the entity is treated under foreign state law.[191]

2. Control

Article 8 of the ILC Articles states "the conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct."[192] While "acting on the instructions" of a state is generally clear and uncontroversial in meaning, the phrase "under the direction or control" is more ambiguous, and has been discussed by multiple tribunals, including the ICJ and the former International Criminal Tribunal for Yugoslavia ("ICTY").[193] Each of these tribunals laid out its own test for determining what "under the direction or control" means.

In the ICJ case, *Military and Paramilitary Activities in and against Nicaragua*, the court set out the "effective control" test.[194] Here, the ICJ determined that state responsibility could be attributed to the respondent if it

---

189 Bosn. & Herz. v. Serbia & Montenegro, 2007 I.C.J. 119 at 43, ¶ 392.

190 Hausler v. JPMorgan Chase Bank, N.A., 845 F. Supp.2d 553, 572 (S.D.N.Y. 2012).

191 *Id.*

192 Draft articles on Responsibility of States for Internationally Wrongful Acts, *supra* note 145, at 47.

193 *Id.*

194 Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. US), Judgment, 1986 I.C.J. 14, ¶ 115 (June 27).

"directed or enforced the perpetration of the acts contrary to human rights and humanitarian law alleged by the applicant state."[195] The court stated, "for this conduct to give rise to legal responsibility . . . it would in principle have to be proved that the State had effective control of the military or paramilitary operations in the course of which the alleged violations were committed."[196]

However, in *Prosecutor v. Du[Ko Tadi]* ("Tadić"), the ICTY rejected the ICJ's reasoning and established its own test — the "overall control" test.[197] This is a much broader test and doesn't require proof "that each operation during which acts were committed in breach of international law was carried out on [the state's] instructions, or under its effective control."[198] The ICJ in *Bosnia & Herzegovina v. Serbia & Montenegro* noted that "the ICTY presented the 'overall control' test as equally applicable under the law of State responsibility for the purpose of [determining] . . . when a State is responsible for acts committed by paramilitary units, or armed forces which are not among its official organs."[199]

In comparing the two tests, the ICJ's effective control test is a harder standard to satisfy, as it requires proving the state had both strategic and tactical control over the actor.[200] Conversely, the ICTY's overall control test merely requires proof of strategic control.[201] For example, a state sending money and arms to their rebels in another country would probably be liable under the ICJ's overall control test, but probably would not be held liable under the ICTY's effective control test.

In determining which approach to apply on two separate issues before the court, the ICJ in *Bosnia & Herzegovina v. Serbia & Montenegro* stated, "it should first be observed that logic does not require the same test to be adopted in resolving the two issues, which are very different in nature."[202] It also noted that "the 'overall control' test has the major drawback of broadening the scope of state responsibility well beyond the fundamental principle governing the law of international responsibility: a State is responsible only for its own conduct."[203]

---

195 *Id.*

196 *Id.*

197 Prosecutor v. Tadic, Case No. IT-94-1, Judgment, ¶ 141 (Int'l Crim. Trib. For the Former Yugoslavia Jul. 15, 1999).

198 Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro), Judgment, 2007 I.C.J. 43, ¶ 402 (Feb. 26).

199 *Id.* ¶ 404.

200 *Compare* Military and Paramilitary Activities in and against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 115 (June 27), *with* Bosn. & Herz. v. Serb. & Montenegro, 2007 I.C.J. at 43, ¶ 404.

201 Bosn. & Herz. v. Serb. & Montenegro, 2007 I.C.J. 43, ¶ 404.

202 *Id.* ¶ 405.

203 *Id.* ¶ 406.

D. State Attribution: Cyber Attribution

Attributing conduct to a state with regard to the cyber domain is referred to as cyber attribution—"the process of tracking, identifying and laying blame on the perpetrator of a cyberattack or other hacking exploit."[204] Attributing conduct to a state carrying out cyberattacks has the potential be incredibly complicated, as "the underlying architecture of the internet offers numerous ways for attackers to hide their tracks."[205] Internet protocol ("IP") addresses are easy to spoof, and attackers can "use techniques such as proxy servers, to bounce their IP addresses around the world to confuse attempts at cyber attribution. Additionally, jurisdictional limitations can hinder attribution in cross-border cybercrime investigations."[206]

Not only is attribution necessary for liability, but it is also vital in understanding the rationale behind attacks, to taking preemptive measures, and lawfully responding to attackers.[207] Additionally, "[a]ttribution is a required pre-cursor to the use of self-defense in response to a malicious cyberincident."[208]

Unfortunately, anonymity is relatively easy to achieve, and is "inherent in cyberspace because a criminal can either use a fake identity or steal someone else's identity to launch an attack."[209] Methods of achieving anonymity include shoulder surfing i.e., looking over someone's shoulder to get their sensitive information, using fake email accounts, spoofing IP addresses, using a proxy, a drive by download attack (where a "computer becomes infected with malicious software simply by visiting a website"[210]), malware, or a cross-site scripting attack ("an attacker can use XXS to send a malicious script to an unsuspecting user…[they] can even rewrite the content of the HTML page"[211]).[212]

There are, however, "different, specialized techniques available for performing cyber attribution . . . [i]nvestigators use analysis tools, scripts, and programs to uncover critical information about attacks."[213] The legal challenge

---

204 Linda Rosencrance, *Cyber Attribution*, SEARCH SEC. (Oct. 2017), https://searchsecurity.techtarget.com/definition/cyber-attribution.

205 *Id.*

206 *Id.*

207 Jawwad A. Shamsi et al., *Attribution in Cyberspace: Techniques and Legal Implications*, WILEY ONLINE LIBR. (Apr. 26, 2016), https://onlinelibrary.wiley.com/doi/full/10.1002/sec.1485.

208 *Id.*

209 *Id.*

210 Brian Laing, *Drive-By Downloads and How to Prevent Them*, LAST LINE (Sept. 21, 2017), https://www.lastline.com/blog/drive-by-download/.

211 Kirsten S., *Cross Site Scripting (XSS)*, OWASP https://owasp.org/www-community/attacks/xss/, (last visited Oct. 1, 2021).

212 Shamsi et al., *supra* note 207.

213 Rosencrance, *supra* note 204.

is figuring out "[w]hat level of certainty/attribution is required to respond to an attack" and how to impose liability for the attack. [214]

III. POTENTIAL SOLUTIONS

A. Homeland and Cyber Threat Act

The Homeland and Cyber Threat Act ("HACT") is a bipartisan bill introduced to the House of Representatives in August of 2019 by representatives Jack Bergman (MI-1, R) and Andy Kim (NJ-3, D).[215] If passed, the bill would amend Title 28 of the U.S. Code section 1605 (FSIA) to "allow claims against foreign states for unlawful computer intrusion."[216] The following proposed language would be inserted after section 1605B:

> **Section 1605C. Computer intrusions by a foreign state**
>
> A foreign state shall not be immune from the jurisdiction of the courts of the United States or of the States in any case not otherwise covered by this chapter in which money damages are sought against a foreign state by a national of the United States for personal injury, harm to reputation, or damage to or loss of property resulting from any of the following activities, whether occurring in the United States or a foreign state:
>
> (1) Unauthorized access to or access exceeding authorization to a computer located in the United States.
>
> (2) Unauthorized access to confidential, electronic stored information located in the United States.
>
> (3) The transmission of a program, information, code, or command to a computer located in the United States, which, as a result of such conduct, causes damage without authorization.
>
> (4) The use, dissemination, or disclosure, without consent, of any information obtained by means of any activity described in paragraph (1), (2), or (3).
>
> (5) The provision of material support or resources for any activity described in paragraph (1), (2), (3), or (4), including by an official, employee, or agent of such foreign state.
>
> (b) APPLICATION.—This Act and the amendments made by this Act shall apply to any action pending on or filed on or after the date

---

214 Shamsi et al., *supra* note 207.

215 *Bergman's Bipartisan HACT Act Gains Momentum as Foreign Cyberattacks Increase in Wake of COVID Crisis*, U.S. HOUSE OF REP. CONGRESSMAN JACK BERGMAN (June 18, 2020), https://bergman.house.gov/news/documentsingle.aspx?DocumentID=695.

216 H.R. 4189, 116th Cong. (2019).

of the enactment of this Act.[217]

At introduction, the bill had 67 co-sponsors—35 Republicans and 32 Democrats—and was eventually passed in the House by a vote of 336-71.[218] This bipartisan support illustrates the issue's importance. HACT was reintroduced in March of 2021, this time by Rep. Colin Allred (TX-32, D) and was co-sponsored by forty-five representatives.[219] This new wave of interest comes in the wake of the "SolarWinds hack," a "massive Russian cyber espionage campaign . . . which . . . had compromised at least nine federal agencies and 100 private companies."[220]

Despite strong support, critics argue that opening up foreign countries to liability in U.S. courts could undermine the American government's ability to resolve issues diplomatically.[221] Additionally, because the bill could invite "reciprocal actions against the United States in foreign courts," some are concerned about America's own extensive extraterritorial cyber activity.[222] By removing immunity from foreign state actors and governments, "[a]llowing US nationals and companies to sue…could open the door for foreign governments to do the same, filing lawsuits against US intelligence agencies. The US government uses cyber operations as a means to collect intelligence."[223]

In addition to this, "attribution becomes a major issue . . . for example, in Russia, it is understood that cyber threat actors are allowed to act freely within the country as long as they do not attack Russian companies or citizens. To demonstrate that this constitutes support from a state actor would be extremely difficult."[224] While this may be true, it seems the benefits could outweigh the costs — foreign state hacking is a very real threat, proven by the SolarWinds incident, and the fact that foreign adversaries have previously targeted American businesses and individuals, wreaking havoc through informational and political

---

217 *Id.*

218 *Id.*

219 Maggie Miller, *Lawmakers Introduce Legislation to Allow Americans to Take Hackers to Court*, THE HILL (Mar. 8, 2021), https://thehill.com/policy/cybersecurity/542157-lawmakers-introduce-legislation-to-allow-americans-to-take-foreign?rl=1.

220 *Id.*

221 David Reaboi, *Bipartisan HACT Act Couldn't Come at a Better Time*, NEWSWEEK (Aug. 26, 2020), https://www.newsweek.com/bipartisan-hact-act-couldnt-come-better-time-opinion-1527577.

222 Chimene Keitner, *Private Lawsuits Against Nation-States Are Not the Way to Deal with America's Cyber Threats*, L. FARE BLOG, (June 15, 2020), https://www.lawfareblog.com/private-lawsuits-against-nation-states-are-not-way-deal-americas-cyber-threats.

223 Patrick Wallenhorst, *Proposed Homeland and Cyber Threat Act Would Allow Claims Against Foreign State Actors*, BINARY DEF. (Mar. 18, 2021), https://www.binarydefense.com/proposed-homeland-and-cyber-threat-act-would-allow-claims-against-foreign-state-actors/.

224 *Id.*

warfare to the tune of billions of dollars.[225] In addition, "adding the ability for US nationals to engage in lawsuits with foreign governments would make for a volatile environment for cyberthreat actors, and may be enough of a deterrent to force them to shift their focus elsewhere."[226]

B. Overruling the Entire Tort Doctrine

Another potential solution to closing the current gap in the law regarding the FSIA and cybercrime is overruling the entire tort doctrine. As previously discussed, the entire tort doctrine was borne from judicial interpretation of the non-commercial tort exception to the FSIA and determines that the exception only applies to torts occurring entirely, "wholly," within the United States.[227] However, the doctrine of stare decisis may deem overruling the entire tort doctrine an unattractive option.

1. Stare Decisis

Stare decisis is a doctrine of precedent, and means "to stand by things decided."[228] Courts give a certain level of deference to prior decisions and are hesitant to either reverse, if it was their own court that made the decision, or contradict, if it was a higher or different court making the decision, decisions that have already been made.[229] This level of deference is supported by multiple policy considerations, including "fairness, stability, predictability and efficiency. Adherence to precedent ensures that like cases will be treated alike, and that similarly situated individuals are subject to the same legal consequences . . . there will be no equal justice under law if a . . . rule is applied in the morning but not the afternoon."[230]

In *Allen v. Cooper*, the Supreme Court discussed stare decisis, as a "foundation stone of the rule of law" and noted that "to reverse a decision, we demand a 'special justification', over and above the belief that the precedent was wrongly decided."[231] Without such justification, the Supreme Court will not overrule its prior decisions.

Characteristics of adjudication which have been suggested as satisfying this

---

225 Reaboi, *supra* note 221.

226 Wallenhorst, *supra* note 223.

227 *Infra* pp. 12–13.

228 Timothy Oyen, *Stare Decisis*, LEGAL INFO. INST., https://www.law.cornell.edu /wex/stare_decisis (last updated March 2017).

229 *Id.*

230 James C. Rehnquist, *The Power that Shall Be Vested in a Precedent: Stare Decisis, the Constitution and the Supreme Court*, 66 B.U. L. Rev. 345, 347 (1986).

231 Allen v. Cooper, 140 S. Ct. 994, 1003 (2020).

burden are:

> (1) reliance upon changed conditions which have undermined the basis of the challenged precedent;
>
> (2) reliance upon the difficulties of the Supreme Court and lower courts in applying the challenged rule;
>
> (3) reliance upon inconsistency between the challenged decision and subsequent precedent;
>
> (4) overruling of a decision which was "wrong" from the start;
>
> (5) overruling of a decision which itself overruled precedent;
>
> (6) reliance upon fundamental constitutional principles;
>
> (7) careful examination of the challenged precedent; and
>
> (8) overruling only after full argument and careful deliberation.[232]

However, this theory has been critiqued as being overly broad, allowing almost any decision to be attacked or defended on the above criteria.[233]

Public perception of the Supreme Court is also a consideration with regard to stare decisis, since the Court's legitimacy "depends upon the public perception that in each case the majority of the Court is speaking for the Constitution itself, rather than simply for five or more lawyers in black robes."[234] It is important that the public sees the Court as fair, and its decisions as final as well as accurate, not only because it is the highest Court in America, but because it would undermine the credibility of the Court if it seemed as if its decisions were made arbitrarily or in connection with who sits on the Court.

While there are good reasons for the existence and continued adherence to stare decisis as a doctrine, there are compelling critiques of it, including that the doctrine "occasionally permits erroneous decisions to continue influencing the law and encumbers the legal system's ability to quickly adapt to change."[235]

Having the Court reverse its interpretation of the non-commercial tort exception such that it only applies to torts occurring wholly within the United States would prove challenging in the face of stare decisis considerations. However, it has been done through legislation — JASTA (section 1605B) abrogated the entire tort doctrine, allowing for jurisdiction over claims regarding terrorism, where the entire tort did not happen solely within the US.[236]

---

232 Rehnquist, *supra* note 230, at 358–59.
233 *Id.* at 359.
234 *Id.* at 354.
235 Oyen, *supra* note 228.
236 28 U.S.C. § 1605B(b)(2) (2016).

C. Expansion of the FSIA's Terrorism Exception

Some think that passing the HACT would be akin to passing the terrorism exception (section 1605A), but in theory, it would be possible to amend that section itself to include a provision on cyberterrorism.

1. Cyberterrorism

There are many differing definitions of cyberterrorism, and the phrase is widely used by the media today. Generally, "cyberterrorism refers to the use of the Internet in order to perform violent actions that either threaten or result in serious bodily harm or even loss of life."[237] Cyberterrorism seems to involve the cybercrime category of "government"— encompassing attacks against the government such as "hacking government, military websites or distributing propaganda."[238] However, there is no clear consensus on the exact definition of cyberterrorism, or even whether the world has yet experienced a cyberterrorism event.[239]

Cyberterrorism is appealing to modern terrorists—it's cheaper than traditional methods of terrorism, it provides terrorists with a veil of anonymity, it can be conducted remotely, the variety and quantity of targets is vast, and it has the potential to affect more people than conventional methods.[240] Could this make the threat more real? More likely? As of now, "[n]either Al Qaeda nor any other terrorist organization appears to have tried to stage a serious cyberattack. For now, insiders or individual hackers are responsible for most attacks and intrusions and the hackers' motives are not political."[241] As such, it can be an elusive term to attach punishment to.

The terrorism exception of the FSIA could be expanded to include cyberterrorism, thereby closing at least part of the legal loophole currently affording foreign-state cyber criminals' immunity from prosecution in U.S. courts. It is possible to add language from the HACT, modifying it to include and define cyberterrorism, or to simply modify the terrorism provision as is, so that the provision becomes broad enough to encompass most cybercrimes within the definition of cyberterrorism.

---

237 *What Are Cyberterrorism and Cyberwarfare?,* LOGSIGN BLOG (May 22, 2020), https://blog.logsign.com/what-are-cyberterrorism-and-cyberwarfare/.

238 PANDA SEC. *surpa* note 111.

239 Gabriel Weimann, *Cyberterrorism: How Real Is the Threat?*, U.S. INST. OF PEACE (Dec. 2004), https://www.usip.org/sites/default/files/sr119.pdf.

240 *Id.*

241 *Id.*

IV. CONCLUSION

As it stands, there is a legal loophole which permits state sponsored cybercriminals to attack U.S. citizens in the United States, without facing liability in U.S. courts. The FSIA currently provides immunity from liability to foreign sovereigns who engage in such behavior, unless a plaintiff can show one of several enumerated exceptions to the FSIA applies to their case. While cybercrime can be considered a tort for purposes of the non-commercial tort exception to the FSIA, this provision does not apply to cybercrimes that originate outside the United States and do not occur 'wholly' within the country, making it easy for cybercriminals, such as those involved in the SolarWinds hack, to get away scot-free.[242]

There is an increasing and imminent need to close this gap in the law, and several ways to do so, including by abrogating the entire tort doctrine, expanding the terrorism exception to the FSIA, or through legislation currently before Congress (HACT). The United States should, and must, act swiftly and decisively to protect its citizens from this very real threat.

---

[242] *See* Bellinger, III et al., *supra* note 8.