Cite as Kurland, 10 J. NAT'L SECURITY L. & POL'Y __ (forthcoming 2019)

Sovereign Immunity in Cyber Space: Towards Defining a Cyber-Intrusion Exception to the Foreign Sovereign Immunities Act

Benjamin Kurland*

While the Mueller investigation continues to probe the Trump campaign's ties to Russia and talk of phony Facebook profiles and fake news takes up much of the current conversation, it is easy to forget the role direct cyber-hacking played in the 2016 election. Russian hacking of the DNC and John Podesta's emails and their subsequent publication, for example, were major storylines of the campaign.[1] Cyber-intrusions by state actors is not just a political issue. The Department of Justice, for example, demonstrated the extent of this threat when it indicted two Russian intelligence officers for the 2014 hacking of 500 million Yahoo accounts.[2]

New strategies abound over means to combat foreign cyber-assaults. But, given the harm to personal privacy, national interests, and the institution of criminal proceedings, it may be time to turn to one of the United States' most trusted means of deterrence: private suit. While the U.S. government discusses indictments, there has been no corresponding rush to the courthouse to redress the harm to individuals whose private information has been compromised. This is particularly surprising given that Congress has provided several private causes of action for various forms of cyber-hacking.[3]

* J.D., Georgetown University Law Center, Class of 2018
[1] Eric Lipton, David E. Sanger & Scott Shane, *The Perfect Weapon: How Russian Cyberpower Invaded the U.S.*, N.Y. TIMES (Dec. 13, 2016), https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html.
[2] Vindu Goel & Eric Lichtblau, *Russian Agents Were Behind Yahoo Hack, U.S. Says*, N.Y. TIMES (Mar. 15, 2017), https://www.nytimes.com/2017/03/15/technology/yahoo-hack-indictment.html.
[3] *See* Wiretap Act, 18 U.S.C. § 2520(a) (2012) (providing a cause of action for communications intercepted during transmission); Stored Communications Act, 18 U.S.C. § 2707 (2012) (providing a cause of action for intentionally accessing stored communications); Computer Fraud and Abuse Act, 18 U.S.C. § 1030(g) (2012) (providing a cause of action for obtaining information or causing damage through unauthorized access to a protected computer).

Russia, however, would not be the sole target of private litigation. Security experts, for example, report that the Chinese government has so thoroughly hacked nearly every institution in Washington, D.C. that the information obtained would be sufficient "to map how power is exercised in Washington to a remarkably nuanced degree."[4] Reported targets include law firms, think tanks, news organizations, human rights groups, contractors, congressional offices, embassies and federal agencies.[5] Even the author's information was part of a trove of information stolen by the Chinese government in a hack of the Office of Personnel Management.[6]

Washington, D.C. is not China's only target. Industrial spying, and the theft of terabytes of sensitive data and intellectual property, has cost companies billions.[7] For example, in July 2016, a Chinese national pled guilty to a conspiracy to hack into the computer systems of Boeing and other government contractors to steal technical data on the C-17 strategic transport aircraft and other fighter jets on behalf of the Chinese military.[8]

Russia and China are still only the tip of the iceberg. In one of the more bizarre government-related cyber-intrusion stories, North Korea stole and released large stockpiles of information from Sony Pictures Entertainment as apparent revenge for the portrayal of Korean leader Kim Jung Un in the Seth Rogan and James Franco movie "The Interview." Notably, the

[4] Craig Timburg, *Chinese Cyberspies Have Hacked Most Washington Institutions, Experts Say*, WASH. POST (Feb. 20, 2013), https://www.washingtonpost.com/business/technology/chinese-cyberspies-have-hacked-most-washington-institutions-experts-say/2013/02/20/ae4d5120-7615-11e2-95e4-6148e45d7adb_story.html?utm_term=.b0adee2eef55.
[5] *Id.*
[6] Devlin Barrett, Danny Yadron & Damian Paletta, *U.S. Suspects Hackers in China Breached About 4 Million People's Records, Officials Say*, WALL ST. J. (June 5, 2015), https://www.wsj.com/articles/u-s-suspects-hackers-in-china-behind-government-data-breach-sources-say-1433451888.
[7] David J. Kappos & Pamela Passman, *Cyber Espionage Is Reaching Crisis Levels*, FORTUNE (Dec. 12, 2015), http://fortune.com/2015/12/12/cybersecruity-amsc-cyber-espionage/.
[8] Press Release, *Chinese National Who Conspired to Hack into U.S. Defense Contractors' Systems Sentenced to 46 Months in Federal Prison*, DEP'T OF JUST. (July 13, 2015), https://www.justice.gov/opa/pr/chinese-national-who-conspired-hack-us-defense-contractors-systems-sentenced-46-months.

Sony hack was the first time the United States government openly attributed a cyber-intrusion to a nation-state.[9]

Another common motive for cyber-intrusion is intimidation and information gathering; foreign governments often target news organizations and human rights groups to identify dissidents and dissension. Google researchers report, for example, that at least twenty-one of the world's top twenty-five news organizations have been targets of "state-sponsored hacking attacks."[10] The Syrian regime has also reportedly targeted human rights activists in the United States,[11] and the Electronic Frontier Foundation reports that it was the target of a Vietnamese malware attack.[12]

Despite the proliferation of cyber-hacking, the actions of nation-state perpetrators have yet to produce significant legal consequences. The first attempt to challenge foreign government cyber-intrusion in U.S. court came in response to the hacking of an Ethiopian asylee living in Silver Spring, Maryland. In *Doe v. Federal Democratic Republic of Ethiopia*, the District Court for the District of Columbia found, and the D.C. Circuit affirmed, that the Foreign Sovereign Immunities Act ("FSIA") barred suit brought under both the Wiretap Act's private cause of action and the common law tort of intrusion upon seclusion.[13] The result is that governments

[9] Stephan Haggard & Jon R. Lindsay, *North Korea and the Sony Hack: Exporting Instability Through Cyberspace*, E.-W. CENT. (May 2015), http://www.eastwestcenter.org/publications/north-korea-and-the-sony-hack-exporting-instability-through-cyberspace.
[10] Jeremy Wagstaff, *Journalists, Media Under Attack From Hackers: Google Researchers*, REUTERS (Mar. 28, 2014), http://www.reuters.com/article/us-media-cybercrime-idUSBREA2R0EU20140328.
[11] Eva Galperin & Morgan Marquis-Boire, *Fake YouTube Site Targets Syrian Activists with Malware*, ELECTRONIC FRONTIER FOUNDATION (Mar. 15, 2012), https://www.eff.org/deeplinks/2012/03/fake-youtube-site-targets-syrian-activists-malware.
[12] Eva Galperin & Morgan Marquis-Boire, *Vietnamese Malware Gets Very Personal*, ELECTRONIC FRONTIER FOUND. (Jan. 19, 2014), https://www.eff.org/deeplinks/2014/01/vietnamese-malware-gets-personal.
[13] 189 F. Supp. 3d 6 (D.D.C. 2016) ("*Doe I*"), *aff'd*, 851 F.3d 7 (D.C. Cir. 2017) ("*Doe II*").

around the world now have precedent to escape liability for targeting the computers of United States citizens, even when those computers are located squarely on U.S. soil.

This article will explore the possibility of overcoming this impunity by introducing a new exception to the FSIA covering foreign government-perpetrated cyber-intrusions. Given the magnitude of the issue of government intrusion, this idea has been surprisingly underexplored. Daniel Blumenthal briefly suggested an exception, even before *Doe*, but it failed to gain traction within the legal community.[14] In the aftermath of the *Doe* decision the need for an exception has become more pressing. A recent blog post from private attorney Alexis Haller has revived the suggestion, and this paper seeks to explore the possibility in greater depth.[15]

Adding a new exception to the FSIA serves the dual purpose of reinforcing U.S. sovereignty through a private-attorney-general-like deterrence mechanism as well as providing redress to those whose privacy rights have been seriously compromised by such attacks. Demonstrating the significance of these rights is the fact that similar attacks would be actionable if carried out by any other actor, including the U.S. government or, potentially, even a foreign citizen.[16]

---

[14] Daniel Blumenthal, *How to Win a Cyberwar with China*, FOREIGN POL'Y (Feb. 28, 2013), http://foreignpolicy.com/2013/02/28/how-to-win-a-cyberwar-with-china-2/.

[15] Alexis Haller, *The Cyberattack Exception to the Foreign Sovereign Immunities Act: A Proposal to Strip Sovereign Immunity When Foreign States Conduct Cyberattacks Against Individuals and Entities in the United States*, FSIA LAW (Feb. 19, 2017), https://fsialaw.com/2017/02/19/the-cyberattack-exception-to-the-foreign-sovereign-immunities-act-a-proposal-to-strip-sovereign-immunity-when-foreign-states-engage-in-cyberattacks-against-individuals-and-entities-in-the-united-stat/#_ftnref15.

[16] The author was unable to find an on-point case of a U.S. national harmed while in the United States bringing suit against a foreign hacker. Gilmore, however, identifies several statutory private causes of action in the Wiretap Act, 18 U.S.C. § 2520(a) (2012); Stored Communications Act, 18 U.S.C. § 2707 (2012); Computer Fraud and Abuse Act, 18 U.S.C. § 1030(g) (2012); as well as the common law torts of trespass and invasion of privacy that provide individuals with redress when hacked. Scott A. Gilmore, *Suing the Surveillance States: The (Cyber) Tort Exception to the Foreign Sovereign Immunities Act*, 46 COLUM. HUM. RTS. L. REV. 227, 233-41 (2015). While the Wiretap Act has been found not to apply extraterritorially when harm is caused abroad, *see* Berlin Democratic Club v. Rumsfeld, 410 F. Supp. 144, 162-63 (D.D.C. 1976), suit has been maintained in a criminal case under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a) (2012), where a foreign individual hacked into a business's computers located in Connecticut. U.S. v. Ivanov, 175 F. Supp. 2d 367 (D. Conn. 2001). In *Ivanov*, the Court specifically found that, for the purpose of the Computer Fraud and Abuse Act, the hack occurred in Connecticut. *Id.* at 372-73.

I. THE PROBLEM

In order to construct an effective exception, it is first worthwhile to explore the confluence of law and events that have given rise to the need. The nature of both computers and the internet, which allow hackers to access larger troves of information from greater distances, is especially problematic given the traditionally strong immunity afforded foreign sovereigns both in international and domestic law. A full recitation of the historical development of the doctrine is beyond the scope of this paper but, where states were once considered absolutely immune from suit,[17] the doctrine has developed to recognize a more restricted approach to immunity now codified in the FSIA.[18]

From an international law perspective, there is no general treaty on sovereign immunity. The United Nations has put together a proposed Convention on Jurisdictional Immunities of States and Their Property but it has not come into effect, and the United States is not a party.[19] Thus, sovereign immunity is considered customary international law ("CIL") (sometimes referred to as Public International Law) at the international level.[20] Some countries, such as the United States, have chosen to codify this CIL in a statute. Once codified, the statute is usually considered a complete set of rules. When a codified statute is inconsistent with CIL, however, numerous U.S. courts have held that the President has the "domestic legal authority" to violate CIL and that it is "subordinate in the U.S. legal system to federal legislation."[21] Thus, the FSIA

Further, in a case where a foreign hacker trespasses into a computer located in the United States, personal jurisdiction could be established by a "minimum contacts" analysis necessary to satisfy Due Process concerns under Int'l Shoe Co. v. Washington, 326 U.S. 310 (1945).

[17] *See* The Schooner Exch. v. McFaddon, 11 U.S. 116, 137 (1812).

[18] 28 U.S.C. § 1602 (2012); for a good history of the doctrine of foreign immunity, *see* CURTIS A. BRADLEY, INTERNATIONAL LAW IN THE U.S. LEGAL SYSTEM 233-56 (2d ed. 2015).

[19] BRADLEY, *supra* note 18, at 233.

[20] *Id.* at 233-32.

[21] *Id.* at 153-54; *See* United States v. Yousef, 327 F.3d 56, 93 (2d Cir. 2003) ("[W]hile courts are bound by the law of nations which is a part of the law of the land, Congress may manifest its will to apply a different rule by passing

and a congressionally enacted exception to the FSIA would prevail over inconsistent CIL, at least in the U.S. domestic legal system.

The FSIA "provides the sole basis for obtaining jurisdiction over a foreign state in the courts of this country."[22] It operates by first providing that "a foreign state shall be immune from the jurisdiction of the courts of the United States"[23] but subsequently enumerates a number of exceptions to that immunity.[24] Most relevant to the topic of this paper are the so-called "non-commercial tort"[25] and state sponsor of terrorism[26] exceptions, but others include waiver, commercial activity, and takings of property.[27]

The FSIA does not, broadly, address the substantive law governing foreign state liability. Instead, it addresses the court's jurisdiction over the foreign state and provides that, when an exception applies, the foreign state "shall be liable in the same manner and to the same extent as a private individual under like circumstances" except that "a foreign state except for an agency or instrumentality thereof shall not be liable for punitive damages."[28] The exception to this normal course, however, is the state sponsor of terrorism exception, which provides a cause of action within the FSIA itself.[29]

---

an act for the purpose.") (internal quotations omitted); Barrera-Echavarria v. Rison, 44 F.3d 1441, 1450-51 (9th Cir. 1995) ("It is well-settled, however, that international law controls only 'where there is no treaty, and no controlling executive or legislative act or judicial decision.'") (quoting The Paquete Habana, 175 U.S. 677, 700 (1900)); Gisbert v. U.S. Attorney General, 988 F.2d 1437, 1447 (5th Cir.), *amended*, 997 F.2d 1122 (5th Cir. 1993) ("Public international law controls, however, only 'where there is no treaty and no controlling executive or legislative act or judicial decision . . . .'") (quoting *Paquete Habana*, 175 U.S. at 700); United States v. Yunis, 924 F.2d 1086, 1091 (D.C. Cir. 1991) ("But the statute in question reflects an unmistakable congressional intent . . . . Our inquiry can go no further."); Garcia-Mir v. Meese, 788 F.2d 1446, 1453 (11th Cir. 1986) ("But public international law is controlling only 'where there is no treaty and no controlling executive or legislative act or judicial decision . . . .'") (quoting *Paquete Habana*, 175 U.S. at 700).

[22] Argentine Republic v. Amerada Hess Shipping Corp., 488 U.S. 428, 443 (1989).

[23] 28 U.S.C. § 1604 (2012).

[24] 28 U.S.C. §§ 1605-1605B (2012).

[25] 28 U.S.C. § 1605(a)(5) (2012).

[26] 28 U.S.C. § 1605A (2012).

[27] *See* 28 U.S.C. §§ 1605(a)(1)-(6) (2012).

[28] 28 U.S.C. § 1606 (2012).

[29] 28 U.S.C. § 1605A(c) (2012).

In the FSIA, "foreign state" includes "a political subdivision of a foreign state or an agency or instrumentality of a state."[30] An "agency or instrumentality of a foreign state" is, in turn, defined to include "organs" of a foreign state as well as corporations that are majority owned by a foreign state.[31] Importantly, the FSIA applies only to foreign countries, and not foreign government officials, meaning that there is no possibility of suing a state official similar to current Eleventh Amendment jurisprudence, which addresses state immunity in the United States.[32]

Overall, the FSIA creates a system in which foreign states are "presumptively immune from the jurisdiction of United States courts"[33] unless a potential litigant can identify a particular exception, creating a significant hurdle to bringing private suit.

Initial efforts to overcome immunity in the context of foreign government cyber-intrusion focused on the non-commercial tort exception.[34] This exception provides that a state "shall not be immune" from suit in instances "not otherwise encompassed in paragraph (2) above," referencing the commercial activity exception at 28 U.S.C. § 16(a)(2), where:

> money damages are sought . . . 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.[35]

[30] 28 U.S.C. § 1603(a) (2012).
[31] 28 U.S.C. § 1603(b) (2012).
[32] Samantar v. Yousuf, 560 U.S. 305 (2010).
[33] Saudi Arabia v. Nelson, 507 U.S. 349, 355 (1993).
[34] *See* Gilmore, *supra* note 16 (Gilmore would later serve as a consulting attorney to the plaintiffs in *Doe v. Federal Democratic Republic of Ethiopia*, discussed in depth below).
[35] 28 U.S.C. § 1605(a)(2) (2012).

Two carve-outs to liability exist, however, where the basis of the claim is either (A) the performance of a "discretionary function" or (B) a "malicious prosecution, abuse of process, libel, slander, misrepresentation, deceit, or interference with contract rights."[36]

Proceeding under the non-commercial tort exception was put to the test in *Doe v. Federal Democratic Republic of Ethiopia*.[37] The plaintiff, who used the pseudonym "Kidane" in connection with his political activities, was an Ethiopian-born, U.S. citizen and asylee, who was involved in the Ethiopian diaspora community in the United States.[38] In his two-count complaint, Kidane charged the Ethiopian government with infecting his home computer, located in Silver Spring, Maryland, with spyware which allowed them to "monitor and record his computer activities and communications."[39] He sought to recover on two bases: first, for a violation of the Wiretap Act, 18 U.S.C. § 2511, and, second, for the common law claim of intrusion upon seclusion.[40] The District Court found that first, the Wiretap Act did not support liability for a country-defendant[41] and second, that the intrusion upon seclusion claim was blocked by the FSIA.[42] The D.C. Circuit upheld this decision finding that, due to the "entire tort rule," the non-commercial tort exception was inapplicable and thus the U.S. did not have jurisdiction over Ethiopian authorities under the FSIA.[43]

---

[36] *Id.*
[37] *Doe I*, 189 F. Supp. 3d 6 (D.D.C. 2016), *aff'd*, No. 16-7081, 2017 WL 971831 (D.C. Cir. 2017).
[38] *Id.* at 9.
[39] *Id.*
[40] Complaint at ¶¶ 90-103, Doe v. Federal Democratic Republic of Ethiopia, 2014 WL 916565 (D.D.C. Mar. 5, 2014) (No. 14 CV 0372) [hereinafter Doe Complaint].
[41] *Doe I*, 189 F. Supp. 3d at 12-15.
[42] *Id.* at 15-28.
[43] *Doe II*, 2017 WL 971831, at *3; additionally, the D.C. Circuit did not reach the question of whether the Wiretap Act authorized Kidane's cause of action, instead concluding that the FSIA "withdraws jurisdiction *in toto*." *Doe II*, 2017 WL 971831, at *2 (emphasis in original).

The first part of the District Court's decision analyzed the text of the Wiretap Act to determine whether Congress meant to create a private cause of action against foreign governments. The court compared the text of 18 U.S.C. § 2511(1), which establishes liability for "*any person*" who "intentionally intercepts . . . any wire, oral, or electronic communication,"[44] with § 2520(a), which provides a private cause of action for civil damages from "*the person or entity*, other than the United States, which engaged in that violation."[45] Based on the discrepancy in language between § 2511(1) making "any person" liable and § 2520(a) providing a cause of action against "the *person or entity*," the District Court concluded that Congress did not intend to hold an entity, like a foreign government, liable for the actions prescribed in § 2511(1).[46]

Next, the District Court proceeded to examine whether Kidane's claim of intrusion upon seclusion fit into the "entire tort" rule embedded in the non-commercial tort exception. FSIA jurisprudence holds that the language in the exception requiring that the injury "occur[] in the United States" means that "not only the injury but also the act precipitating that injury," must occur in the United States.[47] Courts have held this "entire tort" rule to be consistent with

[44] 18 U.S.C. § 2511(1) (2012) (emphasis added).
[45] *Id.* at § 2520(a) (emphasis added).
[46] *Doe I*, 189 F. Supp. 3d at 15 (emphasis added); The District Court did note, however, in contrast to the lack of mention of "entity" liability in § 2511(1), that the Congressional act that added "entity" liability to § 2520(a) simultaneously added "entity" liability to a different section of the Wiretap Act, § 2511(3)(a), which prohibits "a person or entity providing an electronic communication service to the public [from] intentionally divulg[ing] the contents of any communication . . . while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication." *Doe I*, 189 F. Supp. 3d at 14 (quoting 18 U.S.C. § 2511(3)(a)). Thus, the District Court stated that it "does not doubt that the term 'entity,' as used in section 2520, refers to at least some governmental entities for some purposes." *Id.*
[47] Jerez v. Republic of Cuba, 775 F.3d 419, 424 (D.C. Cir. 2014); *see also* O'Neil v. Saudi Joint Relief Comm., 714 F.3d 109, 116 (2d Cir. 2013); O'Bryan v. Holy See, 556 F.3d 361, 381-82 (6th Cir. 2009); Frolova v. Union of Soviet Socialist Republics, 761 F.2d 370, 379-80 (7th Cir. 1985); Asociacion de Reclamantes v. United Mexican States, 735 F.2d 1517, 1525 (D.C. Cir. 1984); Von Dardel v. Union of Soviet Socialist Republics, 736 F. Supp. 1, 7 (D.D.C. 1990).

legislative intent as the exception was adopted to address domestic incidents such as traffic accidents.[48]

The District Court concluded that the infection of Kidane's computer, and the spying conducted thereafter, did not support a finding that the entire tort occurred in the United States.[49] The District Court based its conclusion on several factors including that the tort could not be wholly divorced from the tortfeasor, who precipitated the tort while in Ethiopia.[50] The D.C. Circuit accepted this reasoning and affirmed the holding, stating that "whether in London, Ethiopia or elsewhere, the tortious intent aimed at Kidane plainly lay abroad and the tortious acts of computer programming likewise occurred abroad."[51]

Additionally, the District Court considered other factors including that the expansion of the exception to include "all alleged torts that bear some relationship to the United States," was contrary both to D.C. Circuit jurisprudence and Congressional intent to focus on local incidents.[52] Because such an expansion would involve a "political judgment, raising sensitive issues of foreign relations," the District Court was leery of expanding judicial authority when not otherwise codified in the FSIA.[53] The Court of Appeals did not address this line of reasoning. Instead, it stuck to the contention that the actions alleged did not occur wholly in the United States.

---

[48] Argentine Republic v. Amerada Hess Shipping Corp., 488 U.S. 428, 439-40 (1989) ("Congress' primary purpose in enacting § 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."); *Doe II*, 2017 WL 971831, at *3; *see also* H.R. REP. No. 94-1487, at 20-21 ("Section 1605(a)(5) is directed primarily at the problem of traffic accidents but is cast in general terms as applying to all tort actions for money damages, not otherwise encompassed by section 1605(a)(2).").
[49] *Doe I*, 189 F. Supp. 3d at 25.
[50] *Id.* at 21-23.
[51] *Doe II*, 2017 WL 971831, at *3.
[52] *Doe I*, 189 F. Supp. 3d at 23 (quoting *Reclamantes*, 735 F.2d at 1525).
[53] *Id.* at 23-24.

Despite finding the non-commercial tort exception inapplicable, thus barring jurisdiction over Ethiopia, the District Court proceeded to examine the discretionary function exception laid out in 28 U.S.C. 1605(a)(5)(A) based on "the likelihood that its decision will be appealed and in the interest of judicial efficiency."[54] The D.C. Circuit, however, did not address discretionary function, leaving our only evidence of its applicability with the District Court's reasoning.[55] Discretionary function provides an exception to the non-commercial tort exception, thus re-establishing foreign government immunity, where the alleged tort is "based upon the exercise or performance or the failure to exercise or perform a discretionary function regardless of whether the discretion be abused."[56] In interpreting what actions qualified as discretionary functions, the District Court looked to similar provisions of the Federal Torts Claims Act, in this case 28 U.S.C. § 2680, which governs the United States federal government's immunity in similar circumstances.[57] While declining to reach a decision on a definition, the District Court did reject Ethiopia's argument that their actions should qualify as discretionary by concluding that conduct constituting a serious violation of a U.S. criminal statute did not qualify as discretionary.[58] Overall, however, the District Court stated that "[o]n the present record, the Court can neither conclude that a serious criminal act occurred nor reject the possibility that it did."[59]

Thus, after the *Doe* decisions, plaintiffs looking to establish foreign government liability for hacking into the U.S.-based computers of Americans are left with several lessons. First, since the FSIA provides the sole means for establishing jurisdiction over a foreign government and no current exception applies, a new exception is required to establish liability. Second,

---

[54] *Id.*
[55] *Doe II*, 2017 WL 971831, at *4 n.8 ("We do not reach the applicability of the FSIA provisions governing discretionary functions or torts based upon misrepresentation or deceit. See 28 U.S.C. § 1605(a)(5)(A)–(B)").
[56] 28 U.S.C. § 1605(a)(5)(A) (2012).
[57] *See* MacArthur Area Citizens Ass'n v. Republic of Peru, 809 F.2d 918, 922 (D.C. Cir. 1977).
[58] *Doe I*, 189 F. Supp. 3d at 28.
[59] *Id.*

given the situs requirement in the non-commercial tort exception and the lengthy discussion in *Doe I* about the location of the tort, a new exception will need to explicitly address conduct perpetrated by a foreign government regardless of where that conduct originated. Third, given the District Court's inconclusive statement on the discretionary function exception, a new exception would do well to omit such a requirement while clearly identifying the relevant conduct. Finally, since the District Court's finding that the Wiretap Act is inhospitable to foreign state liability, a new exception will either need to simultaneously amend an existing underlying cause of action or provide a new cause of action. Despite these hurdles, proponents of a new exception should be encouraged by the fact that the District Court also recognized a need for legislative action, suggesting that "[t]he political branches may ultimately deem it advisable to permit suits against foreign sovereigns who, without setting foot on American soil, use technology to commit torts against persons located here."[60]

II. THE SOLUTION

Based on the construction of the FSIA, the current exceptions, and the jurisprudence of FSIA litigation, several key areas must be identified and addressed to construct a new exception. In a recent blog post reaching a similar conclusion about the need for a new cyber-intrusion exception, private attorney Alexis Haller identified these areas as Jurisdictional Provision, Cause of Action, Retroactivity and Statute of Limitations, Appearance/Default, Damages, Execution/Attachment, and Official Immunity.[61] This article adds an additional provision, Executive Designation, and will proceed by exploring the challenges in each area.

Jurisdictional Provision

[60] *Id.* at 25.
[61] Haller, *supra* note 15.

First, a new exception will need a jurisdictional provision to remove the presumption of immunity established in 28 U.S.C. § 1604 and provide a U.S. District Court with jurisdiction. Within such a jurisdictional provision several terms will need to be defined and thus added to 28 U.S.C. § 1603. My suggested new exception, provided below, adds "cyber-intrusion" as a key to liability, establishing the underlying cause of action. Useful terms such as "foreign state" and "United States" are already defined in § 1603.[62]

Cause of Action

Considering the finding in *Doe I* that the Wiretap Act does not support liability for foreign government entities,[63] a new exception must either simultaneously amend an existing cause of action, like the Wiretap Act or the Computer Fraud and Abuse Act ("CFAA"), or provide its own. The state sponsor of terrorism exception, for example, provides a model for a cause of action within the FSIA.[64] Given the desire for uniformity in the FSIA, ease of use and interpretation, and the issues with amending underlying causes of action, this article suggests adding an internal cause of action.

Additionally, the suggested exception borrows language from the Wiretap Act and CFAA in defining "cyber-intrusion," which provides uniformity in determining for which actions foreign governments will be liable.

A. Retroactivity and Statute of Limitations

The state sponsor of terrorism exception includes a retroactivity clause and statute of limitations of 10 years. A 10-year statute of limitations is appropriate but Haller's suggestion

[62] *See* 28 U.S.C. §§ 1603(a)-(b).
[63] *Doe I*, 189 F. Supp. 3d at 12-15.
[64] *See* 28 U.S.C. § 1605A(c).

that a new exception also be made retroactive provides no special reason to break with the norm of non-retroactivity.[65] As such, this article does not adopt that suggestion.

B. Appearance/Default

A major issue in FSIA litigation is appearance and default by defendants. Often, foreign government defendants are unwilling to appear before U.S. courts, even under more benign circumstances. Given the controversy behind cyber-intrusions, a foreign defendant will likely decline to appear, leading to default. The FSIA provides that a court may enter a default judgment if "the claimant establishes his claim or right to relief by evidence satisfactory to the court."[66]

Based on the difficulties of proving attribution in cyber-intrusion cases, and the added difficulty of doing so without discovery in cases of non-appearance, Haller suggests adding a federal law enforcement or intelligence agency certification provision that would allow for the establishment of a rebuttable presumption of liability. Specifically, the suggestion reads:

> If any federal law enforcement or intelligence agency certifies that there is probable cause that a foreign state, or an official, employee or official thereof, committed the act described in section * * *, there shall be a rebuttable presumption that the foreign state, or the official, employee or official thereof, has committed the act. If the foreign state does not appear in the action, that presumption shall be accepted by the district court and shall constitute sufficient evidence to satisfy the requirements of section 1608(e). If the foreign state appears in the action, the rebuttable presumption shall be rendered ineffective until such time, if any, that the foreign state no longer participates in the litigation.[67]

Difficulties with attribution and evidence in cyber-intrusion cases will be discussed later in this article under the "Continuing Issues" section. No form of statutory construction will be able to fully address the problems of proving who attacked a plaintiff. A full analysis of the

[65] *See* Haller, *supra* note 15 (only noting that making statutes retroactive is constitutionally permitted).
[66] 28 U.S.C. § 1608(e) (2012).
[67] Haller, *supra* note 15.

technical means of attributing cyber-intrusions is both beyond the scope of this paper and the technical prowess of its author. This article, however, does not adopt Haller's suggestion.

Relying on government provision of evidence, much of which would most likely be classified, presents numerous issues. Plaintiffs would be dependent on law enforcement agencies and the intelligence community, which often have competing interests. Providing the government with such a large role in litigating a case would, additionally, defeat much of the purpose of devolving the remedy for cyber-intrusions from the realm of foreign policy to the judicial and personal. Further, compelling the law enforcement and intelligence communities to back a claim forces the executive branch into making the awkward political decision of either confronting another sovereign or abandoning their injured citizen. If the government would like to adduce evidence in a particular case by releasing information helpful to a plaintiff, it may do so without being compelled.[68]

While *Doe I* never reached the evidentiary stage, the Complaint sought to establish attribution through the use of a report published by the Munk School of Global Affairs at the University of Toronto, Canada's CitizenLab called "You Only Click Twice: FinFisher's Global Proliferation."[69] The use of this resource shows that private institutions can also furnish plaintiffs with the evidence they need to prove their cases.

C. Damages

The types of damages a foreign state is exposed to varies in the FSIA. First, the FSIA excludes punitive damages against foreign states, but not their agencies or instrumentalities.[70]

[68] *See, e.g.*, Haggard & Lindsay, *supra* note 9 (U.S. government openly attributed cyberattack against Sony to North Korea).
[69] Doe Complaint, *supra* note 40, ¶ 26, Ex. B.
[70] 28 U.S.C. § 1606 (2012).

Next, the state sponsor of terrorism exception removes this hurdle and provides for punitive damages within its cause of action.[71] Under this exception, large punitive damage awards have been common.[72] A new exception should, similar to the terrorism exception, provide for punitive damages to allow for meaningful compensation for plaintiffs' losses.

E. Execution/Attachment

The difficulty of collecting damages is a longstanding issue. Currently, the FSIA provides strong protections against attachment and execution against the property of foreign governments.[73] Similar to the construction of jurisdiction, the FSIA first provides that foreign governments' property will be immune from attachment[74] and then proceeds to remove that immunity through specific, targeted exceptions.[75] For example, even if a plaintiff prior to *Doe* was able to fit their claim into the non-commercial tort exception, the FSIA would limit attachment and execution to "any contractual obligation or any proceeds from such a contractual obligation to indemnify or hold harmless the foreign state or its employees under a policy of automobile or other liability or casualty insurance covering the claim which merged into the judgment."[76]

---

[71] *Id.* at § 1605A(c) ("In any such action, damages may include economic damages, solatium, pain and suffering, and punitive damages."); *id.* at § 1605A(d) ("After an action has been brought under subsection (c), actions may also be brought for reasonably foreseeable property loss, whether insured or uninsured, third party liability, and loss claims under life and property insurance policies, by reason of the same acts on which the action under subsection (c) is based").

[72] *See* JENNIFER K. ELSEA, CONG. RESEARCH SERV., RL31258, SUITS AGAINST TERRORIST STATES BY VICTIMS OF TERRORISM 69 (2008), http://www.fas.org/sgp/crs/terror/RL31258.pdf (providing a chart of compensatory and punitive damage awards).

[73] *See* 28 U.S.C. §§ 1609-1611 (2012).

[74] 28 U.S.C. § 1609 (2012) ("[A] foreign state shall be immune from attachment arrest and execution").

[75] 28 U.S.C. § 1610 (2012).

[76] *Id.* at § 1610(a)(5); Haller, *supra* note 15 ("The plaintiff in a cyberattack case proceeding under the tort exception will be limited to section 1610(a)(5), because the plaintiff likely would not be able to show that the foreign state has waived immunity (§ 1610(a)(1)), that 'the property is or was used for the commercial activity upon which the claim is based' (§ 1610(a)(2)), that 'the execution relates to a judgment establishing rights in property which has been taken in violation of international law or which has been exchanged for property taken in violation of international law' (§ 1610(a)(3)), that 'the execution relates to a judgment establishing rights in property . . . which is acquired by succession or gift, or . . . which is immovable and situated in the United States' (§ 1610(a)(4)), that 'the judgment is

Similar to the terrorism exception, which provides a waiver of immunity from attachment,[77] a new cyber-intrusion exception should have a parallel provision as plaintiffs seeking redress under a new exception will likely face the same challenges of execution as those seeking to collect under the terrorism exception. Additionally, as suggested by Haller, a new exception should also be subject to § 1610(g)(1), "so that plaintiffs can collect from agencies or instrumentalities of the foreign state – even if such agencies or instrumentalities were not involved in the cyber-intrusion at issue."[78]

F. Official Immunity

An additional suggestion is that, since the FSIA applies only to states, there should be a provision allowing injured parties to sue the responsible individuals, regardless of their status as state officials.[79] Adopting such a suggestion, however, is unwise because obtaining jurisdiction over those persons, who would most likely not be in the United States, is difficult. Additionally, current jurisprudence regarding the immunity of foreign state officials is a separate standing body of federal common law. No statute currently codifies such immunity, but strong precedent protects those individuals.[80] Further, the United States has strong obligations to diplomats and consular officials under the Vienna Conventions on Diplomatic and Consular Relations.

based on an order confirming an arbitral award rendered against the foreign state, provided that attachment in aid of execution, or execution, would not be inconsistent with any provision in the arbitral agreement' (§ 1610(a)(6)), or that 'the judgment relates to a claim for which the foreign state is not immune under section 1605A or section § 1605(a)(7) (as such section was in effect on January 27, 2008), regardless of whether the property is or was involved with the act upon which the claim is based' (§ 1610(a)(7)).").

[77] 28 U.S.C. § 1610(a)(7) (2012).

[78] Haller, *supra* note 15.

[79] Haller, *supra* note 15 ("Congress should consider making all of the prior provisions, *mutatis mutandis*, applicable to foreign officials who order or participate in the cyberattack.").

[80] *See* Samantar v. Tousuf, 560 U.S. 305, 324 (2010) (stating that immunity of foreign officials is a matter of common law); Rosenberg v. Pasha, 577 Fed. Appx. 22 (2d Cir. 2014) (upholding District Court's finding of immunity for foreign officials under common law post-*Samantar*); Rishikof v. Mortada, 70 F. Supp. 3d 8, 11-12 (D.D.C. 2014) ("Under common law foreign immunity, a foreign official is entitled to one of two different types of immunity: status-based or conduct-based immunity.").

G. Executive Designation

Finally, an additional element to include in a new exception is executive designation of a foreign state as a "cyber-intruder" and making a private action contingent on that status. The terrorism exception, for example, provides that a court can hear a claim only if the foreign state is designated as a sponsor of terrorism or was so-designated as a result of the incident in question.[81] A designation provision allows the executive to play a gatekeeper role with respect to which countries are potentially liable for suit. It also allows for private causes of action to be linked to a sanctions program, similar to that established by the "State Sponsor of Terrorism" list. Establishing a new sanctions program, and connecting a new cyber-intrusion exception to it, would also assist in finding and seizing assets against which plaintiffs could execute their judgments. Criteria for designation could include frequency of intrusion events, the amount of harm caused, as well as political considerations, as deemed appropriate by the executive.

Taking power away from the executive to determine those liable under the terrorism exception was one of the major points of contention surrounding the passage of the Justice Against Sponsors of Terrorism Act ("JASTA").[82] In essence, JASTA allowed plaintiffs to pursue claims against a government even if the executive had not designated it as a state sponsor of terrorism. The goal was to provide 9/11 victims with a means of pursuing Saudi Arabia, despite the fact that it is not designated on the State Sponsor of Terrorism list.

[81] 28 U.S.C. § 1605A(a)(2)(A)(i) (2012). The term "state sponsor of terrorism" refers to a country which the Secretary of State has determined under section 6(j) of the Export Administration Act of 1979, section 620A of the Foreign Assistance Act of 1961, section 40 of the Arms Export Control Act, or "any other provision of law," has "repeatedly provided support for acts of international terrorism." *See id.* at § 1605A(h)(6).
[82] *See e.g.* James Zogby, *JASTA: Irresponsible And Dangerous*, HUFFINGTON POST (Oct. 01, 2016), http://www.huffingtonpost.com/james-zogby/jasta-irresponsible-and-d_b_12269448.html.

H. The New Exception to the Foreign Sovereign Immunity Act

Congress can add a new exception as either 28 U.S.C. § 1605(a)(8) or 28 U.S.C. § 1605C. Either would be in keeping with the current scheme of the FSIA. The exception should read:

(a) In General.

(1) No Immunity.

A foreign state shall not be immune from the jurisdiction of courts of the United States or of the States in any case in which money damages are sought, including economic damages, solatium, pain and suffering, and punitive damages, for a cyber-intrusion by the foreign state occurring in the United States, regardless of the location of the tortfeasor.

(2) Claim Heard.

The court shall hear a claim under this section if the foreign state is designated as a cyber-intruder at the time the act occurred, or was so designated as a result of such act, and either remains so designated when the claim is filed under this section or was so designated within the 6-month period before the claim is filed under this section.

(b) Limitations.

An action may be brought or maintained under this section if the action is commenced no later than 10-years after the date on which the cause of action arose.

(c) Private Right of Action.

A foreign state that is or was designated as a cyber-intruder by determination of the executive branch, shall be liable to any person who suffers damage or loss by reason of a violation of this section for personal injury caused by acts described in subsection (a). Additionally, Congress should amend 28 U.S.C. § 1610 to add a new section, (a)(8), which should read:

(8) the judgment relates to a claim for which the foreign state is not immune under section 1605(a)(8) [or 1605C], regardless of whether the property is or was involved with the act upon which the claim is based.

Finally, Congress will need to amend 28 U.S.C. § 1603 to add a new definition for cyber-intrusion:

> (f) A "cyber-intrusion" includes:
>
> (1) intentionally intercepting or endeavoring to intercept any wire, oral, or electronic communication; or
> (2) intentionally accesses a computer without authorization or exceeding authorized access, and thereby obtaining information from any protected computer.[83] [84]

III. CONTINUING ISSUES

As the saying goes, "even the best-laid schemes of mice and men may go awry." Alternatively, as adapted for this context, even the best schemed statutory construction may not address all the issues pertinent to future litigation. Thus, it is helpful to predict and discuss several continuing concerns affecting the implementation of a new cyber-intrusion exception that even the best planned exception cannot address.

A. Reciprocity

A common objection to expanding foreign liability, that "if we do it to them, they will do it to us," is relevant here. This critique was expressed by the State Department itself during the

[83] "Protected Computer" is a term borrowed from the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2012), which defines the term at 18 U.S.C. § 1030(e)(2). Therefore, reference can be made to that Act in the context of litigation under the new exception. Additionally, extensive jurisprudence exists on the meaning of "access without authorization" and "exceeds authorized access," which this reference means to incorporate. *See* Gilmore, *supra* note 16, at 237-38.

[84] Definition (1) reflects language from the Wire Tap Act and definition (2) reflects language from the Computer Fraud and Abuse Act. The grammar has been modified slightly to increase clarity.

introduction of the terrorism exception[85] and has continued in criticism of the exception since.[86] It also resurfaced in the wake of JASTA's passage.[87]

Few other countries have terrorism exceptions, as the International Court of Justice ("ICJ") noted in a case between Italy and Germany in which Italy allowed nationals to file a private action in Italian courts against Germany for allegedly violating fundamental human rights norms during World War II.[88] In finding for Germany, the Court also observed that exceptions "limit[ing] . . . immunity on the grounds of the gravity of the acts alleged," like the FSIA, "ha[ve] no counterpart in the legislation of other states."[89] It is also worth noting that Iran has recently initiated suit at the ICJ against the United States over the issue of immunity under the terrorism exception of the FSIA.[90]

Reciprocity, however, has been limited although Cuba and Iran reportedly enacted statutes allowing for suits against the United States for "acts of terrorism or interference."[91] Russia has also adopted a foreign sovereign immunity law based on reciprocity, allowing

[85] *See Foreign Sovereign Immunities Act: Hearing on S. 825 Before the Subcomm. on Courts and Admin. Practice of the S. Comm. on the Judiciary*, 103d Cong. 8-31 (1994) (statements of Stuart Schifter, Deputy Assistant Attorney General, Civil Division, U.S. Department of Justice and Jamison S. Borek, Deputy Legal Advisor, U.S. Department of State) ("In evaluating S. 825, we note the risk of reciprocal treatment by foreign states if we expand our jurisdiction over them.").

[86] *See* Amanda Tuninetti, *Limiting the Scope of the Foreign Sovereign Immunities Act After Zivotofsky II*, 57 HARV. INT'L L.J. 215 (2016); Daveed Gartenstein-Ross, *A Critique of the Terrorism Exception to the Foreign Sovereign Immunities Act*, 34 N.Y.U. J. INT'L L. & POL. 887 (2002); S. Jason Baletsa, *The Cost of Closure: A Reexamination of the Theory and Practice of the 1996 Amendments to the Foreign Sovereign Immunities Act*, 148 U. PA. L. REV. 1247 (2000).

[87] *See* Zogby, *supra* note 82; *Veto Message From The President – S.2040*, WHITE HOUSE (Sept. 23, 2016), *2016* WL 5334803, at *2; Major Gen. (Ret.) Charles E. Tucker Jr., *Saudi 9/11 bill will lead to US military on trial — not our enemies*, THE HILL (Jan. 4, 2017), http://thehill.com/blogs/pundits-blog/defense/312682-saudi-9-11-bill-will-lead-to-us-military-on-trial-not-our-enemies.

[88] Ronald J. Bettauer, *Germany Sues Italy at the International Court of Justice on Foreign Sovereign Immunity – Legal Underpinnings and Implications for U.S. Law*, ASIL INSIGHTS (Nov. 19, 2009).

[89] Jurisdictional Immunity of the State (Ger. v. It.), Judgment, 2012 I.C.J. Rep. 99, ¶ 88 (Feb. 3).

[90] Press Release, International Court of Justice, Iran Institutes Proceedings against the United States with Regard to A Dispute Concerning Alleged Violations of the 1955 Treaty of Amity, (Jun. 15, 2016), [https://web.archive.org/web/20170606022430/http://www.icj-cij.org/docket/files/164/19032.pdf].

[91] Elsea, *supra* note 72, at 9 n.32.

Russian courts to consider the degree of immunity a foreign state affords the Russian Federation.[92]

Reciprocity is a valid concern given the extent of U.S. surveillance programs targeting foreign subjects. The chance of reciprocity is a risk of enacting a new exception, although one the United States has stomached in the past in instituting, and continuing to impose, an exception for state sponsors of terrorism. Executive designation of a country as a "cyber-intruder," as suggested by this article, may limit this risk by only exposing to suit those countries deemed appropriate by the executive. Even so, a larger question exists as to why, if we find such behavior to be a violation of the rights of American citizens and U.S. sovereignty, we conduct such activity on friendly neighbors.

B. Attribution

Conclusively determining who carried out a particular act of cyber-intrusion is challenging.[93] But, this is more of a technical question better addressed by computer experts during the evidentiary portion of a trial rather than legislators at the statutory construction phase. The nature of the internet allows for many opportunities to disguise the origin of an attack, operate in anonymity, or even use proxy organizations to mask state involvement. For example, many attributed the hack of the Democratic National Committee to two online groups called Cozy Bear and Fancy Bear, which reportedly operated in connection with Russian intelligence.[94]

---

[92] Peter Roudik, *Laws Lifting Sovereign Immunity: Russia*, LIBRARY OF CONG. (Oct. 26, 2016), https://www.loc.gov/law/help/sovereign-immunity/russia.php.
[93] *See* Thomas Rid & Ben Buchanan, *Attributing Cyber Attacks*, 38 J. OF STRATEGIC STUD. 4 (2015), http://www.tandfonline.com/doi/abs/10.1080/01402390.2014.977382; *The Attribution Problem in Cyber Attacks*, INFOSEC INSTITUTE (Feb. 1, 2013), http://resources.infosecinstitute.com/attribution-problem-in-cyber-attacks/#gref; Nicholas Tsagourias, *Cyber Attacks, Self-Defence and the Problem of Attribution*, 17(2) J. CONFLICT SECURITY L. 229 (2012), https://academic.oup.com/jcsl/article/17/2/229/852823/Cyber-attacks-self-defence-and-the-problem-of.
[94] David E. Sanger & Nick Corasaniti, *D.N.C. Says Russian Hackers Penetrated Its Files, Including Dossier on Donald Trump*, N.Y. TIMES (June 14, 2016), https://www.nytimes.com/2016/06/15/us/politics/russian-hackers-dnc-trump.html?_r=0.

By using such methods of compartmentalization, foreign intelligence agencies can create extra layers of difficulty in tying shadowy online organizations to brick and mortar foreign intelligence agencies.

As noted above, Haller suggests adding a mechanism for law enforcement and intelligence community certification, which this article rejects. Private firms do exist to help in tracking cyber-attacks. A private cyber-security firm called CrowdStrike assisted the DNC in attributing their cyber-attack to Russia[95] and, as previously mentioned, Kidane submitted a report by CitizenLab as evidence in his complaint.[96] However, as *Doe* was dismissed on jurisdictional grounds, the case never reached the merits and, thus, this evidence was never tested in open court. Only further litigation and borrowing of jurisprudence from domestic cases will determine to what extent attribution will be an issue once the jurisdictional boundary is overcome.

C. Enforcement of Judgments

As mentioned above, even after obtaining a judgment against a foreign state, it can be difficult to collect damages. The FSIA sets up limitations on attachment and execution, which limits the potential pool of assets against which plaintiffs can execute their judgments.[97] Even when such limitations are at their lowest, for example in connection with the terrorism exception, many plaintiffs have found it difficult to collect.[98] For example, judgment amounts under the state sponsor of terrorism exception far exceed the remaining assets of such states in the United States.[99] Those awarded judgments under a new exception will most likely have to line up next to these plaintiffs against many of the same foreign states.

---

[95] *Id.*
[96] Doe Complaint, *supra* note 40, ¶ 26, Ex. B.
[97] 28 U.S.C. § 1610 (2012).
[98] Elsea, *supra* note 72, at 2 ("Nevertheless, U.S. courts have awarded victims of terrorism more than $19 billion against State sponsors of terrorism and their officials, most of which remains uncollected.").
[99] *Id.*

Another obstacle to the enforcement of awards is that, even in the best of circumstances, U.S. judgments travel poorly outside the United States.[100] First, unlike arbitral awards and the Convention on the Recognition and Enforcement of Foreign Arbitral Awards (the "New York Convention"), no convention on the recognition and enforcement of foreign judgments exists.[101]

Thus, the current framework for execution of awards against sovereigns "is notoriously difficult to navigate" with many obstacles, including the lack of independent judiciaries in states against which judgments are sought; the fact that many governments do not have significant holdings outside of their borders and, when they do, corporate instrumentalities often hold them; and that many third party states are hesitant to take "coercive measures" against the property of fellow states.[102] Another reason is jurisdictional, as many foreign courts will not execute a judgment where their own courts would not have had jurisdiction. For example, recently an Italian Court refused to enforce the award in a major state sponsor of terrorism case, *Flatow v. Iran*, because an Italian Court would not have had jurisdiction over the defendant Iran in a similarly situated case in Italy.[103] Since no other country has a cyber-intrusion exception to their foreign sovereign immunity statutes, the same obstacle will likely apply.

There are several mitigating factors to this concern, however. First, like many aspects of litigation, weighing the potential rewards against the obstacles and costs of bringing suit is part

[100] *See* George K. Foster, *Collecting from Sovereigns: The Current Legal Framework for Enforcing Arbitral Awards and Court Judgements against States and their Instrumentalities, and some Proposals for its Reform*, 25 ARIZ. J. INT'L & COMP. L. 665, 680-81 (2008) (excellent examination of the framework for enforcing judgments against foreign sovereigns).

[101] The Hague Conference on Private International Law has an ongoing project to draft a convention on the enforcement of judgments. The Special Commission composed to assemble a draft will have a third meeting tentatively scheduled for November 13-17, 2017. *See The Judgments Project*, HAGUE CONFERENCE ON PRIVATE INT'L LAW, https://www.hcch.net/en/projects/legislative-projects/judgments.

[102] Foster, *supra* note 100, at 666.

[103] Thomas Weatherall, *Flatow n. Iran. No. 21946. 99 Rivista Di Diritto Internazionale 293 (2016). Corte Suprema Di Cassazione Della Repubblica Italiana, October 20, 2015*, 110 AM. J. INT'L L. 540 (2016).

of the calculus of whether a particular suit is worthwhile. Many aspects of private litigation come with potential risks and rewards. FSIA litigation is no different.

Additionally, as suggested earlier, a new exception could be linked to a corresponding sanctions regime to (1) enhance deterrence and (2) provide an asset pool against which to execute judgments. Further, damages awarded under a new exception will, most likely, be significantly less than the awards given out under the terrorism exception. Cyber-intrusions, while causing serious injury, rarely do so in the order of magnitude of terrorist attacks. Compare, for example, the damages sought in *Doe*, whose suit under the Wiretap Act provided for "equitable and declaratory relief, in addition to statutory demands of the greater of $10,000 or $100 per day for each violation" and reasonable attorney's fees[104] with the ultimate award in *Flatow v. Iran* of $247.5 million, including $225 million in punitive damages.[105]

Finally, much of the value of a cyber-intrusion exception will be symbolic, allowing citizens to gain recognition of their harm and attribute it to an offending state. For many defendants, there will be emotional value in being able to publicly shame a perpetrating state.

IV. THE BIGGER PICTURE

Since a cyber-intrusion exception would expand U.S. jurisdiction to actions precipitated outside the United States, especially by foreign sovereigns, many will undoubtedly claim an infringement of international comity. Comity has long been a means of constraining the power of countries outside of their borders. Thus, it is worth exploring the normative fit of a new exception in the international system and weigh its benefit against the goals and restrictions of comity.

[104] Doe Complaint, *supra* note 40, ¶ 98.
[105] James Dao, *Judgment for Terrorism is $248 Million*, N.Y. TIMES (Mar. 12, 1998), http://www.nytimes.com/1998/03/12/nyregion/judgment-for-terrorism-is-248-million.html.

Comity has been both described as an idea "in flux from a legal perspective"[106] and at the same time the basis for nearly all "the doctrines of American law that mediate the relationship between the U.S. legal system and those of other nations."[107] William Dodge, after an impressive survey of court opinions on the subject, defines international comity as "deference to foreign government actors that is not required by international law but is incorporated in domestic law."[108] More specifically, he presents a tabular definition, with one axis defined as the foreign actor to whom deference is targeted, with foreign lawmakers receiving "prescriptive comity," foreign tribunals receiving "adjudicative comity," and foreign governments receiving "sovereign party comity."[109] On the other axis are "principle[s] of recognition," which recognize the acts of those foreign actors and "principle[s] of restraint," which constrain U.S. domestic action from coming into conflict with the acts of those foreign actors.[110]

Comity played an important role in both the development and doctrinal underpinnings of sovereign immunity. Immunity in international law stems from the development of the concept of sovereignty, which dictates that States are supreme within their realms. This, however, leads to the question of what happens when two sovereign entities come into conflict, if one cannot be supreme over the other. "[I]nternational law," as Ernest Bankas asserts, developed by its "very nature [to] support[] the equality of states, as a special ingredient necessary for the harmonious existence of states."[111] The equality of states, then, leads to the development of state immunity, because "[a]lthough classical writers of international law did not explicitly deal at length with the

[106] Dan E. Stigall, *International Law and Limitations on the Exercise of Extraterritorial Jurisdiction in U.S. Domestic Law*, 35 HASTINGS INT'L & COMP. L. REV. 323, 335 (2012).
[107] William S. Dodge, *International Comity in American Law*, 115 COLUM. L. REV. 2071, 2072 (2015).
[108] *Id.* at 2078.
[109] *Id.* at 2079.
[110] *Id.*
[111] ERNEST K. BANKAS, THE STATE IMMUNITY CONTROVERSY IN INTERNATIONAL LAW 6 (2005).

notion of immunity of foreign states from the jurisdiction of domestic courts, at least in the main, their writings in one way or another gave support to the idea of absolute sovereignty which in turn logically gave foundation to the concept of state immunity in international law."[112] Comity, then, is the conceptual tool necessary to effect the harmonious coexistence of coequal sovereigns as one sovereign must consider another's sovereignty when their jursidictions come into contact.

The United States, in fact, played a major role in defining and codifying the theory of sovereign immunity in 1812 in *The Schooner Exchange*.[113] In his opinion, Justice Marshall characterized his finding of immunity as "stemming from both considerations of international comity and from principles of customary international law."[114] This decision was the first instance to give true meaning to the doctrine of immunity in international law and thus carries great precedential weight both domestically and internationally.[115]

The concept of sovereignty, however, has evolved. Governments are no longer considered absolutely immune within their jurisdictions, as evidenced by the fact that American citizens regularly sue the federal and state governments. Similarly, foreign sovereign immunity has moved away from a conception of absolute immunity, as expressed in *The Schooner Exchange*, to a more restricted approach, now codified in the FSIA. The justification for foreign sovereign immunity, however, has not changed and still rests on comity and the principle of maintaining harmonious relations between sovereigns. Comity, as well, should develop to become more permissive to holding foreign governments accountable for actions for which

[112] *Id.* at 14.
[113] *The Schooner Exchange*, 11 U.S. 116 (1812); *see* Republic of Austria v. Altmann, 541 U.S. 677, 688 (2004) ("Chief Justice Marshall's opinion in Schooner Exchange v. McFaddon . . . is generally viewed as the source of our foreign sovereign immunity jurisprudence.").
[114] Bradley, *supra* note 17, at 235.
[115] Bankas, *supra* note 109, at 13 ("In fact, American courts were the first to express their thoughts and perhaps to give true meaning to the doctrine of sovereign immunity.").

domestic governments are already liable. This is already true to a great extent, as restrictive immunity is now the norm.

A new cyber-intrusion exception does not offend modern notions of comity. First, comity is meant to function in times of harmony, ensuring that domestic and foreign law do not conflict. Even Justice Marshall, in his absolutist view of sovereignty, recognized that it was most applicable during peaceful, friendly coexistence.[116] Executive designation of offending nations, as suggested by this article, would bring the aggressive actions of cyber-intruders, which both infringe personal rights and U.S. sovereignty, out of the realm of peaceful coexistence and into the realm of hostility. In essence, a new cyber-intrusion exception cannot work to harmonize coequal legal regimes, because it covers a subject matter of direct conflict.

Second, the Supreme Court has recognized that comity is optional and that although foreign governments prior to the FSIA "had a justifiable expectation that, as a matter of comity, United States courts would grant them immunity for their public acts (provided the State Department did not recommend otherwise), they had no 'right' to such immunity."[117] Removing comity during a hostile and invasive action, like the invasion of another country's sovereignty, would seem like the approriate instance to exercise that optionality.

Finally, a new exception can be seen as actually benefitting comity as it, in a small way, realigns the liabilities of domestic and foreign governments. Our own government's sovereignty does not extend so far as to permit it to hack into our computers. Why should a foreign government's sovereignty extend so far?

---

[116] *Schooner Exchange*¸ 11 U.S. at 147 ("a public armed ship, in the service of a foreign sovereign, *with whom the government of the United States is at peace*, and having entered an American port open for her reception, on the terms on which ships of war are generally permitted to enter the ports *of a friendly power*, must be considered as having come into the American territory, under an implied promise, that while necessarily within it, and demeaning herself *in a friendly manner*, she should be exempt from the jurisdiction of the country.") (emphasis added).
[117] *Altmann*, 541 U.S. at 694 (2004).

V. CONCLUSION

Introducing a new cyber-intrusion exception to the FSIA would allow American citizens harmed and intimidated while on U.S. soil by foreign powers their day in court. The nature of the internet and the ability of those with ill intent to affect people and businesses around the world in near anonymity requires U.S. lawmakers to reexamine the limitations of sovereign immunity in the realities of the internet age. Providing a private cause of action to those harmed can be both an effective deterrent tool and a way of providing redress to those injured by malicious acts. This article has presented a potential exemption and its possible ramifications and continuing issues. Overall, such an exemption is needed and can fit with current conceptions of the extent of U.S. jurisdiction.