NOTE

CYBER ATTACK EXCEPTION TO THE FOREIGN SOVEREIGN IMMUNITIES ACT

Paige C. Anderson†

INTRODUCTION 1087
I. THE INADEQUACY OF THE CURRENT FSIA EXCEPTIONS TO ADDRESS CYBER ATTACKS 1090
A. The Commercial Activity Exception 1091
B. The Tort Exception 1094
II. USING THE TERRORISM EXCEPTION AS A MODEL FOR A CYBER ATTACK EXCEPTION 1097
A. The History and Text of the Terrorism Exception 1097
B. Modeling a Cyber Attack Exception 1101
III. ADDRESSING POTENTIAL PROBLEMS WITH THIS MODEL . 1103
A. Attribution 1103
B. Foreign Relations 1106
IV. COMPARISON TO ALTERNATIVE SOLUTIONS 1108
A. Alternative Solutions Pursued by the United States Government 1108
1. *U.S. Department of Justice's Indictment of Five Chinese Hackers* 1108
2. *U.S.-China Bilateral Cybersecurity Agreement* 1109
3. *The Problems with These Domestic, Government-Controlled Solutions* 1111
B. Alternative Solutions Pursued by Other Parties 1112
CONCLUSION 1113

INTRODUCTION

In December 2013, holiday shoppers at Target became the second-largest group of consumers in history to have their data

† Cornell Law School, Candidate for J.D., 2017. Thanks to Professor Zachary Clopton, whose guidance produced this note; to Steve and Susan Anderson, whose guidance produced the author; and to Nate Smith, for edits and such.

stolen in a cyber attack.[1] Up to 110 million shoppers' credit and debit card numbers, phone numbers, and email addresses comprised the stolen information. During the fallout, consumers and banks held Target alone responsible for the breach.[2] Target settled with the consumers and created a fund of $10 million to compensate those whose data had been compromised.[3] The banks' class-action lawsuit against Target concluded when the U.S. Court of Appeals for the Eighth Circuit dismissed the appeal, thereby affirming the settlement.[4]

In November 2014, Sony Pictures Entertainment was the victim of a breach focused more on retribution than financial gain. In response to the studio's impending release of the movie *The Interview*, hackers stole and published pirated versions of five films, scripts for upcoming projects, and employees' personal data, including salaries and social security numbers.[5] They also installed malware that shut down employees' computers for several days.[6] The Federal Bureau of Investigation identified the North Korean government as the perpetrator of the attack.[7] North Korea's apparent motivation was the content of *The Interview*, which depicted two Central Intelligence Agency agents attempting to kill the North Korean leader Kim Jong-Un.[8] The government had previously de-

---

1 Elizabeth A. Harris & Nicole Perlroth, *For Target, the Breach Numbers Grow*, N.Y. TIMES, Jan. 10, 2014, at B1. The largest group is the credit card users of Heartland Payment Systems in 2009. *Id.*

2 *In re* Target Corp. Customer Data Sec. Breach Litig., 309 F.R.D. 482, 484–85 (D. Minn. 2015).

3 *Target Agrees to Pay $10 Million to Settle Lawsuit from Data Breach*, REUTERS (Mar. 19, 2015), http://www.reuters.com/article/2015/03/19/us-target-settlement-idUSKBN0MF04K20150319 [https://perma.cc/LEX2-PKRS].

4 Judgment, *In re* Target Corp. Customer Data Sec. Breach Litig., No. 15-08017 (8th Cir. June 23, 2016), ECF No. 15.

5 Brooks Barnes & Nicole Perlroth, *Sony Pictures and F.B.I. Widen Hack Inquiry*, N.Y. TIMES, Dec. 3, 2014, at B3; Peter Elkind, *Sony Pictures: Inside the Hack of the Century, Part 1*, FORTUNE (June 25, 2015), http://fortune.com/sony-hack-part-1/ [https://perma.cc/U57Z-4VTN].

6 Nicole Perlroth, *Sony Pictures Computers Down for a Second Day After Network Breach*, N.Y. TIMES: BITS (Nov. 25, 2014), http://bits.blogs.nytimes.com/2014/11/25/sony-pictures-computers-down-for-a-second-day-after-network-breach/ [https://perma.cc/VH7V-D5BP].

7 Nicole Perlroth, *New Study May Add to Skepticism Among Security Experts That North Korea Was Behind Sony Hack*, N.Y. TIMES: BITS (Dec. 24, 2014), http://bits.blogs.nytimes.com/2014/12/24/new-study-adds-to-skepticism-among-security-experts-that-north-korea-was-behind-sony-hack/ [https://perma.cc/X87N-3TPF]. The cybersecurity community did not widely accept the FBI's attribution, but the public statement of attribution by the U.S. government was notable in its own right.

8 Barnes & Perlroth, *supra* note 5, at B3.

nounced the film and called its release an act of war.[9] Following the attack, Sony itself made no attempt to respond or seek compensation; instead, former employees sued Sony for failing to protect their information[10] and President Obama issued an executive order imposing economic sanctions on the North Korean government.[11]

These two examples indicate a broader trend in cyber attacks: when consumers are the target, they sue the companies; when companies are the target, they sue no one. Neither group pursues recourse against the attackers themselves. There are good reasons for this: identifying the perpetrators of cyber attacks is problematic and uncertain,[12] the information on who might be responsible often belongs to the government and is classified,[13] and the seeming likelihood of enforcing a judgment against elusive hackers in a foreign country is nil. However, these obstacles do not preclude a solution so much as they require a creative one.

Liability for these incidents should fall on the most culpable party: the perpetrator of the attack. At least in the case of government-sponsored cyber attacks—which account for a large proportion of such attacks and are often some of the most sophisticated[14]—the solution is a private right of action against the foreign government.[15] Despite the above-mentioned impediments, such a private right of action is feasible and would remedy parties' inability to recover damages from the party who most directly caused their injury.

The United States Congress can provide this right—in fact, it has done so before. In 1996, Congress legislated into existence a private right of action for victims of terrorist attacks

---

9 *North Korea Complains to U.N. About Film Starring Rogen, Franco*, REUTERS (July 9, 2014), http://www.reuters.com/article/2014/07/09/us-northkorea-unfilm-idUSKBN0FE21D20140709 [https://perma.cc/2C56-LSUK].

10 Ryan Faughnder, *Sony Pictures Reaches Settlement in Hacking Lawsuit*, L.A. TIMES (Sept. 2, 2015), http://www.latimes.com/entertainment/envelope/cotown/la-et-ct-sony-hack-studio-reaches-agreement-to-settle-with-plaintiffs-20150902-story.html [https://perma.cc/2AUV-9U2L].

11 Exec. Order No. 13,687, 80 Fed. Reg. 819 (Jan. 2, 2015).

12 David E. Sanger & Julie Hirschfeld Davis, *Hacking Linked to China Exposes Millions of U.S. Workers*, N.Y. TIMES, June 5, 2015, at A1.

13 *See id.*

14 *See* Scott J. Shackelford & Richard B. Andres, *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem*, 42 GEO. J. INT'L L. 971, 974 (2011).

15 Pursuing a judgment against individuals, rather than a government, would increase the likelihood of default judgments against absent defendants.

sponsored by foreign governments.[16] It did so in response to several high-profile terrorist attacks with American victims.[17] Congress created this right by amending the Foreign Sovereign Immunities Act (FSIA) to provide an exception to foreign sovereign immunity where a state sponsor of terrorism had committed or sponsored a terrorist attack.[18] Although other exceptions to the FSIA already existed—namely, the tort exception and the commercial activity exception[19]—these offered insufficient recourse for the victims of terrorist attacks who could not fit their claims neatly into either of those boxes.[20] Terrorist attacks required a specially tailored right of action to address the particularities of such litigation.

This Note argues that Congress should create a similar exception to the FSIA for cyber attacks sponsored by foreign governments. Part I will address the current exceptions to the FSIA and why they are an insufficient remedy for private parties victimized by state-sponsored cyber attacks. Part II will use the terrorism exception as a model for creating a cyber attack exception. Part III will address potential limitations of such an exception and attempt to address several counterarguments to the proposal. The conclusion will briefly discuss why a cyber attack exception is a better solution than the alternatives.

I
THE INADEQUACY OF THE CURRENT FSIA EXCEPTIONS TO ADDRESS CYBER ATTACKS

In addition to the terrorism exception to the FSIA, other exceptions include: (1) waiver of immunity, (2) an exception for tortious activity, (3) an exception for commercial activity, and (4) an exception for expropriation of property.[21] The lattermost is inapplicable in the cyber context because electronic property cannot, strictly speaking, be expropriated; it can be replicated or deleted, but there is no way for a government to *take* it in the

16 Antiterrorism and Effective Death Penalty Act of 1996, Pub. L. No. 104-132, § 221, 110 Stat. 1214, 1241 (1996); Omnibus Consolidated Appropriations Act, 1997, Pub. L. No. 104-208, § 589, 110 Stat. 3009, 3009–172 (1996). Although there was dispute about the scope of this private right, Congress further amended the Foreign Sovereign Immunities Act in 2008 to make the scope unambiguous. *See infra* notes 73–76 and accompanying text.

17 H.R. REP. NO. 104-383, at 37 (1995).

18 28 U.S.C. § 1605A (2012).

19 28 U.S.C. § 1605(a) (2012).

20 *See infra* subpart II.A.

21 28 U.S.C. § 1605(a).

traditional sense.[22] Assuming that foreign governments will not waive their immunity in suits against them for committing or sponsoring cyber attacks, then, the FSIA as is offers two exceptions through which plaintiffs can bring such suits against foreign governments. This Part will examine how each of these exceptions has limited utility for victims of state-sponsored cyber attacks.

A. The Commercial Activity Exception

Perhaps the broadest exception to the FSIA is the commercial activity exception.[23] It provides an exception to sovereign immunity where the sovereign is acting within the market as a private actor would.[24] The exception requires that the claim be "based upon" commercial activity and have some degree of connection to the United States.[25]

Victims of cyber attacks face a major potential problem in proving that an attack is commercial activity at all. In *Republic of Argentina v. Weltover*, the Supreme Court held that whether a foreign government was engaged in commercial activity hinges on whether the government was acting as a "regulator of [the] market" (which would be non-commercial activity) or as "a private player within it"[26] (which would be commercial activity). The government's act must have been of the nature that is "the *type* of action[ ] by which a private party engages in 'trade and traffic or commerce.'"[27] No court has ever considered whether cyber attacks are that type of action.[28]

Whether a cyber attack would be considered commercial depends on how the courts choose to define the relevant activity. If hacking, meaning merely gaining unauthorized access to

---

22 *See, e.g.*, Brief for United States as Amicus Curiae, Weinstein v. Islamic Republic of Iran, Civ. No. 14-7193, 2015 WL 9488371, at 9–13 (D.C. Cir. 2015) (arguing that domain names are not property under federal law). The scholarship surrounding takings in the cyber context is scarce and deserves further development. Without statutory or precedential guidance extending takings doctrine to purely electronic information, claimants are unlikely to succeed on a takings theory.

23 *See* 28 U.S.C. § 1605(a)(2).

24 Republic of Argentina v. Weltover, Inc., 504 U.S. 607, 614 (1992).

25 28 U.S.C. § 1605(a)(2).

26 504 U.S. at 614–15.

27 *Id.* at 614 (quoting BLACK'S LAW DICTIONARY (6th ed. 1990)).

28 The most analogous case, *CYBERsitter, LLC v. People's Republic of China*, involved whether distribution of plaintiff's stolen computer code was commercial activity for the purposes of FSIA. 805 F. Supp. 2d 958 (C.D. Cal. 2011) (applying the commercial activity exception to FSIA where the Chinese government licensed and distributed the software developed by the plaintiff). The plaintiff did not allege that China had obtained the code through hacking. *Id.* at 968–69.

a computer system, is the relevant activity, then any cyber attack might qualify as commercial activity because private actors are as capable of hacking as foreign governments are. This would mean that every time a foreign government deployed a cyber attack, it would be acting no differently than a private player. If, however, the relevant activity is the function that the cyber attack has in the physical world, then only certain attacks would qualify. For example, stealing the intellectual property of a rival player in the market (in the case of commercial cyber espionage) could be commercial activity; targeting a company's computer systems because the company had offended the hacker might not. The former might be construed as "within the market" whereas the latter most likely would not.

Because hacking can serve so many different functions, it seems unlikely that a court would make a blanket statement that all hacking is commercial activity. Categorizing an attack based on its function therefore seems more likely, which would necessarily exclude the many victims of cyber attacks whose victimization is not for commercial gain. Sony Pictures likely could not recover if courts adopted such a definition, because the attack it experienced was retaliatory.[29]

Even if courts were to decide that hacking is the relevant activity, the fact that hacking is criminal under United States federal law suggests that courts would hold that it is non-commercial.[30] In a line of cases claiming that other crimes, such as murder, kidnapping, and assassination fall under this exception, the courts have held that none of these activities are commercial.[31] The only criminal activity which courts routinely find to be commercial under the FSIA is the formation of illegal contracts.[32] These findings are based on the fact that contracts are typical means of private parties operating in the

---

29 *See supra* notes 5–9 and accompanying text.

30 Courts tend to look to domestic law of the foreign state for determining the legality of the conduct in question. *See* Adler v. Fed. Republic of Nigeria, 219 F.3d 869, 877 (9th Cir. 2000).

31 *See* Cicippio v. Islamic Republic of Iran, 30 F.3d 164, 167–68 (D.C. Cir. 1994) (kidnapping); Letelier v. Republic of Chile, 748 F.2d 790, 797 (2d Cir. 1984) (assassination); Berkovitz v. Islamic Republic of Iran, 735 F.2d 329, 331–32 (9th Cir. 1984) (murder).

32 *See* Keller v. Cent. Bank of Nigeria, 277 F.3d 811, 816 (6th Cir. 2002); *Adler*, 219 F.3d at 875; Southway v. Cent. Bank of Nigeria, 198 F.3d 1210, 1217–18 (10th Cir. 1999).

market,[33] thereby meeting the private-player standard articulated in *Weltover*.[34] Because hacking is not a routine function for private parties operating in the market, it is likely that its illegality would make it non-commercial for the purposes of the FSIA.

If a court were to find that a cyber attack was, in fact, commercial activity, the other two requirements—that the claim must be "based upon" commercial activity and that that activity must have a connection to the United States—would be comparatively less problematic. The Supreme Court considered the "based upon" requirement in *Saudi Arabia v. Nelson*[35] and concluded that for commercial activity to form the basis of a claim, the commercial activity must satisfy those elements for which the plaintiff has the burden of proof.[36] Because cyber attacks typically produce some injury, even if that is only invasion of privacy, the attack in question will usually give rise to the victim's injury and therefore form the basis of the victim's claim. Therefore, a cyber attack victim could probably show that the claim is "based upon" the attack.

The degree of connection is also unlikely to be a problem because the exception's connection requirement is quite permissive. The exception requires only that commercial activity abroad "cause[ ] a direct effect in the United States."[37] The Supreme Court has construed "direct effect" broadly, as necessitating merely a non-trivial effect.[38] The non-triviality requirement could exclude certain cyber attack suits where the attack caused *de minimis* harm, but it would most likely include all attacks leading to information being stolen or computer systems being impaired. As long as the claimant experienced these non-trivial effects on a computer in the United States, the claimant could likely show that the attack had caused the effects entailed by the connection requirement.[39]

Again, though, despite the likelihood that the "based upon" requirement and the connection requirement could accommodate the claims of cyber attack victims, this depends on the

---

33 *See, e.g.*, *Adler*, 219 F.3d at 875 ("The fact that the contract was for an illegal purpose, and therefore was unenforceable, does nothing to destroy its commercial nature.").

34 *See supra* notes 26–27 and accompanying text.

35 Saudi Arabia v. Nelson, 507 U.S. 349 (1993).

36 *Id.* at 357.

37 28 U.S.C. § 1605(a)(2).

38 Republic of Argentina v. Weltover, Inc., 504 U.S. 607, 618 (1992).

39 *Cf. In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation, 829 F.3d 197, 208–09 (2d Cir. 2016) (affirming that data's location is that of the server on which it is stored).

open question of whether the attack is commercial activity at all. That open question is unlikely to resolve in favor of this group of potential plaintiffs. The commercial activity exception intends to put foreign governments in the same position as private parties in the market in which they compete, and thus it does not offer a clear path to compensation for victims of cyber attacks that are outside any market. Furthermore, based on the courts' previous construction of criminal activity in the context of this exception, many victims would likely not be able to recover under the exception. They must turn elsewhere for a remedy.

B. The Tort Exception

The FSIA also provides an exception for all torts that do not fall within the commercial activity exception.[40] Congress created this exception specifically to hold foreign governments liable for traffic accidents that their diplomats caused,[41] but included all torts involving personal injury, death, or "damage to or loss of property."[42] The tort exception has two exceptions of its own: it does not cover injury resulting from the performance of a "discretionary function,"[43] and it does not cover "any claim arising out of malicious prosecution, abuse of process, libel, slander, misrepresentation, deceit, or interference with contract rights."[44] Additionally, the tort must have occurred in the United States.[45] In order to fit a cyber attack into the tort box, then, two challenges arise: the attack must have caused "damage to or loss of property," and it must have occurred within the United States. Both of these requirements pose particular difficulty in the cyber context.

Regarding property damage, courts have struggled to answer the question of which electronic effects constitute damage. There are innumerable potential effects of a cyber attack, and few of them give a clear answer: When malware shuts off a computer, is that damage? When it slows the functioning of a computer? When it uses the computer as part of a botnet? When it copies documents from the hard drive and replicates them on the hacker's computer? What about merely recording keystrokes? Each of these effects is common due to the

---

40 28 U.S.C. § 1605(a)(5).
41 H.R. REP. NO. 94-1487, at 20–21 (1976).
42 28 U.S.C. § 1605(a)(5).
43 *Id.* § 1605(a)(5)(A).
44 *Id.* § 1605(a)(5)(B).
45 *Id.* § 1605(a)(5).

proliferation of malware; each poses a definitional problem for property damage.

There is little agreement on which of these examples might qualify. Some courts do not recognize a cyber tort at all.[46] Some courts hold that slowing or otherwise limiting the function of a computer constitutes damage. For example, in the formative California case *Intel Corp. v. Hamidi*, the California Supreme Court held that the use of Intel's servers to send six unsolicited emails to Intel's 35,000 employees was insufficient; because the emails had not limited the servers' functioning, "as by significantly reducing [their] available memory and processing power," there had been no damage.[47] Other courts require a lesser showing—mere unauthorized use of a computer system qualifies as damage.[48] This lack of consensus means that victims of cyber attacks do not have any standard that might predict whether they could recover under the tort exception. Nor does the law seem to be moving in any particular direction; instead, courts offer disjointed, contradictory rules that coalesce only in their discomfort adapting common-law tort doctrines to cyber incidents.[49]

Furthermore, these holdings do not directly address the stealing of data, which is of fundamental concern for individuals with sensitive personal information and for companies with valuable intellectual property. As discussed in the Introduction, companies must rely on the U.S. government to respond to commercial cyberespionage against them.[50] And although the government handles retaliation for these attacks, that retaliation offers no recourse for their victims. Domestic tort law does not give any guidance for how to litigate commercial espionage of intangible information as a tort.[51] Certain exception-

46 *See* Omega World Travel, Inc. v. Mummagraphics, Inc., 469 F.3d 348, 359 (4th Cir. 2006) ("Oklahoma courts appear never to have recognized [a] tort based upon intangible invasions of computer resources."); Inventory Locator Serv., LLC v. Partsbase, Inc., No. 02-2695, 2005 WL 2179185, at *11–12 (W.D. Tenn. Sept. 6, 2005) (noting that Florida "does not recognize a cause of action for trespass to chattels in cyberspace").

47 Intel Corp. v. Hamidi, 71 P.3d 296, 306 (Cal. 2003).

48 *See* Patricia L. Bellia, *Defending Cyberproperty*, 79 N.Y.U. L. REV. 2164, 2226–32 (2004) (discussing cases in which courts have "allowed system owners to exclude unwanted uses when they have provided strong signals that the use is unwanted").

49 Takings law, which comprises the substantive law relevant to the FSIA's expropriation exception, is similarly ill-fitting for cyber attacks. *See supra* note 22 and accompanying text.

50 *See supra* text accompanying notes 11–13.

51 As a point of comparison, courts have held that the current *statutory* law prohibiting commercial espionage does not cover espionage of intangible informa-

ally sophisticated cyber attacks can cause physical damage to the hardware that they infect; these attacks, however, are among the rarest and most sophisticated.[52] Most cyber attacks involve information being stolen but no physical damage to the infiltrated machine.[53] And in these far more common cases, plaintiffs are unlikely to succeed on a tort claim despite cognizable commercial injury.

The requirement that the United States be the situs of the tort creates a second major challenge for victims of cyber attacks bringing tort claims. The situs requirement could hypothetically apply to any or all of the following: the computer from which the attacker launched the attack, the Internet cables through which the malware traveled, the servers on which the victim's data was stored, the personal computer through which the victim accessed that data, or where the effects of the attack manifested.

Even outside the cyber context, there is no workable answer to the question of what conduct must be within the United States. Federal courts tend to require both the tortious conduct and its resulting injury to have occurred domestically.[54] Although a few circuits permit some relevant conduct to have happened abroad, they do so only when the conduct within the United States could, by itself, constitute a tort.[55] In contrast, the Restatement (Third) of Foreign Relations Law says that only the injury must occur domestically.[56] Cyberspace exacerbates this disagreement by offering many potential situses to consider. Adding even more unpredictability, some of the relevant locations to a cyber attack—like where the malware traveled between attacker and victim—may not be controlled by either

---

tion. *Compare* United States v. Aleynikov, 676 F.3d 71, 77 (2d Cir. 2012) (holding "that the theft and subsequent transmission of purely intangible property is beyond the scope of the NSPA"), *with* United States v. Agrawal, 726 F.3d 235, 235–44 (2d Cir. 2013) (finding that when defendant removed computer code which was in a tangible form consisting of thousands of sheets of paper . . . "he was engaged in the theft or conversion of a 'good' in violation of NSPA").

52 Shackelford & Andres, *supra* note 14, at 972.

53 *See generally* David D. Clark & Susan Landau, *Untangling Attribution*, 2 HARV. NAT'L SEC. J. 531, 536–42 (2011) (describing the most common classes of cyber attacks, none of which involve physical damage to hardware).

54 Working Grp. of the Am. Bar Ass'n, Report, *Reforming the Sovereign Immunities Act*, 40 COLUM. J. TRANSNAT'L L. 489, 565–66 (2002).

55 Scott A. Gilmore, *Suing the Surveillance States: The (Cyber) Tort Exception to the Foreign Sovereign Immunities Act*, 46 COLUM. HUM. RTS. L. REV. 227, 254–55 (2015). Gilmore argues that the situs requirement (and the tort exception as a whole) are a workable remedy in the cyber context; this argument seems to ignore the divergent interpretations of the situs requirement.

56 RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 454 cmt. e (AM. LAW INST. 1987).

the attacker or the victim. As a result, the location of the injury could potentially be one that neither the attacker nor the victim anticipated.[57] This too emphasizes how poorly cyber attacks fit within the situs requirement.

As a final note, the discretionary function exception could also pose a problem in certain cases depending on the defendant state. The discretionary function protects government officials who are exercising discretion to implement a state policy.[58] Where cyber attacks further such a state policy, a government and its officials could avoid liability by claiming that the attacks were merely the implementation of that policy. This is not purely hypothetical: China has an official policy that could be interpreted as encouraging commercial espionage.[59] Although it is difficult to predict whether a court would interpret that policy the same way, or if other governments might ever adopt a more explicit policy, it is conceivable that a country could take the diplomatic risk of adopting a pro-cyber attack policy constructed to evade liability under the discretionary function exception.

Ultimately, however, the property damage and situs requirements create the greatest obstacles for claimants. Because neither the damage nor the location of cyber attacks neatly parallels those requirements in the tort exception, this exception is also an unsatisfactory option for victims of cyber attacks. Their claims would have to meet unpredictable, ill-fitting standards, making success under this exception unreliable.

II
USING THE TERRORISM EXCEPTION AS A MODEL FOR A CYBER ATTACK EXCEPTION

A. The History and Text of the Terrorism Exception

In 1996, Congress passed the Antiterrorism and Effective Death Penalty Act (AEDPA), which included an amendment to the FSIA.[60] The AEDPA was a response to a litany of terrorist attacks against U.S. citizens both domestically and abroad.[61]

---

57 Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326, 378–88 (2015).

58 Working Grp. of the Am. Bar Ass'n, *supra* note 54, at 570.

59 Scott J. Shackelford et al., *Using BITs to Protect Bytes: Promoting Cyber Peace by Safeguarding Trade Secrets Through Bilateral Investment Treaties*, 52 AM. BUS. L.J. 1, 11 (2015).

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

61 H.R. REP. NO. 104-383, at 37 (1995).

These attacks, according to the legislative history, represented a "serious and growing threat" that necessitated increased capability to hold the responsible parties liable.[62]

Congress intended the amendment to the FSIA to be an "economic and financial weapon against . . . outlaw states."[63] Specifically, the amendment created a new exception to foreign sovereign immunity for "suits alleging extrajudicial killing, torture, aircraft sabotage, or hostage-taking undertaken by, or on behalf of, a foreign government."[64] The claimant—although not necessarily the victim—must have been a United States national at the time of the attack.[65] The foreign government must have been designated by the State Department as a state sponsor of terrorism either before the attack or as a result of the attack.[66]

In addition to amending the text of the FSIA to include this exception, Congress passed a separate amendment five months later which created a private right of action for victims of such attacks.[67] This amendment, known as the Flatow Amendment, became an explanatory note printed after the list of exceptions to the FSIA.[68] Despite this apparent informality, the Flatow Amendment had the same legal force as the text of the statute.[69] Its scope, however, was construed narrowly so as to exclude suits against foreign governments themselves and to allow only suits against "officials, employees, [or] agents of a foreign state."[70] As for compensation under this private right of action, plaintiffs struggled to collect.[71] Doing so required assistance from the executive branch in freeing blocked assets, which the executive branch was free to withhold for national security reasons and reluctant to give for political reasons.[72]

---

62 *Id.*

63 *Id.* at 62.

64 *Id.* at 41.

65 *Id.* at 62.

66 *See* Flatow v. Islamic Republic of Iran, 999 F. Supp. 1, 16 (D.D.C. 1998).

67 Omnibus Consolidated Appropriations Act, 1997, Pub. L. No. 104-208, § 589, 110 Stat. 3009, 3009–172 (1996).

68 *Flatow*, 999 F. Supp. at 12–13.

69 *Id.* at 13 ("The amendment should be considered to relate back to the enactment of [the terrorism exception] as if they had been enacted as one provision . . . .").

70 Cicippio-Puleo v. Islamic Republic of Iran, 353 F.3d 1024, 1033 (D.C. Cir. 2004).

71 William P. Hoye, *Fighting Fire with . . . Mire? Civil Remedies and the New War on State-Sponsored Terrorism*, 12 DUKE J. COMP. & INT'L L. 105, 118–19 (2002).

72 *See id.* at 119.

In 2008, fed up with judiciary's narrow construction of the Flatow Amendment and especially with the executive branch's barriers to collection,[73] Congress converted the terrorism exception to its current form.[74] Now in its own section separate from the other exceptions, the terrorism exception contains a private right of action, in the statutory text, against both foreign governments and their officials, employees, or agents.[75] A provision concerning attachment of property has removed the barriers previously employed by the executive branch.[76]

As codified in the 2008 amendment, the terrorism exception is precisely tailored to the challenges of litigating suits against state sponsors of terrorism. Unlike the tort or commercial activity exceptions, which concern broad categories of conduct and therefore must be constructed broadly, the terrorism exception need only address particular and comparatively rare suits. This permits a high degree of specificity to address potential interference by the judicial or executive branches.

First, the terrorism exception's private right of action stands in contrast to the other exceptions to the FSIA, which provide only that the courts will have jurisdiction over claims brought under them.[77] This reflects the relative dearth of case law concerning terrorism as compared to that concerning torts, commercial relationships, or property rights. By expressly including a private right of action, Congress removed the possibility of judges finding an insufficient historical or statutory basis for a suit based on a terrorist attack. Congress abrogated the need for such a basis by specifying which four types of actions it meant to proscribe: torture, extrajudicial killing, aircraft sabotage, and hostage-taking.[78] Confining the scope of the exception to these categories also shields it from judicial or political disagreement over what qualifies as terrorism.

Furthermore, the exception imposes liability not just for the commission of terrorist acts, but also for "the provision of material support or resources for such an act."[79] In this way,

---

73 154 CONG. REC. H8,098–01 (daily ed. Sept. 15, 2008) (statement of Sen. Scott).

74 National Defense Authorization Act for Fiscal Year 2008, Pub. L. No. 110-181, § 1083, 122 Stat. 3, 338–44 (codified at 28 U.S.C. § 1605A (2012)).

75 28 U.S.C. § 1605A.

76 28 U.S.C. § 1610(g) (2012).

77 First Nat'l City Bank v. Banco para el Comercio Exterior de Cuba, 462 U.S. 611, 620 (1983).

78 28 U.S.C. § 1605A(1).

79 *Id.* The definition of "material support or resources" is that originally established by the Violent Crime and Law Enforcement Act of 1994, Pub. L. No. 103-322, § 120005, 108 Stat. 1796, 2022–23 (codified at 18 U.S.C. § 2339A(b) (2012)):

Congress included a type of conduct—material support—which is uniquely important for the terrorism exception. Unlike other torts, where material support plays a less proximate role in the injury, Congress determined that material support for terrorism is just as reprehensible, and just as necessary to deter, as perpetration. Rather than leave this to judicial interpretation, the exception clearly identifies it in its intended scope of liability.

Other requirements also ensure that application of the statute will hew closely to Congress's desired remedy. The requirement that the defendant state be designated a state sponsor of terrorism[80] narrows the list of possible defendant states. By limiting suits in this way, Congress avoids numerous pitfalls. First, the executive branch designates which governments may be liable under the exception, which keeps ultimate control over foreign affairs within the executive branch. Second, the governments that have been designated as state sponsors of terrorism are on notice that they may be liable to individuals under this exception, which bolsters the justification for creating another exception to the general principle of foreign sovereign immunity. Third, the designation requirement is temporally flexible: the foreign government may have been designated a state sponsor of terrorism at the time of the attack *or* as a result of the attack. This ensures that the law may be responsive to changing geopolitical conditions.

Moreover, Congress gave the executive branch another limitation on suits under the terrorism exception: the ability to stay discovery to preserve an ongoing investigation or operation "related to the incident that gave rise to the cause of action."[81] This ensures that individual plaintiffs will not compromise the government's ability to respond to terrorist attacks how it sees fit. However, after ten years, the stay can be renewed only if the

---

(1) the term "material support or resources" means any property, tangible or intangible, or service, including currency or monetary instruments or financial securities, financial services, lodging, training, expert advice or assistance, safehouses, false documentation or identification, communications equipment, facilities, weapons, lethal substances, explosives, personnel (1 or more individuals who may be or include oneself), and transportation, except medicine or religious materials;
(2) the term "training" means instruction or teaching designed to impart a specific skill, as opposed to general knowledge; and
(3) the term "expert advice or assistance" means advice or assistance derived from scientific, technical or other specialized knowledge.

80 28 U.S.C. § 1605A(a)(2)(A).

81 28 U.S.C. § 1605(g)(1)(A) (2012).

Attorney General can show it is necessary.[82] By placing the burden of proof on the government after that length of time, Congress has limited the likelihood that the executive branch will unreasonably use secrecy as an excuse for denying recovery to individual plaintiffs.

Finally, the exception contains numerous provisions to address the difficulty plaintiffs have in collecting on their judgments.[83] One automatically establishes a lien on any property of the defendant state within the court's jurisdiction.[84] This circumvents executive control over which plaintiffs may recover which assets. A second provision makes all property of a defendant state subject to attachment following a judgment against the state.[85] It emphasizes that the property will be attachable regardless of the extent to which the defendant state exerts control over it or profits from it. By removing discretionary reasons to deny attaching certain property, Congress increased the effectiveness of the remedy it intended to establish.

These provisions strike a careful balance of executive and judicial control. While respecting the foreign affairs powers of the executive branch, the exception removes executive discretion that could limit plaintiffs' recovery on a case-by-case basis. Crafting numerous carefully-tailored rules to allocate discretion between the branches, Congress designed a private right of action that maximizes its potential to reach its stated goals.

B. Modeling a Cyber Attack Exception

Current conditions are ripe for a cyber attack exception. Much like the seeming increase of terrorist attacks against Americans, which prompted the terrorism exception, cyber attacks against U.S. citizens and companies are on the rise.[86] Unlike the terrorist attacks of the 1980s and 90s, however, the number of cyber attacks is underpublicized;[87] many companies do not go public after being attacked lest it harm their business interests.[88] This indicates that, if anything, cyber attacks are more of a problem than the public knows about.

---

82 *Id.* § 1605(g)(2).

83 28 U.S.C. § 1605A(g); 28 U.S.C. § 1610(g) (2012).

84 28 U.S.C. § 1605A(g).

85 28 U.S.C. § 1610(g).

86 Shackelford & Andres, *supra* note 14, at 974.

87 *See* Alan W. Ezekiel, Note, *Hackers, Spies, and Stolen Secrets: Protecting Law Firms from Data Theft*, 26 HARV. J.L. & TECH. 649, 653 (2013).

88 *See id.*

Given that feelings of cyber-insecurity are already high,[89] there is ample evidence that the time has come for an effective remedy to a persistent problem. What follows is a suggested framework based on the structure and content of the terrorism exception.

> **(a) 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 not otherwise covered by this chapter in which money damages are sought against a foreign state for unprivileged access to or use of proprietary electronically-stored information, impairment of the function of a computer system, damage to computer hardware, or the provision of material support or resources for such acts 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 and such acts cause substantial effects in the United States.
>
> **(b) Claim heard.**—The court shall hear a claim under this section if
>
> (a) the claimant was, at the time the act described in paragraph (a) occurred—
>
> (A) a national of the United States;
>
> (B) a member of the armed forces; or
>
> (C) otherwise an employee of the Government of the United States, or of an individual performing a contract awarded by the United States Government, acting within the scope of the employee's employment; and
>
> (2) the claimant files suit not more than 5 years after the claimant became aware of the conduct that gave rise to the cause of action
>
> **(c) Private right of action**.—A foreign state and any official, employee, or agent of that foreign state while acting within the scope of his or her office, employment, or agency, shall be liable to:
>
> (1) a national of the United States,
>
> (2) a member of the armed forces,
>
> (3) an employee of the Government of the United States, or of an individual performing a contract awarded by the United States Government, acting within the scope of the employee's employment, or
>
> (4) the legal representative of a person described in subparagraph (1), (2), or (3) of this paragraph, for damage

---

89 Shackelford & Andres, *supra* note 14, at 974 ("President Obama has stated that $1 trillion was lost to cybercrime in 2009 . . . . This revelation prompted Rhode Island Democrat Sheldon Whitehouse to argue, 'I believe we are suffering what is probably the biggest transfer of wealth through theft and piracy in the history of mankind.'").

> caused by acts described in paragraph (a) of that foreign state, or of an official, employee, or agent of that foreign state, for which the courts of the United States may maintain jurisdiction under this section for money damages.

Several components of this proposed exception deserve explanation. First, and most importantly, the exception creates a private right of action for cyber attacks. This prevents claimants from having to rely on common-law precedent or ill-fitting statutes to assert their right to a remedy. Second, the statute of limitations for such claims would be five years. This is significantly less than the terrorism exception's statute of limitations because cyber attacks will generally cause less grave harm than terrorist attacks. Notably, however, the statute of limitations is five years after the claimant detects the attack, not after the attack itself. This acknowledges the prevalence of sophisticated cyber attacks capable of causing harm without immediate detection.[90]

The proscribed conduct is modeled after the terrorism exception in that it identifies categories that are broad enough to include most kinds of cyber attacks.[91] Material support, which could use the same definition incorporated into the terrorism exception,[92] is included to account for the possibility of states using individuals who are not government employees to carry out cyber attacks.[93] Finally, the exception requires that the cyber attack produced "substantial effects" in the United States, which would avoid the need to rely on a theory of extraterritorial jurisdiction to prosecute a cyber attack that was conducted in the state sponsor's territory.[94]

III
ADDRESSING POTENTIAL PROBLEMS WITH THIS MODEL

A. Attribution

Attribution is notoriously difficult for cyber attacks, in part because it is so easy for hackers to falsify the source of the

---

90 *See* Ezekiel, *supra* note 87, at 652.

91 Clark & Landau, *supra* note 53, at 536–42 (listing distributed denial of service attacks, spam, identity theft, and data exfiltration as the primary classes of attacks).

92 *See* 28 U.S.C. § 1605A.

93 Shackelford & Andres, *supra* note 14, at 975.

94 For an explanation of extraterritorial jurisdiction and the difficulty facing claims that rely on it, see William S. Dodge, *Understanding the Presumption Against Extraterritoriality*, 16 BERKELEY J. INT'L L. 85 (1998).

attacks.[95] Even high-profile attacks frequently go unattributed.[96] The U.S. government rarely takes the step of publicly attributing an attack to a foreign government, even when there is wide suspicion of a particular actor.[97] When the U.S. government does identify an attacker, as with the Sony attack, neither experts nor the media take this to be conclusive;[98] nor should they, given the classified and possibly politically-motivated nature of such attributions. Given how difficult it is for victims to identify their attackers, let alone to agree on whether that identification is correct, why create a private right of action that depends on attribution to provide any remedy at all?

The answer is that civil litigation is a better context than most to confront the problematic factual question of attribution. In the media, any author can attribute an attack to a foreign government with a minimal level of certainty, constrained only by the journalistic ethics of his or her publication. For the U.S. government, publicly announcing that a foreign government was behind a cyber attack represents a foreign relations decision with major consequences and therefore should only be done with a high degree of certainty.[99] Civil litigation falls in between these two extremes.

In fact, civil litigation offers a modest but radical solution to the problem of attribution: claimants need only prove the identity of their attackers *by a preponderance of the evidence*. This departs markedly from the current process of attribution for cyber attacks, which requires a substantially higher degree of certainty. Moreover, civil litigation routinely relies on expert witnesses to assist laypeople in making complex or highly technical factual determinations. Already there are expert witnesses who testify about cybersecurity and cyber investigations.[100] Similarly, there are experts (not yet widely employed as witnesses) who act as consultants following cyber attacks.[101] Cybersecurity firms have powerful attribution capabilities that they could use as a basis for expert testimony in

---

95 *See, e.g.*, Clark & Landau, *supra* note 53, at 537.

96 For example, the party or parties responsible for the Target data breach have never been publicly identified.

97 *See infra* notes 109–11 and accompanying text.

98 *See, e.g.*, Perlroth, *supra* note 7.

99 *See infra* subpart III.B for further discussion of foreign relations challenges.

100 *See, e.g.*, Music Grp. Macao Commercial Offshore Ltd. v. Foote, No. 14-cv-03078-JSC, 2015 WL 3882448, at *6 (N.D. Cal. June 23, 2015); United States v. Welton, No. CR 09-00153, 2009 WL 4507744, at *5 (C.D. Cal. Nov. 30, 2009).

101 *See, e.g.*, Brooks Barnes & Nicole Perlroth, *Sony Films Are Pirated, and Hackers Leak Studio Salaries*, N.Y. TIMES, Dec. 2, 2014, at B1 (noting that Sony

court.[102] Based on such testimony for either side, the factfinder could evaluate whether the attribution was, more likely than not, correct. In this way, claimants could overcome the difficulties of attribution by using resources (cybersecurity firms) and procedures (expert testimony) already in place.

A valid and serious objection to this system would be that the risk of mistaken attribution is too high. While suits brought under the terrorism exception also depend on the reliability of civil litigation, the consequences of error are constrained by the requirement that the defendant state be designated by the State Department as a state sponsor of terrorism.[103] That way, if the civil suit renders a verdict based on an incorrect finding of fact, then the cost of that mistake will fall on a state whom the United States has little interest in appeasing anyway.

As discussed below, however, constructing an executive-branch limitation on a cyber attack exception might ultimately be undesirable. Alternatively, one way to limit fallout from mistaken attribution would be to include a provision in the exception that limited the *res judicata* effect of any attribution for a particular cyber attack: findings of attribution would not be binding on the same parties or other parties in future suits. Doing so would parallel the protection that the Supreme Court has afforded to the United States against nonnmutual offensive collateral estoppel.[104] By allowing a defendant state to re-litigate the issue in subsequent suits, each factfinder could make its own determination about attribution, thereby increasing the likelihood of eventually correcting the mistake. This would not prevent the embarrassment caused by the first erroneous attribution; however, the risk of that embarrassment might have other benefits. For example, it might incentivize countries to pursue domestic prosecution of hackers whose malware shares identifying features with, and therefore might be mistakenly attributed to, that country's government.

Pictures hired consultants from FireEye, an "online security firm[ ]," to help respond to the cyber attack).

102 The website of the cybersecurity firm employed by Sony Pictures offers "Litigation Support" and notes that it provides expert testimony. MANDIANT CONSULTING, https://www.fireeye.com/services/mandiant-litigation-support.html [https://perma.cc/WU2P-5MY9].

103 *See supra* note 65 and accompanying text.

104 United States v. Mendoza, 464 U.S. 154, 158 (1984).

B. Foreign Relations

As mentioned above, the cyber attack exception I have suggested omits a major foreign-relations safeguard that is in the terrorism exception: the state sponsor of terrorism designation. This omission arguably carries the risk of upsetting the balance of foreign-relations power. By giving the executive branch the exclusive power to enumerate the possible defendants to terrorism-exception suits, the executive branch and not the claimant has ultimate control over the potential for diplomatic embarrassment caused by such a suit. The history of suits under the terrorism exception indicates that the executive branch often prefers to minimize claimants' ability to use the exception at all; critics' chief complaint about these suits has been executive-branch refusal to un-block assets that could compensate victims.[105] Because state sponsors of terrorism have few assets within the United States that are not blocked by the executive branch, this refusal acts as a near-complete bar to plaintiffs' recovery.[106] Arguably, the executive branch would strongly oppose a cyber attack exception given its obvious discomfort with the terrorism exception.

That executive-branch attitude may not extend to the cyber attack context, however. The public stance of the executive branch on terrorist attacks and state sponsors of terrorism is resounding, unwavering condemnation. For cyber attacks sponsored by foreign governments, on the other hand, the executive branch has been hesitant to confront the governments responsible; critics say unjustifiably so.[107] For example, following the revelation that Chinese hackers had stolen data on 21.5 million citizens from the United States Office of Personnel Management in two separate cyber attacks,[108] the executive branch never publicly confirmed the attacks' national origin. Although widely acknowledged in the media as a Chinese operation,[109] the government itself made no such attribution. This

105 Ilana Arnowitz Drescher, *Seeking Justice for America's Forgotten Victims: Reforming the Foreign Sovereign Immunities Act Terrorism Exception*, 15 N.Y.U. J. LEGIS. & PUB. POL'Y 791, 813–15 (2012).

106 *Id.* at 814.

107 *See* David E. Sanger, *Countering Cyberattacks Without a Playbook*, N.Y. TIMES, Dec. 23, 2014, at A3; Jack Goldsmith, *More Harmful Public Hand-Wringing on Possible Sanctions Against China for Cyber Theft*, LAWFARE BLOG (Aug. 31, 2015, 5:45 AM), https://www.lawfareblog.com/more-harmful-public-hand-wringing-possible-sanctions-against-china-cyber-theft [https://perma.cc/7S4H-HTYP].

108 Julie Hirschfeld Davis, *Hacking of Government Computers Exposed 21.5 Million People*, N.Y. TIMES, July 10, 2015, at A1.

109 *See, e.g.*, Michael S. Schmidt et al., *Chinese Hackers Pursue Key Data on U.S. Workers*, N.Y. TIMES, July 9, 2014, at A1; Kevin Liptak et al., *China Might Be*

suggests that even after the most egregious cyber attacks, the executive branch is not eager to assign blame.

One possible reason for that reluctance is that the diplomatic cost of attribution could be very high, and the near-impossibility of attributing an attack with complete certainty makes it even higher. Therefore, while controlling judgments under the terrorism exception offers the U.S. government the chance to quietly soften its stance against the defendant state, judgments under a cyber attack exception would offer the chance to quietly toughen its stance. Doing so might offset the government's inability to take a hard line publicly due to the difficulties of attribution. Were the cyber attack exception to include a designation requirement like that in the terrorism exception, the U.S. government would have to play a role in attribution that it does not seem to want.

The contrary view on a cyber attack exception would be that because it implicates foreign affairs more directly than the traditional, pre-terrorism exceptions to foreign sovereign immunity, the response to cyber attacks should remain under the exclusive control of the executive branch. The executive branch coordinates all of the government's diplomatic efforts, and because cybersecurity agreements are now part of those efforts,[110] giving private parties this mechanism would decrease the coherence and effectiveness of the United States' cybersecurity negotiations. Moreover, if the executive branch decides to take a harder line against state-sponsored cyber attacks in the future, it should be able to set the terms for doing so rather than relying on private actors.

The answer to this objection lies in the scope of the cyber attack exception, which importantly excludes attacks by governments against other *governments*.[111] This means that espionage against government information—military secrets, intelligence capabilities, and internal decision-making processes—may remain free from liability even when conducted in cyberspace. No doubt the United States government conducts precisely these kinds of cyber attacks and would not want to set a precedent of pursuing domestic prosecution for these actions. All that a cyber attack exception would do, then,

---

Building Vast Database of Federal Worker Info, Experts Say, CNN (June 6, 2015, 9:38 AM), http://www.cnn.com/2015/06/04/politics/federal-agency-hacked-personnel-management/ [https://perma.cc/NQ2F-9WHB].

110 Jack Goldsmith, *What Explains the U.S.-China Cyber "Agreement?"*, LAWFARE BLOG (Sept. 26, 2015, 9:20 AM), https://www.lawfareblog.com/what-explains-us-china-cyber-agreement [https://perma.cc/L28C-8277].

111 As does the U.S.-China cyber agreement. *Id.*

is exclude *private* parties as legitimate targets for foreign governments.

Notably, the United States would likely be bound by this exclusion as well, since other countries might well be inspired to pass similar legislation imposing liability on the United States for its cyber attacks against private parties. But this is hardly a drawback. Citizens of other countries deserve protection equally as much as United States citizens. Were every country to pass such a law, it would merely and properly confine government-sponsored attacks to non-civilian targets.

IV
COMPARISON TO ALTERNATIVE SOLUTIONS

A. Alternative Solutions Pursued by the United States Government

1. *U.S. Department of Justice's Indictment of Five Chinese Hackers*

One alternative to the proposed legislation is prosecution of the perpetrators of cyber attacks. For instance, in May 2014, the United States Department of Justice announced the indictment of five members of the Chinese military for their alleged hacking of six U.S. companies in the nuclear, solar power, and steel industries.[112] Notably, this indictment suggested that the Department of Justice had reached the conclusion that the FSIA did not protect these military employees. This came in spite of the fact that the indictment focused on activities that, as discussed above, are problematic under the FSIA's current exceptions: unauthorized access to computers, the transfer of malware, commercial espionage, and trade secret theft.

In doing so, the Department of Justice distinguished between hacking for economic gain and hacking for national security purposes.[113] This distinction is not one recognized by

---

112 *U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage*, OFFICE OF PUBLIC AFFAIRS, U.S. DEP'T OF JUSTICE (May 19, 2014), http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor [https://perma.cc/X2CZ-J7WW]. The hackers were identified as Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, and Gu Chunhui of Unit 61398 in the Third Department of the People's Liberation Army. *Id.* The targeted companies were identified as Westinghouse Electric Company, U.S. subsidiaries of SolarWorld AG, United States Steel Corporation, Allegheny Technologies, Inc., the United Steel, Paper and Forestry, Rubber, Manufacturing, Energy, Allied Industrial and Service Workers International Union, and Alcoa Inc.

113 David E. Sanger, *With Spy Charges, U.S. Draws a Line That Few Others Recognize*, N.Y. TIMES (May 19, 2014), http://www.nytimes.com/2014/05/20/

the Chinese government. The indictment and the surrounding rhetoric met with skepticism from commentators who pointed out that the United States confounds its own distinction when it spies on private foreign companies to gather information relevant to trade deals.[114]

The indictment used domestic liability to deter foreign actors from perpetrating cyber attacks against U.S. private parties, much like an exception to the FSIA would. Rather than rely on international consensus, it was a unilateral declaration of disapproval by the United States. Moreover, it seems to have worked as a deterrent. Although the indicted individuals are unlikely to ever face prosecution,[115] the *Washington Post* reported in November 2015 that the number of cyber attacks by the Chinese military against U.S. companies had dropped significantly since the indictment was announced.[116] The indictment's success illustrates that, should the United States government have the political will to pursue prosecution of those responsible for state-sponsored cyber attacks, that threat of prosecution can cause gradual but effective deterrence of further attacks.

2. *U.S.-China Bilateral Cybersecurity Agreement*

A second alternative to domestic legislation would be bilateral agreements prohibiting cyber attacks against the signatory countries. The United States has already signed such an agreement with China, which has prompted considerable media coverage and skepticism.[117] Announced in September

---

us/us-treads-fine-line-in-fighting-chinese-espionage.html [https://perma.cc/3KWC-J9WL].

114 Jack Goldsmith, *Why Did DOJ Indict the Chinese Military Officers?*, LAWFARE BLOG (May 20, 2014), https://www.lawfareblog.com/why-did-doj-indict-chinese-military-officers [https://perma.cc/A566-WNNW] ("[S]ome elements of the indictment concern cyber-snooping in connection with trade disputes, which at least sounds a lot like the kind of cyber-snooping on firms that the United States does."); Sanger, *supra* note 107 ("[T]he United States spies regularly for economic advantage when the goal is to support trade talks . . . .").

115 Paul Rosenzweig, *More Thoughts on the DOJ China Indictment*, LAWFARE BLOG (May 20, 2014, 9:40 AM), https://www.lawfareblog.com/more-thoughts-doj-china-indictment [https://perma.cc/3AL2-3EPD].

116 Ellen Nakashima, *Following U.S. Indictments, China Shifts Commercial Hacking Away from Military to Civilian Agency*, WASH. POST (Nov. 30, 2015), https://www.washingtonpost.com/world/national-security/following-us-indictments-chinese-military-scaled-back-hacks-on-american-industry/2015/11/30/fcdb097a-9450-11e5-b5e4-279b4501e8a6_story.html [https://perma.cc/4FW7-8RAF].

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

2015, the agreement is the first-ever cyber "arms deal."[118] The agreement addressed the practice of state-sponsored cyber attacks against private parties;[119] both countries agreed to "mitigate malicious cyber activity emanating from their territory" and to forgo "conduct[ing] or knowingly support[ing] cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors."[120] Although the phrase "conduct or knowingly support" is not defined in the agreement, the agreement indicates that China acquiesced to American pressure to desist its sponsorship of commercial espionage.[121]

Despite the obvious step forward that such an agreement represented in cyber-relations between the two countries, the content of the agreement—and what it lacks—may limit its effectiveness. Notably, the agreement does not prohibit cyber espionage conducted for a national security purpose rather than an economic purpose.[122] This could leave certain U.S. private parties with security-related information vulnerable to attacks by the Chinese government.[123] More broadly, the *types* of attack prohibited by the agreement are not those most commonly conducted by China against U.S. targets. As David Sanger of the *New York Times* noted about the negotiations,

> While [the] agreement could address attacks on power stations, banking systems, cellphone networks and hospitals, it

---

ment-cyber [https://perma.cc/R53F-W3WY] (doubting the ability of the agreement to constrain Chinese hacking).

118 David E. Sanger, *U.S. and China Seek Arms Deal for Cyberspace*, N.Y. TIMES (Sept. 19, 2015), http://www.nytimes.com/2015/09/20/world/asia/us-and-china-seek-arms-deal-for-cyberspace.html [https://perma.cc/B4BK-JPX9].

119 *Fact Sheet: President Xi Jinping's State Visit to the United States*, WHITE HOUSE OFF. OF THE PRESS SECRETARY (Sept. 25, 2015), https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states [https://perma.cc/Q9TR-FBJ4].

120 *Id.*

121 Jack Goldsmith, *Correction/Update: China Did Accept the American Formulation in the Cyber Deal*, LAWFARE BLOG (Sept. 27, 2015), https://www.lawfareblog.com/correctionupdate-china-did-accept-american-formulation-cyber-deal [https://perma.cc/QR6U-YBJ8].

122 *See Fact Sheet: President Xi Jinping's State Visit to the United States*, *supra* note 119.

123 *See* Matthew Dahl, *What Effect Could Chinese Military Reorganization Have on the Recent US-China Cyber Agreement?*, LAWFARE BLOG (Nov. 3, 2015, 5:55 PM), https://www.lawfareblog.com/what-effect-could-chinese-military-reorganization-have-recent-us-china-cyber-agreement [https://perma.cc/HF9E-B32X] ("This leaves the door open for cyber espionage against private companies, for example, in the defense sector which China could claim is related to national security, but which the US sees as seeking a competitive commercial advantage.").

> would not, at least in its first version, protect against most of the attacks that China has been accused of conducting in the United States, including the widespread poaching of intellectual property and the theft of millions of government employees' personal data.[124]

Besides the narrow scope of its agreement, the nature of cyber attacks means that the difficulty of attributing cyber attacks to the Chinese government could prevent the United States from effectively enforcing the agreement.[125]

The drawbacks of the agreement have not kept it from catching on: both the UK and Germany signed similar agreements with China within weeks of the United States' agreement.[126] These agreements between several of the world's most powerful countries suggest that a proliferation of such bilateral agreements could substitute for a multilateral convention and allow the prohibition on state-sponsored cyber attacks to develop gradually as it becomes politically palatable.

3. *The Problems with These Domestic, Government-Controlled Solutions*

These solutions, however, share two fundamental problems. First, the pursuit of recourse depends not on the victims' motivation but on the government's. As the U.S. government has already indicated in its response to other major cyber attacks, governments are not always motivated to hold the culpable party responsible.[127] The second problem is that the victims are not compensated for their losses. The indictments, being based in criminal law, may lead to fines, but those payments would go to the U.S. government rather than to the victims.[128] Bilateral cybersecurity agreements, at least in their current form, contain no provisions whatsoever about compensation. Moreover, the agreements are merely statements of the signatories' intention not to conduct cyber attacks against the other; they contain no means for enforcement.[129]

---

124 Sanger, *supra* note 118.

125 *See* Goldsmith, *supra* note 117.

126 Rowena Mason, *Xi Jinping State Visit: UK and China Sign Cybersecurity Pact*, GUARDIAN (Oct. 21, 2015, 12:13 PM), http://www.theguardian.com/politics/2015/oct/21/uk-china-cybersecurity-pact-xi-jinping-david-cameron [https://perma.cc/EL9R-GN23]; Stefan Nicola, *China Working to Halt Commercial Cyberwar in Deal with Germany*, BLOOMBERG (Oct. 29, 2015, 8:31 AM), http://www.bloomberg.com/news/articles/2015-10-29/china-working-to-halt-commercial-cyberwar-in-deal-with-germany [https://perma.cc/D6LU-S3YT].

127 *See supra* notes 105–09 and accompanying text.

128 *See* 18 U.S.C. § 1030 (2008).

129 Goldsmith, *supra* note 117.

Hypothetically, future cybersecurity agreements could contain stronger enforcement provisions, or at least waive the signatories' sovereign immunity for cyber attacks in the other signatories' domestic courts. The extant agreements, however—which are presumably the strongest agreements that are diplomatically achievable at present—contain no such protections beyond the good intentions of the signatories.

B. Alternative Solutions Pursued by Other Parties

In addition to the United States government's current efforts to deter state-sponsored cyber attacks, other alternatives exist that could come from different sources. First, the private sector could strengthen its nascent cybersecurity insurance industry. Currently, insurance companies offer coverage to companies, although not to individuals, for losses from data breaches or hacking.[130] This market could expand its protection to individuals and thereby provide compensation to nearly all of the potential victims of state-sponsored cyber attacks. Although this solution might not deter such attacks, since it would place the financial burden on the consumers and providers in the insurance industry rather than on the state sponsors of the attacks, it would at least provide compensation to the victims. Even so, companies or individuals will have had to purchase insurance ahead of time or indemnity would be unavailable.

On the other hand, the solution could come from the international community. For example, a multilateral convention, containing similar declarations to those contained in the bilateral agreements with China, could establish an international prohibition on state-sponsored cyber attacks. Although international consensus on the issue seems far-fetched at the moment, the international community has agreed before on a multilateral convention concerning cyber attacks: in 2001, the Council of Europe created the Convention on Cybercrime, also known as the Budapest Convention.[131] The goal of the convention was to promote "a common criminal policy aimed at the protection of society against cybercrime," and it entered into force in 2004.[132] The crimes contemplated by the convention

---

130 *Report on Cyber Security in the Insurance Sector*, N.Y. STATE DEP'T OF FIN. SERVS. (Feb. 2015), http://www.dfs.ny.gov/reportpub/dfs_cyber_insurance_report_022015.pdf [https://perma.cc/S75L-242U].

131 *Details of Treaty No. 185*, TREATY OFFICE, COUNCIL OF EUROPE, http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 [https://perma.cc/T543-DA5Y].

132 *Id.*

include computer fraud, breaches of network security, copyright infringement, and child pornography.[133] As of 2016, the convention has fifty-four signatories, forty-seven of whom have ratified it.[134] Although the aim of this treaty was merely encouraging domestic legislation on the subject, it could serve as an example for a more aggressive convention that took the step of actually prohibiting state-sponsored cyber attacks.

An international prohibition could also serve as the basis for litigation in international tribunals. Hypothetically, if there were an international norm against cyber attacks or if there were a treaty conferring jurisdiction on an international tribunal, then states could bring suits against the state sponsors of cyber attacks on behalf of their citizens who were victims. Although there is little movement toward such a norm, let alone one that would provide a right of action in an international tribunal, the development of such a norm would provide an alternative means of prosecuting the state sponsors of cyber attacks.

CONCLUSION

A cyber attack exception to the FSIA has the potential to be a powerful deterrent and compensatory tool. Given sufficient tailoring to the peculiarities of attributing and litigating cyber attacks, such an exception could provide a far more certain and effective remedy than any currently available under the FSIA. Despite valid concerns about the uncertainty of attribution and the delicate balance of foreign-affairs power, a cyber attack exception would be workable and politically palatable. It would also help compensate the victims of cyber attacks who have little recourse against the foreign governments responsible for their losses. Using the terrorism exception as a model, Congress should create a private right of action to serve as a more reliable and just remedy than any of those currently available.

---

133 Convention on Cybercrime, Nov. 23, 2011, ETS No. 185, http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf [https://perma.cc/YYF4-TW8W].

134 *Chart of Signatures and Ratifications of Treaty 185*, TREATY OFF., COUNCIL OF EUROPE, http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures [https://perma.cc/YP2G-7NC4].