Bubbles over Barriers: Amending the Foreign Sovereign Immunities Act for Cyber Accountability

Adam L. Silow*

INTRODUCTION

Cyberspace is a critical domain for technological innovation and state competition. Beyond, however, the bounds of fair competition, states are increasingly using cyberspace to intimidate human rights activists and steal trade secrets from private companies. In doing so, states hire cybersecurity contractors for cyber expertise and assistance in conducting malicious cyberattacks. Section I of this Article outlines the increasing perils for private actors in cyberspace. Section II

* Adam L. Silow is a dual J.D.-Master of Science in Foreign Service candidate at Georgetown University, Class of 2022, and the Student Editor-in-Chief for Volume 12 of the Journal of National Security Law & Policy. He thanks Professor David Stewart for his invaluable advice. He also thanks Lucas Scarasso, Steve Szymanski, Shervin Taheran, and the rest of the JNSLP staff for their excellent feedback and editing. Any and all errors are Adam's alone. As Student Editor-in-Chief of this volume, he took no part in any stage of the consideration and selection of this Article, which occurred before he assumed this role, and he was not aware of the content of those deliberations while they were ongoing.

discusses the inadequacy of government actions and private legal remedies to address this problem. The current U.S. government responses—diplomacy, sanctions, speaking indictments, and some offensive cyber operations—are important, but insufficient to stem the tide of cyberattacks. Human rights activists and private companies have little protection. The Foreign Sovereign Immunities Act ("FSIA") blocks avenues for legal redress. A legislative fix is needed. Section III provides a solution: Congress should create a new and tailored cyber exception to the FSIA that opens liability for states, and their cybersecurity contractors, who threaten human rights with cyber tools and conduct cyber economic espionage. Rather than erect an absolute "barrier" against any cyberattacks—as others have suggested—a tailored exception would create protected "bubbles" around human rights activists and trade secrets. Creating a new private cause of action under the FSIA would improve accountability for states and their contractors, and develop cyber norms protecting human rights and fair economic competition.

I. THE CONTEXT: INCREASING CYBER THREATS

With rapid growth in information technology and digital markets, malicious states have more advanced cyber tools at their disposal and can affect a broader swath of private entities beyond their borders. In this Article, Section I(A) depicts how states shifted their use of cyberspace in recent years and Section I(B) describes the effect this had on cybersecurity contractors, human rights activists, and private companies.

A. Conceptualizing the Privatization of State-sponsored Cyberattacks

As cyberspace has evolved, so too have the ways in which states implement foreign policy. The diagrams below help to conceptualize the growing involvement of private entities in state-sponsored cyberattacks—both as victims and facilitators.

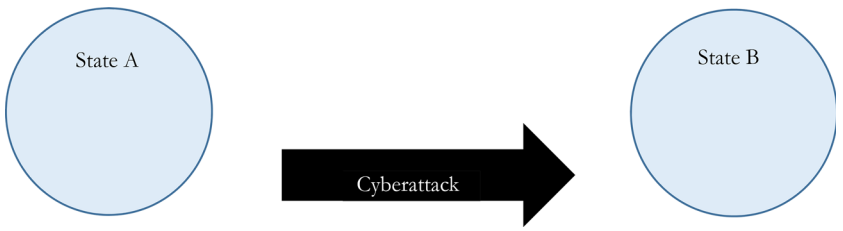


Diagram 1: State A hacks State B.

Diagram 1 highlights how a state-sponsored cyberattack is traditionally conducted against another state in its simplest form. State A uses its own governmental assets and capabilities to execute a cyberattack against the government of State B. Only government actors and assets are involved, both as perpetrators and victims.

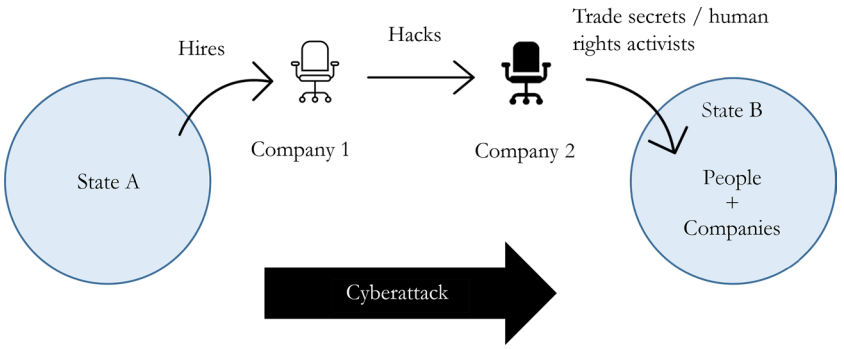


Diagram 2: State A hires Company 1 to facilitate the accessing of digital platforms run by Company 2 to hack private individuals and companies in State B.

Diagram 2 illustrates how states are increasingly involving private actors in their cyberattacks. State A turns to a private contractor, Company 1, for technical training, malicious cyber tools, operational support, or a combination of all three. Next, State A and Company 1 conduct their operations through another private entity—Company 2—to reach their ultimate target. Company 2 may be an email service provider, a smartphone manufacturer, a social media company, or a bank, to name a few. The final important shift between the diagrams is that State A changed its target in Diagram 2. The government of State B is no longer the only, or even primary, end-goal. Instead, State A targets a private company located in State B to steal trade secrets. State A may also target private individuals located in State B, particularly if they openly criticize State A's regime.

Diagram 2 highlights a sharp change in the cyber landscape. State A steps beyond the narrow state-to-state dynamic, broadening cyberattacks to include multiple private entities. Because State B's private entities, rather than its government, are the direct target of the cyberattack, State B may lack the incentives or political will to respond in an adequate and timely manner. Now, four private entities are involved—three are victims facing potentially severe harm, while the fourth is actively involved in facilitating the harm. The shift from Diagram 1 to 2 raises important questions about how the injured private entities can hold the perpetrators, State A and Company 1, accountable.

B. Cyberspace Has Few Rules and Many Victims

Cyberattacks are more than a thought experiment. For states, cyberspace is a domain with concrete advantages and few consequences for conducting malicious activity. The international community has agreed on few international legal agreements, customs, or norms in cyberspace.[1] Although "[c]yberspace is not a

1. The Budapest Convention on Cybercrime is the only significant multilateral treaty concluded with cyber-specific rules. *See* Convention on Cybercrime, Nov. 23, 2001, T.I.A.S. No. 13174, E.T.S. 185.

'law-free' zone,"[2] there is little consensus on how existing international law applies.[3] With few constraints, states are reaching more private entities through cyberattacks that play out in concrete terms every day.

1. Cybersecurity Contractors Proliferating

Much of the work by cybersecurity contractors is not publicly available; however, an ongoing case in the Northern District of California highlights how one digital platform provider is seeking to hold a cybersecurity contractor accountable for hacking on behalf of states.[4] In October 2019, WhatsApp and its parent company, Meta (formerly Facebook), filed suit against NSO Group Technologies ("NSO"), an Israeli cybersecurity firm. WhatsApp alleges that NSO created surveillance malware—spyware—known as Pegasus and sold it to various governments.[5] WhatsApp's complaint alleges Pegasus was used between April 29, 2019 and May 10, 2019 to unlawfully access WhatsApp servers and infect approximately 1,400 devices belonging to WhatsApp users.[6] This Article will return later to the *WhatsApp Inc. v. NSO* case to highlight the issue of liability for cybersecurity contractors.

In addition to NSO's public dispute with WhatsApp, reporters are bringing to light other stories of cybersecurity contractors hired by governments for their hacking prowess. In 2015, for example, Hacking Team, a company based in Italy, faced its own hack, which dumped 400 gigabytes of internal documents online. The leaked documents contained a list of sovereign clients, including the United States.[7] Additionally, reporting in 2019 showed that the United Arab Emirates ("UAE") hired ex-National Security Agency (NSA) hackers to conduct surveillance.[8] Lastly, Myanmar's recent coup demonstrates how the Burmese military

2. Harold Hongju Koh, Legal Adviser, U.S. Dep't State, International Law in Cyberspace, Remarks to the USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012), *in* 54 HARV. INT'L L. J. (FEATURE) 3 (2012).

3. *See, e.g.*, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt ed., 2013); TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (Michael N. Schmitt ed., 2d ed. 2017). Nonetheless, the General Counsel of the U.S. Defense Department recently stated that "initiatives by non-governmental groups like those that led to the Tallinn Manual can be useful to consider, but they do not create new international law, which only states can make." *See* Hon. Paul C. Ney, Gen. Couns., U.S. Dep't Def., Remarks at U.S. Cyber Command Legal Conference (Mar. 2, 2020), https://perma.cc/K3YQ-EL6F.

4. *See* WhatsApp Inc. v. NSO Grp. Techs. Ltd., 472 F. Supp. 3d 649 (N.D. Cal. 2020).

5. Mehul Srivastava, *WhatsApp Voice Calls Used to Inject Israeli Spyware on Phones*, FIN. TIMES (May 13, 2019), https://perma.cc/7Y3G-NZRZ. Pegasus operates by remotely installing spyware through phone calls sent to targeted devices using WhatsApp's call function. The spyware accesses messages and other communications after they are decrypted on the device. This malware is particularly effective because, unlike traditional phishing attacks, it "could be transmitted even if users did not answer their phones." Also, "the calls often disappeared from call logs." *Id.*

6. Complaint at 9, WhatsApp Inc. v. NSO Grp. Techs. Ltd., 472 F. Supp. 3d (N.D. Cal. 2020) (No. 19-cv-07123-PJH) (alleging, based on public reporting, that NSO's government clients included, but are not limited to, Bahrain, the United Arab Emirates, and Mexico, as well as private entities).

7. Andy Greenberg, *Hacking Team Breach Shows a Global Spying Firm Run Amok*, WIRED (July 6, 2015 10:26 AM), https://perma.cc/9KNN-8JNL.

8. Christopher Bing & Joel Schectman, *Inside the UAE's Secret Hacking Team of American Mercenaries*, REUTERS (Jan. 30, 2019), https://perma.cc/M5PA-DWXV.

and law enforcement invested heavily in digital weapons, which were procured not only through "patrons like China and Russia," but also from "firms. . .evading arms embargoes and export bans."[9]

The use of private contractors by governments is not new. The extent, however, to which these private contractors are increasingly involved in cyberattacks against civil society actors and the private sector for economic espionage is novel and alarming.

2. Human Rights Activists Under Threat

Human rights activists are increasingly facing cyber threats for speaking out against governments.[10] Hacks reportedly target human rights activists and journalists from a range of countries.[11] For example, the ex-NSA hackers hired by the UAE "took aim not just at terrorists and foreign government agencies, but also dissidents and human rights activists."[12] NSO's Pegasus spyware is alleged to have targeted "attorneys, journalists, human rights activists, political dissidents, diplomats, and other senior foreign government officials."[13] These cyber tools allow states to reach beyond their borders into supposed "safe havens."[14] A report on Pegasus by Citizen Lab, a research center, found that 36 likely operators were using the spyware to conduct surveillance in 45 countries.[15] A number of the

9. Hannah Beech, *Myanmar's Military Deploys Digital Arsenal of Repression in Crackdown*, N.Y. TIMES (Mar. 1, 2021), https://perma.cc/JC58-V4S5 ("[D]ual-use surveillance technology made by Israeli, American and European companies made its way to Myanmar, despite many of their home governments banning such exports after the military's brutal expulsion of Rohingya Muslims in 2017.").

10. Friedhelm Weinberg, *3 Ways Activists are Being Targeted by Cyberattacks*, WORLD ECON. F. (May 1, 2019), https://perma.cc/CDD5-LSLY (listing phishing, malware, and distributed denial-of-service attacks as three common cyberattacks against human rights activists).

11. *See, e.g.*, AMNESTY INT'L, *Azerbaijan: Activists Targeted by 'Government-Sponsored' Cyber Attack* (Mar. 10, 2017), https://perma.cc/4MXP-DYLL (Azerbaijan); Tania Branigan, *Accounts Invaded, Computers Infected – Human Rights Activists Tell of Cyber Attacks*, GUARDIAN (Jan. 14, 2010), https://perma.cc/G5XF-CSCT (China); JOHN SCOTT-RAILTON, BILL MARCZAK, RAMY RAOOF & ETIENNE MAYNIER, NILE PHISH, (Citizen Lab 2017), https://perma.cc/NEN7-XRKH (Egypt); Iain Marlow & Karen Leigh, *Google Warns Hong Kong's Joshua Wong of Government-Backed Hackers*, BLOOMBERG (July 16, 2019, 5:45 AM), https://perma.cc/E7WW-Y22M (Hong Kong); Press Release, Electronic Frontier Foundation, Malware Linked to Government of Kazakhstan Targets Journalists, Political Activists, Lawyers (Aug. 4, 2016), https://perma.cc/A99R-DRER (Kazakhstan); Azam Ahmed & Nicole Perlroth, *Using Texts as Lures, Government Spyware Targets Mexican Journalists and Their Families*, N.Y. TIMES (June 19, 2017), https://perma.cc/Y4N9-SUGH (Mexico); AMNESTY INT'L, *Pakistan: Campaign of Hacking, Spyware and Surveillance Targets Human Rights Defenders (*May 15, 2018), https://perma.cc/29B3-HJPE (Pakistan); Yinka Adegoke, *A WhatsApp Hack Used Israeli Spyware to Target Rwandan Dissidents*, QUARTZ (Oct. 30, 2019), https://perma.cc/QTL3-VPAH (Rwanda); *see also* Morgan Marquis-Boire & Eva Galperin, *A Brief History of Governments Hacking Human Rights Organizations,* AMNESTY INT'L (Jan. 11, 2016), https://perma.cc/X6RZ-7XNM.

12. Bing & Schectman, *supra* note 8.

13. Complaint, *supra* note 6, at 9.

14. MASASHI CRETE-NISHIHATA, JAKUB DALEK, RONALD DEIBERT, SETH HARDY, KATHARINE KLEEMOLA, SARAH MCKUNE, IRENE POETRANTO, JOHN SCOTT-RAILTON, ADAM SENFT, BYRON SONNE & GREG WISEMAN, COMMUNITIES @ RISK 26 (2014), https://perma.cc/N8FL-2KNA.

15. BILL MARCZAK, JOHN SCOTT-RAILTON, SARAH MCKUNE, BAHR ABDUL RAZZAK & RON DEIBERT, HIDE AND SEEK: TRACKING NSO GROUP'S PEGASUS SPYWARE TO OPERATIONS IN 45 COUNTRIES 6 (2018), https://perma.cc/9DS9-VF4P.

perpetrating states had "dubious human rights records," including six who were "previously linked to abusive use of spyware to target civil society."[16] NSO advertised its products "for fighting terrorism and aiding law enforcement investigations," even though its Pegasus spyware was found on infected devices belonging to civil society actors.[17] In one heinous example, Pegasus was used to access communications between two Saudi dissidents in the months before one of them—Jamal Khashoggi—was murdered and dismembered by Saudi agents in Istanbul in 2018.[18] NSO denies any use of Pegasus related to Khashoggi's murder, although a joint media investigation in 2021 by the Pegasus Project found signs that Pegasus was also used in the months following Khashoggi's murder to spy on his family and close associates.[19] Khashoggi's tragic story is a stark reminder that authoritarian governments may couple cyberattacks against human rights activists with deadly force.

Human rights activists are often particularly vulnerable with few cyber defenses capable of matching the array of cyber tools deployed by governments and their contractors. Traditionally, human rights activists under authoritarian regimes thought that fleeing their country would provide a measure of safety. Today, that is less true than ever. Governments can use cyberattacks to reach human rights activists abroad in what were previously considered "safe havens."[20] Human rights activists often do not have the technical knowhow or resources to properly shore up their cyber defenses.[21] Furthermore, they rely extensively on digital communication to voice their opinions. Cyberattacks disrupt this ability to share information and create a chilling effect on free speech.[22] And, unfortunately, human rights activists are often the last to receive cyber protection from others who are

16. *Id.*

17. *See, e.g.*, Nicole Perlroth & Ronen Bergman, *WhatsApp Rushes to Fix Security Flaw Exposed in Hacking of Lawyer's Phone*, N.Y. TIMES (May 13, 2019), https://perma.cc/JBR2-R99X; David D. Kirkpatrick, *Israeli Software Helped Saudis Spy on Khashoggi, Lawsuit Says*, N.Y. TIMES (Dec. 2, 2018), https://perma.cc/7NNL-6UL4 (writing that NSO has also faced litigation in Israel from journalists, activists, and others, alleging NSO "improperly helped the governments of Mexico and the United Arab Emirates spy on their smartphones even though the individuals had no criminal records and posed no threat of violence").

18. Oren Liebermann, *How a Hacked Phone May Have Led Killers to Khashoggi*, CNN (Jan. 20, 2019, 9:15 AM), https://perma.cc/PL89-QKJS (describing how Citizen Lab analyzed the phone of another Saudi dissident and found NSO Group's malware on the phone, "giving hackers access to virtually his entire phone, including his daily conversations with [Jamal] Khashoggi").

19. Stephanie Kirchgaessner, *Saudis Behind NSO Spyware Attack on Jamal Khashoggi's Family, Leak Suggests*, GUARDIAN (July 18, 2021, 2:32 PM), https://perma.cc/XMP9-GPP9.

20. CRETE-NISHIHATA ET AL., *supra* note 14, at 26.

21. Marie Lamensch, *For Rights Defenders, Cyber Is the New Battleground*, CTR. FOR INT'L GOVERNANCE INNOVATION (Nov. 22, 2021), https://perma.cc/5CX3-WGP5 ("Today, more than ever, human rights activists and journalists depend on the internet and mobile phones to carry out their work. Yet they have few resources to protect themselves against spyware deployed by powerful governments.").

22. *Id.* ("Among the biggest threats are account compromise, malware on devices and communication surveillance."; "Just the thought that one's phone could be hacked and every communication monitored has a chilling effect on the person targeted. When journalists or activists go quiet, civic space shrinks.").

more capable. Dave Aitel, who formerly worked at the NSA as a hacker before leaving to start a cybersecurity firm, said that, "the United States is good at protecting the government, OK at protecting corporations, but does *not* protect individuals."[23]

3. Trade Secrets Stolen

In addition to human rights activists, states have also set their sights on hacking companies and causing significant economic damage. In recent years, cyber economic espionage from China alone is estimated to have cost the United States annually between $20 and $30 billion.[24] A 2015 report estimated that cyberattacks cost U.S. firms on average $15.4 million per year, while the global average was $7.7 million.[25] While the 2015 figures include a broader array of cyberattacks, states stealing trade secrets is a significant issue that is likely to persist. In a 2018 report on foreign cyber economic espionage, the U.S. Office of the Director of National Intelligence noted that "[n]ext-generation technologies such as Artificial Intelligence. . .and the Internet-of-Things. . .will introduce new vulnerabilities to U.S. networks for which the cybersecurity community remains largely unprepared."[26] Even companies with the resources to secure their networks and defend against certain cyberattacks face an uphill battle against the assets of a state. Large companies are target rich environments with massive, often dispersed, networks with many users, each presenting opportunities for social engineering attacks.

Furthermore, companies have no legal options to strike back and deter future cyberattacks by states. In 2017, Representative Tom Graves introduced "hack-back" legislation, which would allow private companies to "engage in self-defense outside their network."[27] While the Active Cyber Defense Certainty Act "excited a great deal of commentary. . .it never emerged from [congressional] committee," largely due to concerns that it may lead to cyber vigilantism with "risks involving mistaken attribution, unintended collateral harms and dangerous escalation."[28] Despite better defensive options than human rights activists, companies are rich targets with little ability to strike back.

---

23. Andy Greenberg, *North Korea Hacked Him. So He Took Down Its Internet*, WIRED (Feb. 2, 2022, 11:43 AM), https://perma.cc/29LN-DW5E.

24. James Andrew Lewis, *How Much Have the Chinese Actually Taken?*, CTR. FOR STRATEGIC & INT'L STUD. (Mar. 22, 2018), https://perma.cc/9U4Z-F846.

25. James Griffiths, *Cybercrime Costs the Average U.S. Firm $15 Million a Year*, CNN (Oct. 8, 2015, 3:28 AM), https://perma.cc/AE7K-CDSZ.

26. NAT'L COUNTERINTEL. & SECURITY CTR., FOREIGN ECONOMIC ESPIONAGE IN CYBERSPACE 5 (2018), https://perma.cc/R95E-WY6N ("China, Russia, and Iran stand out as three of the most capable and active cyber actors tied to economic espionage and the potential theft of U.S. trade secrets and proprietary information. Countries with closer ties to the United States have also conducted cyber espionage to obtain U.S. technology.").

27. Robert Chesney, *Hackback Is Back: Assessing the Active Cyber Defense Certainty Act*, LAWFARE (June 14, 2019, 5:31 PM), https://perma.cc/9K9N-WEL5.

28. *Id.*

II. THE PROBLEM: INADEQUATE RESPONSES

The current set of available responses by the U.S. government and private actors is inadequate to address the increased state-sponsored hacking of trade secrets and human rights activists. The federal government has taken the most active response; however, this has proven insufficient to stem the tide of cyberattacks. Moreover, few of the victim companies or individuals have been able, or even tried, to obtain redress in U.S. courts because one significant piece of federal legislation shields states from liability.

The Foreign Sovereign Immunities Act ("FSIA") was passed by Congress in 1976 and serves as "the sole basis for obtaining jurisdiction over a foreign state in [U.S.] courts."[29] States receive immunity from suit in U.S. courts *unless* one of the statute's enumerated exceptions apply, such as commercial activity, torts, or terrorism. At its core, the FSIA defines what it means to be and act like a legitimate state—providing broad immunity with a few exceptions for illegitimate behavior warranting liability.[30] The following Sections II(A) – (B) outline the deficiency of U.S. government efforts to protect private actors and the litigation block created by the FSIA in its current form.

A. Government Policies Are Important, but Insufficient

The U.S. government tries to prevent and deter cyberattacks using a combination of cyber, diplomatic, legal, and economic tools. Under its "defend forward" strategy, the United States conducts cyberoperations, including with offensive cyber capabilities, to "disrupt or halt malicious cyber activity at its source."[31] The U.S. government has focused its offensive cyberoperations against major adversaries, particularly those who target U.S. government facilities or functions. In response to economic espionage or the hacking of its private individuals, the U.S. government has yet to rely (at least publicly) on offensive cyberoperations. The United States' reluctance may be due to the actual or perceived risk of conflict

29. Foreign Sovereign Immunities Act of 1976, Pub. L. No. 94-583, 90 Stat. 2891 (1976) (codified as amended at 28 U.S.C. §§ 1330, 1391(f), 1441(d), and 1602-11 (2000)); *see also* Argentine Republic v. Amerada Hess Shipping Corp., 488 U.S. 428, 434 (1989); DAVID P. STEWART, THE FOREIGN SOVEREIGN IMMUNITIES ACT: A GUIDE FOR JUDGES 1 (2d ed. 2018), https://perma.cc/CG27-M8GH (explaining that the FSIA "governs all litigation in both state and federal courts against foreign states and governments, including their 'agencies and instrumentalities'").

30. Mark B. Feldman, *The United States Foreign Sovereign Immunities Act of 1976 in Perspective: A Founder's View*, 35 INT'L & COMP. L.Q. 302, 305 (1986) ("The drafters of the [FSIA] believed that the jurisdiction of the United States courts for claims against foreign States should depend both on the character of the acts of the foreign State forming the basis of the claim and the connection between those acts and the territorial jurisdiction of the United States."); *see generally* CURTIS A. BRADLEY, INTERNATIONAL LAW IN THE U.S. LEGAL SYSTEM 223-256 (2d ed. 2015) (detailing the history of the doctrine of foreign immunity); STEWART, *supra* note 29 (outlining the history, purpose, and application of the FSIA).

31. U.S. DEP'T DEF., SUMMARY CYBER STRATEGY 1 (2018), https://perma.cc/GFP8-3786 ("[The Department of Defense] will defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict."); *see also* Julian E. Barnes, *Cyber Command Operation Took Down Russian Troll Farm for Midterm Elections*, N.Y. TIMES (Feb. 26, 2019), https://perma.cc/5XBM-QH3X.

escalation and the availability of other risk-averse policy tools. For example, one major cyber diplomatic effort the United States undertook was a 2015 bilateral agreement to end China's cyber economic espionage, although China continues to steal U.S. trade secrets.[32]

While diplomacy has done little so far, the United States regularly uses indictments and sanctions to counter cyber economic espionage, although their efficacy is also disputed.[33] In 2014, the United States publicly announced criminal indictments against state hackers for the first time, alleging Chinese state actors conducted cyberattacks to steal intellectual property from U.S. companies.[34] Between 2014 and 2020, the U.S. Department of Justice brought twenty-three additional indictments against ninety-three state-sponsored hackers from China, Russia, Iran, North Korea, and Syria.[35] Prosecutors describe these charges as "speaking indictments" because they include more facts than are necessary to press charges to bolster attribution and publicly "name and shame" the defendant state.[36] Due to the protection afforded states by the FSIA, the U.S. government brings criminal charges not against the perpetrating state itself, but against the hackers in their individual capacities.[37] Few of the defendants, though, are ever extradited to the United States.[38] States may face lesser consequences, including international embarrassment or condemnation. Generally, states are not held liable and the victims do not face their perpetrators in court.

The United States also uses sanctions as a penalty.[39] Sanctions provide for asset freezes and travel bans against the malicious cyber actors, as well as those who assist or benefit from them. Nonetheless, sanctions are based on the foreign

32. Christopher Bing & Michael Martina, *U.S. Accuses China of Violating Bilateral Anti-Hacking Deal*, REUTERS (Nov. 8, 2018, 7:49 PM), https://perma.cc/3MRJ-44ER.

33. *See, e.g.*, Jack Goldsmith & Robert D. Williams, *The Failure of the United States' Chinese-Hacking Indictment Strategy*, LAWFARE (Dec. 28, 2018, 9:00 AM), https://perma.cc/263Q-NMC9.

34. Indictment, United States v. Wang Dong, No. 14-118 (W.D. Pa. May 1, 2014).

35. Garrett Hinck & Tim Maurer, Persistent Enforcement: Criminal Charges as a Response to Nation-State Malicious Cyber Activity, 10 J. NAT'L SECURITY L. & POL'Y 525, 526-27 (2020).

36. Sarah Grant, Quinta Jurecic, Matthew Kahn, Matt Tait & Benjamin Wittes, *Russian Influence Campaign: What's in the Latest Mueller Indictment*, LAWFARE (Feb. 16, 2018, 10:55 PM), https://perma.cc/F89M-RBCY ("The purpose of a speaking indictment is more than to simply list charges; it is to tell a story.").

37. *Cf.* Matthew D. Slater, Carmine Boccuzzi, Jonathan S. Kolodner, Rahul Mukhi, Boaz S. Morag, Rathna Ramamurthi & Hyatt Mustefa, *SDNY District Court Rules Foreign Sovereigns Are Not Immune From Criminal Jurisdiction In U.S. Court*, CLEARY GOTTLIEB (Oct. 12, 2020), https://perma.cc/WP72-A9DA (some courts are growing more amenable to the idea that the FSIA does not preclude criminal jurisdiction); Chimène Keitner, *Prosecuting Foreign States*, 61 VA. J. INT'L L. 221, 227 (2021) (arguing that because the FSIA is silent on criminal proceedings, "foreign state-owned companies are subject to the criminal jurisdiction of U.S. courts, at least with respect to their commercial activities").

38. Andrea Vittorio, *U.S. Efforts to Catch Cybercriminals Abroad Hinge on Extradition*, BLOOMBERG L. (Dec. 7, 2021, 5:00 AM), https://perma.cc/4EGH-DUCW ("Extradition is especially challenging when hackers work directly for a foreign government.").

39. *See* Exec. Order No. 13694, 80 Fed. Reg. 18077 (Dec. 31, 2015) (declaring "malicious cyber-enabled activities" a "national emergency" and authorizing sanctions in response); *see also OFAC Recent Actions*, U.S. DEP'T TREASURY, https://perma.cc/JTB5-X6P9 (listing the Treasury Department's recent cyber-related designations).

policy discretion of the executive branch, not on a court's finding of liability. Furthermore, sanctions designations do not help individual or corporate victims of state-sponsored cyberattacks receive compensation for their injuries.

Government responses have not stopped the wave of cyberattacks and do not provide victims with restitution. Due to FSIA restrictions, the U.S. government indirectly targets states by charging government hackers in their individual capacities. Proponents argue speaking indictments are an important tool for attribution, disrupting networks, coordinating with other U.S. agencies, providing "some psychological restitution for victims," naming and shaming states, and signaling international norms of behavior.[40] Nonetheless, critics argue the indictment strategy is a "magnificent failure" because it has not stopped states from hacking.[41] The harm from public attribution is "offset by the massive benefits" in commercial information obtained by the hacking states.[42] Diplomacy, indictments, and sanctions have failed to sufficiently change the cost-benefit calculus of hacking states, leaving victims with no recompense, other than potentially "some psychological restitution."[43] Thus, the government's current response architecture is important, but insufficient to curb the onslaught of cyberattacks on private companies and individuals.

B. Private Suits Are Blocked by the Current FSIA

Compared to the government, private victims have seen even less success holding malicious cyber state actors accountable in U.S. courts because of restrictions under the FSIA. The law was passed before the modern digital era and does not properly account for modern cyber threats. Even the more recently created FSIA exceptions do not account for cyberattacks. Additionally, the issue of private cybersecurity contractors adds another complicating factor to the question of liability. The FSIA does not provide a clear answer on whether private contractors receive derivative foreign sovereign immunity based on their government clients. Contractors providing legitimate cyber services for intelligence, defense, and law enforcement activities are left uncertain about the potential liability they face.

1. Current FSIA Exceptions Do Not Apply to Cyberattacks

The FSIA provides nine distinct exceptions from immunity for which states may be held liable.[44] In essence, these exceptions outline the areas of state

40. Garrett Hinck & Tim Maurer, *What's the Point of Charging Foreign State-Linked Hackers?*, LAWFARE (May 24, 2019, 11:20 AM), https://perma.cc/3R79-GZED.

41. Goldsmith & Williams, *supra* note 33.

42. Goldsmith & Williams, *supra* note 33.

43. Hinck & Maurer, *supra* note 40.

44. *See generally* STEWART, *supra* note 29, at 47-136 (outlining the scope and elements of all nine exceptions, which include waiver, commercial activity, expropriations, rights in certain kinds of property in the United States, noncommercial torts, enforcement of arbitral agreements and awards, state-sponsored terrorism, maritime liens and preferred mortgages, and counterclaims); *see also* 28 U.S.C. §§ 1605(a)(1)-(6), 1605(b)-(d), 1605(A), 1607.

behavior that are deemed illegitimate, or at least outside the norm of behavior deemed inherent to a foreign sovereign. States conducting such behavior no longer benefit from immunity and may be held liable in U.S. court. In the context of cyberspace, three of the exceptions—commercial activity, tortious conduct, and terrorism—are worth examining as potentially relevant (assuming immunity is not waived by a state). None, however, provide injured parties, particularly private companies facing trade secret hacks and human rights activists under malicious cyber intrusions, with an effective avenue of accountability in U.S. courts against hacking states.

The most litigated FSIA exception is for commercial activity.[45] The commercial activity exception strips sovereign immunity for a state conducting commercial activities as a private individual or company would in business.[46] The statute defines commercial activity as "either a regular course of commercial conduct or a particular commercial transaction or act."[47] In addition, the FSIA emphasizes commercial activity is determined by its nature, not its purpose.[48] Thus, commercial activity is not based on a profit motive, but "whether the government's particular actions (whatever the motive behind them) are the *type* of actions by which a private party engages in commerce."[49] The Ninth Circuit recently concluded that "a foreign government's conduct of clandestine surveillance and espionage against a national of another nation in that other nation is not 'one in which commercial actors typically engage.'"[50] Cyberattacks against human rights activists—individuals with no clear business connection—are also unlikely to constitute commercial activity.

In a recent article, Jerry Goldman and Bruce Strong argued that the commercial activity exception covers hacking trade secrets based on a D.C. District Court decision in *Azima v. RAK Investment Authority*.[51] The District Court in *Azima* found that a UAE state investment entity's hack of a businessman constituted commercial activity under the FSIA.[52] The District Court focused on the overlap in timing, emphasizing that the UAE entity hacked the businessman as mediation

45. STEWART, *supra* note 29, at 50-51.

46. 28 U.S.C. § 1605(a)(2).

47. 28 U.S.C. § 1603(d).

48. *Id.*

49. Republic of Argentina v. Weltover, Inc., 504 U.S. 607, 607 (1992) (finding Argentina's issuance of bonds with repayment in U.S. dollars in several markets, including New York, was a commercial activity with a "direct effect in the United States" under the FSIA).

50. Broidy Cap. Mgmt., L.L.C. v. Qatar, 982 F.3d 582, 594 (9th Cir. 2020); *see also* Democratic Nat'l Comm. v. Russian Federation, 392 F. Supp. 3d 410, 429 (S.D.N.Y. 2019) (finding that Russia's hacks against the Democratic National Committee in 2015 did not constitute commercial activity because "transnational cyberattacks are not the 'type of actions by which a private party engages in trade and traffic or commerce'").

51. Jerry Goldman & Bruce Strong, *Overcoming Immunity of Foreign Gov't Cyberattack Sponsors*, LAW360 (Dec. 2, 2020 5:07 PM), https://perma.cc/8YWV-85E5.

52. Azima v. RAK Inv. Auth., 305 F. Supp. 3d 149 (D.D.C. Mar. 30, 2018), *rev'd*, 926 F.3d 870 (D.C. Cir. 2019) (reversing the District Court on separate grounds because a forum selection clause established England as the proper venue).

began between both parties.[53] Based on the *Azima* Court's reasoning, Goldman and Strong argued that "steal[ing] trade secrets for the purpose of giving their own companies a competitive commercial advantage" would "neatly fall under the commercial activity exception."[54] Not so—hacking during mediations is different from cyber economic espionage. Unlike the facts in *Azima*, hacks of trade secrets are unlikely to occur simultaneous with a commercial activity. A company receiving the stolen trade secrets will likely be unable to take commercial advantage of the information until long after the actual hack is complete. Establishing the causal link between a hack and a commercial activity without an easy temporal inference will require significantly more evidence and resources. The District Court's reliance in *Azima* on a close-in-time overlap in activity means plaintiffs will struggle to bring cases involving cyber economic espionage that link hacks with ongoing commercial activity.

The FSIA also includes a noncommercial tort exception, which provides that states are not granted immunity for cases:

> in which money damages are sought against a foreign state for personal injury or death, or damage to or loss of property, *occurring in the United States* and caused by the tortious act or omission of that foreign state or of any official or employee of that foreign state while acting within the scope of his office or employment (emphasis added).[55]

In 2015, one author, Scott Gilmore, envisaged the FSIA's tort exception as a possible path for holding state-sponsors of cyberattacks accountable.[56] Gilmore pointed to two cases—*Letelier v. Republic of Chile*, and *Liu v. Republic of China*—in which assassinations by foreign agents in the United States satisfied the tort exception.[57] Nonetheless, the D.C. Circuit in 2017 refused to apply the tort exception in the context of a cyberattack by Ethiopia against a human rights activist in Maryland.[58] The D.C. Circuit distinguished the foreign cyberattack from the assassination cases by emphasizing the tort exception's situs requirement, which provides that the entire tort must occur in the United States. Although the assassins in *Letelier* and *Liu* were foreign agents, their tortious conduct occurred in the United States—the Taiwanese agent shot a man California, and the Chilean agents "constructed, planted and detonated a car bomb in Washington, D.C."[59]

---

53. *Id.* at 166 ("Azima starts off noting that the hacking of his computer began in October of 2015 and continued through the summer of 2016—a time period that roughly corresponds with the time in which Azima served as a mediator between RAKIA and its former CEO.").

54. Goldman & Strong, *supra* note 51.

55. 28 U.S.C. § 1605(a)(5).

56. Scott A. Gilmore, *Suing the Surveillance States: The (Cyber) Tort Exception to the Foreign Sovereign Immunities Act*, 46 COLUM. HUM. RTS. L. REV. 223 (2015); Goldman & Strong, *supra* note 51.

57. Letelier v. Republic of Chile, 488 F.Supp. 665 (D.D.C. 1980); Liu v. Republic of China, 892 F.2d 1419 (9th Cir. 1989).

58. Doe v. Federal Democratic Republic of Ethiopia, 851 F.3d 7, 11 (D.C. Cir. 2017).

59. *Id.*

While there is an argument that the planning of the assassinations in *Letelier* and *Liu* occurred abroad, the D.C. Circuit emphasized that the injury caused by Ethiopia's cyberattack included not only an "intent to spy" from abroad but also an "initial dispatch" of malware in Ethiopia, meaning "integral aspects of the final tort. . .lay solely abroad."[60] States rely on cyberattacks precisely because of the ability to affect targets in a different location from where the attack is launched. Cyberspace provides a means of covertly reaching across borders and harming entities or states that are otherwise inaccessible. Therefore, most cyberattacks are likely to run afoul of the tort exception's situs requirement.

Congress passed several FSIA amendments related to terrorism. In 1996, Congress added an exception for state-sponsored terrorism, removing immunity for certain acts of terrorism, such as torture, extrajudicial killing, aircraft sabotage, hostage taking, or material support.[61] An important provision in the new exception provided that immunity would only be removed for states formally designated by the U.S. Secretary of State as a sponsor of terrorism. With the state sponsors of terrorism list, the executive branch acts as a gatekeeper, tightly limiting the number of countries who may face liability in U.S. courts. When the terrorism exception passed in 1996, only seven states were on the list: Cuba, Iran, Libya, North Korea, Sudan, Syria, and Iraq.[62] As of February 2022, only Cuba, North Korea, Iran, and Syria remain.[63]

Congress broadened the terrorism exception in 2008 under 28 U.S.C. § 1605A by removing the bar on punitive damages and creating a federal cause of action that could be applied retroactively.[64] In 2016, Congress passed—over the President's veto—an additional exception under 28 U.S.C. § 1605B known as the Justice Against Sponsors of Terrorism Act ("JASTA").[65] Frustrated by the executive branch's refusal to list certain countries, specifically Saudi Arabia, Congress passed JASTA to provide another legal avenue against perpetrating states, regardless of designation by the Secretary of State. JASTA also removed the entire tort requirement for acts of international terrorism that take place in the United States, as defined by the Antiterrorism Act ("ATA").[66] Nonetheless, plaintiffs have not yet succeeded in bringing claims under JASTA. For example, the

60. *Id.*

61. Anti-Terrorism and Effective Death Penalty Act of 1996, Pub. L. No. 104-132, § 221, 110 Stat. 12241 (1996) (codified at 28 U.S.C. § 1605(a)(7)).

62. Patterns of Global Terrorism 1996, IRP FAS, https://perma.cc/Q8QZ-RSRG.

63. *See* State Sponsors of Terrorism, U.S. DEP'T STATE, https://perma.cc/SL3C-J63R.

64. 28 U.S.C. § 1605A (including three other limitations: 1. a ten-year limitations period; 2. the claimant or victim was a U.S. national, member of the armed forces, or otherwise a U.S. employee or contractor; and 3. the claimant must first afford the "foreign state a reasonable opportunity to arbitrate the claim in accordance with the accepted international rules of arbitration").

65. Pub. L. No. 114-222, 130 Stat. 852 (2016); *see* Rachael E. Hancock, *'Mob-Legislating': JASTA's Addition to the Terrorism Exception to Foreign Sovereign Immunity*, 103 CORNELL L. REV. 1293, 1294 (2018) ("On September 28, 2016, a politically divided United States Senate overrode President Barack Obama's veto for the first and only time in a particularly decisive vote: 97–1.").

66. 18 U.S.C. § 2331 (defining international terrorism as activities involving: a) violent acts or acts dangerous to human life that b) appear to be intended to intimidate or coerce a civilian population,

families of the 9/11 victims protested the removal of Sudan in December 2020 from the state sponsors of terrorism list because it would remove their ability to bring claims under §1605A and they did not see JASTA as a viable path for their claims against Sudan.[67] Despite Congress' intentions, JASTA has not yet demonstrated that it is a suitable alternative to §1605A.

The FSIA's terrorism exceptions under either §1605A or §1605B (JASTA) were created to address a specific harm—violent terrorist acts—and, therefore, do not fit well for harms in cyberspace. Nonetheless, some authors argue otherwise.[68] Goldman and Strong acknowledge that the state sponsor exception "does not at first blush appear to apply to hacking," but continue on to provide examples they believe could apply.[69] They argue hacking an airplane or air traffic control could constitute aircraft sabotage, hacking a hospital causing patients to die without access to medical care might be extrajudicial killing, and hacking "infrastructure that traps people in a particular location" might be hostage-taking.[70] The authors provide no evidence that any of these hyper-specific examples are widespread phenomena or have ever occurred. For example, in September 2020, a ransomware attack on a German hospital was suspected as causing "the first known death from a cyberattack,"[71] but police later clarified the patient's poor health was the cause of death and "the delay [in medical care from the ransomware] was of no relevance to the final outcome."[72] While a cyberattack that causes physical damage to humans may constitute a violent terrorist act, such attacks make up few, if any, of the current wave of cyberattacks. In addition, plaintiffs relying on §1605A's state sponsors exception are currently only able to sue the four listed states—Cuba, Iran, North Korea, and Syria. Other state sponsors of malicious cyberactivity, notably Russia and China, face no liability under the state sponsors exception.

John Martin writes that cyberattacks fit under §1605B (JASTA), which relies on the substantive elements under the ATA, rather than the limited acts enumerated in §1605A's state sponsors exception. Martin argues the ATA's inclusion of "acts dangerous to human life" is broad enough to cover cyberattacks.[73] JASTA,

---

influence the policy of a government by intimidation or coercion, or affect the conduct of a government by mass destruction, assassination, or kidnapping).

67. Lara Jakes, *U.S. Prepares to Take Sudan Off List of States That Support Terrorism*, N.Y. TIMES (Sept. 24, 2020), https://perma.cc/6PXP-GNKW (The delisting of Sudan resolved Sudan's payments to victims of the 1998 East Africa Embassy bombings and the 2000 Cole bombing, but 9/11 families also believe they have viable claims against Sudan for supporting Al-Qaeda. The 9/11 victims' families "broadly objected to the immunity legislation before their own legal cases against Sudan are resolved.").

68. *See, e.g.*, John J. Martin, *Hacks Dangerous to Human Life: Using JASTA to Overcome Foreign Sovereign Immunity in State-Sponsored Cyberattack Cases*, 121 COLUM. L. REV. 119 (2021); Goldman & Strong, *supra* note 51 (arguing that both § 1605A and § 1605B apply).

69. Goldman & Strong, *supra* note 51.

70. Goldman & Strong, *supra* note 51.

71. Melissa Eddy & Nicole Perlroth, *Cyber Attack Suspected in German Woman's Death*, N.Y. TIMES (Sept. 18, 2020), https://perma.cc/G3GB-HFAE.

72. Patrick Howell O'Neill, *Ransomware Did Not Kill a German Hospital Patient*, MIT TECH. REV. (Nov. 12, 2020), https://perma.cc/EQ9B-FJRD.

73. Antiterrorism Act (ATA), 18 U.S.C. § 2331(1)(A).

according to Martin, could provide protection for political dissidents if, for example, "the act of distributing secret information after a data breach could endanger human life if it contains personal information about an individual that then subjects them to potential targeting and harassment."[74] Plaintiffs, however, would need to prove a complicated chain of causation connecting several disparate points—specifically, the perpetrating state, the hack itself, the breached secret information, and the harassment that causes dangers to human life. Stealing trade secrets is even more attenuated to proving "acts dangerous to human life." Even if human rights activists could prove this lengthy chain of causation, private companies are less likely to see success under JASTA. For example, hacking a private company's designs for semiconductors may cause significant economic damage without endangering any human lives. JASTA is, therefore, not a viable avenue for private companies hoping for redress against trade secret hacks.

Martin is also too quick to dismiss the argument that JASTA was intended "for one specific purpose: to allow [9/11] victims' families to sue Saudi Arabia."[75] And even the 9/11 families' claims, for which the statute was created, have not gone far under JASTA.[76] Judges will likely be wary to read into JASTA a new type of claim for cyberattacks that Congress did not specifically anticipate. Applying cyberattacks to these terrorism statutes is like fitting a square peg in a round hole. The state sponsors exception and JASTA were created to mitigate harm for physically destructive acts of terrorism. These exceptions were not drafted to capture the less tangible but still significant harms created by malicious states in cyberspace.

In summary, cyberattacks do not fit under the FSIA's exceptions as they stand today. Malicious states may act with impunity in cyberspace under the current FSIA exceptions. Human rights activists and companies with valuable trade secrets do not have viable avenues for legal redress as they face a rising wave of cyberattacks from states aiming to oppress human rights and steal intellectual property.

2. A Nascent Circuit Split on Derivative Immunity Creates Uncertainty and Liability Risks for Contractors

In the ongoing litigation between WhatsApp and NSO—concerning foreign governments using NSO's Pegasus spyware to hack WhatsApp users—the Ninth Circuit diverged from the Fourth Circuit and ruled that the FSIA does not provide foreign sovereign immunity to private companies.[77] Discovery in the NSO case

74. Martin, *supra* note 68, at 150-51.

75. Martin, *supra* note 68, at 155-56.

76. *See In re* Terrorist Attacks on Sept. 11, 2001, 298 F. Supp.3d 631 (S.D.N.Y. 2005).

77. The closest any of the direct victims have come to challenging NSO Group is a lawsuit by Amnesty International (AI) against NSO Group in Israel to have the company's export license revoked for monitoring human rights activists, including one of AI's researchers. The Tel Aviv District Court Judge dismissed the lawsuit for failure to "substantiate" the claim, finding the Israeli Defense Ministry's "thorough and meticulous" process for granting export licenses was sufficiently sensitive to human

stalled in 2020 over the issue of derivative foreign sovereign immunity when NSO filed a motion to dismiss WhatsApp's complaint, arguing, in part, that the District Court lacked subject matter jurisdiction because NSO enjoyed derivative foreign sovereign immunity based on its foreign sovereign clients. None of the current FSIA exceptions likely apply to cyberattacks (as outlined in the next Section). Therefore, if NSO could avail itself of derivative foreign sovereign immunity, then WhatsApp and other injured parties would not have viable claims for relief against NSO. The FSIA does not explicitly provide derivative immunity for contractors. Consequently, the question has been left to judicial interpretation. NSO argued that the court should adopt the rule outlined by the Fourth Circuit in *Butters v. Vance Int'l Inc*.[78] The Fourth Circuit upheld derivative foreign sovereign immunity for a U.S. security company hired by Saudi Arabia when one of its employees sued the company for gender discrimination. The Fourth Circuit drew its conclusion from the rule that U.S. domestic contractors receive the privilege of derivative immunity when contracting for the U.S. government. The Fourth Circuit held that it is "but a small step to extend this privilege to the private agents of foreign sovereigns."[79]

The Northern California District Court, affirmed by the Ninth Circuit, found NSO was asking for a larger step than it conceded. On July 16, 2020, Chief District Court Judge Phyllis J. Hamilton denied NSO's motion to dismiss and rejected the adoption of derivative foreign sovereign immunity.[80] Judge Hamilton emphasized that the Ninth Circuit has not adopted the derivative rule from *Butters*, and even if it had, NSO would not satisfy the standard because it is incorporated outside the United States.[81] Judge Hamilton also objected to the Fourth Circuit's reasoning, arguing "there are different rationales underlying domestic and foreign sovereign immunity."[82] *Domestic* sovereign immunity is grounded in exercising valid constitutional authority from the U.S. federal government. *Foreign* sovereign immunity, on the other hand, is "a matter of grace

rights violations. Oliver Holmes, *Israeli Court Dismisses Amnesty Bid to Block Spyware Firm NSO*, GUARDIAN (July 13, 2020), https://perma.cc/HP5C-TUC9.

78. 225 F.3d 462, 466 (4th Cir. 2000).

79. *Id.*

80. Although it is beyond the scope of this Article, the District Court's approximately seventy-four-page order covers a host of fascinating, complex cyber issues, including how personal jurisdiction is analyzed under the tests of purposeful direction and purposeful availment for foreign defendants alleged to have hacked into the forum state. WhatsApp Inc. v. NSO Grp. Techs. Ltd., 472 F. Supp. 3d 649 (N.D. Cal. 2020) (finding that the court had subject matter jurisdiction and personal jurisdiction, while granting the motion to dismiss WhatsApp's fourth cause of action for trespass to chattels because WhatsApp failed to allege actual damage to infected servers).

81. *Id.* at 667 ("In *Butters*, the defendant asserting derivative sovereign immunity was a U.S. corporation and the Fourth Circuit's reasoning indicated that the U.S. citizenship of the company was necessary to its holding.").

82. *Id.* (citing Broidy Cap. Mgmt. L.L.C. v. Muzin, No. 19-CV-0150 (DLF), 2020 WL 1536350, at *7 (D.D.C. Mar. 31, 2020) (denying derivative foreign sovereign immunity to defendant companies working for Qatar, who were sued for hacking into the plaintiff's computers in response to his criticism of Qatar)).

and comity on the part of the United States," wrote Judge Hamilton.[83] Judge Hamilton did not imply derivative foreign sovereign immunity is unconstitutional, or even unwise as a policy matter. Rather, her reasoning suggests the doctrine of derivative foreign sovereign immunity is for the legislative and executive branches to resolve, not the judiciary. Judge Hamilton also concluded that NSO is not entitled to "conduct-based immunity," which is a common law form of immunity that "potentially applies to the acts of foreign officials not covered by the FSIA."[84] The court found that NSO did not qualify as foreign officials under the common law doctrine because any final judgment would bind only NSO, not their government clients.[85]

On November 8, 2021, the Ninth Circuit affirmed the lower court's order on other grounds. Judge Forest, writing for the Ninth Circuit, held that the FSIA applies to entities, whereas common law immunity applies only to "natural persons."[86] NSO does not fit within the FSIA's "broad definition of 'foreign state'" because it is not a sovereign, "'an organ. . .or political subdivision' of a sovereign," or have a foreign sovereign as its majority owner.[87] Instead, NSO is a "private corporation" selling to "several" sovereigns.[88] Despite NSO's claim to support the "inherently sovereign function" of law enforcement, the court found it irrelevant what governments do with NSO's products and services for the purposes of Congress's definition of a "foreign state" in the FSIA.[89]

The question of derivative foreign sovereign immunity should not be left solely to the courts. The Ninth Circuit's decision is the start of a circuit split with the Fourth Circuit over immunity for contractors. In addition to this growing legal uncertainty between courts of appeal, the Ninth Circuit's rejection of derivative foreign sovereign immunity, while legally accurate under the current FSIA, creates bad policy outcomes. There are significant reasons to hold NSO accountable in light of the numerous reports of misuse of its Pegasus spyware. In fact, in November 2021, Apple also sued NSO and the U.S. Department of Commerce placed NSO on its "Entity List" that prohibits U.S. companies from doing business with NSO and its subsidiaries.[90] Nonetheless, NSO is just the tip of the iceberg of a rapidly growing array of cybersecurity contractors, many of whom provide legitimate products and services to government clients. Providing them with no legal protection is a problem.

---

83. *Id.* (quoting Verlinden B.V. v. Central Bank of Nigeria, 461 U.S. 480, 486 (1983)).

84. *Id.* at 664 (citing Samantar v. Yousuf, 560 U.S. 305, 322 (2010)).

85. *Id.* at 665.

86. WhatsApp Inc. v. NSO Grp. Techs. Ltd., 17 F.4th 930, 933 (9th Cir. 2021).

87. *Id.* at 933, 940 (citing the FSIA's definition of an "agency or instrumentality of a foreign state" under 28 U.S.C. § 1603(b)(2)).

88. *Id.* at 940.

89. *Id.*

90. Nicole Perlroth, *Apple Sues Israeli Spyware Maker, Seeking to Block Its Access to iPhones*, N.Y. TIMES (Nov. 23, 2021), https://perma.cc/HTP8-BAP4; Press Release, U.S. Dep't Com., Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities (Nov. 3, 2021) https://perma.cc/MTD8-ZBHR.

The result of the Ninth Circuit's decision is that cybersecurity companies supporting legitimate state functions of law enforcement and national security are now exposed to litigation risks, even though their government partners enjoy immunity. Even if other circuit courts disagree with the Ninth Circuit and, instead, follow the Fourth Circuit in extending derivative foreign sovereign immunity, it will not solve the problem. Under such an interpretation of the law, cybersecurity contractors like NSO would escape all liability for their actions because the FSIA, in its current form, would provide blanket immunity with none of the current exceptions being applicable, even for those contractors conducting malicious cyberattacks. Even if the Supreme Court addresses the question of derivative sovereign immunity it is unlikely to expand or create any new exceptions to cover cyberattacks. The problem of immunity for cybersecurity contractors without distinguishing between legitimate and illegitimate uses of cyberattacks will continue, unless Congress and the executive branch weigh in.

There is an additional reason why derivative foreign sovereign immunity is best left to the other branches—customary international law ("CIL"). In their decisions rejecting NSO's claims for immunity, both the Ninth Circuit and the Northern California District Court emphasized the reciprocal nature of foreign sovereign immunity between governments based on "grace and comity."[91] The Ninth Circuit wrote that "[t]his cooperative acknowledgement that each nation has equal autonomy and authority promotes exchange and good relationships between nations."[92] This statement implies that the reciprocity of foreign sovereign immunity is transactional. This interpretation slightly misses the mark on the basis of foreign sovereign immunity. Scholar David Stewart writes that grace and comity, despite frequent reference, "are nowhere to be found" in Chief Justice John Marshall's "seminal" opinion in *The Schooner Exchange,* which first recognized foreign sovereign immunity.[93] Instead, Stewart explains that Marshall's opinion "refers to the usage and principles adopted by the unanimous consent of nations—what today we refer to as customary international law."[94] CIL is created by opinio juris—a sense of legal obligation—and general and consistent state practice.[95]

The President and Congress are the primary drivers of U.S. state practice as part of CIL. Under the U.S. Constitution, the executive and legislative branches are given primacy over the judiciary in foreign affairs. Under Article II, the President is commander-in-chief of the armed services and has the power to conduct diplomacy.[96] Under Article I, Congress is given the foreign commerce power and authority to create and maintain the military, declare war, and "define

91. WhatsApp Inc. v. NSO Grp. Techs. Ltd., 17 F.4th 930, 938 (9th Cir. 2021); WhatsApp Inc. v. NSO Grp. Techs. Ltd., 472 F. Supp. 3d 649, 667 (N.D. Cal. 2020).

92. 17 F.4th at 938.

93. STEWART, *supra* note 29, at 6; *see also* Schooner Exchange v. McFaddon, 11 U.S. (7 Cranch) 116, 136–37 (1812).

94. STEWART, *supra* note 29, at 6.

95. RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 102(2) (Am. L. Inst. 1987).

96. U.S. CONST. art. II, § 2, cl. 1-2.

and punish piracies and felonies committed on the high seas, and *offenses against the law of nations*" (emphasis added).[97] Although foreign sovereign immunity is entrenched in CIL, derivative immunity is not.

Congress should pass, and the President should sign, derivative foreign sovereign immunity into law. Doing so would not only produce good policy in an otherwise murky area of U.S. law, but it would also begin a new state practice that could crystalize into CIL. Derivative foreign sovereign immunity would create certainty because cybersecurity companies contracting with states are currently operating in an area of heightened liability. For most contractor industries—such as construction or physical security—immunity in several foreign courts will not be an issue as they only need to worry about legal liability from the jurisdiction in which they physically operate. Contractors in the cybersecurity industry, however, are at a higher risk of complex, foreign litigation because they provide services and products that can cause substantial effects and harm across multiple borders. Cybersecurity contractors' cross-border activities affect a broader pool of potential foreign plaintiffs and raise complicated conflict of laws questions regarding jurisdiction, choice of law, and judgment-recognition.

It is in the United States' interest to clarify its position on liability for cybersecurity contractors by extending derivative immunity. A new international custom of derivative foreign sovereign immunity would help create legal certainty for U.S. and foreign cybersecurity contractors. The current status of the law for foreign sovereign immunity—no applicable FSIA exceptions and no derivative immunity—provides little guidance to governments and their contractors on legitimate versus illegitimate uses of cyberspace. Instead, the law risks creating perverse outcomes for actors in cyberspace. Without derivative foreign sovereign immunity, cybersecurity contractors are increasingly likely to face liability for their work on behalf of states, regardless of whether they provide services for legitimate purposes or not. On the other hand, judge-made derivative foreign sovereign immunity without a new FSIA exception for cyberattacks would be no better: no accountability for cyberattacks with blanket immunity afforded to both states *and* their cybersecurity contractors. Instead, a legislative fix is needed.

III. THE SOLUTION: A CYBERATTACK EXCEPTION TO THE FSIA

Congress should amend the FSIA and add a new exception to address the growing problem of cyberattacks. This Article is not the first to make the case for a new cyber exception. There are a growing number of commentators who recognize that a law passed almost fifty years ago in 1976—the year the Queen of England "became one of the first heads of state to send an e-mail"—fails to adequately account for 21st century challenges in cyberspace.[98] A member of

97. U.S. CONST. art. I, § 8, cl. 3, 10-15. More broadly, Congress can influence U.S. foreign affairs through its power of the purse and the necessary and proper clause. U.S. CONST. art. I, § 9, cl. 7; *id*. art. I, § 8, cl. 18.

98. American researchers brought ARPANET, the earliest ancestor of the modern internet, to England, where the Queen set up her email account to send a message on March 26, 1976 with the

Congress, Representative Jack Bergman, has proposed a bill to enact a cyberattack exception to the FSIA.[99] Critics, such as Chimène Keitner, argue the bill and other proposals for a cyberattack exception use overbroad language that does not capture typical malicious cyberattacks and might hamstring legitimate state uses of cyberspace.[100] This Article agrees with both: the FSIA provides a potential avenue for addressing state-sponsored cyberattacks, and the prior proposals would create more problems than they solve (and do not account for cybersecurity contractors). Rather than using the FSIA to build an absolute "barrier" against any cyberattacks, this Article argues for creating protected "bubbles" around two particularly vulnerable targets—human rights activists and trade secrets.

A. Absolute "Barriers": Prior Proposals Are Too Broad

Three authors—Alexis Haller, Paige Anderson, and Benjamin Kurland—put forward separate proposals for a new cyberattack exception to the FSIA, although they all contain the same fatal flaw by creating an absolute "barrier" against a broad range of cyberattacks.[101] Each proposal is comprehensive and contains useful suggestions, the advantages and disadvantages of which are worth highlighting, before addressing their shared pitfall.

In his proposal, Haller emphasizes the FSIA's provisions for execution of judgments and attachment of assets, particularly under the terrorism exception. In addition to jurisdictional immunity, the FSIA provides immunity from pre-judgment attachment and post-judgment execution of government property. Plaintiffs were often prevented from receiving compensation, despite winning on the merits, due to these provisions; however, Congress, in 2008, loosened the attachment and execution provisions for the terrorism exception.[102] Haller is right to point out the importance of these provisions because they raise the costs on perpetrating states by allowing a prevailing plaintiff to attach property in the United States belonging to the defendant foreign state and its agencies or instrumentalities.[103] Removing immunity for state property is a powerful means for changing the cost-benefit calculus of hacking states.

---

username "HME2" (Her Majesty, Elizabeth II). *See* Cade Metz, *How the Queen of England Beat Everyone to the Internet*, WIRED (Dec. 25, 2012, 6:30 AM), https://perma.cc/N5WE-WMN4.

99. Homeland and Cyber Threat Act, H.R. 4189, 116th Cong. (2019).

100. *See* Chimène Keitner & Allison Peters, *Private Lawsuits Against Nation-States Are Not the Way to Deal With America's Cyber Threats*, LAWFARE (June 15, 2020, 9:09 AM), https://perma.cc/TU2W-VWKB.

101. *See* 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 L. (Feb. 19, 2017), https://perma.cc/94Y8-JQWW; Paige C. Anderson, *Cyber Attack Exception to the Foreign Sovereign Immunities Act*, 102 CORNELL L. REV. 1087, 1090 (2017); Benjamin Kurland, *Sovereign Immunity in Cyber Space: Towards Defining a Cyber-Intrusion Exception to the Foreign Sovereign Immunities Act*, 10 J. NAT'L SECURITY L. & POL'Y, 225, 268-69 (2019).

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

103. Haller, *supra* note 101.

Anderson models her proposal largely on the terrorism exception under §1605A. She notes that Congress included material support for terrorism because "material support. . .is just as reprehensible, and just as necessary to deter, as perpetration."[104] Hinting at the role of cybersecurity contractors, Anderson includes a material provision in her proposal "to account for the possibility of states using individuals who are not government employees to carry out cyber attacks."[105] Anderson's material support provision is a step in the right direction by outlining the damage supporting actors may cause alongside perpetrating states. Nevertheless, the model language of her proposal does not address the issue of contractors directly because it still refers to material support by a foreign state.[106]

Kurland's cyber exception proposal also draws from the terrorism exception, particularly for its punitive damages. In conjunction with attachment and execution of property, punitive damages are important because they further raise the costs of malicious cyberactivity. Additionally, Kurland proposes using a similar designation process as the state sponsor exception, whereby suits may only be brought against a state designated by the Secretary of State as a "cyber-intruder."[107] While a designation requirement would limit the effect of Kurland's broad prohibition on cyberattacks, it would go too far by effectively stonewalling most suits even before they begin. Unlike terrorism, many states conduct cyberattacks. The executive branch is unlikely to upset so many diplomatic relationships with "cyber-intruder" designations, as evidenced by the United States' poor track record on calling out cyberattacks. As Anderson notes, the United States stayed quiet and refused to make public attribution long after Chinese hackers stole data on 21.5 million Americans from the U.S. Office of Personnel Management in 2015.[108]

Despite a few differences, all three proposals would remove jurisdictional immunity and create a substantive private cause of action for cyberattacks. Each proposal uses slightly different definitions of cyberattack; however, they share similarly broad language removing immunity for cyberattacks by states with only a few limits. Haller suggests drawing from federal anti-hacking laws, and Kurland explicitly does so, using language from the Wiretap Act and the Computer Fraud and Abuse Act ("CFAA").[109] Anderson's proposal would prohibit cyber activity including "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."[110] Anderson would limit cyberattacks by requiring they produce

104. Anderson, *supra* note 101, at 1100.
105. Anderson, *supra* note 101, at 1103.
106. Anderson, *supra* note 101, at 1102.
107. Kurland, *supra* note 101, at 270.
108. Anderson, *supra* note 101, at 1106-07.
109. Haller, *supra* note 101; Kurland, *supra* note 101, at 263.
110. Anderson, *supra* note 101, at 1102.

"substantial effects" in the United States;[111] however, she provides no definition for "substantial," which would likely create significant unpredictability in judicial outcomes.

Anderson also argues her proposal is properly tailored and avoids issues of reciprocity because "all [it] would do. . .is exclude *private* parties as legitimate targets for foreign governments."[112] Private parties, however, are not per se illegitimate targets. Law enforcement investigations of transnational criminal organizations and intelligence collection on terrorist organizations are examples of states targeting private parties. Few would argue these are illegitimate purposes. States with legitimate purposes may also need to access networks of private companies, even if they are not stealing trade secrets. Anderson's proposal creates a binary distinction between public and private domains that is unhelpful for delineating legitimate and illegitimate targets.

The focus by all three proposals on the means—forms of cyberattacks—rather than the ends—targets of cyberattacks—is imprudent because there are legitimate uses for cyberspace which may constitute a cyberattack. Other exceptions, such as terrorism, are easier to draw lines around because it is readily accepted that any form of terrorism is not legitimate statecraft. There is no such consensus around cyberspace. It is an immense and ultimately futile challenge to tailor what forms of cyberattacks are permissible, particularly in a field that rapidly innovates new forms of cyberattacks. Despite some variations, each of these prior proposals for a new FSIA cyber exception focuses on regulating forms of cyberattacks that are overly broad. They capture a wide range of both legitimate and illegitimate cyberattacks. Ultimately, legitimate and illegitimate cyberattacks are not differentiated by the form of the cyberattack. For example, a state's cyberattack on a foreign military installation and on a hospital may involve the same cyber tools; however, most people would likely accept that the cyberattack on the hospital is an illegitimate cyberattack, while a military installation attack is legitimate (assuming it is lawful under jus ad bellum and jus in bello rules). The distinction is driven by the nature of the target. Therefore, an absolute "barrier" on forms, rather than protecting the targets, of cyberattacks misses the mark.

B. Protected "Bubbles": New Solution Tailored to Specific Targets and Covering Cybersecurity Contractors

Re-imagining a contemporary FSIA does not require reinventing the wheel. Despite their overly broad cyberattack provisions, the authors described above put forward important ideas related to attachment and execution, punitive damages, and material support, from which a more tailored

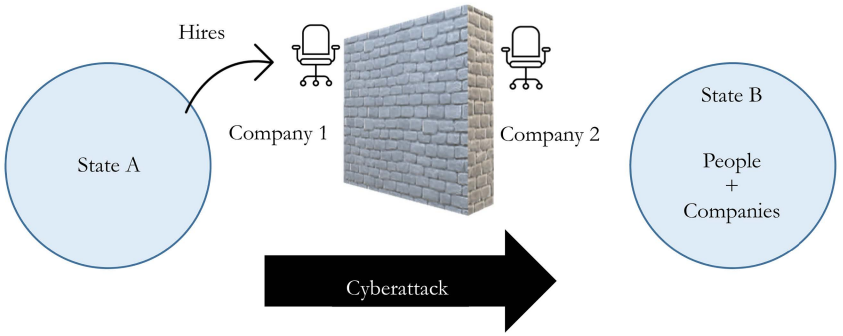
111. Anderson, *supra* note 101, at 1102.
112. Anderson, *supra* note 101, at 1107-08.

cyberattack exception can be built. Two important issues, though, must be added for creating "protected bubbles" around vulnerable targets—trade secrets and human rights activists—and addressing the issue of derivative immunity.

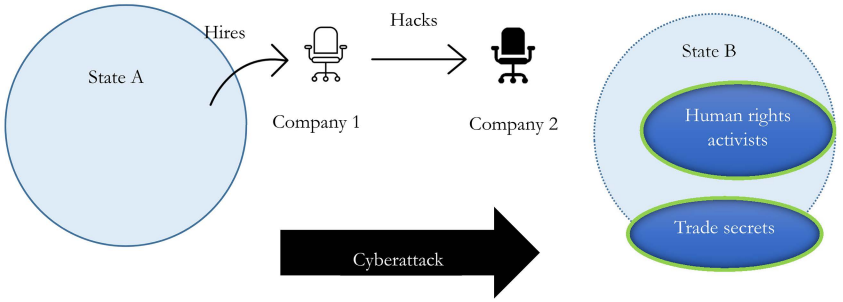
Rather than focus solely on the form of cyberattack, Congress should limit the new exception to removing liability only for cyberattacks targeting trade secrets and human rights activists. As highlighted above, these two protected classes are particularly vulnerable, either as companies presenting target rich environments and few offensive capabilities or as individuals with even fewer resources for defense. These protected targets create a limiting principle missing from the prior proposals. Under the prior proposals, the executive branch would rightly be concerned about reciprocity. For example, if other states enacted similar cyberattack exceptions as the prior proposals, the United States might find itself dragged into foreign courts for disrupting foreign servers, regardless of whether the United States targeted the servers to steal trade secrets or prevent a troll farm from interfering in U.S. elections. Similarly, the United States might face the same amount of liability for conducting a cyberattack against a cartel leader for law enforcement purposes as it would if it hacked into the device of a human rights activist who criticized the U.S. administration online. The lesson here is not that the United States, or any state, should be free to conduct all these operations. Instead, these examples highlight that cyberattacks may be used for legitimate and illegitimate purposes. Treaties and CIL provide few rules outlining which types of cyberattacks fall into each category. Congress should pass a new and tailored cyberattack exception in the FSIA to begin developing norms—with the aim of eventually crystallizing into custom—by drawing lines around legitimate state behavior in cyberspace.

In addition, the question of derivative immunity is an important one that Congress should address, rather than wait for circuit courts to parse through various interpretations. Congress should act by explicitly providing derivative foreign sovereign immunity for cybersecurity contractors under the FSIA. Immunity should be only for cybersecurity contractors because, as noted in Section II(B)(2), cybersecurity contractors face heightened cross-border litigation risks compared to other government contractors, warranting unique immunity. A new cyberattack exception should also include Anderson's suggestion for a material support provision. Cybersecurity contractors should face liability for malicious cyberattacks, even if they do not, themselves, conduct the attacks. Liability must also be imposed on those who facilitate malicious cyberattacks by providing the requisite training, infrastructure, or software.

To frame, in simple terms, the differences between the prior proposals (absolute "barriers") and this Article's proposal (protected "bubbles"), it is useful to return to the original diagrams from Section I(A). The diagram below is then followed by model legislative language proposed by this Article.



Absolute "barriers": prior proposals block all cyberattacks, regardless of the target



Protected "bubbles": new proposal to prevent attacks on illegitimate targets

The model language below outlines this Article's proposed cyberattack exception, including provisions for jurisdictional immunity, derivative immunity, substantive cause of action, and definitions for key terms. In addition, the new exception would include Haller's suggestion to amend the FSIA's attachment and execution language under 28 U.S.C. § 1610(g)(1) to include cyberattack cases.[113] The new exception would read as follows:

28 U.S.C. § 1605C. Cyberattack exception to the jurisdictional immunity of a foreign state

(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 for a cyberattack by the foreign state targeting—

(A) any human rights activists, who are U.S. persons or are located in the United States;

(B) any trade secrets owned by business entities which are incorporated or have their principal place of business in the United States; or

113. *See* Haller, *supra* note 101.

(C) servers or other computers located in the United States in order to reach either of the protected classes listed in (A) and (B).

(2) **Derivative immunity.—** A private cybersecurity contractor operating as an agent or instrumentality of the foreign state shall receive the same immunity as the foreign state under § 1604 for actions taken while acting within the scope of employment or agency except for providing material support to, facilitating, or otherwise conducting cyberattacks, on behalf of the foreign state, that target the protected classes listed in § 1605C(a)(1)(A)-(C).

(b) **Private Right of Action.—**

(1) A foreign state and any official, employee, or agent of that foreign state, including any private cybersecurity contractor, while acting within the scope of his or her office, employment, or agency, shall be liable to any person or business entity described in subsection (a)(1) and (2) for money damages sought, including economic damages, solatium, pain and suffering, and punitive damages.

(2) Definitions.

(A) A "cyberattack" means:

(i) intentionally intercepting or endeavoring to intercept any wire, oral, or electronic communication; or

(ii) intentionally accessing a computer without authorization or exceeding authorized access, and thereby obtaining information from any protected computer.[114]

(B) "Human rights activists" means individuals, groups, and associations contributing to the effective elimination of all violations of human rights and fundamental freedoms of peoples and individuals, including, but not limited to, mass, flagrant, or systematic violations, such as those resulting from apartheid, all forms of racial discrimination, colonialism, foreign domination or occupation, aggression or threats to national sovereignty, national unity or territorial integrity, and from the refusal to recognize the right of peoples to self-determination and the right of every people to exercise full sovereignty over its wealth and natural resources.[115]

---

114. This definition of cyberattack is drawn from the proposal by Benjamin Kurland, who used language from the Wiretap Act, 18 U.S.C. § 2511(1)(a) (2018), and the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(e)(2) (2012). *See* Kurland, *supra* note 101, at 268-69.

115. The language for this definition of "human rights activists" is drawn from the UN General Assembly's Declaration on Human Rights Defenders. Although it is a non-binding document, the Declaration was adopted by consensus and is based on other legally binding instruments, such as the International Covenant on Civil and Political Rights. G.A. Res. 53/144, Declaration on the Right and

(C) "Trade secrets" means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if—
  (i) the owner thereof has taken reasonable measures to keep such information secret; and
  (ii) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information.[116]
(D) "Cybersecurity contractors" means any private individual, group of individuals, or business entity selling cybersecurity services or products to a foreign state.

CONCLUSION

Amending the FSIA will be no easy task. Foreign sovereign immunity in cyberspace raises competing interests related to reciprocity, legitimate uses of cyberattacks, the role of private cyber actors, and cyber norm creation. The new FSIA cyberattack exception proposed by this Article strikes the proper balance. Cybersecurity contractors providing services for legitimate activities would enjoy derivative immunity. Companies, such as NSO, who create and sell malware to states using it to threaten human rights would find their immunity stripped away in U.S. courts. The new exception would ensure injured private parties—individuals and companies—are able to affirmatively assert their claims in U.S. courts against malicious state-sponsored cyberattacks. Recognizing that other states will likely pass similar legislation, the United States is more likely to enact a tailored exception than a broad proposal prohibiting any cyberattacks.

As cyberspace becomes an ever more dynamic and critical domain for competition, the United States should lead in developing prudent norms for legitimate state practice. Cyber risks are rapidly proliferating, and U.S. and international law must catch up. This Article's proposed exception would provide an effective legislative patch to the FSIA's cyber vulnerabilities. It is time foreign sovereign immunity receives an update for the digital era.

Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms (Dec. 9, 1998), https://perma.cc/7E7U-HGC9.

116. The definition of "trade secrets" is drawn from the Economic Espionage Act. 18 U.S.C. § 1839 (3) (2016).