

2021

Leveraging Domestic Law Against Cyberattacks

Justin Malzac

Follow this and additional works at: <https://digitalcommons.wcl.american.edu/nslb>



Part of the [Internet Law Commons](#)

Recommended Citation

Justin Malzac "Leveraging Domestic Law Against Cyberattacks," American University National Security Law Brief, Vol. 11, No. 1 (2021).

Available at: <https://digitalcommons.wcl.american.edu/nslb/vol11/iss1/2>

This Article is brought to you for free and open access by the Washington College of Law Journals & Law Reviews at Digital Commons @ American University Washington College of Law. It has been accepted for inclusion in American University National Security Law Brief by an authorized editor of Digital Commons @ American University Washington College of Law. For more information, please contact kclay@wcl.american.edu.

Leveraging Domestic Law Against Cyberattacks

Justin Malzac*

“It is almost impossible to overstate the gap between the rate at which the cybersecurity threat is getting worse relative to our ability to effectively address it. The simple fact of the matter is that no nation has yet found an effective solution to stop foreign malevolent cyber activity. We will continue to be confronted by this challenge in 2020.”

Glenn Gerstell, General Counsel for the National Security Agency¹

INTRODUCTION

Over the past two decades, cyberspace has become a key area of operations, for both criminals and states alike, as they pursue their particular interests internationally. The United States has been struggling to adapt to this new paradigm, as have most democratic countries across the globe. Most recently, malicious cyber actors have been targeting medical systems

*Justin Malzac is the Senior Paralegal at a DOD joint component command. He is an Army civilian employee and 18-year veteran of the Army Reserves. He has an M.A. in History from Pittsburg State University and a B.A. in English from the University of Minnesota, and was previously published in the *International Journal of Korean Studies*. The views expressed in this article are those of the author and do not necessarily reflect the official policy or position of the United States Army, the Department of Defense, or the United States Government. The author would like to graciously thank Major David Lai, Lieutenant Colonel Israel King, and Lieutenant Colonel Christopher Berhow, all military judge advocates, for their comments on this paper and for their years of mentorship. This project would not have been possible without their enduring support. The author would also like to thank the editorial staff of the National Security Law Brief for their detailed feedback, which helped make this paper the best it could be.

American University National Security Law Brief, vol. 11, issue 1 (Spring 2021), pp. 1–51.
© 2021 by the American University National Security Law Brief at Washington College of Law.
All rights reserved.

¹ Glenn Gerstell, *NSA General Counsel Remarks to the American Bar Association*, LAWFARE (Jan. 17, 2020, 10:00 AM), <https://www.lawfareblog.com/nsa-general-counsel-remarks-american-bar-association>.

during the COVID epidemic.² As highlighted in May of this year by Adina Ponta, “Recent reports and Interpol warnings show a surge in low-level cyber operations during the ongoing pandemic against hospitals, clinics and pharmaceutical companies.”³ Cyber criminals continue to grow more sophisticated and more prolific.

In March of this year, the Cyberspace Solarium Commission, established by the Fiscal Year 2019 National Defense Authorization Act, released its full report to Congress.⁴ While the report presents many innovations in cyber defense, it suffers from one significant weakness—a fixation on a cyber doomsday scenario that has yet to occur. In the executive summary, the authors argue “During the Cold War, our best minds were tasked with developing Continuity of Government plans to ensure that the government could survive and the nation recover after a nuclear strike. We need similar planning today to ensure that we can reconstitute in the aftermath of a national-level cyberattack.”⁵ While referencing nuclear war in a cyber debate makes for a good political show, it bears little connection to reality. Such doomsday scenarios have played out numerous times on the silver screen, but not a single one has yet occurred in real life and the possibility remains unlikely.⁶ The majority of attacks that have made headlines in the

² See, e.g., Chris Fox & Leo Kelion, *Coronavirus: Russian Spies Target Covid-19 Vaccine Research*, BBC NEWS (Jul. 16, 2020), <https://www.bbc.com/news/technology-53429506> (detailing a recent cyberattack on a Covid-19 research lab).

³ Adina Ponta, *Cyber Operations Against Medical Facilities During Peacetime*, LAWFARE (May 1, 2020, 10:33 AM), <https://www.lawfareblog.com/cyber-operations-against-medical-facilities-during-peacetime>. Ponta also notes here that such attacks “mostly consist in spreading false information about cures, prevention measures, and stocks of medical supplies,” or in seizing personal data for the sake of blackmail. See also *id.*

⁴ CYBERSPACE SOLARIUM COMMISSION, U.S. CYBERSPACE SOLARIUM COMMISSION FULL REPORT (2020), https://drive.google.com/file/d/1ryMCIL_dZ30QyJFqFkkf10MxIXJGT4yv/view.

⁵ Senator Angus King & Representative Mike Gallagher, *Chairmen’s Letter to U.S. CYBERSPACE SOLARIUM COMMISSION EXECUTIVE SUMMARY*, at ii (2020), <https://drive.google.com/file/d/1c1UQI74Js6vkfJUowI598NjwaHD1YtIY/view>.

⁶ See Lee Jarvis & Stuart Macdonald, *Responding to Cyberterrorism: Options and Avenues*, 16 GEO. J. INT’L AFF. 134, 139 (2015) (“[I]t seems reasonable to suggest that doomsday scenarios around cyberterrorism may be located somewhere between misguided and unlikely.”).

past decade have targeted personal information, not infrastructure.⁷ Even the Stuxnet worm, which targeted and damaged centrifuges connected to the Iranian nuclear program, only caused around \$2 million worth of damage.⁸ Moreover, it caused little to no civil disruption, and Iran was able to recover from the physical damage within months, even while under sanctions.⁹ Most recently, the so-called "hack of the decade" by suspected Russian agents against U.S. government systems, which hit the news last December, represented relatively benign behavior—foreign agents only accessed unclassified government networks and caused no physical damage in the process.¹⁰

The government certainly must prepare for a catastrophic cyber event, but should prioritize efforts to defend against the smaller attacks that happen on a daily basis, and are primarily directed against private industry. NASA works to defend us against a statistically unlikely asteroid collision, but they spend much more time and money on realistic and attainable goals, such as sending astronauts to low orbit and unmanned craft to nearby planets.¹¹ Malicious cyberattacks happen every day, and they overwhelmingly target private entities, not the

⁷ See, e.g., Catalin Cimpanu, *A Decade of Hacking: The Most Notable Cyber Security Events of the 2010s*, ZDNET (Dec. 12, 2019, 10:52 PM), <https://www.zdnet.com/article/a-decade-of-hacking-the-most-notable-cyber-security-events-of-the-2010s/> (summarizing noteworthy cyberattacks of the 2010s).

⁸ Jarvis & Macdonald, *supra* note 6, at 138-39.

⁹ See Joby Warrick, *Iran's Natanz Nuclear Facility Recovered Quickly from Stuxnet Cyberattack*, WASH. POST (Feb. 15, 2011), https://www.washingtonpost.com/world/irans-natanz-nuclear-facility-recovered-quickly-from-stuxnet-cyber-attack/2011/02/15/ABUIkoQ_story.html.

¹⁰ See Kimberly Dozier, *U.S. Cyber Experts Scramble to Assess the Scope of the 'Hack of a Decade'*, TIME (Dec. 18, 2020), <https://time.com/5923056/cyber-attack-us-government/> (While certainly harmful to U.S. national security and representative of the general threat of cyberattacks, this "worst-ever" incident, as some have called it, was far from the apocalyptic scenarios requiring the "reconstitution" of government and society still being pushed today in government reports such as that of the Cyberspace Solarium Commission. Lost in the hyperbolic news-cycle was the fact that this attack affected private industry as much, or even more, than the government.)

¹¹ See NASA, NATIONAL AERONAUTICS AND SPACE ADMINISTRATION FY 2020 SPENDING PLAN FOR APPROPRIATION 2 (May 28, 2020), https://www.nasa.gov/sites/default/files/atoms/files/fy_2020_spend_plan.pdf (reporting \$150M earmarked for planetary defense out of the total \$22.7B NASA 2020 spending plan).

government and its information or infrastructure.¹² According to Norton, “Cybercriminals will steal an estimated 33 billion records in 2023.”¹³ In 2019, Cyber Defense Magazine noted that “43% of all cyberattacks are aimed at small businesses.”¹⁴ Bringing those harrowing statistics home, Norton also suggested there is an expectation for “more than half of all data breaches globally to occur in the United States by 2023.”¹⁵ Many of these small companies without their own internal capacity to defend themselves.¹⁶

In recent years there have been several high-profile cyber incidents tied to states, including the hacking of Sony Pictures by North Korea in 2014, and the election manipulation campaign and hacking of computer networks controlled by the Democratic National Committee by Russia-tied groups in 2016.¹⁷ Many of these incidents, though clearly attributed to states, fell below the threshold of an “armed attack” per the UN Charter, preventing a lawful self-defense response by the government.¹⁸ Indeed, most cyberattacks fall below this threshold, creating ambiguity for the legal responses victim states may take.¹⁹ The need to respond to such large-scale attacks should not be skirted, but it also should not be the sole, or even primary focus of national cyber policy.

¹² See Nick Galov, *Cyber Security Statistics for 2019*, CYBER DEF. MAG. (Mar. 21, 2019), <https://www.cyberdefensemagazine.com/cyber-security-statistics-for-2019/> (detailing the effects of cybercrime on businesses).

¹³ *10 Cyber Security Facts and Statistics for 2018*, NORTON (2018), <https://us.norton.com/internetsecurity-emerging-threats-10-facts-about-todays-cybersecurity-landscape-that-you-should-know.html>.

¹⁴ Galov, *supra* note 12.

¹⁵ NORTON, *supra* note 12.

¹⁶ See Galov, *supra* note 12 (“Many small businesses have minimal security infrastructure, making them easy prey for data predators.”).

¹⁷ For details on the indictment of Russian agents for the DNC hack, see, e.g., Alex Ward, *Read: Mueller Indictment Against 12 Russian Spies for DNC Hack*, VOX (Jul. 13, 2018, 12:30 PM), <https://www.vox.com/2018/7/13/17568806/mueller-russia-intelligence-indictment-full-text> (detailing the indictment of Russian agents for the DNC hack).

¹⁸ See Ryan Goodman, *Cyber Operations and the U.S. Definition of “Armed Attack”*, JUST SECURITY (Mar. 8, 2018), <https://www.justsecurity.org/53495/cyber-operations-u-s-definition-armed-attack/>.

¹⁹ See generally *id.* (describing inconsistencies in different countries’ responses to cyberattacks); see also Galov, *supra* note 12 (“In 2017, 61% of data breach victims were companies with less than 1000 employees.”).

As noted above, the vast majority of cyberattacks fall on small, private enterprises, not on government infrastructure. This reality requires civil and domestic responses, rather than military ones. Even so, the United States government is still fixated on big government, if not military-led responses to cyberattacks.²⁰ As shown recently by Jason Healy, “federal cybersecurity spending on civilian departments like the departments of Homeland Security, State, Treasury, and Justice is overshadowed by that going toward the military.”²¹ Indeed, as Healy noted, “The White House and National Cyber Strategy emphasize the need to protect the American people and our way of life, yet the budget does not reflect those values. Rather, the budget clearly shows that the Defense Department is the government’s main priority.”²²

The current buzzword in cyber politics is “Defend Forward,” first presented in the 2018 Department of Defense Cyber Strategy, the DOD’s subordinate document to the National Cyber Strategy.²³ The unclassified introduction to the plan argues that the DOD’s “primary role in this homeland defense mission is to defend forward by leveraging our focus outward to stop threats before they reach their targets.”²⁴ This involves using military cyber means to monitor, disrupt, or even counterattack malicious cyber actors.²⁵ What was originally designed as a strictly military plan, focusing on the United States’ “most capable and dangerous adversaries in

²⁰ See U.S. DEPARTMENT OF DEFENSE, SUMMARY: DEPARTMENT OF DEFENSE CYBER STRATEGY 1 (Sep. 18, 2018), https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF [hereinafter SUMMARY: DEPARTMENT OF DEFENSE CYBER STRATEGY 1].

²¹ Jason Healey, *The Cyber Budget Shows What the U.S. Values—And It Isn’t Defense*, LAWFARE (Jun. 1, 2020, 11:21 AM), <https://www.lawfareblog.com/cyber-budget-shows-what-us-values%E2%80%94and-it-isnt-defense>.

²² *Id.*

²³ SUMMARY: DEPARTMENT OF DEFENSE CYBER STRATEGY 1, *supra* note 20.

²⁴ *Id.* at 2.

²⁵ *Id.*

cyberspace” and leaving the “lesser threats” to civil authorities, has since been adopted by the Cyberspace Solarium Commission into its domestic agenda.²⁶

In a speech to the American Bar Association this past January, Glenn Gerstell, General Counsel for the NSA, painted a grave picture for the coming years in regards to the cyber threat faced by the United States, ultimately concluding in part that “these challenges will present a series of policy choices, and those in turn will require new laws or amendments to existing laws.”²⁷ Action must be taken. As the Cyberspace Solarium Commission chairmen pointed out, “Today most cyber actors feel undeterred, if not emboldened, to target our personal data and public infrastructure.”²⁸ The question is not whether the United States should respond to cyberattacks and cybercrime, but how to respond and who should be in the lead.

This paper is a response to recent U.S. government policy developments and is constructed in two parts. First is an examination of how international law has been largely unable to tackle the growing cyber epidemic.²⁹ Domestic measures are necessary because of the lack of enforceable international law norms, the weakness of international law responses, and the challenged posed by near-peer competitor states that are employing domestic measures of their own. The second part consolidates a range of domestic policy options as a means of defense against increasing cyber aggression below the threshold of war and as a counter proposal to the big government-centric options currently being touted in front of Congress.³⁰

Ultimately, as the number of cyberattacks against the United States—both by state and non-state actors—continues to swell, swift action must be taken. And since international law has

²⁶ Jeff Kosseff, *The Contours of ‘Defend Forward’ Under International Law*, in 2019 11TH INT’L CONF. ON CYBER CONFLICT: SILENT BATTLE 307, 310 (T. Minárek et al. eds., 2019), https://ccdcoe.org/uploads/2019/06/CyCon_2019_BOOK.pdf.

²⁷ Gerstell, *supra* note 1.

²⁸ King & Gallagher, *supra* note 5, at i.

²⁹ See *infra* Part I.

³⁰ See *infra* Part II.

largely failed to address the epidemic, we must rely on domestic means of defense, but the question still stands as to which types of measures will be most effective. This paper argues that the best way to address the rash of smaller, localized cyberattacks is to empower attribution mechanisms such as private cyber security (“hack back”) and passive military posturing (“defend forward”) in order to support actions in domestic U.S. courts (criminal prosecution and civil liability). Contrary to recent proposals, big government is not the answer. The only feasible approach to combat thousands of daily cyberattacks is a decentralized one.

I. THE INADEQUACIES OF INTERNATIONAL LAW

It has been widely accepted for some time that a cyber operation meeting the recognized definition of an “armed attack”—such as a cyberattack which causes physical damage or deaths at the affected site—is governed by the same international law which regulates kinetic attack (i.e., *jus ad bellum* or *jus in bello*).³¹ However, decades on, there is still little consensus on what, if any, elements of international law govern cyber operations or intrusions below the threshold of armed attack.³² The lack of consensus on cyber and sovereignty has been reiterated by scholars such as Harriet Moynihan, who wrote in 2019 that “to date most States have not put on record their views, and as yet, the matter is not clear or settled.”³³ The current discussion on sovereignty is highly “western-centric,” with Russia and China voicing contrary interpretations in recent

³¹ See generally Eitan Diamond, *Applying International Humanitarian Law to Cyber Warfare*, in LAW & NAT’L SECURITY: SELECTED ISSUES 67 (Pnina Sharvit Baruch & Anat Kurz eds., 2014) (comparing and contrasting the application of IHL to cyberattacks). See also Harold Hongju Koh, *International Law in Cyberspace: Remarks as Prepared for Delivery by Harold Hongju Koh to the USCYBERCOM Inter-Agency Legal Conference Ft. Meade, MD, Sept. 18, 2012*, 54 HARV. INT’L L. J. 1, 7 (2012) (discussing the enduring U.S. government perspective).

³² See Goodman, *supra* note 18 (contrasting the U.S. and international approaches to self-defense in response to low level cyberattacks).

³³ Harriet Moynihan, *The Application of International Law to Cyberspace: Sovereignty and Non-intervention*, JUST SECURITY (Dec. 13, 2019), <https://www.justsecurity.org/67723/the-application-of-international-law-to-cyberspace-sovereignty-and-non-intervention/>.

meetings of the UN Group of Experts for cyber.³⁴ Even U.S. experts have voiced their doubts. For example, Gary Corn, the former Staff Judge Advocate at U.S. Cyber Command, has noted, “the fact that States have developed vastly different regimes to govern the air, space, and maritime domains underscores the fallacy of a universal rule of sovereignty with a clear application to the domain of cyberspace.”³⁵ Most, if not all, recent cyber incidents have fallen well below the threshold of war, and under the purview of peacetime international law.³⁶ However, the mechanisms of the peacetime regime have thus far been inadequate to stem, or even largely respond to these attacks.

The power and authority of international law comes from a consensus of views, actions, and recognized legal norms.³⁷ When the international community stands apart, gaps appear in the legal bulwark that can be exploited by opportunist or maleficent actors.³⁸ For example, despite overt international support for UN sanctions against North Korea, that country has been able to maintain its nuclear and military programs in part because China and other countries have violated trade restrictions.³⁹ International law is largely inadequate in addressing malicious cyber

³⁴ *Id.*

³⁵ Gary P. Corn & Robert Taylor, *Sovereignty in the Age of Cyber*, 111 AM. J. INT’L L. 207, 210 (2017), <https://doi.org/10.1017/aju.2017.57>.

³⁶ See Goodman, *supra* note 18 (discussing the legal and factual ambiguities surrounding state use of cyber tactics). See also Galov, *supra* note 12 (detailing 2019 cyberattack statistics).

³⁷ See Bruce Cronin, *International Legal Consensus and the Control of Excess State Violence*, 11 GLOBAL GOVERNANCE 311, 311 (2005) (Current dominant theories on international law focus on state consent as the basis of customary law. Cronin argues that a new regime of “consensus-based” law has emerged, largely following WWII. He differentiates traditional customary law from consensus-based law by suggesting that the former is established only after years of consistent state practice, whereas the latter is created to preempt unwanted practice. In the case of cyber law, the many international working groups such as the GGE or OEWG are often concerned with large-effect cyber questions that have yet to manifest in enduring state practice. This aligns these efforts with Cronin’s definition of consensus-based international law.).

³⁸ See Stewart M. Patrick, *Is the International Community Growing Part?*, COUNCIL ON FOREIGN RELS. (Feb. 4, 2013), <https://www.cfr.org/blog/international-community-growing-apart> (arguing that a lack of international unity has prevented an effective global response to cybercrime).

³⁹ See, e.g., Michelle Nichols, *Exclusive: North Korea Enhanced Nuclear, Missile Programs in 2019 in Breach of Sanctions*, REUTERS (Feb. 10, 2020, 1:34 PM), <https://www.reuters.com/article/us-northkorea-sanctions-un-exclusive/exclusive-north-korea-enhanced-nuclear-missile-programs-in-2019-in-breach-of-sanctions-u-n-report-idUSKBN20426J> (detailing the DPRK’s use of China to conduct ship-to-ship transfers of coal).

activities for several reasons, including the lack of customary law, the weakness of the responses allowed under international law, and the strengthening of domestic measures by rival states.

A. Customary International Law

The multiple sources of international law are described in Article 38 of the Statute of the International Court of Justice, and include: international conventions (treaties), international custom (customary law and norms), the general principles of law recognized by civilized nations (*opinio juris*), and international court decisions which are binding on the parties involved.⁴⁰

Article 38 also suggests that other judicial decisions, such as those of the International Court of Justice, and “highly qualified” academic work, such as the *Tallinn Manual*, may be relied up as “subsidiary means for the determination of rules of law.”⁴¹ In the end, though, treaty law is king. Treaties create clear and binding obligations on the states that join them.⁴² When treaty obligations and customary law conflict, treaty will almost always trump custom.⁴³

In absence of any treaty, which is currently true of cyberattacks below the threshold of armed attack—most states agree that cyberattacks meeting the threshold of an armed attack are governed by long-established rules for armed conflict, such as the UN Charter and the Geneva Conventions—customary international law fills the legal void.⁴⁴ Custom exists when states

⁴⁰ Statute of the International Court of Justice art. 38.

⁴¹ *Id.* The United States does not strongly support the ICJ and has long rejected ICJ authority. The U.S. withdrew from the ICJ’s compulsory jurisdiction in 1986, in response to the Nicaragua Decision, and the Trump administration has been moving to withdraw from secondary treaties which may provide the court with indirect means of jurisdiction. Even so, Article 38 lays out the foundations of International Law in a manner that most American jurists would agree with.

⁴² See Rebecca Crootof, *Change Without Consent: How Customary Law Modifies Treaties*, 41 YALE J. INT’L L. 237, 240 (2016) (“States explicitly consent to be bound by a treaty, but their consent to customary international law (to the extent it exists) usually must be inferred.”).

⁴³ See *id.* (“[M]ost tend to presume that, where the two sources require contradictory outcomes, treaty law will prevail.”).

⁴⁴ See *id.* at 246 (“In the absence of directly relevant treaty law, and in need of reliable guiding principles, states are developing practices standardizing their rights and duties in these new spheres.”).

commonly exhibit a standard of behavior and accept that standard as obligatory.⁴⁵ Acceptance is generally determined through the public policy statements or legal interpretation, known as *opinio juris*, of the state.⁴⁶ Customary international law acts in a similar way to treaty law, requiring a type of state consent, but in the form of state practice or published opinion related to the issue.⁴⁷ The establishment of an international norm does not require universal acceptance, but states that persistently object to an emerging custom are generally not held to it.⁴⁸

Unfortunately, states have yet to agree on how international law should handle below-the-threshold cyberattacks. Just within the UN there are two competing processes. One of these, the Group of Governmental Experts or GGE, is the continuation of an enduring process championed by the United States. The other, called the Open-Ended Working Group or OEWG, was recently sponsored by Russia, as that state seeks to redirect and dominate the cyber discussion to its own ends. Neither of these processes are likely to produce concrete results in the near future.⁴⁹

One source offers a glimpse of what that consensus might eventually be like, at least if Western perspectives win out. This is the *Tallinn Manual* [hereinafter “the Manual”].⁵⁰ The first edition was released in 2013, the second in 2017, and both were collaborative projects sponsored by the NATO Cooperative Cyber Defense Centre of Excellence.⁵¹ The second manual, dubbed

⁴⁵ See Rebecca Crootoof, *International Cybertorts: Expanding State Accountability in Cyberspace*, 103 CORNELL L. REV. 565, 642 (2016) (defining the elements of customary international law).

⁴⁶ See Hiroshi Taki, *Opinio Juris and the Formation of Customary International Law: A Theoretical Analysis*, 51 GERMAN Y.B. INT'L L. 447, 448 (2008) (providing a definition and analysis of “*opinio juris*”).

⁴⁷ See Crootoof, *Change Without Consent*, *supra* note 42, at 240.

⁴⁸ See Cronin, *supra* note 37, at 314 (“[S]tates can exempt themselves from customary law by maintaining a persistent and consistent objection to it over a period of time.”).

⁴⁹ See Elaine Korzak, *What’s Ahead in the Cyber Norms Debate?*, LAWFARE (Mar. 16, 2020, 12:08 PM), <https://www.lawfareblog.com/whats-ahead-cyber-norms-debate> (arguing that “The fundamental differences and political divisions that torpedoed the discussions of the 2016-2017 GGE are unlikely to dissipate anytime soon.”).

⁵⁰ *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Michael N. Schmitt ed., Cambridge U. Press, 2017); see also *Tallinn Manual 2.0*, NATO CCDCOE, <https://ccdcoc.org/research/tallinn-manual/> (last visited Aug. 14, 2020) (describing the manual’s history, contributors, and aspirations).

⁵¹ *Tallinn Manual 2.0*, NATO CCDCOE, *supra* note 50.

Tallinn Manual 2.0, is now one of the most cited documents relating to cyber law.⁵² However, it is important to note that the Manual is not itself customary international law, nor an expression of state policy.⁵³ In fact, the authors explicitly affirm the opposite, writing the Manual does not “reflect the position of any other organization or state represented by . . . participation as [authors] or as peer reviewers by individuals who hold government positions.”⁵⁴ In the case of the *Tallinn Manual*, several of the world’s most active cyber players—Russia, North Korea, Iran, Cuba—did not participate in the writing of the book.⁵⁵ As noted by Robert Papp of the Wilson Center, “The Tallinn Manual could be a starting point [for a future cyber treaty], although the Russian Federation played no part in its drafting and would want its own input.”⁵⁶

The authors of the Manual intended to capture the contemporary state of customary international law related to cyberattacks. However earnest this endeavor was, it is severely weakened by internal disagreements on the most critical issues (such as sovereignty), the rapidly changing landscape of published *opinio juris*, and the distance certain countries (including the United States) have built between their own policies and the Manual’s “rules.”⁵⁷

⁵² *Id.*

⁵³ There are countless examples of academic work which overlook this fact and cite to the *Tallinn Manual* as though it were established primary authority. Not only do the authors of the manual disagree on many points among themselves, but states such as the U.S. have distanced themselves from some of its key rules. Any reference to the *Tallinn Manual* should include a caveat that it is not customary legal authority. See, e.g., Ponta, *supra* note 3 (failing to clarify the limited authority of the manual).

⁵⁴ *Introduction*, in TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 2 (Michael N. Schmitt ed., Cambridge Univ. Press 2d ed. 2017) [hereinafter *Introduction*, TALLINN MANUAL 2.0].

⁵⁵ See, e.g., *The Hague Launch of the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations and a Panel Discussion*, ASSER INST. (Feb. 13, 2017), <https://www.asser.nl/media/3515/report-the-hague-launch-of-the-tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations.pdf> (mentioning that the Tallinn Manual Hague process included some participation from Chinese and Belarusian delegates, but not Russians); Robert G. Papp, *Kennan Cable No. 41: A Cyber Treaty with Russia*, WILSON CTR., <https://www.wilsoncenter.org/publication/kennan-cable-no-41-cyber-treaty-russia> (last visited Sept. 3, 2020) (“Given these myriad challenges, what would a cyber treaty with Russia look like? We would need to start with terms of reference, carefully defined and mutually agreed upon. The ‘Tallinn Manual’ could be a starting point, although the Russian Federation played no part in its drafting and would want its own input.”).

⁵⁶ Papp, *supra* note 55.

⁵⁷ Brian J. Egan, *Remarks on International Law and Stability in Cyberspace*, U.S. DEP’T OF STATE (Nov. 10, 2016), <https://2009-2017.state.gov/s/l/releases/remarks/264303.htm> (conceding that “the Tallinn Manuals will make a valuable contribution to underscoring and demonstrating [that existing international law applies to State behavior in

Much of the ambiguity regarding international cyber norms lies in states' interpretation—at least those which have published opinions on the matter—on how the long held international principles of sovereignty and non-intervention apply to cyber operations.⁵⁸ As noted recently by Gary Corn, “only a handful of states have offered official views on the application of the non-intervention rule in the cyber context, providing little insight into their views of the rule’s internal content.”⁵⁹ Representatives from United States and the United Kingdom have both offered opinions that there is no strict sovereignty rule in regards to cyberspace.⁶⁰ Rather, the issue arises with any violation of the principle of non-intervention.⁶¹ This principle, described in the *Nicaragua Case*, establishes that states are prohibited from coercive intervention in matters that are the exclusive right of another state (e.g., elections, policing, and other government matters).⁶²

However, in 2019 the Netherlands offered the opinion “that respect for the sovereignty of other countries is an obligation in its own right, the violation of which may in turn constitute an internationally wrongful act.”⁶³ At the same time, the French have gone further, suggesting that

cyberspace] across a number of bodies of international law, even if we do not necessarily agree with every aspect of the Manuals.”).

⁵⁸ *Introduction*, TALLINN MANUAL 2.0, *supra* note 54, at 6.

⁵⁹ Gary Corn, *Punching on the Edges of the Grey Zone: Iranian Cyber Threats and State Cyber Responses*, JUST SECURITY (Feb. 11, 2020), <https://www.justsecurity.org/68622/punching-on-the-edges-of-the-grey-zone-iranian-cyber-threats-and-state-cyber-responses/>.

⁶⁰ Egan, *supra* note 57 (stating “remote cyber operations involving computers or other networked devices located on another State’s territory do not constitute a per se violation of international law. In other words, there is no absolute prohibition on such operations,” especially when they have de minimis effects).

⁶¹ *See, e.g., id.*; Jeremy Wright, *Cyber and International Law in the 21st Century*, GOV.UK (May 23, 2018), <https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century>.

⁶² *Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.)*, Judgment, 1986 I.C.J. Rep. 14, ¶ 205 (June 27) (“the principle forbids all States or groups of States to intervene directly or indirectly in internal or external affairs of other States. A prohibited intervention must accordingly be one bearing on matters in which each State is permitted, by the principle of State sovereignty, to decide freely. One of these is the choice of a political, economic, social and cultural system, and the formulation of foreign policy. Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones.”).

⁶³ GOV’T OF THE NETH., APPENDIX: INTERNATIONAL LAW IN CYBERSPACE 2 (2019), <https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace>.

“any unauthorized penetration” of systems in a state’s territory “via a digital vector may constitute, at the least, a breach of sovereignty.”⁶⁴ More recently, the Czech representative to the OEWG concurred with the idea of “the principle of sovereignty as an independent right and the respect to sovereignty as an independent obligation,” but provided a limited list of the types of cyber intrusions which would constitute a violation, disagreeing with the French perspective.⁶⁵ The United States, for its part, has argued for a *de minimis* approach, where a certain threshold of effect must be crossed before the intrusion becomes a wrongful act.⁶⁶

These are just the views of the traditional western powers. Russia offered the International Law of the Sea (i.e. UNCLOS) as an analog for cyber rules, with all the territorial rigidity that entails,⁶⁷ and Cuba has rejected the well-established right to react to malicious cyber operations through sanctions and countermeasures.⁶⁸ As one last bit of evidence showing clearly the lack of substantial cyber norms today, the DOD General Counsel recently remarked that due to the “lack of agreement among states on how such rules apply” it is necessary that “DOD lawyers provide advice guided by how existing rules apply to activities in other domains, while

⁶⁴ MINISTERE DES ARMEES, INTERNATIONAL LAW APPLIED TO OPERATIONS IN CYBERSPACE 6 (2019), <https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf>.

⁶⁵ Richard Kadlčák, *Statement at the 2nd Substantive Session of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security*, CZECH (Feb. 11, 2020), https://www.nukib.cz/download/publications_en/CZ%20Statement%20-%20OEWG%20-%20International%20Law%2011.02.2020.pdf.

⁶⁶ See David Simon et al., *Legal Considerations Raised by the U.S. Cyberspace Solarium Commission Report*, LAWFARE (Jul. 20, 2020, 10:04 AM), <https://www.lawfareblog.com/legal-considerations-raised-us-cyberspace-solarium-commission-report> (elaborating on the *de minimis* approach).

⁶⁷ See Nele Achten, *New U.N. Debate on Cybersecurity in the Context of International Security*, LAWFARE (Sep. 30, 2019, 8:00 AM), <https://www.lawfareblog.com/new-un-debate-cybersecurity-context-international-security> (emphasizing Russia’s reluctance to adopt more flexible laws for cybersecurity).

⁶⁸ See Elaine Korzak, *UN GGE on Cybersecurity: The End of an Era?*, THE DIPLOMAT (Jul. 31, 2017), <https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/> (raising Cuba’s rejection of legal norms as a sign pending change).

considering the unique, and frequently changing, aspects of cyberspace.”⁶⁹ Military lawyers of the United States, who should know the requirements of international law as well as anyone, are still providing analysis through analogy.⁷⁰ It should be a safe prediction that an international consensus on these, many other cyber-related issues, will not be achieved any time soon.

B. Weakness of International Law Responses

Even if customary norms are established regarding below-the-threshold cyber operations, states have limited recourses against violations of international law. If the cyber operation meets the threshold of an “armed attack,” a state is allowed to respond in individual or collective self-defense, per Article 51 of the UN Charter.⁷¹ While the exact conditions when an attack would breach this threshold are still actively debated, there is a general consensus that any cyberattack which generates harm or damage equivalent to a kinetic strike would be an armed attack.⁷² However, the overwhelming majority of cyber operations today do not reach that level.⁷³

States are allowed to take certain measures in response to harm received when other states fail or violate their international obligations. In general, states are obligated to respond to international crimes.⁷⁴ For example, the commentary on the *Draft Articles on Responsibility of States for Internationally Wrongful Acts* [hereinafter “Draft Articles”], adopted by the UN

⁶⁹ Paul C. Ney, Jr., *DOD General Counsel Remarks at U.S. Cyber Command Legal Conference*, DEP’T OF DEF. (Mar. 2, 2020), <https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/>.

⁷⁰ *Id.*

⁷¹ U.N. Charter art. 51 (stating that “[n]othing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations.” Note that this would theoretically allow a state to respond in collective self-defense to an attack on another UN Member State, though that typically involves a request for aid).

⁷² Sean Watts & Theodore Richard, *Baseline Territorial Sovereignty and Cyberspace*, 22 LEWIS & CLARK L. REV. 771, 793-94 (2018).

⁷³ *Id.*

⁷⁴ *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, in Report of the International Law Commission on the work of its fifty-third session, 56 GAOR Supp. No. 11, at 75, U.N. Doc A/56/10 (2001) [hereinafter *Draft Articles*].

General Assembly in 2001, cited the *Tellini Case* of 1923.⁷⁵ This case addressed a dispute between Italy and Greece involving an assassination that occurred on Greek territory.⁷⁶ The Special Commission of Jurists ruled a state may be responsible for “the commission in its territory of a political crime against the persons of foreigners if the state has neglected to take all reasonable measures for the prevention of the crime and the pursuit, arrest and bringing to justice of the criminal.”⁷⁷

In treaty law, there are several examples of agreements which require prosecution of cybercrimes and cyberattacks. One is the *2001 EU Council Convention on Cybercrime* (Budapest Convention), which has, as of this writing, 65 parties including the United States and other non-European states such as Japan.⁷⁸ It is worth noting that Russia, China, Iran, Cuba, and North Korea are not Contracting States.⁷⁹ Through the convention, the signatories have agreed to “ensure that the criminal offences established in accordance with [the Convention] are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.”⁸⁰ These offenses include: the illegal access or interception of data, the interference with computer data or systems, the development of devices and software for hacking, and computer-related fraud or forgery.⁸¹ More importantly, the convention clarifies jurisdiction for a state to include when an offence is committed in its territory, on board one of its flagged ships or registered aircrafts, or by one of its nationals (a form of extraterritorial jurisdiction).⁸²

⁷⁵ *Id.*

⁷⁶ *Id.*

⁷⁷ *Id.*

⁷⁸ *Chart of signatures and ratifications of Treaty 185*, COUNCIL OF EUR., https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=exhG7iJ7 (last visited Aug. 19, 2020) (displaying a lack of signature by Russia, Cuba, Iran, or North Korea).

⁷⁹ *Id.*

⁸⁰ Convention on Cybercrime, art. 13, Nov. 23, 2001, E.T.S. 185 [hereinafter Budapest Convention].

⁸¹ *Id.* arts. 2-8.

⁸² *Id.* art. 22.

Another set of treaties which require states to take action against criminal acts, including presumably cyberattacks, are the Chicago and Montreal Aviation Conventions. The latter, formerly titled the *Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation*, includes as offenses when any person “communicates information which he knows to be false, thereby endangering the safety of an aircraft in flight.”⁸³ One could reasonably argue that sending a virus or other malware to an aircraft computer would constitute communicating false information.⁸⁴ Article 3 of this convention requires member states to make the listed offenses “punishable by severe penalties.”⁸⁵ These and other treaties require states to take action against cybercrimes within their respective territories. This, therefore, implicates states who sanction or condone such operations.

International law allows states to respond to breaches in certain ways. The most significant of these responses are countermeasures.⁸⁶ These actions have long been an enduring aspect of international law, but were implemented in detail in the *Draft Articles*.⁸⁷ These actions are defined in Article 22 of Part I of the *Draft Articles*, which declares “The wrongfulness of an act of a state not in conformity with an international obligation towards another State is precluded if and to the extent that the act constitutes a countermeasure,” against a state which is responsible for an internationally wrongful act.⁸⁸ Countermeasures are further detailed in Part III, Chapter II of the *Draft Articles*.⁸⁹ As noted in the commentaries, countermeasures “may have a coercive character, but as is made clear in Article 49, their function is to induce a wrongdoing

⁸³ Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation, art. 1, Sept. 23, 1971, 974 U.N.T.S. 117 [hereinafter Montreal Convention].

⁸⁴ *Id.*

⁸⁵ *Id.* art 3.

⁸⁶ *Draft Articles*, *supra* note 74, at 75.

⁸⁷ *Id.*

⁸⁸ *Id.*

⁸⁹ *Id.* at 128.

State to comply with obligations of cessation and reparation towards the state taking the countermeasures.”⁹⁰ This definition justifies reparations as an exception to the prohibition on use of countermeasures. “in response to an internationally wrongful act that has ceased and is unlikely to be repeated.”⁹¹ Even if the cyber operation itself has ceased, if the offending state has not taken action to make amends and to be fully compliant with international law (e.g., prosecuting those responsible for the operation per the Budapest Convention), then countermeasures seeking such reparations might be allowed.⁹²

A lighter response to malicious cyber operations would be “retorsions,” which unlike countermeasures, are not internationally wrongful acts themselves.⁹³ These are political acts used to apply pressure on an offending state, such as imposing sanctions or expelling diplomats.⁹⁴ For example, in 2016 President Obama expelled 35 diplomats in response to Russia’s meddling in U.S. elections.⁹⁵ However, many have voiced doubts as to the effectiveness of these actions.⁹⁶

One example showing the ineffectiveness of retorsions, as compared to domestic measures, is the recent news of Sudan offering reparations to the victims of the U.S.S. Cole bombing.⁹⁷ The attack was carried out by Al-Qaida militants, allegedly with support from the government of Sudan.⁹⁸ After almost 20 years, Sudan has agreed to pay \$30 million to the

⁹⁰ *Id.* at 70.

⁹¹ Crootof, *International Cybertorts*, *supra* note 45, at n.51.

⁹² *See Draft Articles*, *supra* note 74, at 70 (“...their function is to induce a wrongdoing State to comply with obligations of cessation and reparation towards the State taking the countermeasures, not to coerce that State to violate obligations to third States.”).

⁹³ Crootof, *International Cybertorts*, *supra* note 45, at 578-79.

⁹⁴ *See generally* Egan, *supra* note 57.

⁹⁵ Lauren Gambino, Sabrina Siddiqui & Shaun Walker, *Obama expels 35 Russian diplomats in retaliation for US election hacking*, THE GUARDIAN (Dec. 30, 2016, 2:47 AM), <https://www.theguardian.com/us-news/2016/dec/29/barack-obama-sanctions-russia-election-hack>.

⁹⁶ *See, e.g.*, Crootof, *International Cybertorts*, *supra* note 45, at 586.

⁹⁷ *See USS Cole Bombing: Sudan Agrees to Compensate Families*, BBC (Feb. 13, 2020), <https://www.bbc.com/news/world-africa-51487712>.

⁹⁸ *See* Bill Chappell, *Sudan Says it is Settling Lawsuit from Families and Victims of USS Cole Attack*, NPR (Feb. 13, 2020), <https://www.npr.org/2020/02/13/805571875/sudan-says-it-is-settling-claims-with-families-and-victims-of-uss-cole-attack>.

victims.⁹⁹ Last year, the Supreme Court reversed and remanded a judgment of \$315 million against Sudan under the terrorism exceptions to the *Foreign Sovereign Immunities Act*.¹⁰⁰ However, the case was reversed on a technicality—a required notice of the lawsuit was sent to the wrong place—rather than on the merits.¹⁰¹ The court left the door open for a new suit, which would have likely garnered the same severe judgment, if not more.¹⁰² Sudan was much better off paying \$30 million now instead of ten times as much a year from now.¹⁰³ If this was a driving factor in the decision, it means domestic civil measures accomplished in years what took two decades with classic retorsions.

C. Domestic Policies of Rival States

Another reason the United States needs to strengthen its domestic legal apparatus against cyberattacks is the ongoing development in the East of so-called “cyber sovereignty” policies.¹⁰⁴ Both China and Russia have begun to assert absolute authority in their domestic cyber spheres. As some have argued, one need only look at

the competing groups at the U.N.—the U.S.-led Group of Governmental Experts and the Russia and China-supported Open-Ended Working Group—to identify the key fault lines between those who argue for cybersecurity in order to undergird the personal and economic freedom of their citizens and those who would use the bugaboo of cyber threats to control their populations and shape their domestic political environments.¹⁰⁵

⁹⁹ See Nima Elbagir, Nada AlTaher & Yassir Abdallah, *Sudan will pay \$30 million to families of USS Cole attack victims, its leaders say*, CNN (Feb. 13, 2020), <https://edition.cnn.com/2020/02/13/africa/sudan-uss-cole-settlement-intl/index.html>.

¹⁰⁰ See Jessica Gresko, *Supreme Court tosses \$315 Million Award in USS Cole Lawsuit*, ASSOCIATED PRESS (Mar. 26, 2019), <https://apnews.com/6cfc87d63964b0297f301b334790b22>.

¹⁰¹ *Id.*

¹⁰² *Id.*

¹⁰³ *Id.*

¹⁰⁴ See Valetin Weber, *The Sinicization of Russia's Cyber Sovereignty Model*, COUNCIL ON FOREIGN REL. (Apr. 1, 2020), <https://www.cfr.org/blog/sinicization-russias-cyber-sovereignty-model>.

¹⁰⁵ See Keith Alexander & Jamil Jaffer, *UN's Cybercrime 'Law' Helps Dictators and Criminals, not their Victims*, THE HILL (Nov. 26, 2019), <https://thehill.com/opinion/cybersecurity/471897-uns-cybercrime-law-helps-dictators-and-criminals-not-their-victims>.

Russia and China are among a group of states—whose membership includes many on the global cyber naughty list (Cuba, Iran, North Korea)—which is promoting a U.N. resolution on cybercrime that is intentionally vague.¹⁰⁶ This alternative is being pushed despite the already wide support for the Budapest Cybercrime Convention.¹⁰⁷ None of the countries noted above are signatories of the Budapest Convention.¹⁰⁸ A draft treaty offered by Russia “would allow countries to solidify their hold over information and communications technology within their borders, enabling some countries to further restrict activities and speech on the internet, while also stressing governments’ sovereignty in cybercrime investigations.”¹⁰⁹

Contrary to the U.S. goal of an open and free internet,¹¹⁰ China and now Russia are attempting to erect walls of cyber sovereignty around their domestic networks.¹¹¹ Last year in comments to the Chinese state-run World Internet Conference, President Xi Jinping wrote that states must govern responsible internet use.¹¹² While the “great firewall” of China has been around for years, Russia has recently been strengthening its control over the domestic internet.¹¹³ On November 1st, 2019, Russia adopted a new law allowing the government to assert more control over the domestic internet.¹¹⁴ In its shorthand, the “sovereign internet law” evokes the same language which has been used by China for years as an excuse to censor web content.

¹⁰⁶ *Id.*

¹⁰⁷ See *Chart of signatures and ratifications of Treaty 185*, *supra* note 78.

¹⁰⁸ See *id.*

¹⁰⁹ See Allison Peters, *Russia and China are Trying to set the U.N.’s Rules on Cybercrime*, FOREIGN POLICY (Sep. 16, 2019), <https://foreignpolicy.com/2019/09/16/russia-and-china-are-trying-to-set-the-u-n-s-rules-on-cybercrime>.

¹¹⁰ See generally Galov, *supra* note 12. See also Egan, *supra* note 57 (“The Internet must remain open to the free flow of information and ideas. Restricting the flow of ideas also inhibits spreading the values of understanding and mutual respect that offer one of the most powerful antidotes to the hateful and violent narratives propagated by terrorist groups”).

¹¹¹ See Weber, *supra* note 104.

¹¹² See Justin Sherman, *How Much Cyber Sovereignty is Too Much Cyber Sovereignty?*, COUNCIL ON FOREIGN REL. (Oct. 30, 2019), <https://www.cfr.org/blog/how-much-cyber-sovereignty-too-much-cyber-sovereignty>.

¹¹³ See Weber, *supra* note 104.

¹¹⁴ See Merit Kennedy, *Russia ‘Sovereign Internet’ Law Gives Kremlin Sweeping Control Over Internet*, NPR (Nov. 1, 2019), <https://www.npr.org/2019/11/01/775366588/russian-law-takes-effect-that-gives-government-sweeping-power-over-internet>.

However, the Russian version of cyber sovereignty takes the concept to the next level, “banning the use of private networks and proxy servers” and instead establishing a Russia-specific domain name system (DNS), which “will in theory drive all internet traffic seeking to connect with Russian websites through government-controlled entry points.”¹¹⁵ This will, in effect, create a content valve between the Russian internet and the rest of the world, allowing the government to disconnect the domestic web at will, to monitor all traffic, and to likely even screen content. It will also make it more difficult to deal with cyber threats emanating from Russian territory.

In a recent speech at U.S. Cyber Command, General Counsel for the Department of Defense Paul Ney laid out the threat posed by near-peer competitors and specifically addressed the three most commonly cited cyber threats.¹¹⁶ First, he noted that the Strategic Support Force, under the People’s Liberation Army or PLA, provides China the cyberwarfare capability to establish information dominance.¹¹⁷ He also suggested Russia “consistently uses cyber capabilities for what it calls ‘information confrontation’ during peacetime and war.”¹¹⁸ Finally, Ney noted that cyber operations have become a cheap “form of gaining real power, especially for impoverished adversaries like North Korea.”¹¹⁹ Even though these rival states are ones the U.S. typically views as military adversaries, Ney argued the DOD’s policies must only be a part of a greater government-wide effort to “promote stability in cyberspace and adherence to the rules-based international order.”¹²⁰ The response cannot be only a military one.

¹¹⁵ See Candace Rondeaux, *Why Russia’s Attempt to Create Its Own Tightly Controlled Internet Could Backfire*, WORLD POL. REV. (Nov. 1, 2019), <https://www.worldpoliticsreview.com/articles/28313/why-russia-s-attempt-to-create-its-own-tightly-controlled-internet-could-backfire>.

¹¹⁶ See Ney, *supra* note 69.

¹¹⁷ *Id.*

¹¹⁸ *Id.*

¹¹⁹ *Id.*

¹²⁰ *Id.*

The United States is one of the largest victims of cybercrime and malicious cyber operations in the world.¹²¹ There is much at stake in the coming years. As Glenn Gerstell argued, we must develop resources and resiliency against cyberattacks, “But our laws and government structures are not where they need to be to facilitate that task and confront this rapidly mutating threat.”¹²² By updating and expanding domestic laws and policies, the United States can influence the international discussion by showing that cyber defense and an open internet are not mutually exclusive. The U.S. must rally like-minded states against the growing movement towards cyber lockdown and the employment of cybercrime as a political tool.

II. EMPLOYING DOMESTIC MEASURES AGAINST STATE-SPONSORED CYBER OPERATIONS

Since an international consensus on cyber law is unlikely in the near future, the United States must strengthen and more fiercely employ its domestic laws and policies in order to provide deterrence against cyberattacks. This effort can be broken into two parts. First, new measures must be adopted to support attribution efforts—identifying the individuals and organizations responsible for specific attacks. Second is employing decentralized government actions, primarily in the courts, to sanction or punish those involved.

A. *Efforts to Support Attribution*

Attribution has been a notoriously difficult problem, in part because it often deals in classified information, but mostly because the organizations currently conducting attribution analysis are government intelligence agencies.¹²³ The government can only do and see so much,

¹²¹ See J. Clement, *U.S. Consumers and Cyber Crime – Statistics and Facts*, STATISTA (Aug. 14, 2019), <https://www.statista.com/topics/2588/us-consumers-and-cyber-crime/>.

¹²² See Gerstell, *supra* note 1.

¹²³ See Lily Hay Newman, *Hacker Lexicon: What is the Attribution Problem?*, WIRED (Dec. 24, 2016), <https://www.wired.com/2016/12/hacker-lexicon-attribution-problem/>.

and the trail of a hacker can quickly fade into the data stream. We can start to address this problem with policies that go wide, empowering private security entities to conduct traces at the moment of attack and employing military assets throughout the web for passive monitoring.

i. Deputizing the Private Sector

Glenn Gerstell argued the government “will increasingly rely on the private sector to achieve national security goals, and the private sector will increasingly bear some responsibilities historically borne solely by the public sector.”¹²⁴ He describes how the delineation of responsibility between the public and private sectors used to be clear, but as technology has changed, private entities have become more capable of both launching devastating cyberattacks and defending against them.¹²⁵ This sentiment is echoed in the Cyberspace Solarium Commission’s report, though in a more restrained manner.¹²⁶ The report includes a pillar to “Operationalize Cybersecurity Collaboration with the Private Sector” and a recommendation that “Congress should direct the executive branch to strengthen a public-private, integrated cyber center in CISA [the Cybersecurity and Infrastructure Security Agency].”¹²⁷ Though the Cyberspace Solarium report acknowledges that “in cyberspace the government is often not the primary actor” and that the government “must support and enable the private sector,” it falls short of providing private entities the authority for active defense.¹²⁸ The report still imagines a government-focused, even military-led effort, with the private sector participating as planners and passive information sources.¹²⁹ The U.S. government should do more to empower private

¹²⁴ See Gerstell, *supra* note 1.

¹²⁵ *Id.*

¹²⁶ See CYBERSPACE SOLARIUM COMMISSION, *supra* note 4, at 96.

¹²⁷ *Id.*

¹²⁸ *Id.*

¹²⁹ *Id.* at 103.

security entities, specifically for the immense task of attribution and tracing. This is often referred to as “hack back” authority.¹³⁰

Recently, scholars such as Jonathan Reiber and Benjamin Bahney have argued “Companies own, operate, and control the infrastructure of cyberspace, and they may be able to sense threats, shut off adversaries’ access to their services, or manipulate their own infrastructure to block an attack.”¹³¹ Efforts are still ongoing to encode this partnership into statute.¹³² Originally proposed in 2017 by Representative Tom Graves, and reintroduced by Graves and Representative Josh Gottheimer in 2019, the yet unpassed *Active Cyber Defense Certainty Act* (ACDC Act) seeks to provide certain exceptions to 18 U.S.C. § 1030 (the Computer Fraud and Abuse Act or CFAA).¹³³ These exceptions would allow private entities to respond to cyberattacks with countermeasures and not be held criminally liable (though still potentially subject to civil liability). Under the *ACDC Act*, private entities may take actions to establish attribution or place beacons, disrupt a continued attack, or monitor malicious cyber behavior.¹³⁴ These permissions do not include causing damage to systems, recklessly causing physical injury or financial loss, causing a threat to public safety, causing disruptions to internet connectivity, or intentionally creating remote access to an intermediary’s computer.¹³⁵ Additionally, under the *ACDC Act*, the private organization must notify the FBI before initiating a response.¹³⁶

¹³⁰ See Chris Kennedy, *What does the Hack Back Bill mean to your Business*, INFO-SECURITY MAG. (Jan. 10, 2020), <https://www.infosecurity-magazine.com/opinions/hack-back-bill-mean/>.

¹³¹ Jonathan Reiber & Benjamin Bahney, *The U.S. Government Can Deepen Its Operational Partnership with the Private Sector to Better Defend the U.S. in Cyberspace*, LAWFARE (Mar. 13, 2020), <https://www.lawfareblog.com/us-government-can-deepen-its-operational-partnership-private-sector-better-defend-us-cyberspace>.

¹³² See Robert Chesney, *Hackback Is Back: Assessing the Active Cyber Defense Certainty Act*, LAWFARE (June 14, 2019), <https://www.lawfareblog.com/hackback-back-assessing-active-cyber-defense-certainty-act>.

¹³³ See Active Cyber Defense Certainty Act (ACDC Act), H.R.3270, 116th Cong. § 3(k) (2019).

¹³⁴ *Id.* § 4(l)(3)(B)(i)(II)(bb).

¹³⁵ *Id.* § 4(l)(3)(B)(ii).

¹³⁶ See also Chesney, *supra* note 132.

Perhaps most significant of the allowed countermeasures is beaconing. As noted by Glenn Gerstell, “The ability to obfuscate one's tracks in the cyber domain presents obvious challenges to our national security. Anonymity is the gateway drug to cyber maliciousness.”¹³⁷ The ACDC Act allows private cyber security forces to hack back into an attacker’s system in order to place a beacon, which can later be traced by law enforcement.¹³⁸ Allowing private entities to react in real time to cyberattacks, to trace and identify the sources, would help to solve the enduring problem of attribution. As noted in the Cyber Solarium Commission’s report, “The U.S. Government is currently not designed to act with speed and agility necessary to defend the country in cyberspace.”¹³⁹ It is questionable that the government will ever be agile or fast enough to respond to the majority of cyberattacks. Nor would the federal government be inclined to spend the massive amounts of money such efforts would require, just to protect random small businesses.

As of 2019, 43% cyberattacks targeted small businesses, but only 14% of such businesses reported being prepared to defend themselves. These attacks cost businesses an average of \$200,000.¹⁴⁰ Providing private entities the limited authority to hack back for beaconing and attribution analysis will no doubt help relieve some of these pressures. It may also provide market opportunities for larger security companies such as Symantec or Norton to provide active defense services to businesses which do not have their own cyber defense teams. As currently written, the *ACDC Act* requires coordination with the FBI.¹⁴¹ It could be rewritten to reflect the recommendation by the Cyberspace Solarium to establish a CISA cyber center. This could be an

¹³⁷ See Gerstell, *supra* note 1.

¹³⁸ See ACDC Act, H.R.3270 § 3(k)(1).

¹³⁹ See CYBERSPACE SOLARIUM COMMISSION, *supra* note 4, at 2.

¹⁴⁰ Scott Steinberg, *Cyberattacks now cost companies \$200,000 on average, putting many out of business*, CNBC (Oct. 13, 2019), <https://www.cnbc.com/2019/10/13/cyberattacks-cost-small-companies-200k-putting-many-out-of-business.html>.

¹⁴¹ See ACDC Act, H.R.3270 § 6(a).

interagency operations floor where cyberattacks, big or small, from around the country, are tracked. In the cyber ops center, the legislatively empowered private security entities do the legwork and front the fiscal burden, but are coordinated by government agencies such as the FBI and CISA. The operations floor could also seat one or more attorneys to provide real-time legal advice on international law issues and domestic criminal law procedures. Interagency JOCs (joint operations centers) have proven very successful in responding to terrorism or humanitarian crises, why not to the cyber crisis?

Some have cautioned against allowing private entities to engage in the sort of countermeasures usually reserved for states. Chris Cook has specifically argued against the *ACDC Act*, suggesting that other countries may interpret the actions as U.S.-sanctioned and that such actions could harm U.S. credibility because “[f]or years, the U.S. has pushed the idea that unauthorized hacking is illegal, and should not be done.”¹⁴² However, Cook’s analysis is flawed. Cook has argued that review by the FBI was only voluntary under the framework of the original bill.¹⁴³ However, both the original 2017 and updated 2019 version of the *ACDC Act* require the private entity to notify the FBI and to wait for “a response from the FBI acknowledging receipt of the notification prior to using the measure.”¹⁴⁴ This notification requirement, and the information the defenders are required to provide, is for FBI oversight.¹⁴⁵ This implies direct

¹⁴² Chris Cook, *Cross-Border Data Access and Active Cyber Defense: Assessing Legislative Options for a New International Cybersecurity Rulebook*, 29 STAN. L. & POL’Y REV. 205, 219, 221 (2017) (omitting analysis on Sec. 5 which shows the intent of mandatory notification is for FBI oversight that implies authority to intervene, by stating “All that is required under the current proposal [2017] is that users of ACD measures must notify FBI of their intent to use such techniques. The pre-emptive review itself and actually getting the FBI’s permission to take specified action is voluntary”).

¹⁴³ Active Cyber Defense Certainty Act, H.R. 4036, 115th Cong. § 6 (2017).

¹⁴⁴ ACDC Act, H.R.3270 § 5.

¹⁴⁵ *Id.* (There is a contradiction in the text of the bill. Sec. 6 states that “A defender who intends to prepare an active defense measure under section 4 *may* submit their notification to the FBI National Cyber Investigative Joint Task Force in advance of its use so that the FBI and other agencies can review the notification.” However, Sec. 5 states the defender *must* “receive a response from the FBI acknowledging receipt of the notification *prior* to using the measure.” Based on this, and the intent for FBI oversight stated in Sec. 5, prior notification is required and allows

coordination, if not concurrence by the FBI prior to any private entity launching countermeasures.¹⁴⁶ If the FBI saw an issue with the planned measure, they could intervene.¹⁴⁷ Moreover, the recommendation here is a much more robust government role in private “hack back.”¹⁴⁸ The CISA ops center would be government-led, and any responses would be authorized state actions, though executed by private entities. This would eliminate this ambiguity Cook criticizes. Though the action would be taken by a private individual, it would be a state-sanctioned countermeasure.

Additionally, Cook suggests that there is a lack of international consensus on the issue, and that imputed state responsibility could open the U.S. up for retaliation.¹⁴⁹ This is incorrect. First and foremost, retaliation is illegal under international law.¹⁵⁰ However, retorsions and countermeasures by states have been accepted under international law for some time, though significantly limited in scope.¹⁵¹ With coordination and concurrence by the FBI or CISA, these active defense measures would be state-sanctioned countermeasures, legal and legitimate under the circumstances. Moreover, it is unreasonable to argue that the attacking state, when facing such legitimate countermeasures, would be allowed to respond with countermeasures of their own. That would create an endless cycle of authorized counterattacks. No, a state that is conducting or sanctioning a blatantly illegal cyberattack has no entitlement to respond to legal

the FBI, in their acknowledgement to the notification, plenty of opportunity to order the defender to cease and desist.)

¹⁴⁶ *Id.*

¹⁴⁷ *Id.*

¹⁴⁸ See Kennedy, *supra* note 130.

¹⁴⁹ *Id.* at 215-216.

¹⁵⁰ See *Reprisal*, JRANK, <https://law.jrank.org/pages/9791/Reprisal.html> (last visited Aug. 18, 2020) (“There is a fine distinction between a ‘lawful reprisal,’ and an act of revenge or retaliation, which are always illegal under international law.”).

¹⁵¹ Catherine Lotrionte, *Reconsidering the Consequences for State-Sponsored Hostile Cyber Operations Under International Law*, CYBER DEF. REV. 73, 91 (Sept. 5, 2018), <https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1620229/reconsidering-the-consequences-for-state-sponsored-hostile-cyber-operations-und/>.

countermeasures.¹⁵² Regardless, the point of measures like the *ACDC Act* is not to create a cyber wild west, but rather to deputize the private sector in a coordinated, whole-of-government fight against cybercrime. To be certain, the bill should be rewritten, both to limit the scope of authority to only beaconing and attribution tracing, but also to require government coordination, if not concurrence, on any actions taken.

The federal government simply does not have the resources or bandwidth to respond to every cyberattack, so coordination with, and employment of, private security apparatuses is a reasonable solution to a growing problem. The bottom line is that if we never get past the attribution wall, no action can be taken against the offenders.

ii. Defend Forward as a Cyber Monitoring Tool

Currently, the “Defend Forward” concept, first coined by the Department of Defense in 2018, focuses on offensive military action in cyberspace.¹⁵³ As described by Paul Ney, “the strategy envisions that our military cyber forces will be conducting operations in cyberspace to disrupt and defeat malicious cyber activity that is harmful to U.S. national interests.”¹⁵⁴ This follows the general top-down, government and military-led approach to cyber policy embodied by the Cyberspace Solarium Commission’s report. Indeed, the report even includes a pillar dedicated to employing “the military instrument of power.”¹⁵⁵ What seems to be lost in the din of saber rattling are the ways “defend forward” can be used in a more passive manner. Military cyber capabilities can be used to create a passive monitoring infrastructure in cyberspace—cyber passive sonar, so to speak, rather than active targeting and collection.

¹⁵² *Id.*

¹⁵³ See C. Todd Lopez, *DOD More Assertive, Proactive in Cyber Domain*, DEP’T OF DEF. (Jun. 28, 2019), <https://www.defense.gov/Explore/News/Article/Article/1891495/dod-more-assertive-proactive-in-cyber-domain/>.

¹⁵⁴ Ney, *supra* note 69.

¹⁵⁵ See CYBERSPACE SOLARIUM COMMISSION, *supra* note 4, at 7.

This idea is already incorporated into the DOD strategy as “positioning” activities.¹⁵⁶ Similar to reactive beaconing, positioning seems to involve Cyber Command proactively placing monitoring functions on the internet abroad, so that they can detect immediately when an attack is incoming.¹⁵⁷ As noted above, the United States’ legal position—as well as that of the U.K., the Czech Republic, and others—is that passive cyber intrusions with little to no manifest effect would not constitute a violation of sovereignty.¹⁵⁸ This passive web would enable rapid attribution, enabling follow on civil responses, rather than military actions that might provoke retaliatory responses. This intelligence could also be used to prosecute non-state actors caught in the dragnet, whereas international law only allows active countermeasures to be used against another state which has violated an international obligation. There are certain to be some issues revolving around classified information and political prerogative, but having passive cyber monitoring in place puts our courts in a better position than they would be otherwise.

iii. Legal Support Agreements

As some scholars have noted, “the main challenge for effective investigation, prosecution, and eventually extradition of proxies, is gathering sufficient evidence.”¹⁵⁹ As previously mentioned, the Budapest Convention requires states to investigate and prosecute cybercrimes, as well as provide mutual assistance to other states.¹⁶⁰ To this end, the U.S. has been moving to bolster legal support regimes.

¹⁵⁶ *Id.*

¹⁵⁷ *Id.*

¹⁵⁸ See Kosseff, *supra* note 26 (providing a nuanced analysis on passive cyberattacks).

¹⁵⁹ See Ponta, *supra* note 3.

¹⁶⁰ See *Explanatory Report to the Convention on Cybercrime*, COUNCIL OF EUROPE (Nov. 23, 2001), <https://rm.coe.int/16800cce5b>.

One example is the *Clarifying Lawful Overseas Use of Data Act* (CLOUD Act), enacted in 2018.¹⁶¹ This law provides two benefits to U.S. law enforcement in cyber cases. First, it amends a portion of the *Stored Communications Act* (18 U.S.C. § 2713) so that internet providers, when presented with a lawful warrant, must turn over data on U.S. users, even if that data is being stored abroad.¹⁶² Secondly, the Act “amends multiple parts of the *Electronic Communications Privacy Act* (ECPA) . . . to allow providers to permit disclosures to certain foreign governments—but only those that have struck executive agreements with the U.S.”¹⁶³ This will enable the cross-sharing of information and allow U.S. investigators to pursue foreign agents in allied territory.

This sort of bilateral or international coordination and support has been critical to bringing hackers to justice in the past. One glowing example was the conviction in 2016 of Vladimir Tsastin, an Estonian who infected more than four million computers with malware.¹⁶⁴ Tsastin was extradited by Estonia to the United States, tried in the Southern District of New York, and ultimately sentenced to eighty-seven months confinement.¹⁶⁵ Without coordination and mutual support between the United States, Estonia, and other countries, this case would have never reached a successful conclusion.

First and foremost, the required assistance agreements must be established with as many like-minded nations as possible. The Cyberspace Solarium Commission recommends

¹⁶¹ Clarifying Lawful Overseas Use of Data Act (CLOUD Act), H.R. 4943, 115th Cong. (2018).

¹⁶² See Andrew Woods & Peter Swire, *The CLOUD Act: A Welcome Legislative Fix for Cross-Border Data Problems*, LAWFARE (Feb. 6, 2018), <https://www.lawfareblog.com/cloud-act-welcome-legislative-fix-cross-border-data-problems>.

¹⁶³ *Id.*

¹⁶⁴ See *Estonian Cybercriminal Sentenced for Infecting 4 Million Computers in 100 Countries with Malware in Multimillion-Dollar Fraud Scheme*, DEP’T OF JUST. (Apr. 26, 2016), <https://www.justice.gov/usao-sdny/pr/estonian-cybercriminal-sentenced-infecting-4-million-computers-100-countries-malware> [hereinafter *Estonian Cybercriminal Sentenced*].

¹⁶⁵ *Id.*

streamlining legal assistance treaties and also increasing the number of FBI cyber attachés abroad.¹⁶⁶ Partnerships with allied states have proven effective;¹⁶⁷ however, it is highly unlikely that the agreements required by the *CLOUD Act* will be made with more adversarial states. Even so, as long as the internet remains open, the U.S. will have potential access to data flowing through the territory of friendly nations, which only increases the ability to head off “cyber sovereignty” policies and to prosecute foreign cyber criminals.¹⁶⁸ More can certainly be done to support this effort.

B. Prosecuting Cyber Criminals

Once positive attribution is attained, and evidence is collected, the government should take action. This can be accomplished through several mechanisms. First is with extraterritorial application of domestic criminal law. As Egan pointed out in 2016, “Disrespecting another state’s domestic laws can have serious legal and foreign policy consequences. As a legal matter, such an action could result in the criminal prosecution and punishment of a state’s agents in the United States or abroad.”¹⁶⁹ Individuals, whether they are state agents or not, can be held criminally liable as long as the right jurisdictional rules are in place.¹⁷⁰ Second, law governing international lawsuits, such as the *Foreign Sovereign Immunities Act*, can be changed to allow states to be held financially liable for cyberattacks.¹⁷¹ Such action can only be taken against state

¹⁶⁶ See *FBI Deputy Director David Bowdich’s Statement on Cyberspace Solarium Commission Report*, FBI NAT’L PRESS OFF. (Mar. 11, 2020), <https://www.fbi.gov/news/pressrel/press-releases/fbi-deputy-director-david-bowdichs-statement-on-cyberspace-solarium-commission-report>.

¹⁶⁷ See *Estonian Cybercriminal Sentenced*, *supra* note 164.

¹⁶⁸ See Woods & Swire, *supra* note 162.

¹⁶⁹ See Egan, *supra* note 57.

¹⁷⁰ *Id.*

¹⁷¹ See generally Foreign Sovereign Immunities Act of 1976, Pub. L. 94-583, 90 Stat. 2891 (1976) [hereinafter the FSIA].

actors, though other measures such as private sanctions and the freezing of assets can be used against non-state criminals.

i. Employing Domestic Criminal Law

The question of applying domestic law to cyberattacks perpetrated by foreign actors is simplified when those actors are within the territory of the victim state. Much of the right of states to enforce their domestic law against foreign residents and immigrants stems from general principles of sovereignty.¹⁷² In the case of cyberspace, despite the inanimate nature of data, information is still required to flow through physical infrastructure that is located within sovereign territory.¹⁷³ Even though the developers of the internet may have envisioned a free and borderless digital world, that has not proven the case.¹⁷⁴ Indeed, “the internet has been to some extent Balkanized by security controls erected and maintained by states.”¹⁷⁵ Prosecutors are able to enforce domestic law not only against the agents operating within their borders, but also on any data passing through.¹⁷⁶

However, U.S. prosecutorial efforts have been hindered when the attack comes from abroad. As Glenn Gerstell noted, responding to the cyber epidemic will require updating U.S. domestic law.¹⁷⁷ His statements were in line with the National Cyber Strategy published in 2018, which stated that the current presidential administration intends to “work with the Congress to update electronic surveillance and computer crime statutes to enhance law enforcement’s

¹⁷² See *Enforcement of Judgments*, BUREAU OF CONSULAR AFF., <https://travel.state.gov/content/travel/en/legal/travel-legal-considerations/international-judicial-assistance/Enforcement-of-Judgments.html> (last visited Aug. 19, 2020).

¹⁷³ See Egan, *supra* note 57.

¹⁷⁴ See Jack Goldsmith & Timothy Wu, *Digital Borders: National Boundaries Have Survived in the Virtual World—And Allowed National Laws to Exert Control Over the Internet*, LEGAL AFF. (Jan.-Feb. 2006), https://www.legalaffairs.org/issues/January-February-2006/feature_goldsmith_janfeb06.msp.

¹⁷⁵ See Watts & Richard, *supra* note 72, at 779.

¹⁷⁶ See Egan, *supra* note 57.

¹⁷⁷ See Gerstell, *supra* note 1.

capabilities to . . . impose appropriate consequences upon malicious cyber actors.”¹⁷⁸ The administration is right to believe that computer crime statutes can be an effective defense against malicious cyber operations.¹⁷⁹ Applying them, however, can be difficult.

The fundamental barrier to employing domestic law is jurisdiction. Though required by international law to take action against certain types of cybercrime, and clearly interested in responding to the malicious actions of rival states such as China and Russia, the United States is hindered by the complexity of international jurisdiction.¹⁸⁰ The *Lotus Case* defined rules of jurisdiction in a couple important ways.¹⁸¹ First, within its own territory a state may exercise jurisdiction as it sees fit, providing such action does not violate international law or obligations.¹⁸² Second, and more importantly, states may exercise jurisdiction abroad over an offense when the effects of that offense occur in the territory of the state.¹⁸³ The International Court of Justice ruling states, “It does not, however, follow that international law prohibits a state from exercising jurisdiction in its own territory, in respect of any case which relates to acts which have taken place abroad, and in which it cannot rely on some permissive rule of international law.”¹⁸⁴ Of course, as with domestic jurisdiction, this would not include anything expressly prohibited by international law. Many types of cyber operations, such as hacking and spying, are analogous to espionage. Despite being a state action that is largely sanctioned, or

¹⁷⁸ THE WHITE HOUSE, NATIONAL CYBER STRATEGY 11 (2018), <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>. See also THE WHITE HOUSE, INTERIM NATIONAL SECURITY STRATEGIC GUIDANCE 18 (2021) (reiterating the ideas in the 2018 cyber strategy, stating “We will work together to manage and share risk, and we will encourage collaboration between the private sector and the government at all levels . . . We will renew our commitment to international engagement on cyber issues . . . And we will hold actors accountable for destructive, disruptive, or otherwise destabilizing malicious cyber activity, and respond swiftly and proportionately to cyberattacks by imposing substantial costs through cyber and noncyber means”).

¹⁷⁹ See *id.*

¹⁸⁰ See *The Case of the S.S. Lotus (Fr. v. Turkey)*, Judgment, 1927 I.C.J. 9, 19 (Sept. 7).

¹⁸¹ *Id.*

¹⁸² *Id.*

¹⁸³ *Id.*

¹⁸⁴ *Id.*

perhaps ignored, by international law, espionage is rigidly enforced by most states' domestic law.¹⁸⁵

The U.S. courts have long supported a presumption against the extraterritoriality of U.S. statutes.¹⁸⁶ In *United States v. Bowman*, a 1922 case which dealt with a conspiracy to defraud a corporation in which the United States was a stockholder, the Supreme Court reinforced the premise where the lack of a clear statement by Congress that a statute applies extraterritorially “will negative the purpose of Congress in this regard,” or demonstrate Congress’s intent that it should not apply.¹⁸⁷ However, *Bowman* provided an exception for statutes “enacted because of the right of the Government to defend itself against obstruction, or fraud wherever perpetrated,” noting that a strict domestic jurisdiction “would be greatly to curtail the scope and usefulness of the statute and leave open a large immunity for frauds as easily committed by citizens on the high seas and in foreign countries as at home.”¹⁸⁸

In 2010, the Supreme Court finally returned to the issue in *Morrison v. National Australia Bank*, which examined the extraterritorial effect of U.S. securities legislation, and the court held that “when a statute gives no clear indication of an extraterritorial application, it has none.”¹⁸⁹ The Court established that statutes apply to conduct abroad when: (1) Congressional intent is clear in the statute that it applies extraterritorially, or (2) there is a clear and significant

¹⁸⁵ See Corn & Taylor, *supra* note 35, at 209 (“it is widely recognized that states have unquestioned authority to prohibit espionage within their territory under their domestic laws, but it is also widely recognized that international law does not prohibit espionage.”).

¹⁸⁶ See, e.g., Zachary D. Clopton, *Bowman Lives: The Extraterritorial Application of U.S. Criminal Law after Morrison v. National Australia Bank*, 67 N.Y.U. ANN. SURV. OF AM. L. 137, 138 (2011) (discussing how this treatment limits application of civil statutes).

¹⁸⁷ *United States v. Bowman*, 260 U.S. 94, 98 (1922).

¹⁸⁸ *Id.*

¹⁸⁹ *Morrison v. National Australia Bank*, 561 U.S. 247, 255 (2010).

domestic “focus” so as to apply the statute domestically.¹⁹⁰ *Morrison* did not state whether the rule applied to criminal law, but the Second Circuit Court of Appeals addressed the matter in *United States v. Vilar*, holding that “the presumption against extraterritoriality applies to criminal statutes.”¹⁹¹ Though coming from a circuit court, this opinion has dominated thenceforth.

Bowman and *Morrison* together establish three ways to approach a case of cybercrime perpetrated by a foreign person abroad. First, if the crime is directed at the United States government, then the exception to *Bowman*, allowing the government to defend itself, may apply.¹⁹² Second, if a criminal conduct is clearly domestic-focused, one can apply relevant domestic statute under *Morrison*.¹⁹³ Third, if Congress makes clear in the text of statute that the statute applies extraterritorially, then the conduct at issue can be prosecuted accordingly.¹⁹⁴

Prosecutors may argue extraterritoriality by showing “clear evidence of congressional intent to apply a statute beyond our borders.”¹⁹⁵ Congress added such clear intent to several fraud statutes when it passed the *USA PATRIOT Act* in 2001, amending the definition of “protected computer” in 18 U.S.C. § 1030 (the Computer Fraud and Abuse Act or CFAA) to make clear that this term includes computers outside of the United States so long as the illegal action affects

¹⁹⁰ *Id.* (“It is a ‘longstanding principle of American law ‘that legislation of Congress, unless a contrary intent appears, is meant to apply only within the territorial jurisdiction of the United States.’” (quoting *EEOC v. Arabian Am. Oil Co.*, 499 U.S. 244, 248 (1991))).

¹⁹¹ *United States v. Vilar*, 729 F.3d 62, 72 (2d Cir. 2013).

¹⁹² *Bowman*, 260 U.S. at 98–99, 102 (“But the same rule of interpretation should not be applied to criminal statutes which are, as a class, not logically dependent on their locality for the Government’s jurisdiction, but are enacted because of the right of the Government to defend itself against obstruction, or fraud· wherever perpetrated, especially if committed by its own citizens, officers or agents.”).

¹⁹³ *See Morrison*, 561 U.S. at 266 (“Applying the same mode of analysis here, we think that the focus of the Exchange Act is not upon the place where the deception originated, but upon purchases and sales of securities in the United States.”).

¹⁹⁴ *Id.* at 255 (quoting *Arabian Am. Oil Co.*, 499 U.S. at 248) (“‘[U]nless there is the affirmative intention of the Congress clearly expressed’ to give a statute extraterritorial effect, ‘we must presume it is primarily concerned with domestic conditions.’”).

¹⁹⁵ DEP’T OF JUST., PROSECUTING COMPUTER CRIMES 115 [hereinafter COMPUTER CRIMES MANUAL] (quoting *United States v. Gatlin*, 216 F.3d 207, 211 (2d Cir. 2000)) <https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf>.

“interstate or foreign commerce or communication of the United States,”¹⁹⁶ and revising sections of 18 U.S.C. § 1029 (governing access device fraud) by applying it to persons “outside the jurisdiction of the United States.”¹⁹⁷ Congress has yet to give the same treatment to several other commonly charged statutes, such as 18 U.S.C. § 1343 (wire fraud).¹⁹⁸

Nevertheless, federal prosecutors continue to charge foreign hackers with wire fraud. Most recently, the Justice Department charged four members of the Chinese People’s Liberation Army (PLA) for several computer and conspiracy offences, including wire fraud, in relation to the hacking of credit agency Equifax and the theft of personal data and trade secrets in 2017.¹⁹⁹ To be clear, the hackers were not in the United States at the time of the crime, having accessed the Equifax network via a Swiss server.²⁰⁰ Government prosecutors have accepted that wire fraud cannot currently be charged extraterritorially.²⁰¹ Rather, they have been arguing for several years that the mere use of U.S. wires to commit a fraud scheme is sufficient to charge wire fraud *as a domestic offense*.²⁰² This has required some dexterous legal arguments.

¹⁹⁶ 18 U.S.C. § 1030(e)(2)(b) (2012); Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub. L. No. 107-56, § 814(d)(1), 115 Stat. 272, 384 (2001).

¹⁹⁷ 18 U.S. Code § 1029(h) (2015) (“Any person who, outside the jurisdiction of the United States, engages in any act that, if committed within the jurisdiction of the United States, would constitute an offense under subsection (a) or (b) of this section, shall be subject to the fines, penalties, imprisonment, and forfeiture provided in this title if the offense involves an access device issued, owned, managed, or controlled by a financial institution, account issuer, credit card system member, or other entity organized under the laws of the United States, or any State, the District of Columbia, or other territory of the United States.”)

¹⁹⁸ 18 U.S. Code § 1343 (2008).

¹⁹⁹ See Office of Public Affairs, *Chinese Military Personnel Charged with Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Credit Reporting Agency Equifax*, DEP’T OF JUST. (Feb. 10, 2020), <https://www.justice.gov/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking>.

²⁰⁰ See Criminal Indictment at 9, *United States v. Zhiyong*, No. 2:20-cr-00046 (N.D. Ga. Jan. 28, 2020).

²⁰¹ Precedent on the extraterritorial application of wire fraud is still weak, but the firmest case currently is *United States v. Sidorenko*, 102 F. Supp. 3d 1124, 1127 (N.D. Cal. 2015) (rejecting any extraterritorial application of § 1343 and now seems to have most influenced the present conversation).

²⁰² See, e.g., Brief for the United States as Appellee at 8, *United States v. Hussain*, No. 19-10168 (9th Cir. Nov. 15, 2019) [hereinafter *Hussian Appellate Brief*] (arguing for domestic application of the wire fraud statute in a case involving alleged crimes conducted by a British citizen in Britain).

In cases such as *United States v. Hussain*, the government has argued that Section 1343's focus is solely the "misuse of the wires."²⁰³ This case involved a British national, based in Britain, who used electronic means such as email, press releases, and phone calls to falsely inflate the finances of a company which was eventually bought out by Hewlett-Packard.²⁰⁴ Though the district court ultimately ruled in favor of the government—due mostly to the precedent of the controlling appeals circuit—the opinion revealed what shaky ground such an argument rests on.²⁰⁵ In his opinion, District Judge Charles Breyer acknowledged "there is little precedent regarding how to assess whether § 1343 is properly applied domestically in a particular instance" and that views "generally break into two camps: those emphasizing the wires and those looking to the fraud."²⁰⁶ Moreover, the opinion accepts that Hussain's argument which asserts that the wire fraud statute "concerns itself with the execution of the fraudulent scheme as a whole," has merit, but ultimately holds that "[u]nfortunately for him, however, the test is out of step with Ninth Circuit case law concerning how the government may charge a Section 1343 violation."²⁰⁷ It is not surprising, therefore, that Hussain appealed. The case is currently at the Ninth Circuit, who seem to be free to overturn their previous support of the "focus is the wires" argument.²⁰⁸

The focus on the use of wires is based on an enduring idea that the wire fraud statute was meant to emulate the mail fraud statute, which itself focuses on "use of the mails itself, not on

²⁰³ *Id.*

²⁰⁴ See *Former Autonomy CFO Sentenced To 60 Months in Prison*, DEP'T OF JUST. (May 13, 2019), <https://www.justice.gov/usao-ndca/pr/former-autonomy-cfo-sentenced-60-months-prison>.

²⁰⁵ See *United States v. Hussain*, No. 16-cr-00462-CRB-1, 2017 WL 4865562, at *5 (N.D. Cal. Oct. 27, 2017) (citing *United States v. Garlick*, 240 F.3d 789, 793 (9th Cir. 2001)).

²⁰⁶ *Id.* at *3 (quoting *United States v. Gasperini*, No. 16-CR-441 (NGG), 2017 WL 2399693, at *7 (E.D.N.Y. June 1, 2017)).

²⁰⁷ *Id.* at *5.

²⁰⁸ See Brief for the United States as Appellee, *supra* note 202, at 1.

the underlying scheme or a particular fraud victim.”²⁰⁹ Of course, when the wire fraud statute was first enacted in 1952, Congress was incapable of conceiving where digital technology would end up six decades thence.²¹⁰ Even telephone and television were underdeveloped technologies at the time.²¹¹ In 1952, a person passing a communication via U.S. wires was very likely either in the United States himself or connecting directly to someone in the country.²¹² The analogy to mail is no longer sustainable in the high-speed internet age. Those two means of communication have become wildly dissimilar. While it is highly unlikely that a physical package shipped from Russia to Brazil would pass through the United States today (it would probably be air mailed directly to the destination), an internet communication between the same countries is likely to bounce through the networks of several unrelated states before reaching its destination.²¹³ Should each of those states be allowed domestic jurisdiction over an offence, which does not affect their citizens or interests, simply because the transmission passed through their networks?

Judge Breyer highlighted this conundrum best when he acknowledged:

The government’s proposed rule that § 1343 is properly applied domestically whenever a wire is transmitted within the United States is in some tension with *Morrison*’s insistence on the presumption against extraterritoriality, because it would tend to allow the government to prosecute conduct with minimal domestic connections. One can imagine, for instance, a global click-fraud scheme similar to the one in *Gasperini* in which a defendant combines servers worldwide into a “botnet” from which to launch an attack on an extraterritorial entity. So long as one of the servers is in the United States, application of § 1343 would be

²⁰⁹ *Hussain*, 2017 WL 4865562, at *5 (quoting *Garlick*, 240 F.3d at 792).

²¹⁰ See generally *Wire Fraud*, JUSTIA, <https://www.justia.com/criminal/offenses/white-collar-crimes/wire-fraud/> (last visited Aug. 20, 2020) (“In 1952, Congress enacted the wire fraud statute in order to extend the prohibitions on mail fraud to *newer* communications technologies.”) (emphasis added).

²¹¹ See generally Andrew Anthony, *A History of Television, the Technology that Seduced the World – and Me*, THE GUARDIAN (Sept. 7, 2013), <https://www.theguardian.com/tv-and-radio/2013/sep/07/history-television-seduced-the-world>.

²¹² See generally *Telephone Transmission*, ENGINEERING AND TECH. HIST. WIKI, https://ethw.org/Telephone_Transmission (last visited Aug. 20, 2020) (detailing the innovations of phone systems and stating that in the 1950s, over half of telephones were in the U.S.).

²¹³ See Adam Satariano, *How the Internet Travels Across Oceans*, N.Y. TIMES (Mar. 10, 2019), <https://www.nytimes.com/interactive/2019/03/10/technology/internet-cables-oceans.html> (describing the process of international online communication).

proper. . . . but this result is dubious as a matter of statutory interpretation. The drafters of § 1343 did not envision the statute applying to internationals bouncing wires into and out of the United States, with no participation from any U.S. resident, in order to defraud international entities. The government’s bright-line rule thus appears to be problematically broad in application.²¹⁴

In *Hussain*, even the government clearly accepts that its own interpretation is not solid.²¹⁵ When it introduces this argument in the appellate brief, it also notes, “even if [the statute’s] focus were the scheme to defraud [as opposed to the use of U.S. wires], here the evidence easily sufficed for a rational juror to find domestic wire fraud and conspiracy.”²¹⁶ Some scholars have agreed that the statute requires both the scheme to defraud and the use of wires to have a domestic focus in order to charge as a domestic offense.²¹⁷

One might ask, why would the government charge wire fraud if extraterritorial prosecution under the CFAA is already supported by precedent? The DOJ’s *Computer Crimes Manual* suggests “[p]rosecutors may also want to consider charges under the wire fraud statute” because it carries “stiffer penalties” (up to 20 years confinement for wire fraud, versus 10 years for single charge under 18 U.S.C. § 1030).²¹⁸ Additionally, it may be easier to prove wire fraud than computer crimes if the government’s argument in *Hussain* is successful. One would just need to establish “a scheme to defraud another out of money”²¹⁹ which at least partially passed through U.S. wires, unlike Section 1030, which requires proving unauthorized access to a protected computer.²²⁰

²¹⁴ *Hussain*, 2017 WL 4865562, at *4.

²¹⁵ *Hussain* Appellate Brief, *supra* note 202, at 8.

²¹⁶ *Id.*

²¹⁷ See Julie Rose O’Sullivan, *The Extraterritorial Application of Federal Criminal Statutes: Analytical Roadmap, Normative Conclusions, and a Plea to Congress for Direction*, 106 GEO. L.J. 1021, 1074 (2018) (describing the “best reading” of a wire fraud cause as involving domestic elements).

²¹⁸ COMPUTER CRIMES MANUAL, *supra* note 195, at 26.

²¹⁹ *Criminal Resource Manual* § 941, DEP’T OF JUST. (Jan. 21, 2020), <https://www.justice.gov/archives/jm/criminal-resource-manual-941-18-usc-1343-elements-wire-fraud>.

²²⁰ See 18 U.S.C. § 1030 (2012).

Since the Department of Justice seems to be strongly in favor of charging wire fraud whenever possible, and in light of the ambiguity as to when it can be charged as a domestic offense, it would behoove Congress to update the statute. Limited extraterritoriality can be built in to Section 1343, triggering when an electronic fraud perpetrated abroad nonetheless causes harm to U.S. citizens or interests.²²¹ This would be little different from the extraterritorial application of Section 1030, and would put the current uncertainty faced by the courts to rest for good.

Demonstrating the effectiveness of extraterritorial criminal statutes, the 2001 case of *United States v. Ivanov* was the first to apply the new extraterritorial definitions in § 1029 and § 1030 added by the *USA PATRIOT Act*.²²² This case involved a hacker who broke into the computers of the Online Information Bureau, “then threatened OIB with the destruction of its computer systems (including its merchant account database) and demanded approximately \$10,000 for his assistance in making those systems secure.”²²³ Most notably, Ivanov’s motion to dismiss based on the fact “he was physically located in Russia when the offenses were committed” was denied.²²⁴ Ultimately, he pled guilty and was sentenced to forty-eight months of confinement and three years of supervised release.²²⁵

Moving forward, new laws written to deal with the cyber threat should contain an extraterritorial clause or current laws should be amended to eliminate any ambiguity. There are several criminal statutes that might benefit from the same revisional treatment given to 18 U.S.C.

²²¹ See generally 18 U.S. Code § 1343 (2008).

²²² *United States v. Ivanov*, 175 F. Supp. 2d 367, 370, 373, 375 (D. Conn. 2001).

²²³ *Id.* at 369.

²²⁴ *Id.* at 368.

²²⁵ *Russian Man Sentenced for Hacking into Computers in the United States*, DEP’T OF JUST. (July 25, 2003), <https://www.justice.gov/archive/criminal/cybercrime/press-releases/2003/ivanovSent.htm>.

§ 1029 and § 1030.²²⁶ These include the wire fraud statute, as previously mentioned. It also includes 18 U.S.C. § 2701, the *Unlawful Access to Stored Communications Act*, which focuses on protecting email and voicemail from unauthorized access.²²⁷ As noted in the *Computer Crimes Manual*, “At heart, Section 2701 protects the confidentiality, integrity, and availability of these communications stored by providers of electronic communication services pending the ultimate delivery to their intended recipients.”²²⁸ This seems particularly applicable to the Russian hacks of Democratic National Committee emails and subsequent delivery to WikiLeaks, which posted the private communications on its public site.²²⁹ These are just the statutes currently in effect; nothing is preventing Congress from passing completely new criminal statutes with extraterritoriality built in, in order to address the rising cyber threat.

Of course, extraterritorial criminal indictments are far from a cyber panacea. More often than not, it seems, foreign agents are charged and never brought to trial.²³⁰ Indeed, this has been one of the key arguments against the idea.²³¹ It is highly unlikely that China would ever extradite their hackers.²³² However, we should not ignore the effect that illuminating these networks will have. Those who have been indicted are, for all intents and purposes, burned.²³³ Moreover, they

²²⁶ See generally 18 U.S.C. § 1029 (2015); 18 U.S.C. § 1030 (2012).

²²⁷ 18 U.S.C. § 2701 (2012).

²²⁸ COMPUTER CRIMES MANUAL, *supra* note 195, at 89.

²²⁹ Second Amended Complaint at 76–77, Democratic Nat’l Comm. v. Russia, No. 1:18-cv-03501-JGK (S.D.N.Y. Jan. 17, 2019) (alleging violations of the Stored Communications Act based on the hack).

²³⁰ See generally Graham Webster, *What Exactly Do the New PLA Indictments Accomplish?*, LAWFARE (Feb. 11, 2020, 2:29 PM), <https://www.lawfareblog.com/what-exactly-do-new-pla-indictments-accomplish>.

²³¹ See generally *id.* Interestingly, Webster admits that John Carlin, DOJ’s National Security Division head, argued “the 2014 indictments that led up to the 2015 no-commercial-hacking pledge were an effective warning.” *Id.* Also, in suggesting the Equifax data has no apparent value to the Chinese, Webster fails to address the extensive black market that deals richly in identity information.

²³² See generally *Laws on Extradition of Citizens*, LIBR. OF CONGRESS (July 2013), <https://www.loc.gov/law/help/extradition-of-citizens/chart.php> (detailing various nations’ record of extradition and their laws regarding extradition and displaying that China declines to extradite its citizens).

²³³ See generally *Language of Espionage*, SPY MUSEUM, <https://www.spymuseum.org/education-programs/spy-resources/language-of-espionage/> (last visited Sept. 10, 2020) (“Burned: When a case officer or agent is compromised”).

face *de facto* sanctions, being unable to travel for fear of extradition by friendly states, or invest in the global economy for fear of losing their assets.²³⁴ One might argue that the more the U.S. pursues Chinese hackers in court, the more its own agents face the same risk. Yet, there is nothing stopping China from publishing the names of spies and hackers it discovers regardless. No courtroom is required, and this would burn those agents just as effectively as any criminal indictment, preventing them from traveling internationally and limiting their freedom in other ways for fear of their lives. But an honest indictment requires evidence of a crime, and in providing such evidence, investigations and indictments generate legitimacy in a way that press leaks in today's age cannot.²³⁵ They also raise public awareness and send political signals abroad as to what behavior in cyberspace is or is not acceptable.²³⁶ The latter should help to begin developing international cyber norms.

ii. *Increasing State Liability*

One fundamental weakness with domestic criminal law, despite any potential extraterritoriality, is that states cannot be held criminally liable, only individuals can.²³⁷ This also means that the attribution of acts by individuals to states does nothing to enable the government

²³⁴ See generally *A Guardian Guide to Extradition*, GUARDIAN (July 2, 2013), <https://www.theguardian.com/world/interactive/2013/jul/02/guardian-guide-extradition-interactive> (articulating standard language in extradition treaties).

²³⁵ Cf. John T. Nelson, *L'Affaire d'Assange: Why His Extradition May Be Blocked*, JUST SECURITY (June 7, 2019), <https://www.justsecurity.org/64425/laffaire-dassange-why-his-extradition-may-be-blocked/> (suggesting that indicting an individual who would likely never be extradited would still provide “proof of the United States’ ability to investigate exfiltration of secret government data and of its preparedness to prosecute those who publish it”).

²³⁶ For an example of this discussion, see generally Ryan Lucas, *Charges Against Chinese Hackers Are Now Common. Why Don't They Deter Cyberattacks?*, NPR (Feb. 5, 2019), <https://www.npr.org/2019/02/05/691403968/charges-against-chinese-hackers-are-now-common-why-dont-they-deter-cyberattacks>.

²³⁷ Crootof, *International Cybertorts*, *supra* note 45, at 589.

to seek criminal penalties against the sponsors, only the agents.²³⁸ However, civil liability can still be assessed against offending states in certain circumstances.

Limited state liability is supported by international law. The commentaries of Article 31 of the *Draft Articles* describe the requirement states have to provide reparation for internationally wrongful acts.²³⁹ The commentary notes that “reparation must, as far as possible, wipe out all the consequences of the illegal act and reestablish the situation which would, in all probability, have existed if that act had not been committed.”²⁴⁰ Of course, resetting from a massive data breach would be impossible, so alternatively, the commentary provides for “[r]estitution in kind, or, if this is not possible, payment of a sum corresponding to the value which a restitution in kind would bear” and for “damages for loss sustained which would not be covered by restitution in kind or payment in place of it.”²⁴¹

Additionally, some international cases have suggested that a state could be held liable for transboundary harms. Rebecca Crootoof cites the 1941 *Trail Smelter Case* between the United States and Canada, which centered on damages caused to an orchard in the United States by pollutants from a smelter across the Canadian border.²⁴² The case resulted in a ruling that “no state has the right to use or permit the use of its territory in such a manner as to cause injury by fumes in or to the territory of another or the properties of persons therein.”²⁴³ The implication here is that states are liable for transboundary harm caused by the state or proxies attributable to the state.²⁴⁴ More specifically, Gordon Christenson argued that the Canadian Government's fault

²³⁸ *Id.*

²³⁹ *Draft Articles*, supra note 74, at 91.

²⁴⁰ *Id.* (citing *Factory at Chorzów*, Germany v. Poland, Jurisdiction, Judgment No. 8, 1927, P.C.I.J., Series A, No. 9).

²⁴¹ *Id.*

²⁴² Crootoof, *International Cybertorts*, supra note 45, at 601.

²⁴³ *Id.* (citing *Trail Smelter Case* (U.S. v. Can.), 3 R.I.A.A. 1905, 1965 (Perm. Ct. Arb. 1938 and 1941)).

²⁴⁴ See *id.* (citing Beatrice A. Walton, Note, *Duties Owed: Low-Intensity Cyber Attacks and Liability for Transboundary Torts in International Law*, 126 YALE L.J. 1460, 1479 (2017)).

lied in its failure to “maintain a regime of control in the face of the duty recognized in the *compromis* as grounded in international law,” and that such failure would “constitute an act of omission attributable to the state.”²⁴⁵ States can be held liable when they fail to fulfill their international obligations (i.e. omissions), such as the requirements of treaties and norms to prevent or prosecute cybercrimes.

However, U.S. law has long protected states from civil liability through mechanisms such as *Foreign Sovereign Immunities Act* or FSIA, which protects foreign states from liability with some limited exceptions.²⁴⁶ These include the noncommercial tort exception, which allows an individual sue a state for a tort which occurs wholly inside the United States.²⁴⁷ Recently, there has been a resounding call to add a cyber exception to the Act.²⁴⁸

In August of 2019, a New York federal judge dismissed a civil lawsuit brought against Russia by the Democratic National Committee (DNC), in relation to the hacking of the DNC’s servers and the theft of internal emails.²⁴⁹ In its ruling, the court cited the “whole tort” rule as making it impossible to sue Russia for the operation, despite evidence showing clear attribution, “because the hackers were not in the United States.”²⁵⁰ In several recent cases, such as the DNC hack case, the courts have rejected FSIA hacking claims based on foreign attacks when the whole of the tort could not be claimed to have occurred in the U.S. If the 2019 ruling stands, it

²⁴⁵ Gordon A. Christenson, *Attributing Acts of Omission to the State*, 12 MICH. J. INT’L L. 312, 314 n.10 (1991).

²⁴⁶ 28 U.S.C. § 1602 (1976).

²⁴⁷ 28 U.S.C. § 1605(a)(5) (1976).

²⁴⁸ See *All Information (Except Text) for H.R. 4189 - Homeland and Cyber Threat Act*, CONGRESS.GOV, <https://www.congress.gov/bill/116th-congress/house-bill/4189/all-info> (last visited Aug. 20, 2020) (showing 67 current cosponsors for the bill).

²⁴⁹ Sam Kleiner & Lee Wolosky, *Time for a Cyber-Attack Exception to the Foreign Sovereign Immunities Act*, JUST SECURITY (Aug. 14, 2019), <https://www.justsecurity.org/65809/time-for-a-cyber-attack-exception-to-the-foreign-sovereign-immunities-act>.

²⁵⁰ *Id.*

opens a critical gap in relation to malicious cyber activity.²⁵¹ All it would take for a state to avoid liability—even for cyber operations fully planned and executed in the United States—is for the operators to route their transmission through a foreign server and claim the whole tort rule is not satisfied.

However, Congress has passed several exceptions to the FSIA over the years, hinting to what can be done to establish cyber liability. In 1996 and 2016, Congress added exceptions relating to terrorism which added to the law “a civil cause of action against foreign states for injury or death occurring in the United States based on an act of international terrorism occurring in the United States.”²⁵² Many have argued that a similar exception should be enacted relating to state-sponsored cyber operations resulting in torts.²⁵³

There are several reasons why state liability for cyber offenses could be useful. First, as with criminal jurisdiction, it decentralizes the response. The State Department simply cannot respond to every little state-sponsored cyber action, nor would they want to. Which leads to the second benefit, removing the decision to take action from political hands. Leaving the politically-interested executive branch as the sole authority to respond to attacks increases the likelihood that no action will be taken. This risk is clearly shown in the government’s unwillingness to address Saudi Arabia’s role in the 9/11 terrorist attacks.²⁵⁴ Movement towards some sort of just resolution in that case only began after Congress passed a FSIA amendment,

²⁵¹ See generally *id.* (finding “courts have generally interpreted the exception narrowly to require that the ‘entire tort’ must have occurred in the United States.”).

²⁵² *Id.* (stating Congress enacted the Justice Against Sponsors of Terrorism Act in 2016 as a narrow amendment to FSIA).

²⁵³ See *id.* (finding “civil suits could be more effective at confronting cyber attacks undertaken by foreign actors.”).

²⁵⁴ See generally Tim Golden & Sebastian Rotella, *The Saudi Connection: Inside the 9/11 Case that Divided the FBI*, N.Y. TIMES (Jan. 23, 2020) <https://www.nytimes.com/2020/01/23/magazine/9-11-saudi-arabia-fbi.html> (noting the United States’ complex and often-troubled relationship with the Saudi regime was an unavoidable fact throughout [FBI] investigations. Saudi authorities became more cooperative with the United States in fighting Al Qaeda after 2003, but they were minimally helpful when it came to the 9/11 inquiry.).

allowing victim families to pursue the issue in civil court.²⁵⁵ Lastly, financial judgments can be effective. Kleiner and Wolosky suggest “the threat of judgments worth billions of dollars that can be seized and then lost would be far more of a deterrent than the hollow threat of criminal indictments against hackers who may never set foot in this country.”²⁵⁶ This is supported by Sudan’s sudden change of tone in relation to the U.S.S. Cole bombings after being threatened with heavy civil damages.²⁵⁷

Congress has already begin moving towards a FSIA cyber exception, in the form of the *Homeland and Cyber Threat Act* or *HACT Act*.²⁵⁸ This bill was introduced in the House and referred to committee in June of 2019, and has been generating a lot of momentum lately, gaining nine new cosponsors in May of 2020.²⁵⁹ As urged by Kleiner and Wolosky, this Act would amend the FSIA to add an exception for “Foreign state computer intrusions.”²⁶⁰

This bill is not without its problems, though. As noted recently by Chimène Keitner and Allison Peters, “the categories of malicious cyber activity covered in this bill are so broad that they would include activity that the United States itself intentionally and legitimately conducts on a regular basis.”²⁶¹ The types of covered activities under the *HACT Act* are borrowed from the

²⁵⁵ Kleiner & Wolosky, *supra* note 249 (stating “in 1996 Congress amended [FSIA] to allow Americans who had been the victims of terrorism to sue foreign states that had been designated by the State Department as ‘State Sponsors of Terrorism.’” However, Saudi Arabia was not a designated State Sponsor of Terrorism and plaintiffs were left to argue Saudi Arabia committed a noncommercial tort).

²⁵⁶ *Id.*

²⁵⁷ Ali Younes, *Sudan Finalizes Settlement with U.S. Families Over USS Cole Bombing*, AL JAZEERA (Apr. 7, 2020), <https://www.aljazeera.com/news/2020/04/sudan-finalises-settlement-families-uss-cole-bombing-200407091952504.html> (reporting Sudan’s government reached a settlement to pay victim’s families as part of a strategic effort to remove itself from the US list of state sponsors of terror).

²⁵⁸ Homeland and Cyber Threat Act, H.R. 4189, 116th Cong. (2019) <https://www.congress.gov/bill/116th-congress/house-bill/4189/all-info>.

²⁵⁹ *Id.*

²⁶⁰ *Id.*

²⁶¹ Chimène Keitner & Allison Peters, *Private Lawsuits Against Nation-States Are Not the Way to Deal with America’s Cyber Threats*, LAWFARE (Jun. 15, 2020), <https://www.lawfareblog.com/private-lawsuits-against-nation-states-are-not-way-deal-americas-cyber-threats>.

CFAA (18 U.S.C. § 1030) and include simply accessing a computer without authorization.²⁶²

Another covered activity is providing “material support” to unauthorized access, which would directly implicate the government if coordinated “hack back” is executed.²⁶³ These covered activities are used as a justification to seek damages, so there is also a requirement that harm be caused.²⁶⁴ However, the type of damages allowed under the Act are also too broad, including personal injury, harm to reputation, and damage or loss of property.²⁶⁵ A private cyber security firm might claim “harm to reputation” for the mere fact that a foreign agent breached their firewall, even if they took no further harmful actions. The terrorism exception to the FSIA is used to respond to terrorist acts that have manifest effects.²⁶⁶ Victims are killed or wounded, and therefore deserve the right to seek compensation. Any cyber exception should also be tied to specific manifest effects, such as physical damage, blackmail, or active identity theft.

Additionally, as noted by Keitner and Peters, “the HACT Act fails to include any standards for who can authoritatively attribute the harmful activity to a particular foreign state.”²⁶⁷ It is critical to establish standards and authorities for attribution, and this could be tied directly to the “hack back” and “defend forward” coordination efforts suggested above. To put it bluntly, the *HACT Act* requires a lot of polish before it can be a productive counter-cyber measure.

²⁶² *Id.* (finding the HACT Act covers a number of actions currently covered by the Computer Fraud and Abuse Act, including unauthorized access to a U.S. based computer, damage caused to computers by various forms of malicious cyber activity, and material support for such activity).

²⁶³ *Id.*

²⁶⁴ *See id.* (finding the HACT Act “would create an FSIA exception to allow a U.S. national to seek money damages from a foreign government for personal injury, harm to reputation, or damages or losses to property resulting from malicious cyber activity, regardless of whether the activity occurs in the United States.”).

²⁶⁵ *See generally id.* (noting a flaw in the broad drafting of types of damage included in the HACT Act as “the bill makes no mention of the motivations of the foreign state for such actions and includes no standards for who can authoritatively attribute the harmful activity to a particular foreign state.”).

²⁶⁶ *See* 28 U.S.C. § 1605(B)(a) (2016) (citing “international terrorism” as defined by 18 U.S.C.A. § 2331(1)(A-B) (2001)).

²⁶⁷ Keitner & Peters, *supra* note 261.

Regarding increasing sovereign liability, especially the sort of punitive damages levied against Sudan, some have argued it sets a “dangerous and counterproductive” precedent.²⁶⁸ Haim Abraham argued that awarding massive punitive damages against states—for example, under the terrorism exception to the FSIA—makes it more difficult for victims to actually receive the compensation, and may even cause a financial crisis in the offending state, setting off ripples through the global economy which could affect the United States itself.²⁶⁹ Abraham argues that such judgements against states should be limited to compensatory damages, or to only those costs reflective of the actual losses.²⁷⁰ This is arguably how the long-standing non-commercial tort exception of the FSIA functions. Abraham’s argument is compelling, but moreover, like with criminal sanctions, civil judgements against offending states serve to “name and shame,” highlighting the bad behavior on the global stage.²⁷¹ It’s more than just making the offending states pay, literally. Limiting the scope of FSIA judgments to compensatory damages would serve the same purpose while avoiding the risks Abraham highlights.

CONCLUSION

As scholars have recently noted, “daily cybercrime complaints have quadrupled during [the COVID] crisis, as non-state actors look to exploit the pandemic for financial gain and nation-states turn to cybercrime to collect valuable intelligence.”²⁷² The proposals here are not without their drawbacks. Many of these measures are currently being developed, but in a

²⁶⁸ See generally Haim Abraham, *Awarding Punitive Damages Against Foreign States Is Dangerous and Counterproductive*, LAWFARE (Mar. 1, 2019), <https://www.lawfareblog.com/awarding-punitive-damages-against-foreign-states-dangerous-and-counterproductive>.

²⁶⁹ *Id.* (finding that awarding large punitive damages can be counterproductive because “the amount of punitive damages may be so high that it obstructs the ability of individuals to enforce awards of compensation against foreign states within the United States” and if the U.S. asserts power over a foreign state to enforce a court’s ruling for the foreign state to pay punitive damages, it undermines the principle of state sovereignty).

²⁷⁰ *Id.*

²⁷¹ See Lucas, *supra* note 236.

²⁷² See Keitner & Peters, *supra* note 261.

piecemeal manner. It would be more efficient to pursue them all as a unified package, one bill encompassing “hack back” authority, interagency coordination, expanded criminal jurisdiction and state liability. Passing measures one by one will most certainly create gaps and frictions between them.

Ultimately, employing domestic measures to tackle international problems cannot be the desired end state. Indeed, U.S. policy has been consistent over the past decade that international law can and should address the growing cyber crisis.²⁷³ Brian Egan reiterated in 2016 that “existing principles of international law form a cornerstone of the United States’ strategic framework of international cyber stability during peacetime and during armed conflict.”²⁷⁴ The Cyberspace Solarium Commission recommended creating an Assistant Secretary of State, in a new Bureau of Cyberspace Security and Emerging Technologies, “who will lead the U.S. government effort to develop and reinforce international norms in cyberspace.”²⁷⁵ But if the past decade and the failure of multiple international working groups to reach any consensus on cyberattacks shows anything, it’s that the effort to define cyber norms is going to take years, if not decades. Even the DOD still reviews the legality of cyber operations through analogy. Currently, there are multiple cyber working groups which are headed in different directions.²⁷⁶ Therefore, international consensus seems a long way off. The United States should undoubtedly continue to lead efforts to establish clear cyber norms, but other immediate action is required now to address the growing epidemic of cybercrime.

²⁷³ *Id.* (advocating for Congress to improve high-level diplomatic leadership to lead negotiations on cyber issues and to establish a new cyber bureau at the state department to push governments to cooperate on cyber investigations).

²⁷⁴ Egan, *supra* note 57; *see also* Koh, *supra* note 31.

²⁷⁵ CYBERSPACE SOLARIUM COMMISSION, *supra* note 4, at 3.

²⁷⁶ *See* Korzak, *supra* note 49.

Some have suggested that “we may be witnessing the opening rounds of a struggle for the legal soul of cyberspace.”²⁷⁷ It is quite common today to read a news report or even an academic article suggesting the time has come for a cyber Geneva Convention, that the world needs a new treaty to confront the reality of increasing cyberattacks.²⁷⁸ However, hoping for cyber issues to be resolved through international law anytime soon seems more and more like a pipe dream. It is unlikely that any sort of cyber treaty will be adopted by those to whom it would be most applicable—the United States, China, Russia, North Korea, Iran, etc. Chinese and Russian participation in the UN GGE process has shown an unwillingness to accede to western views, and even an effort to drive the discussion in the opposite direction.²⁷⁹ No, a comprehensive cyber treaty is not a likely solution.

Instead, the support of treaties like the Budapest Convention have revealed a “growing recognition among states that cyberattacks must be stopped, and that the way to do so is through vigorous law enforcement.”²⁸⁰ Therefore, the United States must expand, empower, and decentralize domestic policy to take action against both state-sponsored cyber operations and non-state cybercrime.²⁸¹ Most importantly, the U.S. must respond quickly and definitively to

²⁷⁷ Watts & Richard, *supra* note 72, at 839.

²⁷⁸ See, e.g., Brad Smith, *The need for a Digital Geneva Convention - Microsoft on the Issues*, MICROSOFT (Feb. 14, 2017), <https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/>.

²⁷⁹ Justin Sherman & Mark Raymond, *The U.N. Passed a Russia-Backed Cybercrime Resolution. That’s Not Good News for Internet Freedom.*, WASH. POST (Dec. 4, 2019) <https://www.washingtonpost.com/politics/2019/12/04/un-passed-russia-backed-cybercrime-resolution-thats-not-good-news-internet-freedom/> (“[O]utcomes like the Russian cybercrime resolution and current developments in the U.N. General Assembly First Committee, where many Internet governance discussions are occurring, demonstrate that Moscow and Beijing are becoming far more skilled in using procedural rules and practices to advance their agendas.”).

²⁸⁰ Matthew J. Sklerov, *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the use of Active Defenses Against States Who Neglect Their Duty to Prevent*, 201 MIL. L. REV. 1, 66 (2009).

²⁸¹ See Michael Schmitt, *Top Expert Backgrounder: Russia’s SolarWinds Operation and International Law*, JUST SECURITY (Dec. 21, 2020), <https://www.justsecurity.org/73946/russias-solarwinds-operation-and-international-law/> (Providing a convincing argument that the recent digital supply chain hacks by Russian agents were not violations of international law. These acts were analogous to traditional espionage which did not result in a use of force, nor coercive intervention, and thus do not allow severe international responses such as countermeasures. They were, however, certainly violations of U.S. domestic law, such as 18 U.S. Code § 1030. This once again shows the inherent weakness of International Law in addressing the most common types of cyberattacks.)

cyberattacks. As Jack Goldsmith argued on *Lawfare*, past patterns of “vacillation in response to very damaging cyber operations will not deter our adversaries; it will embolden them.”²⁸²

History has already shown that domestic law can be an effective tool in responding to malicious cyber activity, such as in the conviction of Aleksey Ivanov, the first person charged extraterritorially under changes to the CFAA.²⁸³ It is within Congress’s power to revise other criminal statutes to include extraterritoriality, and to authorize private entities to support an interagency effort to tackle the problem of attribution. When cyberattacks are attributed directly to individuals, these criminal need to be prosecuted swiftly and aggressively. Extraterritorial clauses in criminal statutes, such as the wire fraud statute, will provide prosecutors with greater reach and judges with greater sentencing power. When an action is attributed to a rival government, those states need to be named and held liable. Even when their agents are arrested and prosecuted, there is little that can currently be done to the sponsoring state. To this end, adding cyber exceptions to the FSIA or other civil provisions would allow states who sponsor malicious cyber operations to be held accountable, if only in the pocketbook.

Clearly, more needs to be done in cyber defense and response.²⁸⁴ Every day that Congress stalls and does not pass new, innovative legislation, is another step ahead for the hackers. The

²⁸² Jack Goldsmith, *The DNC Hack and (the Lack of) Deterrence*, LAWFARE (Oct. 9, 2016), <https://www.lawfareblog.com/dnc-hack-and-lack-deterrence>.

²⁸³ See *United States v. Ivanov*, 175 F. Supp. 2d 367, 373 (D. Conn. 2001) (finding the court “has subject matter jurisdiction over each of the charges against Ivanov, whether or not the statutes under which the substantive offenses are charged are intended by Congress to apply extraterritorially, because the intended and actual detrimental effects of the substantive offenses Ivanov is charged with in the indictment occurred within the United States.”).

²⁸⁴ See Jemima McEvoy, *‘It Happened On My Watch’: Chris Krebs Says Russia Exploited Outdated Systems For Cyberattack*, FORBES (Dec. 20, 2020), <https://www.forbes.com/sites/jemimamcevoy/2020/12/20/it-happened-on-my-watch-chris-krebs-says-russia-exploited-outdated-systems-for-cyberattack/?sh=2ccec86e26eb> (Summarizing a TV interview with Former CISA Director Chris Krebs, who took responsibility for the recent Russian cyber espionage on U.S. government unclassified systems. Krebs noted that several factors enabled the attacks including “seams” between outdated systems throughout the government and because CISA’s authority to monitor networks was limited. Krebs noted, however, that these might be resolved through legislation, such as through the NDAA. As argued in this paper, having one central agency leading from an interagency cyber ops center or JOC would be a prudent start in addressing these problems, along with supporting legislation.)

evolution of technology is accelerating and if stronger deterrence is not offered now, it might prove too little, too late.