VOLUME 5 June 2024 ISSUE 2

JOURNAL ON EMERGING TECHNOLOGIES

ARTICLES

LAYERED CYBER DETERRENCE: PANACEA OR SETBACK FOR U.S. CYBER POLICY?

Bryan Hance

ABSTRACT

This paper critically examines a new U.S. policy called layered cyber deterrence and its proposed implementation under international law. The policy is introduced in an extensive report prepared by the Cyberspace Solarium Commission, a group of key U.S. academics, policymakers, cybersecurity experts, and others. It is billed as a more cohesive, extensively developed, and aggressive U.S. cyber policy than earlier strategies like persistent engagement and defend forward. It also is the first time the United States has articulated a whole-of-nation approach to defending itself against cyberattacks both below and above the use of force threshold. It is not, however, without its shortcomings. This paper supports the Solarium Commission's observation that the United States must become more aggressive in responding to harmful cyberattacks. It argues, however, that the layered cyber deterrence strategy has yet to be accompanied by more aggressive action to back it up. Moreover, the strategy contains weaknesses that ultimately undermine its effectiveness and, in fact, may put the U.S. at increased risk of violating international law.

Part I briefly describes the Cyberspace Solarium Commission and the work leading up to its report. Part II begins an analysis of several issues that can arise under the layered cyber deterrence strategy. They include a public-private partnership that may cause a reduction of government control over the strategy, attribution, and due diligence problems that can lead to U.S. accountability for private misconduct, law of war concerns that make civilians and civilian objects potential military targets, and an overreliance on an ineffective deterrence by denial strategy. Part III discusses the need for greater

U.S. deterrence by punishment and considerations related to threats and uses of force under layered cyber deterrence. Parts IV and V address circumstances in which the United States may violate State sovereignty and the nonintervention principle respectively under layered cyber deterrence. Part VI considers defenses available to the United States should it violate international law in the implementation of the strategy. It further advocates for the U.S. to lead by example in establishing sound precedents in cyberspace where international law is silent or unclear. Part VII offers some overarching conclusions for consideration. Finally, because layered cyber deterrence was only recently introduced, earlier cyber incidents are interspersed throughout the paper for helpful insights into the lawfulness of U.S. conduct under the strategy.

LAYERED CYBER DETERRENCE: PANACEA OR SETBACK FOR U.S. CYBER POLICY?

Bryan Hance

I. THE CYBERSPACE SOLARIUM COMMISSION AND ITS REPORT

The inspiration for the Cyberspace Solarium Commission ("the Solarium Commission" or "the Commission") was President Dwight Eisenhower's 1953 "Project Solarium" plan to alter the U.S. strategy for responding to Soviet expansion at the start of the Cold War.[1] It grew out of conversations he had with key national security officials in the Solarium room of the White House in which he learned that the existing strategy was inadequate to address a myriad of issues. Over the course of six weeks, Eisenhower pitted three teams of experts against each other at the National War College to design what eventually became known as his New Look deterrence policy. This whole-of-nation approach called on the U.S. government, together with U.S. citizens, corporations, and academia, to implement a sustainable variant of containment against the Soviet Union.[2]

The Solarium Commission has many similarities to its Cold War namesake. Its purpose is to develop a strategic approach to defend the United States in cyberspace against cyberattacks of significant consequence.[3] The Commission's work is important in helping to protect

---

[1] *See generally,* William B. Pickett, GEORGE F. KENNAN AND THE ORIGINS OF EISENHOWER'S NEW LOOK: AN ORAL HISTORY OF PROJECT SOLARIUM (2004).; Raymond Millen, *Eisenhower and US Grand Strategy*, 44 U.S. ARMY WAR COLL. Q.: PARAMETERS 35-47 (2014); *Project Solarium*, WIKIPEDIA (2020), https://en.wikipedia.org/wiki/Project_Solarium (last visited June 30, 2020).

[2] U.S. CYBERSPACE SOLARIUM COMM'N, FINAL REP. 20 (Mar. 2020), www.solarium.gov/report.

[3] H.R. 5515, 115th Cong. §1652 (2018), The Commission's duties are six-fold and described as follows:

> 1. To weigh the costs and benefits of various strategic options to defend the United States, including the political system of the United States, the national security industrial sector of the United States, and the innovation base of the United States. The options to be assessed should include deterrence, norms-based regimes, and active disruption of adversary attacks through persistent engagement.
> 2. To evaluate the best means for executing such options, and how the United States should incorporate and implement such options within its national strategy.
> 3. To review and make determinations on what norms-based regimes the United States should seek to establish, how the United States should enforce such norms, how much damage the United States should be willing to incur in a deterrence or persistent denial strategy,

U.S. cybersecurity interests with today's rapidly developing technology. The Solarium Commission describes the critical cyber threats the United States faces in rather stark terms.

> [M]uch has changed in the past ten years. Our adversaries have abused open platforms for sharing knowledge and views by creating troll farms for disinformation. Terrorists have used the Internet to control forces and recruit new members. Portions of critical infrastructure, such as the power supply in Ukraine, have been disabled. Advances in artificial intelligence, autonomous vehicles, and 5G networks will only complicate this landscape of threats. In large part to account for these and other changes, Congress established the Cyberspace Solarium Commission in 2019 to prepare for the next ten years and consider new approaches to keeping the United States safe in cyberspace.[4]

The Solarium Commission Report ("the Report") defines layered cyber deterrence as a strategy that combines enhanced cyber resilience and attribution capabilities with a clearer signaling strategy and collective action by U.S. partners and allies. Though simple in name, layered cyber deterrence is both nuanced and far-reaching in scope. The Commission's 182-page report contains six policy pillars underlying the strategy with over seventy-five recommendations for actions across both the public and private sectors. The recommendations are based on an extensive study that included a literature review and over 300 interviews with key academics; industry and cybersecurity experts; federal, state, and local policymakers; and officials from international organizations and foreign countries. The goal is to enable the United States to "evolve into a hard target, a good ally, and a bad enemy."[5] According to the

---

> what attacks warrant response in a deterrence or persistent denial strategy, and how the United States can best execute those strategies.
> 4. To review adversarial strategies and intentions, current programs for the defense of the United States, and the capabilities of the Federal Government to understand if and how adversaries are currently being deterred or thwarted in their aims and ambitions in cyberspace.
> 5. To evaluate the effectiveness of the current national cyber policy relating to cyberspace, cybersecurity, and cyber warfare to disrupt, defeat, and deter cyberattacks.
> 6. To consider possible structures and authorities that need to be established, revised, or augmented within the Federal Government.

Id.

[4] Paul M. Nakasone & Michael Sulmeyer, *How to Compete in Cyberspace*, FOREIGN AFFS. (Aug. 24, 2020), https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity.

[5] U.S. CYBERSPACE SOLARIUM COMM'N, *supra* note 2, at v. "The strategy should clearly express that defend forward is an integral part of a comprehensive approach that

Solarium Commission, the current U.S. cyber strategy invites aggression and establishes a dangerous pattern of actors attacking the United States without fear of reprisal. In the Commission's words, "Adversaries are increasing their cyber capabilities while U.S. vulnerabilities continue to grow."[6] A bedrock of layered cyber deterrence is significant U.S. government reorganization to better handle cyberspace issues that will, in turn, promote cybersecurity and enable the United States to respond to attacks with greater speed and agility.[7]

As its name implies, layered cyber deterrence is comprised of three layers of progressively offensive strategies designed to shape adversaries' behavior, deny them benefits, and impose costs when they threaten or harm American interests. The aim of the first layer is to build coalitions of allies to strengthen collective capacity and increase costs to adversaries to minimize the number of cyber targets in the United States.[8] Layer two prioritizes the U.S. government's partnerships with the private sector to collectively reduce cyber vulnerabilities and deny benefits to American adversaries.[9] This requires securing vital networks to promote national resilience and increase the security of the U.S. cyber environment. Layer three in some ways is the most ambitious and potentially problematic from an international law perspective. It proposes that the United States impose costs not only below the level of armed conflict, but, if necessary, to prevail in war by employing the full spectrum of American military capabilities.[10] While this paper discusses issues related to all three layers, the focus of the analysis is on layers two and three.

Like Eisenhower's New Look policy, layered cyber deterrence involves not merely whole-of-government, but whole-of-nation collaboration.[11] While the ambitious proposal is formidable in design, this paper begins by discussing some of the significant shortcomings of a public-private partnership, including potentially placing critical U.S. infrastructure at increased risk and causing the United States to violate international law. Layered cyber deterrence builds on a long history of U.S. cyber policy,[12] most notably the original Department of Defense

---

encompasses all of the instruments of national power beyond the employment of strictly military capabilities; these include trade and economic efforts, law enforcement activities, and diplomatic tools." *Id.* at 33.

[6] *Id.* at 7.

[7] *Id.* at 2.

[8] *Id.* at 7.

[9] *Id.* at 24–25. "When U.S. vulnerabilities are reduced and adversaries are forced to expend more resources, burn sensitive accesses, or utilize unique and expensive cyber weapons to achieve their desired results, cyberattacks will be reduced." *Id.*

[10] *Id.* at 25.

[11] *Id.* at 1.

[12] Below is a list of key reports, initiatives, and events leading up to the creation of the Cyberspace Solarium Commission and the layered cyber deterrence strategy.

- The Ware Report (1970)
- War Games (1983)

defend forward policy of 2018.[13] The Solarium Commission describes layered cyber deterrence as a reimagining and an expansion of defend forward that is intended to stop malicious cyber activities at their source rather than waiting for them to occur here in the United States.[14] To be sure, norms of acceptable cyberspace behavior will not emerge unless the U.S. and its allies impose meaningful costs on bad actors to change their behavior.[15] Thus, the Report expands the defend forward logic to achieve

---

- Obama Administration's "Strategy for Operating in Cyberspace" Department of Defense Policy (2011)
- State Department Legal Advisor Harold Koh's Remarks on Cyber Space (2012)
- Department of Defense Cyber Strategy Protecting the Department, as Well as Civilian, Government, and Private Sector Networks (2015)
- Department of Defense Law of War Manual, Chapter 16 Regarding Cyber (2015)
- State Department Legal Advisor Brian Egan's Remarks on Cyber Space (2016)
- Persistent Engagement Strategy (2018)
- Defend Forward from USCYBERCOM (2018)
- Defense Department General Counsel Paul C. Ney, Jr.'s Remarks (2020)

[13] U.S. CYBERSPACE SOLARIUM COMM'N, *supra* note 2, at 29.

> First, like the DoD concept, it operates as a general strategic principle during day-to-day competition, in which the U.S. government "will defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict." This posture includes operating in "gray" and "red" space in a manner consistent with international law. *Second, it plays a role in ensuring that the U.S. government retains the ability to apply all instruments of power to respond to crisis or conflict. Applied to military power, this includes ensuring "the cybersecurity and resilience of DoD, DCI [Defense Critical Infrastructure], and DIB [Defense Industrial Base] networks and systems." Finally, cyber layered deterrence, like defend forward, secures critical infrastructure and safeguards American networks by finding ways "to stop threats before they reach their targets."* (emphasis added)(citations omitted).

Id.

[14] The concept of defending forward is not new in the U.S. military lexicon as forward-deployed military forces have been used to advance American interests since the end of World War II. *Id.* at 28. This strategic posture was an integral component of the grand strategy of containment for the United States and the North Atlantic Treaty Organization. Cold War forward defense involved both projecting power by positioning U.S. and allied forces on the front lines of the potential battlefields of the next world war and leveraging multiple instruments of power. These forward-deployed forces served several purposes: Deterrence and signaling U.S. resolve and capabilities to the Soviet Union and its communist allies; enabling rapid response from a more advantageous position if conflict should break out; a source of intelligence and early warning; and a form of credible commitment to allies." *Id.* These purposes are strikingly similar to those of the layered cyber deterrence strategy.

[15] *Id.* at 33.

this goal by embracing all available instruments of national power.[16] In the end, however, some of the more aggressive activities under layered cyber deterrence that are designed to disrupt and defeat adversary campaigns beyond America's borders may come at the expense of U.S. compliance with international law. These areas of potential non-compliance and other observations on the costs and benefits of the proposed layered cyber deterrence strategy also are discussed in this paper. Inasmuch as layered cyber deterrence is a new strategy with little cyber activity conducted pursuant to it, the paper additionally looks at prior U.S. cyber operations and examines how this new, more aggressive strategy may well be problematic for a State that hopes to shape adversary behavior and to lead by example in the developing military realm of cyberspace.

II. CONCERNS WITH THE PUBLIC-PRIVATE "WHOLE OF NATION" PARTNERSHIP

There are several characteristics that make cyberspace a unique battlefield. Two of them are discussed in this paper: The combatants and the location of the combat zone. As to the combatants, unlike the four traditional military domains of land, sea, air, and space, cyberspace is largely privately owned and shaped by market forces. According to estimates, eighty-five percent of critical U.S. infrastructure is managed by the private sector[17], while ninety-eight percent of government communications use systems that are civilian owned and operated.[18] Unlike other military domains, the government cannot secure U.S. cybersecurity interests on its own. The layered cyber deterrence strategy, for better or worse, must rely heavily on non-governmental entities to achieve the goal of defending U.S. cyber infrastructure.[19] The drafters of the strategy acknowledge this dependence by expressly envisioning a close partnership between the United States government and the private sector. In fact, operationalizing cybersecurity collaboration between the two is one of the six pillars of the strategy. The Solarium Commission Report repeatedly emphasizes a whole-of-nation approach in which the U.S. government's relationship with the private sector is strengthened in

---

[16] *Id.* at 110. Changes to the law in the FY2019 National Defense Authorization Act (NDAA) and the issuance of National Security Presidential Memorandum (NSPM) 13 enable the U.S. government to adopt a defend forward posture. *Id.* at 29.

[17] *But see* Paul Rosenzweig, *Is It Really 85 Percent?*, LAWFARE (May 11, 2021), https://www.lawfareblog.com/it-really-85-percent (last visited July 23, 2021).

[18] Benjamin Jensen, *Layered Cyber Deterrence: A Strategy for Securing Connectivity in the 21st Century*, LAWFARE (Mar. 11, 2020), https://www.lawfareblog.com/layered-cyber-deterrence-strategy-securing-connectivity-21st-century (last visited Feb. 25, 2021). Eric Talbot Jensen, *Cyber Warfare and Precautions Against the Effects of Attacks*, 88 TEX. L. REV. 1533, 1534 (2009).

[19] U.S. CYBERSPACE SOLARIUM COMM'N, *supra* note 2, at 23.

order to establish joint collaboration and an enhanced level of common situational awareness.[20]

A. A Reduction of Government Control Over the Strategy

This proposed power-sharing arrangement, however, while arguably necessary to protect U.S. cyber interests, is not without significant potential drawbacks. Perhaps most evident, layered cyber deterrence places the federal government in a precariously dependent partnership with commercial entities and has the potential to substantially diminish its control over the strategy's implementation. This inevitably will result in governmental reliance on a free enterprise system of diverse actors with competing interests and varying degrees of motivation and technological sophistication.[21] The private and public sectors are governed and influenced by different rules and forces that shape their behavior, raising the specter that cyberattacks on the former will place government agencies and functions at increased risk and lead to substantial consequences in the public sector.[22] Critical U.S. infrastructure that once operated largely in isolation, such as power grids and the public health and safety sectors, are now far more complex and reliant on networks of interconnected devices.[23] This public-private

---

[20] *Id.* at 4.
[21] *Id.* at 23.
[22] Erica D. Lonergan & Shawn W. Lonergan, *Ensuring the Cybersecurity and Resilience of the Defense Industrial Base*, LAWFARE (Mar. 12, 2020), https://www.lawfareblog.com/ensuring-cybersecurity-and-resilience-defense-industrial-base (last visited Feb. 25, 2021). Cyberattacks on the Defense Industrial Base could be catastrophic.

> Cyber-enabled intellectual property theft from the Defense Industrial Base (DIB) and adversary penetration of DIB networks and systems pose an existential threat to U.S. national security.... Intellectual property theft can enable adversaries to replicate cutting-edge U.S. defense technology without comparable investments in research and development. Adversary access to the DIB could inform the development of offset capabilities. It could even provide insights or access points that enable adversaries to thwart or manipulate the intended functioning of key weapons and systems designed and manufactured within the DIB.

Id. "Though these intrusions have thus far focused on exfiltrating weapons system designs, a persistent and capable adversary could attack a weapons system through the contractor's own network, implementing malware that can disrupt or disable the system." Madison Creery, *Critical Gaps Remain in Defense Department Weapons System Cybersecurity*, LAWFARE (Mar. 13, 2020), https://www.lawfareblog.com/critical-gaps-remain-defense-department-weapons-system-cybersecurity (last visited Feb. 25, 2021).
[23] AGCS Global, *Cyber Attacks on Critical Infrastructure*), ALLIANZ (June 2016) https://www.agcs.allianz.com/news-and-insights/expert-risk-articles/cyber-attacks-on-critical-infrastructure.html (last visited July 5, 2021).

linkage will only grow as the layered cyber deterrence strategy is implemented over time and the number of non-State and State-sponsored actors rises. As it does so, government agencies and critical infrastructure will be increasingly vulnerable to new attacks at the weakest points of the public, and now the private, sectors, and these weaknesses will serve as ever-increasing entry points for U.S. adversaries. Nowhere is this vulnerability between private and public entanglement more evident than the 2020 cyberattack on the SolarWinds software company.

The SolarWinds Orion platform is produced by a private government contractor to help over thirty thousand customers, including several government agencies and Fortune 500 companies, manage information technology resources. The cyberattack on SolarWinds allowed a Russian intelligence agency to penetrate deep into national security infrastructure across the United States government, spying for months on the Department of Defense, Homeland Security, Commerce, State, Energy, the Treasury, the National Security Administration, and several private corporate giants such as Microsoft, Intel, Cisco, and Deloitte, among other victims. According to an alert issued by the Cybersecurity and Infrastructure Security Agency ("CISA") shortly after the attack was made public, the operation posed not merely a significant or substantial risk, but rather a "grave risk" to the nation's critical infrastructure entities, and in particular, the Department of Energy that oversees the nation's nuclear weapons stockpile and operates the nuclear laboratory at Los Alamos National Laboratory.[24] Quite the opposite of a mere shot across the bow or pure cyber espionage, this was an attack of unprecedented proportion that gave a foreign adversary the capability to destroy U.S. government networks and disable critical infrastructure. Indeed, the full consequences of the attack may not be known for years to come, if ever. A major concern for many corporate victims is the hackers' ability to now access their clients' networks, their clients' clients' networks, and so forth, creating a ripple effect of immeasurable harm.[25] Despite receiving nearly ten billion dollars in funding in 2021, the Defense Department and its U.S. Cyber Command charged with defending U.S. networks not only were unable to prevent the attack, they

---

[24] *Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations*, CISA (Dec. 17, 2020), https://us-cert.cisa.gov/ncas/alerts/aa20-352a. In describing the severity of the security breach in its alert, the Cybersecurity and Infrastructure Security Agency concluded that, "This threat poses a grave risk to the Federal Government and state, local, tribal, and territorial governments as well as critical infrastructure entities and other private sector organizations." *Id.*

[25] Microsoft, for example, discovered that nearly twenty of its customers who were victims of the attack were information technology service companies, which often have broad access to their customers' networks. Kevin Poulsen et al., *SolarWinds Hack Victims: From Tech Companies to a Hospital and University,* WALL ST. J., (Dec. 21, 2020) https://www.wsj.com/articles/solarwinds-hack-victims-from-tech-companies-to-a-hospital-and-university-11608548402.

did not even discover it themselves.[26] Fifteen months after the start of the attack, a private cybersecurity firm finally was able to do so.[27]

B. Attribution and a Failure to Exercise Due Diligence May Create U.S. Liability for Private Misconduct

Another concern with expanding the public-private partnership under layered cyber deterrence lies at the crossroads between attribution and due diligence. Attribution and due diligence are in some ways two sides of the same coin in that they can both expose a State to and shield it from, potential international law violations. Much of the current attribution scholarship focuses on the difficulty of determining the source of a cyberattack and the role of attribution as a prerequisite to initiating a countermeasure. While attribution remains a significant challenge in many cyberattacks today, recent technological advancements are giving States the tools to more accurately attribute cyber intrusions.[28] As a result, States are increasingly more willing to attribute cyberattacks to other States and to collaborate to identify malicious State-sponsored cyber operations.[29] Recently the United States formally accused Russia's top spy agency, the Foreign Intelligence Service, of initiating the SolarWinds cyberattack.[30] A release by the U.S. Treasury stated that, "[t]The U.S. Intelligence Community has high confidence in its assessment of [Russian] attribution."[31] Another example is the United States' nearly immediate attribution of Iran's attempts to interfere in the 2020 U.S. presidential election. The U.S. Director of National Intelligence held a news conference within twenty-seven hours after Islamic Revolutionary Guard Corps hackers sent threatening emails to American voters and posted a video attempting to

---

[26] De Lewes, *US government to spend over $18 billion on cyber security in 2021*, SECURITYWORLDMARKET.COM (Mar. 7, 2020), https://www.securityworldmarket.com/int/News/Business-News/us-government-to-spend-over-18-billion-on-cyber-security-in-20211.

[27] Poulsen, et al., *supra* note 25 (SolarWinds said that it traced activity from the hackers back to at least October 2019); *see also Solarwinds Hack Timeline*, KIUWAN (Jan. 19, 2021), https://www.kiuwan.com/solarwinds-hack-timeline/ (last visited Apr. 22, 2021).

[28] NEIL C. ROWE, THE ATTRIBUTION OF CYBER WARFARE CYBER WARFARE: A MULTIDISCIPLINARY ANALYSIS 61–72 (J. Green, et al. eds., 2015).

[29] HARRIET MOYNIHAN, THE APPLICATION OF INTERNATIONAL LAW TO STATE CYBERATTACKS: SOVEREIGNTY AND NON-INTERVENTION 3–4 (Dec. 2019), https://www.chathamhouse.org/2019/12/application-international-law-state-cyberattacks.

[30] Natasha Turak & Amanda Macias, *Biden Administration Slaps New Sanctions on Russia for Cyberattacks, Election Interference*, CNBC (Apr. 15, 2021), https://www.cnbc.com/2021/04/15/biden-administration-sanctions-russia-for-cyber-attacks-election-interference.html.

[31] *Id.*

weaken confidence in the voting process.[32] The United States unequivocally and openly blamed Iran for the operation, making it the fastest public cyber attribution in U.S. history.[33]

Attribution can work against the United States, however, under the layered cyber deterrence strategy. This is so even if a breach was not caused by the federal government at all, but rather by a private party. Comments 2 and 3 to Rule 33 of the influential Tallinn Manual 2.0 (hereinafter the "Tallinn Manual" or "the Manual") explain the general view that cyber operations by non-State actors ordinarily do not violate sovereignty, constitute intervention, or amount to a use of force because such breaches can only be committed by States.[34] However if a private individual or group acts as an auxiliary or instrument of the United States, for instance when providing instruction, direction or control over a cyber operation, the U.S. itself can be deemed to have engaged in such

---

[32] Ellen Nakashima, *U.S. Undertook Cyber Operation Against Iran as Part of Effort to Secure the 2020 Election*, WASH. POST (Nov. 3, 2020), https://www.washingtonpost.com/national-security/cybercom-targets-iran-election-interference/2020/11/03/aa0c9790-1e11-11eb-ba21-f2f001f0554b_story.html.

[33] *Id.*

[34] TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 175 (Michael N. Schmitt et al. eds., 2017) [hereinafter TALLINN MANUAL 2.0]. It is important to note that the Tallinn Manual was intended to be the starting point for a larger, more substantive discussion on the applicability of international law to States' cyber operations*; see generally* Eric Talbot Jensen, *The Tallinn Manual 2.0: Highlights and Insights,* 48 GEO. J. INT'L L. 735 (2016). It was neither created by States nor is it presently binding on them. Nevertheless, it is comprehensive in nature, based on expert analysis, and includes both State and peer comments, so it serves as meaningful guidance in this analysis.

Some commentators, however, argue against the Tallinn Manual's characterization as a restatement of international law. Jack Goldsmith and Alex Loomis, for example, contend that Rule 4 and its commentary in the Tallinn Manual 2.0 is not representative of customary international law and, in fact, is contrary to both State practice and *opinio juris*. They nevertheless acknowledge the utility of these perspectives from highly-qualified publicists in norm development. As Goldsmith and Loomis conclude:

> The simple fact is that Rule 4's commentary does not align with how States practice or talk about international law. That is dispositive because international law is constituted by what States do, say, and agree to.... There is, to be sure, an important role for private norm entrepreneurship when developing new rules of international law. But we should recognize that the Rule 4 commentary fits squarely in that category. In sum, the legal status of the rules articulated in Rule 4 is not a hard question: they are (at most) *lex ferenda*, not *lex lata*. States have intensively engaged in cyber operations below the use-of-force line for a long time, and have failed after decades of efforts to reach consensus about whether and how better-established, sovereignty-based rules of international law, such as use of force, apply in cyberspace.

Jack Goldsmith & Alex Loomis, *"Defend Forward" and Sovereignty,* HOOVER WORKING GROUP ON NAT'L SEC., TECH., AND LAW, Aegis Series Paper No. 2102 (April 29, 2021).

actions.[35] For example, if the U.S. government were to contract with a private company under layered cyber deterrence that planned and supervised an operation to imbed a virus into software widely used in Iranian government computers, the company's conduct likely would be attributable to the United States.[36] If that virus then crippled the Iranian government's ability to carry out its essential functions, the United States likely would have violated international law. By increasing the number of private individuals and entities participating as auxiliaries or instruments of the United States under layered cyber deterrence's whole-of-nation plan, the U.S. increases its potential for violating another State's sovereignty or engaging in an unlawful intervention or use of force.

This increase in auxiliaries or instruments of the United States is not inconsequential. Though they do not define the term "private sector," it is generally understood that both the Solarium Commission Report and the USA PATRIOT Act broadly refer to owners or operators of cybersecurity firms, tech companies, and critical U.S. infrastructure.[37] It is difficult to estimate with precision what this number is, but undoubtedly there are tens of thousands of such entities in the United States. Depending on how one defines these terms, as of the date of this writing, there are over 3,500 U.S. cybersecurity companies,[38] 394 public and 492,156 private tech companies,[39] and countless thousands of key assets that qualify as "critical infrastructure." The USA PATRIOT Act defines critical infrastructure as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any

---

[35] TALLINN MANUAL 2.0, *supra* note 34, at 94.

> As a general rule, the cyber operations of private persons or groups are not attributable to States. However, Article 8 of the Articles on State Responsibility provides that "[t]he conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct."

Id. at 95.

[36] *Id.* at 96.

[37] Other types of actors and non-profit entities can contribute to a national cyber strategy as well.

[38] CYBERDB, https://www.cyberdb.co/ (last visited June 29, 2021).

[39] Emma G. et al., *Statistics about the tech work force in the US. How many employees? How many work in private companies? How many in public companies? How many companies are private and how many public? How many of the private companies are startups?*, WONDER (July 5, 2017), https://askwonder.com/research/statistics-tech-work-force-us-employees-work-private-companies-public-companies-1rhg054r5 (last visited June 29, 2021).

combination of those matters."[40] CISA identifies sixteen systems and assets under this definition that include chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials, and wastewater; transportation; and water and wastewater systems.[41] Many of these sectors, such as financial services, transportation, healthcare, and information technology, are virtually entirely owned and/or operated by the private sector. Differentiating critical from non-critical assets within the transportation sector alone is a formidable task. One report by the National Research Council describes the extent of the U.S. domestic transportation system as follows:

> Transportation systems require vast amounts of physical infrastructure and assets. The U.S. highway system consists of 4 million interconnected miles of paved roadway, including more than 45,000 miles of Interstate freeway and 600,000 bridges. Freight rail networks extend for more than 300,000 miles, and commuter and urban rail systems cover some 10,000 miles. Even the more contained civil aviation system has around 500 commercial-service airports and another 14,000 smaller general aviation airports scattered across the country. These networks also contain many other fixed facilities, such as terminals, navigation aids, switchyards, locks, maintenance bases, and operation control centers.[42]

The Solarium Commission prioritizes certain critical infrastructure for greater protection by narrowing the definition even further to that which is "systemically important." This still constitutes, however, an enormous list of private actors. The Commission characterizes systemically important critical infrastructure as those entities that "manage systems and assets whose disruption could have cascading, destabilizing effects on U.S. national security, economic security, and public health and safety."[43] By this definition, the Commission is referring to national critical functions that support national security programs, government or military operations, essential

---

[40] 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, 84 Stat. 1116.

[41] CISA, *Critical Infrastructure Sectors*, https://www.cisa.gov/critical-infrastructure-sectors (last visited May 1, 2021).

[42] TRANSPORTATION RESEARCH BOARD STAFF, DETERRENCE, PROTECTION, AND PREPARATION: THE NEW TRANSPORTATION SECURITY IMPERATIVE 13 (2002); *see also,* U.S. DEP'T OF TRANSP., BUREAU OF TRANSP. STAT., TRANSPORTATION STATISTICS ANNUAL REPORT 2020 (2020), https://rosap.ntl.bts.gov/view/dot/53936.

[43] U.S. CYBERSPACE SOLARIUM COMM'N, *supra* note 2, at 96.

economic functions, the national distribution of goods and services, and public health and safety that are so foundational that their disruption could endanger human life on a massive scale.[44] Examining just one of these sectors more closely reveals a sizeable number of potential private actors under layered cyber deterrence. With regard to public health alone, out of the 6,090 hospitals in the United States, only 208 are owned or operated by the federal government.[45] Thus, one can begin to appreciate both the enormity and complexity of this whole-of-nation strategy and how the attribution of a major indiscretion by even one private auxiliary or instrument can have significant legal, political, and economic implications for the United States under layered cyber deterrence.

The U.S. also would not be permitted to stand idly by while a non-State actor within its territory carries out a known unlawful cyber operation that benefits the U.S. government. In some instances, the United States' failure to terminate a cyber operation conducted by a non-State actor within its territory would constitute a breach of the requirement to exercise due diligence.[46] Many States use proxies and non-State actors to perpetrate malicious cyber operations that ultimately threaten international peace and security and weaken the rules-based international order.[47] Russia, for example, has repeatedly denied its involvement in numerous cyberattacks against the United States, Ukraine, and other States, but evidence confirms that much of it was carried out by private Russian actors, some of whom purportedly were acting on behalf of the State. The vast public-private partnership contemplated under layered cyber deterrence, however, places a considerable burden on the federal government to maintain its due diligence obligations in the face of an exponentially higher number of new actors. Analogous to voluntarily assuming a duty where there was none that results in tort liability, the United States now could be liable for the actions of non-governmental, private sector conduct that it otherwise would not have been prior to layered cyber deterrence. This is particularly concerning given that some private companies may lack the requisite technical capabilities or business acumen to effectively engage U.S. adversaries under this new strategy.

A closer, more collaborative public-private partnership also means that the federal government may have a greater awareness of private actors' misconduct yet lack the control beforehand to do anything about it. Similar to a State's due diligence obligation, such actual or

---

[44] *Id.* at 98.

[45] SHARON MCDANIEL, FAST FACTS ON U.S. HOSPITALS (Jan. 2021), https://www.aha.org/system/files/media/file/2021/01/Fast-Facts-2021-table-FY19-data-14jan21.pdf.

[46] TALLINN MANUAL 2.0, *supra* note 34, at 175.

[47] Joint Statement on Information and Telecommunications in the Context of International Security (Oct. 26, 2018), https://www.international.gc.ca/world-monde/international_relations-relations_internationales/un-onu/statements-declarations/2018-10-26-info_telecommunications.aspx?lang=eng).

constructive knowledge could impose a duty on the federal government to take all feasible measures to terminate cyber operations that produce serious adverse consequences in other States or that otherwise affect their rights under international law.[48] A failure to take such measures means the United States could be legally responsible for the actions of an enormous number of private individuals and entities acting in the cyber realm. Layered cyber deterrence and its whole-of-nation partnership is an expansive net that is virtually impossible for the United States to fully comply with at all times. Moreover, the U.S. could face international backlash and become the target of countermeasures for private sector misconduct it neither sanctioned nor requested.

On the other hand, proving the connections between private actors and a State can be difficult in many cases. This can allow a State to accomplish its cyber objectives through private operatives while potentially avoiding both attribution and retribution. Under layered cyber deterrence, the public-private entanglement allows a larger number of actors to conduct cyber operations on behalf of the U.S. government that potentially contravene international laws or norms, yet shield the United States from legal responsibility.[49] Put another way, U.S. involvement with a non-State actor to further layered cyber deterrence may violate international law even if the cyber operation cannot be attributed to the United States. Suppose that under the layered cyber deterrence strategy, a private U.S. company merely provides technical knowledge to an insurgent group in another State that allows the group, on its own initiative, to attack its own government that ultimately furthers U.S. interests. The mere provision of this technical knowledge may be insufficient to attribute the group's operation to the United States. Depending on the facts, however, it may violate international law as an unlawful intervention into the internal affairs of another State or a prohibited use of force.[50]

---

[48] TALLINN MANUAL 2.0, *supra* note 34, at 43.

[49] U.S. Department of Defense, *DOD Has Enduring Role in Election Defense*, U.S. CYBER COMMAND (Feb. 10, 2020), https://www.defense.gov/Explore/News/Article/Article/2078716/dod-has-enduring-role-in-election-defense/. "'[The FBI will] engage with social media companies,' [NSA election security lead, David] Imbordino said. 'That information can enable a social media company to then use their platform, where they have very unique insights that we don't have, to mitigate and potentially unravel [malicious] social media influence campaigns.'" *Id.* "When NSA and Cybercom see a cyberattack happening against a certain victim, they communicate that information to appropriate government offices, which, in turn, work with private-sector partners to provide notification and enable future cyber defense." *Id.*

[50] *See* TALLINN MANUAL 2.0, *supra* note 34, Rules 66 and 68 and the comments thereunder.

C. Legal Challenges with the Distinction Principle and the Disclosure of Private Information

There are other concerns for the United States under layered cyber deterrence's public-private partnership. Under the law of war, parties to a conflict are required to segregate civilians and civilian objects from military objectives and protect them from the dangers of military operations to "the maximum extent feasible."[51] If private companies are now engaged in this whole-of-nation approach to fighting cyberwarfare under the layered cyber deterrence strategy, they, along with their hardware, software, networks, and communications systems, can become

legitimate targets for U.S. adversaries during armed conflict and are owed a duty of protection by the federal government.[52] Time and again, however, the federal government has demonstrated its inability to even protect itself from debilitating cyberattacks. Moreover, the increased entanglement between public and private sector cyber activities will make it exceedingly difficult for the United States to segregate its cyber capabilities from civilian objects.

There also is the practical reality of precisely how this public-private partnership will work. One key to the success of layered cyber deterrence is the free-flowing exchange of cyber information and data between the two sectors. But here again, given the divergent interests and market forces at play in the private sector, query whether companies will be forthcoming and transparent when the U.S. government begins asking for information and data to protect national security. Sharing private information will raise confidentiality and privacy issues, and companies will have an obligation to their customers, boards, and shareholders to not divulge this information without good faith efforts to protect it. Apple, for example, is increasingly framing privacy as a fundamental human right in its marketing campaigns and providing greater privacy controls on its iPhone to prevent third-party companies from tracking people's online activities.[53] The federal government, of course, can subpoena the information, but this process can be arduous, expensive, and perhaps most importantly, time-consuming in an environment in which time is of the essence and the need to respond to

---

[51] Protocol Additional to the Geneva Conventions of 12 Aug. 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) of 8 June 1977 *Article 58 — Precautions against the effects of attacks:* The Parties to the conflict shall, to the maximum extent feasible: a) without prejudice to Article 49 of the Fourth Convention, endeavor to remove the civilian population, individual civilians and civilian objects under their control from the vicinity of military objectives; b) avoid locating military objectives within or near densely populated areas; c) take the other necessary precautions to protect the civilian population, individual civilians and civilian objects under their control against the dangers resulting from military operations. *Id.*

[52] Jensen, *supra* note 18, at 1534–35.

[53] *See Privacy*, APPLE, https://www.apple.com/privacy/ (last visited July 1, 2021).

an adversarial cyber operation must be swift. Apple, Facebook, Microsoft, and other major tech companies have a history of fighting legal requests for data and are increasingly doing so following privacy violations during the 2020 U.S. presidential election. In 2015 and 2016, Apple challenged nearly a dozen orders issued by U.S. district courts seeking to compel it to extract data from locked iPhones and refused to cooperate with the U.S. Justice Department attempting to force it to unlock the iPhone of one of the killers in a mass shooting in San Bernardino, California.[54] Though not insurmountable, these legal maneuvers can pose a significant obstacle to the federal government's goal under layered cyber deterrence of obtaining cyber threat data as expeditiously and seamlessly as possible in response to cyberattacks.

D. The Strategy's Overly Defensive Posture and Overreliance on Deterrence by Denial

Another major shortcoming with the layered cyber deterrence strategy is its overreliance on deterrence by denial that the public-private partnership will only exacerbate. SolarWinds and numerous other successful cyberattacks aimed at critical infrastructure underscore that such a deep dependence on defensive measures for U.S. cybersecurity is misguided. Even if the federal government adopts all of the pillars and recommendations in the Solarium Commission Report, implementing them with the hope of ensuring complete cybersecurity would require strict compliance at all times by all employees and contractors of all parties, public and private, national and international alike. That, of course, will never happen. For one, unlike the federal government, market forces drive companies' business and risk management decisions and will lead some to avoid their obligations under the layered cyber deterrence strategy.[55] While the government undoubtedly will impose meaningful consequences for non-compliance, some companies will make cost-benefit calculations and act purely out of self-interest notwithstanding the strategy and imposition of penalties, or perhaps believing that the difficulties of cyber attribution will prevent their detection. Such is inevitable in a partnership in which one side is operating within a capitalist system based on free market principles. Integrating cybersecurity measures into new products will remain secondary for some companies' intent on quickly getting their products into the marketplace. Even companies that choose to play by the rules

---

[54] Jenna McLaughlin, *New Court Filing Reveals Apple Faces 12 Other Requests to Break into Locked iPhones,* THE INTERCEPT (Feb. 23, 2016), https://theintercept.com/2016/02/23/new-court-filing-reveals-apple-faces-12-other-requests-to-break-into-locked-iphones/.

[55] David Forscey & Herb Lin, *'Just Say No' Is Not a Strategy for Supply Chain Security*, LAWFARE (Mar. 25, 2020), https://www.lawfaremedia.org/article/just-say-no-not-strategy-supply-chain-security.

and adhere to layered cyber deterrence can pose vulnerabilities to U.S. infrastructure. For example, many private-sector, for-profit corporations have a fiduciary duty to seek lower cost vendors. This can pose security risks up and down the global information and communications technology supply chain as western companies routinely depend on components originating in non-western States.[56] Meanwhile, other well-meaning companies may interpret ambiguities in the layered cyber deterrence rules differently, resulting in reduced, arbitrary, or patchwork defenses that can put U.S. infrastructure at risk.

Convincing some governments and their overseas companies to abide by U.S. rules and guidelines under layered cyber deterrence also will be difficult for both political and practical reasons. As one example, over the past twenty years, nearly every major update to the internet that the United States has proposed has been rejected in other parts of the world. Those modest updates that *were* generally accepted, such as incremental improvements to authentication and digital certificate revocation, were purely voluntary, meaning that some entities could choose not to participate.[57] A company that, for whatever reason, chooses to use a vendor outside the accepted supply chain, reduces its cybersecurity due diligence, neglects to adhere to the layered cyber deterrence strategy, or otherwise intentionally or accidentally engages in any number of other risky behaviors, can place an entire sector of the U.S. infrastructure at risk as SolarWinds demonstrated. As we have seen, even a single misguided or disillusioned individual, such as an Evgeniy Bogachev, who some consider Russia's most notorious hacker, can cause substantial harm to the digital ecosystem.[58]

The United States today clearly is losing the struggle for deterrence by denial and its continued overreliance on its under layered cyber deterrence is destined for failure. Perfect cyber defense is impossible and decades of building defensive cyber measures and imposing minor counterattacks, countermeasures, and retorsions have failed to deter U.S. adversaries.[59] In fact, it likely has had the opposite effect, as the lack of any meaningful offensive strategy has produced a sharp increase in the number of major cyberattacks against the United

---

[56] *Id.* The U.S. government also relies almost exclusively on civilian vendors for computer software and hardware products, services, and maintenance. Jensen, *supra* note 18, at 1534–35.

[57] Roger A. Grimes, *The real reason we can't secure the internet*, CSO ONLINE (Dec. 27, 2016), https://www.csoonline.com/article/3152818/the-real-reason-we-cant-secure-the-internet.html.

[58] *FBI's Most Wanted: Evgeniy Mikhailovich Bogachev*, FED. BUREAU INVESTIGATION (last visited July 22, 2021), https://www.fbi.gov/wanted/cyber/evgeniy-mikhailovich-bogachev. *See generally*, Garrett M. Graff, *Inside the Hunt for Russia's Most Notorious Hacker,* WIRED (Mar. 21, 2017), https://www.wired.com/2017/03/russian-hacker-spy-botnet/. Bogachev created the malware named "Zeus" and its variants that were used to capture bank account numbers and logins and over $100 million. The malware affected over a million computers.

[59] ANN E. HAMMER, ET AL., CYBER RESILIENCE AS A DETERRENCE STRATEGY, SANDIA NATIONAL LABORATORIES (Sept. 2020), https://www.osti.gov/servlets/purl/1668133.

States in recent years. While the U.S. struggles to keep up and defend itself against millions of cyberattacks each day, its adversaries now use supercomputers rather than humans to run artificial intelligence algorithms all day, every day, to attack every IP address they can find on the Internet.[60] In a major cybersecurity development, the U.S. Department of Energy announced in 2020 that it was constructing a virtually un-hackable quantum internet, but cybersecurity experts say that nothing is un-hackable.[61] And given that a prototype will not be available for another ten years, it is not a viable deterrent option at present, particularly when a major cyberattack can be deployed in seconds or minutes, not months or years.[62] As with all technologies designed to make systems faster and safer, there will always be gaps in the system. The next generation of computers known as quantum computing is expected to perform calculations millions of times faster than current technology, but it also will render current Advanced Encryption Standard technology obsolete.[63] Absent countermeasures, this exponential increase in speed will jeopardize the security of all data transmitted via the internet today, including military, financial, and national security communications, and leave older computers and network systems increasingly vulnerable to security threats.[64]

---

[60] CISA, *supra* note 24.

[61] *U.S. Department of Energy Unveils Blueprint for the Quantum Internet at 'Launch to the Future: Quantum Internet' Event*, U.S. DEP'T ENERGY (July 23, 2020), https://www.energy.gov/articles/us-department-energy-unveils-blueprint-quantum-internet-launch-future-quantum-internet.

[62] Davey Winder, *U.S. Government Says It's Building A 'Virtually Unhackable' Quantum Internet*, FORBES (July 25, 2020), https://www.forbes.com/sites/daveywinder/2020/07/25/us-government-to-build-virtually-unhackable-quantum-internet-within-10-years/. ("There is no such thing as completely secure. A brand new and unboxed computer might have had malware installed somewhere along the supply chain, and the operating system will likely have vulnerabilities.... Great, in theory. In practice, and there are plenty of [quantum key distribution] networks operating already, it's the weak spots such as optical fiber termination points, switches and connections that will be targeted by hackers. Not forgetting the human element, be that by way of configuration errors, bad actors or social engineering attacks. Security does not involve one single point of attack, quantum or otherwise.")

[63] Marissa Norris, *Quantum Computers Will Break The Internet, But Only If We Let Them,* RAND CORP. (Apr. 9, 2020), https://www.rand.org/blog/articles/2020/04/quantum-computers-will-break-the-internet-but-only-if-we-let-them.html; Lonergan & Lonergan, *supra* note 22 ("The modern battlefield is more interconnected than ever before....A breach in the weakest link can have severe consequences for the integrity of an entire mission...The department's ability to test and evaluate cyber vulnerabilities is not keeping pace with increasingly aggressive adversary attacks.").

[64] MICHAEL J. D. VERMEER & EVAN D. PEET, SECURING COMMUNICATIONS IN THE QUANTUM COMPUTING AGE: MANAGING THE RISKS TO ENCRYPTION 3, RAND CORP. (Apr. 9, 2020), https://www.rand.org/pubs/research_reports/RR3102.html.

E. Deterrence by Denial is a Necessary, but Ineffective Strategy

Cyber deterrence by denial has proven largely ineffective to date for the United States, yet the layered cyber deterrence strategy and its antecedents have placed a disproportionate emphasis on it for years. This is not to say that it should be abandoned. On the contrary, the U.S. must never be an easy target for its adversaries. One need only look to the consequences of Ukraine's weak cyber defenses against Russia's multi-year attacks on Kiev's infrastructure as Russia tested new cyberweapons and tactics.[65] But precisely because a cyberattack could devastate a State's infrastructure and economy, a much more resilient and offensive posture must be taken. The U.S. must not allow its adversaries to jeopardize critical infrastructure and put lives at risk as was done in Ukraine, let alone steal billions of dollars' worth of intellectual property and defense secrets, simply because the theft was by cyber and not by physical force. Repeated hacks of U.S. government networks demonstrate the destructive force of cyberattacks that can go virtually unnoticed or whose impact can be minimized because there is little tangible evidence of loss. CSIS maintains an ongoing report, currently over ninety pages long, that lists notable cyberattacks since 2006.[66] In one entry regarding a May 2006 attack on U.S. State Department networks by unknown foreign hackers in which terabytes of information were stolen, CSIS observed that, "If Chinese or Russian spies had backed a truck up to the State Department, smashed the glass doors, tied up the guards and spent the night carting off file cabinets, it would constitute an act of war. But when it happens in cyberspace, we barely notice."[67] One of the United States' first publicly known offensive cyber strikes against Russia designed to counter interference in U.S. elections likewise was scarcely noticed. In February 2019, the U.S. Cyber Command blocked internet access of the Internet Research Agency, a significant Russian online influence operation. As one commentator put it, "If the U.S. had done so using a missile (by, say, destroying the facility where the Internet Research Agency is located) it would have been an armed attack" and potentially the basis for armed retaliation.[68] And yet, neutralizing it via cyber means it largely evaded public scrutiny.

Despite the devastating impacts of such cyberattacks, the United States government has routinely treated them as espionage rather than acts of war, and it has responded passively with measures that can best

---

[65] Andy Greenberg, *How an Entire Nation Became Russia's Test Lab for Cyberwar,* WIRED (June 20, 2017), https://www.wired.com/story/russian-hackers-attack-ukraine/.

[66] *Significant Cyber Incidents Since 2006*, CTR. FOR STRATEGIC & INT'L STUD., https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents (last updated Dec. 2023).

[67] *Id.*

[68] Paul Rosenzweig, *The New Contours of Cyber Conflict,* LAWFARE (Feb. 27, 2019, 12:19 PM), https://www.lawfaremedia.org/article/new-contours-cyber-conflict.

be described as merely annoying. Annoyance, however, is not enough to deter sophisticated adversaries who have launched repeated, major cyberattacks against the U.S., stealing billions of dollars' worth of sensitive data and costing hundreds of billions more in defensive measures and lost productivity. Global losses from cybercrime now total over $1 trillion, representing a more than 50 percent increase from 2018.[69] By some estimates, global cyber crime is expected to reach $10.5 trillion dollars annually by 2025.[70] However, as one Defense Department official described the new U.S. cyber strategy, "Part of our objective is to throw a little curveball, inject a little friction, sow confusion."[71] But pinpricks, curveballs, and sand-throwing are not effective deterrent strategies when faced with millions of sophisticated attacks daily against critical U.S. infrastructure. U.S. deterrence must be in kind or greater. And more importantly, U.S. adversaries must expect such a response. Offensive cyber operations must cause them to rethink their attack calculations. And to do so, the U.S. must invest not only in cyber defense that raises adversaries' costs of achieving their goals, but also much more aggressively in cyber resilience[72] and offensive operations both below, and if necessary, above the line of armed conflict. Having maximized its

---

[69] James Andrew Lewis et al., *The Hidden Costs of Cybercrime,* CTR. FOR STRATEGIC & INT'L STUD. (Dec. 9, 2020), https://www.csis.org/analysis/hidden-costs-cybercrime; Tom Gann, *The Hidden Costs of Cybercrime on Government,* MCAFEE (Dec. 21, 2020), https://www.mcafee.com/blogs/other-blogs/executive-perspectives/the-hidden-costs-of-cybercrime-on-government/.

[70] Steve Morgan, *Cybercrime To Cost The World $10.5 Trillion Annually By 2025,* CYBERCRIME MAG. (Nov. 13, 2020), https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/ ("Cybersecurity Ventures expects global cybercrime costs to grow by 15 percent per year over the next five years reaching $10.5 trillion USD annually by 2025....The damage cost estimation is based on historical cybercrime figures including recent year-over-year growth, a dramatic increase in hostile nation-state sponsored and organized crime gang hacking activities, and a cyberattack surface which will be an order of magnitude greater in 2025 than it is today. Cybercrime costs include damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, postattack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm.").

[71] Ellen Nakashima, *U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms*, WASH. POST (Feb. 27, 2019), https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html#.

[72] HAMMER ET AL., *supra* note 59, at 7. Layered cyber deterrence incorporates cyber resilience as part of its layer two strategy of denying benefits. Cyber resilience acknowledges that perfect defense in the cyber realm is impossible. It differs from cyber deterrence by focusing less on threats of retaliation (deterrence by punishment) and denying adversaries' aims (deterrence by denial). *Id.* at 12. Instead, it emphasizes the ability to adapt to changing conditions and withstand and recover quickly from disruptions. Key cyber resilience concepts include having systems in place that minimize the impact of an attack, sustaining operations during an attack, and recovering and adapting to new conditions after an attack. *Id.* at 7.

denial and resilience capabilities, clearly signaled its intent to respond swiftly and decisively to well-defined red line attacks and attributed the attack with reasonable certainty to a particular adversary, the United States must then use all means necessary to punish and deter future attacks. Cyber deterrence by denial and resilience, therefore, must be accompanied by deterrence by punishment.

III. DETERRENCE BY PUNISHMENT AND THE THREAT OR USE OF FORCE

Throughout its report, the Cyberspace Solarium Commission paints a dire picture of U.S. cybersecurity readiness and suggests that the country faces an imminent cyber disaster unless bold action is taken. As the Report notes:

> Our country is at risk, not only from a catastrophic cyberattack, but from millions of daily intrusions disrupting everything from financial transactions to the inner workings of our electoral system.... A major cyberattack on the nation's critical infrastructure and economic system would create chaos and lasting damage exceeding that wreaked by fires in California, floods in the Midwest, and hurricanes in the Southeast.[73]

Given these potential catastrophic consequences, the Solarium Commission acknowledges deterrence through some form of punishment as a component of its strategy, though it uses terms such as "punish" or "punishment" fewer than twenty times throughout its 181-page Report.[74] Instead, the Commission uses vague language that the U.S. must be prepared to "impose costs" to deter its adversaries and, if necessary, "fight and win in conflict using all instruments of national power."[75] Layered cyber deterrence thus attempts to advance existing

---

[73] U.S. CYBERSPACE SOLARIUM COMM'N, *supra* note 2, at v.
[74] *Id.* at v–vi.
[75] *Id.*

> To best implement layered cyber deterrence, *the United States must be prepared to impose costs to* deter and, *if necessary; fight and win in conflict,* as well as counter and reduce malicious adversary behavior below the level of armed conflict. *Therefore, this pillar comprises implementing defend forward in day-to-day competition to counter adversary cyber campaigns and impose costs, as well as being prepared to prevail in crisis and conflict. Importantly, the military instrument of cyber power is intended to complement, rather than supplant, other instruments.* The result *is* the coordinated employment of all instruments of national power.

Id. at 110 (emphasis added).

U.S. policy in reserving the right to use all means in responding to a major cyberattack, though this is far from clear.

While it is not the first time such a policy has been expressed, it is nevertheless one of the more forcefully articulated to date. In May 2011, the Obama Administration stated its willingness to use force in response to a serious cyberattack. Emphasizing the importance of deterrence, the White House issued a brief report stating that certain hostile acts in cyberspace also could trigger a U.S. military response.[76] It did not, however, identify what those hostile acts might be and it came at the end of a rather quixotic report describing the internet in lofty terms as a place where is hoped that norms of responsible, just and peaceful conduct among States and peoples will flourish.[77] The United States also declared its intention to use force in response to a major cyberattack in its 2019 National Defense Authorization Act (NDAA). Section 1632 of the NDAA allows the U.S. Cyber Command to take proportionate action in response to active, systematic, and ongoing campaigns by Russian, Chinese, Iranian, and North Korean cyberattacks as determined by the National Command Authority and defines those responses as constituting traditional military activities.[78]

Current U.S. cyber practice, however, still lacks three fundamental ingredients necessary to deter U.S. adversaries even as layered cyber deterrence is rolled out: Credibility; a clear definition of what adversary actions will result in retaliation; and the imposition of strong, meaningful consequences. All three are necessary to better defend U.S. cyber

---

[76] THE WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD 14 (May 2011). As the report states:

> [w]hen warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. All States possess an inherent right to self-defense, and we recognize that certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners. *We reserve the right to use all necessary means—diplomatic, informational, military, and economic—as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests*. In so doing, we will exhaust all options before military force whenever we can; will carefully weigh the costs and risks of action against the costs of inaction; and will act in a way that reflects our values and strengthens our legitimacy, seeking broad international support whenever possible.

Id. (emphasis added); *See also* Thomas Rid, *Cyber War Will Not Take Place,* 35 J. OF STRATEGIC STUD. 5, 29 (2012); *Id.* at 14 n.70. In May 2011, the Obama White House stressed deterrence in cyberspace and made clear that "certain hostile acts conducted through cyberspace" could trigger a military response by America (in using "all necessary means", the document explicitly included military means). But the White House did not make clear what certain hostile acts (p. 14) or "certain aggressive acts in cyberspace" (p. 10) actually mean. THE WHITE HOUSE, *supra* note 76, at 10–14.

[77] THE WHITE HOUSE, *supra* note 76, at 14.

[78] John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, 132 Stat. 1636 (2018) [hereinafter FY2019 NDAA].

networks. U.S. cyber policy will only be as effective as its cyber practices and such practices must include the third layer of layered cyber deterrence, cost imposition. Those cyberattacks that cause substantial harm to U.S. national security and economic prosperity must be of the highest order and dealt with much more forcefully than has been done in the past. Attacks that cause outright destruction must be distinguished from, and responded to differently than, those involving mere intelligence gathering. It is no secret that the U.S., like many States, engages in large-scale cyber espionage operations and will continue doing so. While damaging and disruptive, such conduct is neither unexpected nor unlawful. However, the United States must do a better job of distinguishing such conduct with cyberattacks against it that threaten critical infrastructure, damage essential computer systems, and interfere with political elections. Moreover, the United States must clearly signal its intent to swiftly, fully and unequivocally respond to attacks that meet certain criteria. Once attribution is reasonably certain, meaningful action must be taken. Consistency in responding to repeated major cyberattacks is critical to signal the United States' determination to follow through on its commitment to layered cyber deterrence and signal a shift in past practice from acquiescence and weakness to action and strength. Our adversaries must know that repeated, major cyberattacks against U.S. infrastructure will not be tolerated and is not worth the costs of engagement. Nations such as North Korea and Iran, in particular, have shown remarkable resilience to U.S. political and economic pressure and may be difficult to deter without credible threats of military action.

The Biden administration had the opportunity to demonstrate the United States' commitment to layered cyber deterrence and cost imposition in response to Russia's SolarWinds attack, interference in U.S. elections, and other abuses. Unfortunately, the U.S. reaction was tepid at best and unlikely to achieve the goal of deterring future cyberattacks from Russia or other adversaries. Despite signaling in the Solarium Commission Report the United States' intent to respond swiftly and decisively to attacks of this magnitude, and the U.S. attributing the attacks with reasonable certainty to Russia's Foreign Intelligence Service, the federal government stopped short of a strong and forceful response. Instead, it imposed financial sanctions on several entities and individuals and expelled ten officials from Russia's U.S. diplomatic mission. Though many viewed this as the strongest U.S. response to date and a watershed moment in breaking with years of tolerating cyber espionage, it was remarkably weak for several reasons.[79] First, not surprisingly, Russia simply denied its involvement and expelled ten U.S. embassy staff in a tit-for-tat rejoinder, punishing the United States the same way it

[79] Turak & Macias, *supra* note 30.

punished Russia and providing the U.S. with a zero sum gain.[80] Second, retorsions generally are viewed as mere slaps on the wrist. They are intended to send a message of disapproval to the wrongdoer rather than carry any meaningful punitive value. Third, the U.S. response did nothing to address the enormous toll the SolarWinds attack took on the private sector. It is estimated that approximately one hundred companies were impacted by the attack and the burden of repairing the damage largely fell on them.[81] Fourth, further explanation was required as to why Russia's behavior in this case merited a more aggressive response than a typical cyber espionage attack. It thus was a missed opportunity to link the U.S. response to a more clearly-defined policy of zero tolerance and cost imposition under layered cyber deterrence for attacks that cause substantial harm to major U.S. national security and economic interests. Lastly, and perhaps most importantly, it did little to deter subsequent attacks and to significantly impact U.S. adversaries' future cost-benefit calculations. In short, given the lackluster U.S. response, there was little disincentive for Russia or any other State to not do it again and again.[82]

A. International Law and the Threat or Use of Force

Given the increasing frequency and severity of recent cyberattacks on critical U.S. infrastructure such as those on a Kansas nuclear power plant in 2017 (the Wolf Creek Nuclear Operating Corporation), one of the nation's largest gas pipelines in May 2021 (Colonial Pipeline), a Florida city's water supply in February 2021 (Oldsmar water treatment facility), and one of the world's largest meat producers in May 2021 (JBS USA) to

---

[80] Gleb Stolyarov et al., *Putin Warns West of Harsh Response if it Crosses Russia's 'Red Lines',* REUTERS (Apr. 20, 2021, 6:16 PM), https://www.reuters.com/world/europe/navalny-supporters-seek-drown-out-putin-speech-with-mass-protests-2021-04-20/.

[81] Dustin Volz, *In Punishing Russia for SolarWinds, Biden Upends U.S. Convention on Cyber Espionage,* WALL ST. J. (Apr. 17, 2021, 5:30 AM), https://www.wsj.com/articles/in-punishing-russia-for-solarwinds-biden-upends-u-s-convention-on-cyber-espionage-11618651800.

[82] According to Maximilian Hess, head of political risk at London-based advisory firm Hawthorn Advisors, "The key portion" of these sanctions "is the barring of U.S. entities from the primary market for ruble-denominated debts by the Russian government." However, Hess noted, this "will not have a major impact, particularly given Russia's manageable debt load." For Timothy Ash, senior emerging markets strategist at Bluebay Asset Management, *the measures are far from harsh*. "It's like guys, come on, you need to do better than this," Ash wrote in a note following the announcement. "Sovereign primary still allows U.S. entities to hold this debt. So U.S. institutions cannot buy Russian sovereign debt in primary issuance, but can get their Russian bank friends to buy it for them in primary, give them a fee, and then buy it in the secondary." Turak & Macias, *supra* note 30 (emphasis added).

name a few,[83] why does the United States *not* respond much more aggressively? At what point can and should the U.S. use force or threats of force to stop these cyberattacks that continually threaten and harm critical U.S. infrastructure?

One reason is that many existing international laws that govern States' threats, uses of force, and obligations to peacefully settle their disputes apply in cyberspace. Article 2(4) of the United Nations Charter makes no distinction as to the means by which States are prohibited from using threats or force against the territorial integrity or political independence of another State.[84] Similarly, Chapter 6 of the United Nations Charter instructs States to peacefully settle their disputes that threaten international peace and security regardless of the types of disputes States may have, and Rule 65 of the Tallinn Manual specifically applies this obligation to States' conduct in cyberspace.[85] The Tallinn Manual further provides that any cyber activity that constitutes a threat or use of force against the territorial integrity or political independence of any State, or that is in any other manner inconsistent with the purposes of the United Nations, is unlawful.[86]

With regard to *jus in bello* principles, the Tallinn Manual states that the law of war applies to cyber operations in an armed conflict.[87] Although the U.S. Department of Defense's position is that cyber operations do not rise to the level of armed conflict and thus the principles of military necessity, proportionality, and distinction do not apply, the Department says it applies the law of war anyway, regardless of the context.[88]

---

[83] Rishi Iyengar & Clare Duffy, *Hackers have a devastating new target,* CNN BUS. (June 4, 2021, 7:19 AM), https://www.cnn.com/2021/06/03/tech/ransomware-cyberattack-jbs-colonial-pipeline/index.html.

[84] U.N. Charter art. 2, ¶ 4.

[85] Rule 65 of the Tallinn Manual entitled, "Peaceful settlement of disputes" provides that, "(a) States must attempt to settle their international disputes involving cyber activities that endanger international peace and security by peaceful means. (b) If States attempt to settle international disputes involving cyber activities that do not endanger international peace and security, they must do so by peaceful means." TALLINN MANUAL 2.0, *supra* note 34, at 303.

[86] Rule 68 of the Tallinn Manual entitled "Prohibition of threat or use of force" states that, "[a] cyber operation that constitutes a threat or use of force against the territorial integrity or political independence of any State, or that is in any other manner inconsistent with the purposes of the United Nations, is unlawful." *Id.* at 329.

[87] Rule 80 of the Tallinn Manual entitled "Applicability of the law of armed conflict" states that, "[c]yber operations executed in the context of an armed conflict are subject to the law of armed conflict." *Id.* at 375.

[88] Hon. Paul C. Ney, Jr., General Counsel, Dep't of Def., Remarks at U.S. Cyber Command Legal Conference (Mar. 2, 2020).

> It is also longstanding DoD policy that U.S. forces will comply with the law of war "during all armed conflicts however such conflicts are characterized and *in all other military operations."* Even if the law of war does not technically apply because the proposed military cyber

With regard to *jus ad bellum* principles, both the International Court of Justice and the Tallinn experts broadly interpret their application to contexts other than traditional military activities. In its 1996 advisory opinion entitled *Legality of the Threat or Use of Nuclear Weapons*, the International Court of Justice held that both the prohibition on the use of force and the self-defense doctrine apply to "any use of force, regardless of the weapons employed."[89] Likewise, the Tallinn Manual experts unanimously applied this reasoning to cyber warfare, stating that:

> [T]he mere fact that a computer (rather than a more traditional weapon, weapon system, or platform) is used during an operation has no bearing on whether that operation amounts to a 'use of force' (or, for that matter, whether a State may use force in self-defence pursuant to

---

> operation would not take place in the context of armed conflict, DoD nonetheless applies law-of-war principles. This means that the *jus in bello* principles, such as military necessity, proportionality, and distinction, continue to guide the planning and execution of military cyber operations, even outside the context of armed conflict.

Id.

[89] Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 22 (July 8). In paragraphs 38 and 39 of the advisory opinion, the International Court of Justice states as follows:

> 38. The Charter contains several provisions relating to the threat and use of force. In Article 2, paragraph 4, the threat or use of force against the territorial integrity or political independence of another State or in any other manner inconsistent with the purposes of the United Nations is prohibited. That paragraph provides:
>
> "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the Purposes of the United Nations."
>
> This prohibition of the use of force is to be considered in the light of other relevant provisions of the Charter. In Article 51, the Charter recognizes the inherent right of individual or collective self-defense if an armed attack occurs. A further lawful use of force is envisaged in Article 42, whereby the Security Council may take military enforcement measures in conformity with Chapter VI1 of the Charter.
>
> 39. *These provisions do not refer to specific weapons. They apply to any use of force, regardless of the weapons employed. The Charter neither expressly prohibits, nor permits, the use of any specific weapon, including nuclear weapons.* A weapon that is already unlawful *per se*, whether by treaty or custom, does not become lawful by reason of its being used for a legitimate purpose under the Charter. (emphasis added).

> Rule 71). In the cyber context, it is not the instrument used that determines whether the use of force threshold has been crossed, but rather, as described in Rule 69, the consequences of the operation and its surrounding circumstances.[90]

Another reason why threats or force have not been used in response to major cyberattacks is likely that Russia and other States have already positioned themselves to disrupt U.S. critical infrastructure in the event of a conflict. Responding to a Russian or Chinese cyberattack with threats or force may unleash unknown harm to U.S. national interests, and an unknown threat often can be more debilitating than a known threat. Allowing major cyberattacks to continue without major consequences, however, is not an effective option either.

B. The Threat or Use of Force Under Layered Cyber Deterrence

This leads to the question of when a cyber activity constitutes an unlawful use or threat of force under layered cyber deterrence. Several sources address this question, including the Tallinn Manual, current U.S. policy, the U.N. Charter and customary international law, as well as the third layer of layered cyber deterrence discussed in the Solarium Commission Report. According to the Tallinn Manual, an unlawful use of force in cyberspace occurs when the scale and effects of the cyber act are comparable to non-cyber operations that rise to the level of a use of force.[91] With regard to unlawful cyber *threats*, Rule 70 provides that they are unlawful when, if carried out, they would constitute "an unlawful use of force."[92] An operation is less likely to be deemed a use of force under the Tallinn Manual if its effects have a limited scope, duration, and intensity and the attack does not cause physical damage, bodily harm, or, most importantly, casualties.[93] The manual offers eight factors to consider in analyzing whether a cyber act constitutes a use of force. They include the severity of the harm, the immediacy of the results, the directness between the cause and effect of the cyber act, the invasiveness into the target State, the measurability of the cyber act's effects, the

---

[90] TALLINN MANUAL 2.0, *supra* note 34, at 328. Paragraph 1 of Chapter 14 on the use of force also states that, "The International Court of Justice has stated that Articles 2(4) (Rules 68-70) and 51 (Rule 71-5) of the United Nations Charter, regarding the prohibition of the use of force and self-defense respectively, apply to 'any use of force, regardless of the weapons employed'." *Id.*

[91] *Id.* at 330.

[92] *Id.* at 338.

[93] Jeff Kosseff, *The Contours of* 'Defend Forward' *Under International Law*, *in* 2019 11th INTERNATIONAL CONFERENCE ON CYBER CONFLICT: SILENT BATTLE 6 (T. Minárik et al. eds., 2019), https://ccdcoe.org/uploads/2019/06/Art_17_The-Contours-of-Defend-Forward.pdf.

military character of the cyber act, the degree of the offending State's involvement, and the presumptive legality of the act.[94]

Current U.S. policy acknowledges that a cyberattack can rise to the level of a use of force under Article 2(4) of the United Nations Charter and customary international law if it satisfies a so-called "effects test." According to the Department of Defense, a cyberattack can constitute a use of force if it causes physical injury or damage that would be deemed a use of force if caused solely by traditional means, such as with a missile or land mine.[95] While layered cyber deterrence allows for an outcome in which the U.S. deploys the full force of its military to deter its adversaries under those circumstances, the Pentagon has stopped short of saying that the use of force threshold can be crossed in other instances, such as a major cyberattack on vital data and networks in a State's financial system.[96] The Pentagon's position thus appears inconsistent with the Tallinn factors and commentary on the use of force that considers more than just the nature and severity of the act. For example, suppose the United States provided an organized armed rebel group with malware and training necessary to carry out a cyberattack on an adversary State's dam control system that, over the period of several days, led to flooding and drownings. Such a result might not rise to the level of a use of force under current U.S. policy because the malware and training did not immediately and directly cause physical injury or damage as with an explosive device in a crowded street or a rocket attack on a commercial building. It may, however, rise to the level of an unlawful use of force under the Tallinn Manual if the additional criteria mentioned above are considered, particularly the legality of the act, the degree of U.S.

---

[94] TALLINN MANUAL 2.0, *supra* note 34, at 333–47.

[95] Ney, Jr., *supra* note 88.

> *Depending on the circumstances, a military cyber operation may constitute a use of force within the meaning of Article 2(4) of the U.N. Charter and customary international law*. In assessing whether a particular cyber operation—conducted by or against the United States—constitutes a use of force, DoD lawyers consider *whether the operation causes physical injury or damage that would be considered a use of force if caused solely by traditional means like a missile or a mine*. Even if a particular cyber operation does not constitute a use of force, it is important to keep in mind that the State or States targeted by the operation may disagree, or at least have a different perception of what the operation entailed. (emphasis added).

See also Robert Chesney, *The Pentagon's General Counsel on the Law of Military Operations in Cyberspace,* LAWFARE (Mar. 9, 2020, 12:33 PM), https://www.lawfaremedia.org/article/pentagons-general-counsel-law-military-operations-cyberspace.

[96] *See* Chesney, *supra* note 94.

involvement, the invasiveness into the target State, and the measurability of the cyber act's effects.[97]

Malware implanted into the *domaine réservé* of a State could, depending on the severity of its consequences, constitute a prohibited use of force under Article 2(4) of the United Nations Charter and customary international law.[98] There is a lack of consensus, however, regarding the point at which a cyber operation becomes a prohibited use of force. Clearly an operation that causes death or substantial bodily injury would qualify. Substantial property damage or severe economic or political consequences might qualify as well, but there is less certainty. Anything below that is unlikely to be deemed a use of force.[99]

Turning to the Solarium Commission Report, the third layer of cyber deterrence is the most aggressive of the three tiers from a military engagement vantage point. While the current defend forward policy applies to cyber operations that fall below the level of a use of force, layered cyber deterrence in theory includes the use of all forms of military power to protect U.S. interests.[100] At several places in the Report, the

---

[97] Like a double-edged sword, this position also can cut against the U.S. For example, if the U.S. adopts a policy that any cyberattack on its financial systems does, in fact, constitute a use of force, then any cyberattack the U.S. initiates on another State's financial system likewise can be deemed an unlawful use of force.

[98] U.N. Charter art. 2, ¶ 4.

[99] *See generally* Michael Schmitt, *U.S. Cyber Command, Russia and Critical Infrastructure: What Norms and Laws Apply?*, JUST SEC. (June 18, 2019), https://www.justsecurity.org/64614/u-s-cyber-command-russia-and-critical-infrastructure-what-norms-and-laws-apply/.

[100] U.S. CYBERSPACE SOLARIUM COMM'N, *supra* note 2, at 23. According to the Solarium Commission Report, critical to implementing the layered cyber deterrence strategy is the prospect of employing the full instrument of military power. Although the term "military instrument" is not universally defined, the concepts of force, threat of force, and force enabling are at its core. The National War College defines force in its national security strategy primer as, "[T]the application of violence by one party to coerce, subdue or eradicate another, and it can occur in any domain (Land, Sea, Air, Space, and Cyber)." SCOTT M. CHAMBERS (CIV US NDU/CASL), NATIONAL SECURITY PRIMER FOR AY21 16–7 (2017), https://www.scribd.com/document/480687835/National-Security-Primer-for-AY21.

> The military instrument of power entails applying, threatening to apply, or enabling other parties to apply or threaten to apply force in furtherance of political aims. The use of the military instrument in war is potentially the most dangerous action a state can undertake; strategists and leaders should apply it only with a clear understanding and assessment of its nature, capabilities, limitations, and costs/risks. Though there are no universally accepted definitions of the aspects of the military instrument, the concepts of "Force," "Threat of Force," and "Force Enabling" capture its essence and provide an appropriate framework for such assessment.
>
> – Force is the application of violence by one party to coerce, subdue or eradicate another, and it can occur in any domain (Land, Sea, Air, Space, and Cyber). Force may include overt, clandestine, and covert

> activities; small-unit actions; single targeted strikes; employment of proxies; the use of destructive cyber power; or any other activity in which violence is applied to achieve political aims and their associated specific objectives.
>
> – Threat of force is used to modify coercively an adversary's current behavior or shape its future actions. Like force, the threat of force is used to achieve political aims, it can be used either defensively/preventatively to *deter* an adversary from initiating damaging action for fear of the consequences, or offensively to *compel* an adversary into ceasing damaging action or giving up something of value. In either case, the key determinant of effectiveness is credibility; the adversary must believe in both one's *capability and willingness* to make good on the threat. Moreover, the threat of force can be *explicit or implicit;* diplomats and heads of state frequently express or imply it in diplomatic messages, adding weight to the diplomatic instrument of power.
>
> – Force enabling consists of improving the capacity/capability of international partners to apply or threaten force and encompasses a wide array of concepts. It may be used to help state or non-state actors bolster their military capability, to improve state or regional security, to enhance elements or institutions of military power, to make an allied or aligned state a more effective partner, or to link a foreign state to one's own by way of military cooperation. Force enabling activities are frequently, though not exclusively, conducted by the armed forces and intelligence services. Such efforts often tie closely the diplomatic, information, and economic instruments.

Id. The Solarium Commission Report makes clear that force or threats of force are one tool to combat the strategic realities of consistent, destructive cyberattacks against the United States. As its authors describe it:

> [T]he U.S. government must maintain ready and resilient military capabilities. These include cyber tools to be employed as an independent military capability and as enablers of conventional operations and campaigns.... These strategic realities create an imperative for the United States to preserve and employ the military instrument of power in and through cyberspace, including the intersection of cyberspace with conventional and nuclear military capabilities, while deliberately managing potential escalation risks.

U.S. CYBERSPACE SOLARIUM COMM'N, *supra* note 2, at 110–111.

Moreover, it is not just the threat or use of force that undergirds layered cyber deterrence, the strategy also commits the United States to gaining access, pursuing adversaries where they operate, and "deliver[ing] effects against adversary infrastructure and capabilities." *Id.* The Solarium Commission Report consequently expands the defend forward logic by incorporating both non-military and military instruments of power. *Id.* at 110.

> The Commission reimagines and expands the core logic of [the Department of Defense's] concept of defend forward to incorporate both military and non-military instruments of power.... To accomplish

Solarium Commission affirms the United States' commitment to impose costs to not only deter cyberattacks, but if necessary, prevail in war by employing the full spectrum of its capabilities.[101] For obvious political

---

> objectives in support of defend forward, credible deterrence, and the ability to win if deterrence fails, the U.S. government must maintain ready and resilient military capabilities. These include cyber tools to be employed as an independent military capability and as enablers of conventional operations and campaigns.

Id.

More specifically, the Solarium Commission report recommends that the United States declare a new two-tiered policy defining the use of force for deterrence purposes to communicate its resolve that cyberattacks will be met with serious and immediate consequences. This two-tiered approach suggests that the use of force is simply one of several options to respond to a cyber use of force. *Id.*

> The United States' declaratory policy regarding cyberspace now is organized around a use-of-force threshold – - which is deliberately politically and legally ambiguous – - and reserves the right for the United States to respond to a cyberattack in a time, place, and manner of its choosing. There are two notable challenges with the current stance.
>
> First, the existing declaratory policy does not sufficiently communicate resolve or articulate a compelling logic of consequences. Therefore, *the U.S. government should promulgate a new declaratory policy around a use-of-force threshold. Specifically, the U.S. government should publicly convey that it will respond using swift, costly, and, where possible, transparent consequences against cyber activities that constitute what the United States defines as a use of force.* This would reinforce deterrence of strategic cyberattacks.
>
> Second, our adversaries are clearly exploiting the current threshold to conduct a range of malicious activities that do not rise to a level warranting a major retaliatory response. Examples include cyber-enabled large-scale theft of intellectual property and cyber-enabled influence operations. Therefore, *the U.S. government should announce a second declaratory policy. This policy should clearly state that the United States will respond using cyber and non-cyber capabilities to counter and impose costs against adversary cyber campaigns below a use-of-force threshold.* These responses would create sufficient costs to alter the adversary's calculus, but they would be different from responses to adversary actions above the use-of-force threshold in their means (e.g., conventional vs. unconventional military capabilities) and their magnitude, consistent with international law. *Essentially, the U.S. government should publicly declare that it will defend forward, and couple its declaration with decisive and consistent action across all elements of national power.*

Id. (emphasis added.)

[101] *Id.* at 25. The Report states:

and legal reasons, the Solarium Commission stops short of stating that the United States will respond with lethal force against an adversary that launches a cyber attack, but it seems to imply it. And that may be precisely the point. The layered cyber deterrence strategy creates a veiled threat to use all military options to defend U.S. interests, presumably including conventional weapons, with the hope that signaling will deter adversaries from planning such attacks and the capability to use such force will prevent adversaries from initiating them.

And yet, the Report sends a mixed message in various places and once again fails to clearly signal the United States' intentions to U.S. adversaries under layered cyber deterrence. On the one hand, the third layer of the layered cyber deterrence strategy exhorts the United States to use all instruments of national power to protect its interests and signal to rival States the risks and costs of attacking it in cyberspace.[102] Recent

> In the third layer, the United States is prepared to impose costs to deter conflict, limit malicious adversary behavior below the level of armed conflict, *and, if necessary, prevail in war by employing the full spectrum of its capabilities*. Deterrence must extend to limiting attacks on the U.S. election system and preventing large-scale intellectual property theft. To that end, the *U.S. government must demonstrate its ability to impose costs using all instruments of power, while establishing a clear declaratory policy that signals to rival states the costs and risks associated with attacking America in cyberspace*. Defend forward is an important part of the cost imposition layer. The original defend forward concept put forth by DoD focuses on the military instrument of power to impose costs to "disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict." *Reimagined as a key element of layered cyber deterrence, defend forward in this context comprises the proactive and integrated employment of all of the instruments of power*. Defend forward requires the United States to have the capability and capacity for sustained engagement in cyberspace to impose costs on adversaries for engaging in malicious cyber activity. *The cost imposition layer also demands that the U.S. government protect its ability to respond with military force at a time and place of its choosing. A key aspect of this ability is ensuring the security and resilience of critical weapons systems and functions in cyberspace.*

Id. 25–26 (emphasis added). Though implied, the Report does not explicitly state that it reserves the right to use military, as opposed to strictly cyber, force to deter adversaries and engage in conflict. Likewise, it does not distinguish between traditional and cyber warfare, and traditional and cyber military force.

[102] *Id.* at 6. Layered cyber deterrence seeks to:

> maintain the capacity, resilience, and readiness to employ cyber and non-cyber capabilities across the spectrum of engagement from competition to crisis and conflict…[and to] defend forward to limit malicious adversary behavior below the level of armed attack, deter conflict, and, *if necessary, prevail by employing the full spectrum of its capabilities, using all the instruments of national power*….To achieve these ends, the U.S. government must demonstrate its ability

changes to certain U.S. laws seem to support this position. Section 1642 of the National Defense Authorization Act of 2019 allows the U.S. Cyber Command to take proportionate action in response to active cyber campaigns by Russia, China, Iran, and North Korea as determined by the National Command Authority. Notably, it states that these responses constitute "traditional military activities."[103] A clandestine military cyberspace operation is explicitly considered one such traditional military activity under section 1632 of the same statute.[104] In addition, the issuance of National Security Presidential Memorandum 13 gives the Secretary of Defense the authority to quickly and aggressively conduct time-sensitive military operations under layered cyber deterrence without prior presidential approval.[105] On the other hand, the Solarium Commission Report also asserts the United States' reluctance to implement deterrence by cyber punishment, believing that it either violates international law or is ineffective, thus seeming to negate several potential consequences to U.S. adversaries.[106] Instead, the Report

---

> to impose costs, while establishing a clear declaratory policy that signals to rival states the costs and risks associated with attacking the United States in cyberspace.

Id. (emphasis added).

[103] John McCain & Jack Reed, *National Defense Authorization Act for Fiscal Year 2019 4,* U.S. SENATE ARMED SERV. COMM., (2019). *See also* U.S. CYBERSPACE SOLARIUM COMM'N, *supra* note 2, at 164.

[104] McCain & Reed, *supra* note 103, at 2123–24. The statute provides as follows:

> (a) AUTHORITY TO DISRUPT, DEFEAT, AND DETER CYBER ATTACKS.— (1) IN GENERAL.—In the event that the National Command Authority determines that the Russian Federation, People's Republic of China, Democratic People's Republic of Korea, or Islamic Republic of Iran is conducting an active, systematic, and ongoing campaign of attacks against the Government or people of the United States in cyberspace, including attempting to influence American elections and democratic political processes, *the National Command Authority may authorize the Secretary of Defense, acting through the Commander of the United States Cyber Command, to take appropriate and proportional action in foreign cyberspace to disrupt, defeat, and deter such attacks under the authority and policy of the Secretary of Defense to conduct cyber operations and information operations as traditional military activities.*

Id. (emphasis added). Moreover, 10 U.S.C. § 394(c) provides that, "Clandestine Activities or Operations - A clandestine military activity or operation in cyberspace shall be considered a traditional military activity for the purposes of section 503(e)(2) of the National Security Act of 1947 (50 U.S.C. 3093(e)(2))." *Id.*

[105] Dwight Weingarten, *Congress Receives Long-Awaited Memorandum From White House on Cyber Policy,* MERITALK (Mar. 17, 2020), https://www.meritalk.com/articles/congress-receives-long-awaited-memorandum-from-white-house-on-cyber-policy/.

[106] U.S. CYBERSPACE SOLARIUM COMM'N, *supra* note 2.

loosely explains the desire to impose costs on adversaries through targeting key government or illicit, as opposed to commercial and civilian, networks and infrastructure used to conduct cyber campaigns.[107] But it offers few specifics on how or under what circumstances this would be accomplished. Moreover, the above measures are rarely invoked to the public's knowledge, even in response to a cyberattack as egregious and harmful to the United States as SolarWinds. The inevitable conclusion is that the United States must not only be clear in signaling its intention to use all available options to address these cyberattacks, but it then must actually take action to back up its words.

IV. VIOLATIONS OF STATE SOVEREIGNTY UNDER LAYERED CYBER DETERRENCE

The second characteristic that makes cyberspace a unique battlefield is location, and it creates additional international legal issues under layered cyber deterrence. Unlike the four traditional military domains of land, sea, air, and space, cyber warfare can occur in hundreds of locations at once and attacks can spread to States across the globe in a matter of seconds or minutes. Of the three layers that comprise the layered cyber deterrence strategy, the third one pertaining to cost imposition is the most concerning for the United States under international law because of the intrusion into other States' sovereign territory to disrupt or terminate cyber threats. The Solarium Commission expressly incorporates defend forward into its layered cyber deterrence strategy in order to pursue and counter operations and impose costs anywhere that threats exist in cyberspace.[108] Though not explicitly stated in the Report, this certainly would include adversaries' internal computer systems and networks. The Solarium Commission report thus raises other potential legal issues under layered cyber deterrence given that States bear responsibility for their cyber actions constituting a breach of an international legal obligation.[109] These legal issues include, among others, violations of State sovereignty and the nonintervention and non-usurpation principles.

> Punishment strategies—that is, strategies seeking to impose costs—which include constant operations as a matter of public policy are self-defeating in cyberspace, because there is no wider conception of how the adversary will react. Hunting forward in operation is no guarantee of preemptively disrupting ongoing operations—and it does not impose clear signaled costs on the opposition, as is needed to dissuade limited cyber operations in the realm of espionage.
>
> Benjamin Jensen et al., *The Strategic Implications of SolarWinds*, LAWFARE (Dec. 18, 2020), https://www.lawfareblog.com/strategic-implications-solarwinds.

[107] U.S. CYBERSPACE SOLARIUM COMM'N, *supra* note 2, at 2.

[108] *Id.*

[109] *See* TALLINN MANUAL 2.0, *supra* note 34, at 84.

When analyzing sovereignty violations in cyberspace under layered cyber deterrence, three threshold questions must be addressed. One is whether sovereignty is a rule of international law or merely a principle. If it is a rule, a second question is whether it can be enforced against the United States given the difficulty of defining sovereignty in cyberspace. And if the United States has committed an unlawful breach of sovereignty, a third question is whether it has any defenses that would excuse the breach. Each is discussed below.

A. State Sovereignty: Rule Versus Principle Under International Law and Why it Matters

There is an ongoing debate in the international community as to whether sovereignty is a rule that is capable of violation or merely a principle from which rules such as the prohibition against intervention arise. Both the United States and United Kingdom argue that sovereignty is an international law principle, not a rule that is necessarily violated by all cyber intrusions into another State's computers or networks.[110] The U.S. position is that not all infringements on another State's sovereignty in cyberspace violate international law.[111] It cites States' tolerance of espionage as lawful under international law even when it involves a physical or virtual intrusion into another State's territory.[112] The Department of Defense acknowledges that, while some operations might violate sovereignty and international law under certain unspecified conditions, precisely when a non-consensual cyber operation violates the sovereignty of another State is a question that has yet to be resolved through the practice and *opinio juris* of States.[113] Adding to the confusion is the fact that both Tallinn Manuals refer to sovereignty in cyberspace as both a principle and a rule.[114] The first rule of the Tallinn Manual is captioned, "Sovereignty (general *principle*)", and the very first line states that, "Sovereignty is a foundational *principle* of international law" (emphasis added).[115] On the other hand, Rule 4 of the Manual explains

---

[110] Kristen E. Eichensehr, *Cyberattack Attribution as Empowerment and Constraint*, HOOVER WORKING GROUP ON NAT'L SEC., TECH., AND LAW, Aegis Series Paper No. 2101, at 5 (Jan. 15, 2021), https://www.lawfareblog.com/cyberattack-attribution-empowerment-and-constraint.

[111] Ney, Jr., *supra* note 88, at 6.

[112] *Id.*

[113] *Id.* at 4.f.

[114] Michael Schmitt, *In Defense of Sovereignty in Cyberspace,* JUST SEC. (May 8, 2018), https://www.justsecurity.org/55876/defense-sovereignty-cyberspace/ ("In short, the Tallinn Manual and Tallinn Manual 2.0 experts agreed that sovereignty is both a principle of international law from which certain rules, such as the prohibition of intervention into the external or internal affairs of other states, derive, and a primary rule of international law susceptible to violation. For them, the challenge is to identify the sorts of cyber operations that cross the violation line.").

[115] TALLINN MANUAL 2.0., *supra* note 34, at 11.

how sovereignty is a rule of international law that can be independently violated.[116] The conclusion that sovereignty is a rule, however, is consistent with considerable State practice, judicial opinions, and academic scholarship, even if few States have publicly stated their position on the issue.[117]

This principle versus rule distinction is important under layered cyber deterrence because of the U.S.'s commitment to search and destroy targets anywhere in the world. The distinction also has important consequences. If sovereignty is not a rule of international law, then States may intrude into other States' territories to imbed malware in their public and private cyber infrastructure so long as the consequences are not severe enough to implicate other international laws.[118] If sovereignty is not a rule, then responding to cyber operations that implant harmful malware in another State, as distinct from those used solely for espionage, may be permissible as a rejoinder to such operations by another State. The response would constitute an act of retorsion that need not be justified on any ground precluding wrongfulness under the law of State responsibility. Ironically, however, the original target State would not be entitled to take non-cyber countermeasures as discussed below since countermeasures must be in response to an internationally wrongful act.[119] Proponents of sovereignty as a rule point out that the absence of such a rule may lead to more intrusive cyber operations, potentially producing more misunderstandings and counter attacks, leading to escalating hostilities between States and an unstable and increasingly dangerous domain.[120] Regardless, even if sovereignty is a

---

[116] *Id.* at 23–26.

[117] Schmitt, *supra* note 99.

[118] *Id.*

> In the absence of a rule of sovereignty (or even in the presence of a rule but with a high threshold for what type of cyber activity constitutes a sovereignty violation, as in limiting violations to operations that cause physical damage), States will generally be free to implant harmful malware in the private or public cyber infrastructure of other States so long as the immediate consequences of the operation are not, as explained below, extremely severe. It does not matter whether the operation is inspired by deterrent purposes or is malevolent; by the UK interpretation, motive has no bearing on the lawfulness of such operations. This reality should cause States to pause uncomfortably before adopting the same position.

Id.

[119] *Id.*

[120] *Id.*

> Those States that embrace minimalist legal standards or normative ambiguity as affording them freedom of action to defend their national interests are badly misguided, for international law and agreed non-binding norms have long proven a stabilizing force in international

rule of international law rather than a principle, it is still difficult to define what a violation of State sovereignty in cyberspace is and what physical or virtual impact is required for such a violation.[121]

B. The Challenge of Defining State Sovereignty in Cyberspace

A second threshold question with layered cyber deterrence is how one defines sovereignty in cyberspace when there are no common areas such as outer space or the high seas. Unlike navigating oceans or flights in international airspace where boundaries are defined, there is little consensus on a cyberspace equivalent.[122] Equally unclear is how the United States intends to implement layered cyber deterrence with sovereignty in cyberspace as an open question.[123] The interconnectedness of cyber space creates an imperative for the U.S. to counter adversaries' cyber operations through global strategies such as defend forward and persistent engagement, yet the lack of clear territorial boundaries and the difficulty with determining the extent to which the United States may lawfully advance create considerable legal challenges.[124] During the Cold War, the United States could anticipate where the front lines would be and deploy tanks and ships just beyond the border. In cyberspace, anticipating the battlefield or clearly

---

> relations. If the rule of sovereignty exists, however, as it almost certainly does, States will enjoy the deterrent benefits of international law while retaining the right to respond as necessary to hostile cyber operations by other States.

Id.

[121] David Simon et al., *Legal Considerations Raised by the U.S. Cyberspace Solarium Commission Report,* LAWFARE (July 20, 2020, 10:04 AM), https://www.lawfareblog.com/legal-considerations-raised-us-cyberspace-solarium-commission-report.

[122] Mark Pomerleau, *Two Years In, How Has a New Strategy Changed Cyber Operations?,* C4ISRNET (Nov. 11, 2019), https://www.c4isrnet.com/dod/2019/11/11/two-years-in-how-has-a-new-strategy-changed-cyber-operations/ ("Unlike freedom of navigation operations in international waters or flights in international airspace, there is no agreed upon international cyberspace equivalent. 'As soon as you're sailing out of the harbor, as soon as you pass the break water, you're sailing in networks that other people built for their own purposes. When the U.S. says "gray space," they mean other people's personal property,' Jason Healey, a senior research scholar at Columbia University specializing in cyber operations, told Fifth Domain. 'It's like if the Navy wanted to take over rain or say that they can operate in any river or stream or puddle in the world. We are all dependent on this cyberspace. It is touching all of our lives.'").

[123] Erica D. Lonergan, *Operationalizing Defend Forward: How the Concept Works to Change Adversary Behavior,* LAWFARE (Mar. 12, 2020), https://www.lawfareblog.com/operationalizing-defend-forward-how-concept-works-change-adversary-behavior.

[124] MICHAEL P. FISCHERKELLER & RICHARD J. HARKNETT, INST. FOR DEF. ANALYSES, PERSISTENT ENGAGEMENT, AGREED COMPETITION, AND CYBERSPACE INTERACTION DYNAMICS AND ESCALATION 3 (2018).

identifying the theater of operations is much more challenging. Unlike a traditional defend forward strategy, the connectivity and global reach of cyberspace blur the lines between national and international territories, as well as international legal concepts of sovereignty. Ransomware, viruses and other types of cyberattacks can travel far beyond their initial targets to infect countless other networks.[125] The same can occur with U.S. cyber operations under layered cyber deterrence given the United States' explicit intention of seeking out and destroying threats across the globe.

The NotPetya virus graphically demonstrates the extensive reach of the cyber domain with an attack that began in one remote location and rapidly spread throughout the world, traversing territorial boundaries without regard for sovereignty or international norms. The layered cyber deterrence strategy envisions just such a global battlefield. The attack began in Ukraine in June 2017 when Russia's military launched destructive malware against computers at the headquarters of worldwide shipping magnate, Maersk, using financial software from the Linkos Group with headquarters only a few miles away. Taking advantage of vulnerabilities in the Windows operating system widely used in both the public and private sectors, the virus quickly spread throughout the world and infected the computers of tens of thousands of individuals, organizations, and businesses.

> The release of NotPetya was an act of cyberwar by almost any definition - one that was likely more explosive than even its creators intended. Within hours of its first appearance, the worm raced beyond Ukraine and out to countless machines around the world, from hospitals in Pennsylvania to a chocolate factory in Tasmania. It crippled multinational companies including Maersk, pharma-ceutical giant Merck, FedEx's European subsidiary TNT Express, French construction company Saint-Gobain, food producer Mondelēz, and manufacturer Reckitt Benckiser. In each case, it inflicted nine-figure costs. It even spread back to Russia, striking the state oil company Rosneft. The result was more than $10 billion in total damages, according to a White House assessment.... [former Homeland Security adviser Tom] Bossert confirmed...that Russia's military—the prime suspect in any cyberwar attack targeting Ukraine—was responsible for launching the malicious code.... 'While there was no loss

---

[125] U.S. CYBERSPACE SOLARIUM COMM'N, *supra* note 2, at 28. As law professor Robert Chesney of the University of Texas described it, "We used to park ships within sight of the shore. Now, perhaps, we get access to key systems like the electric grid." David E. Sanger & Nicole Perlroth, *U.S. Escalates Online Attacks on Russia's Power Grid,* N. Y. TIMES (June 15, 2019), https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html.

> of life, it was the equivalent of using a nuclear bomb to achieve a small tactical victory,' Bossert says.[126]

The Tallinn Manual provides several rules and commentary regarding the question of sovereignty in cyberspace. In fact, the manual's first rule makes clear that State sovereignty applies in cyberspace.[127] The 1928 *Island of Palmas* award from the Permanent Court of Arbitration broadly defines sovereignty as independence, and that "[i]ndependence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State."[128] In defining sovereignty in the context of cyberspace, the Tallinn Manual distinguishes between the physical layer of network components, the logical connections between hardware and software, and the social layer consisting of the individuals and groups engaged in cyber activities.[129] All three of these layers overlap to some extent.

C. Layered Cyber Deterrence Involves Strategic Actions That Can Violate State Sovereignty Under the Physical, Logical and Social Layers of Cyberspace

The surest way of determining a breach of sovereignty in cyberspace is under the *physical* layer, when individuals or equipment from one State are located and cause harm to physical network components within another State's territory. This is because a State enjoys internal sovereignty over the individuals and cyber infrastructure and activities located within its borders, subject to any international laws to the contrary.[130] Internal sovereignty includes a

---

[126] Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History,* WIRED (Aug. 22, 2018), https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/; *see also* Benjamin Jensen, *The Cyber Character of Political Warfare,* 24 BROWN J. OF WORLD AFF., no. 1, Fall/Winter 2017, at 159.

[127] TALLINN MANUAL 2.0, *supra* note 34, at 11.

[128] Island of Palmas Case (U.S. v. Neth.), 2 R.I.A.A. 831, 838 (Perm. Ct. Arb.1928).

[129] TALLINN MANUAL 2.0, *supra* note 34, at 12.

[130] *Id.* at 13. Moreover, "the State's sovereignty over its territory affords it the right under international law to protect cyber infrastructure and safeguard cyber activity that is located in, or takes place on, its territory."

State's *domaine réservé*,[131] giving it authority to decide its political, social, cultural, economic, and legal order.[132]

A sovereign State also enjoys the right to control the *logical* layer of cyberspace within its territory, meaning the connections that exist between network devices such as applications, data, and protocols that allow the exchange of data across the physical layer.[133] U.S. actions under layered cyber deterrence thus cannot physically intrude into an adversary State's territory to incapacitate or destroy critical networks and infrastructure located within that State's borders without violating international law absent a valid defense. Similarly, individuals and groups engaging in such unlawful extra-territorial cyber activity pursuant to the *social* layer may constitute another ground for violating sovereignty.

While details of American cyber operations typically are sparse, there is little doubt the United States engages in such extra-territorial cyber activity to protect itself from potential attacks. For example, safeguarding U.S. elections is a significant government priority. Layered cyber deterrence requires the United States to closely engage its foreign adversaries beyond Department of Defense networks before their cyberattacks reach U.S. borders and disrupt those elections. Prior to the 2020 U.S. presidential election, the Department of Defense launched a

---

[131] KATJA S. ZIEGLER, MAX PLANCK ENCYCLOPEDIAS OF INT'L L., DOMAINE RÉSERVÉ (Oxford University Press, 2013), https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1398?rskey=whtGUj&result=1&prd=OPIL ("The notion of *domaine réservé* (reserved domain) describes the areas of State activity that are internal or domestic affairs of a *State* and are therefore within its domestic jurisdiction or competence. Its precise content may vary over time according to the development of *international law,* but the closely linked principle of *sovereignty* of States entails that at least some matters remain within the regulatory competence of States. Hence the *domaine réservé* describes areas where States are free from international obligations and regulation. Non-interference in the *domaine réservé* is a fundamental right of States derived from sovereignty and protected by the principle of non-intervention in their internal affairs.").

[132] TALLINN MANUAL 2.0, *supra* note 34, at 15.

[133] *Id.* at 12.

> 6. In addition to authority over the physical layer, the principle of sovereignty affords States the right to control aspects of the logical layer of cyberspace within their territories. For instance, a State may promulgate legislation that requires certain e-services to employ particular cryptographic protocols, such as the Transport Layer Security protocol, to guarantee secure communications between web servers and browsers. Similarly, a State may legislatively require electronic signatures to meet particular technical requirements, such as reliance on certificate-based encryption or that the certificates include certain information, such as their cryptographic fingerprint, owner, or expiration date.

Id. at 14.

hunt forward operation[134] in which cyber teams of individuals were deployed around the world to search for and terminate numerous malicious hacking operations.[135] Cyber Command sent teams to Europe, the Middle East, and Asia to find Russian, Iranian, Chinese, and North Korean hacking groups and discover how they broke into U.S. computer networks.[136] The teams acquired detailed information identifying risks to critical U.S. infrastructure, networks, and data. The insights from these missions provided real-time situational awareness for U.S. Cyber Command to better enable the United States to detect, defend against, and destroy threats to its elections. The physical presence of these teams and the activities they conducted on foreign soil, however, may well have been a violation of those States' sovereignty rights.[137] In another example, during the 2018 midterm elections, Cyber Command also took at least one Russian troll farm offline. According to current and former military officials, after getting close to foreign adversaries' own networks, Cyber Command then typically infiltrates them to identify and potentially neutralize attacks on the United States.[138] The deputy head of Cyber Command, Lt. Gen. Charles L. Moore Jr., confirmed that in the Russian troll farm case, diffusing the cyber threats on Russia's own terrain was indeed the objective, explaining that, "We want to find the bad guys in red space, in their own operating environment. We want to take down the archer rather than dodge the arrows."[139] Whether these examples constituted a breach of sovereignty or mere espionage is unclear because the Defense Department refused to comment on the details of the missions, including precisely where troops or the cyber operations were deployed, for how long and under what circumstances.[140] It nevertheless is not a stretch of the imagination to conclude that such actions constituted a physical breach of sovereignty in those instances or will in future operations under layered cyber deterrence where offensive forward positioning is expected.

---

[134] Cyber Command refers to its efforts to find enemy hackers as "hunt forward" operations. Julian E. Barnes, *U.S. Cyber Command Expands Operations to Hunt Hackers From Russia, Iran and China,* N.Y. TIMES (Mar. 3, 2023), https://www.nytimes.com/2020/11/02/us/politics/cyber-command-hackers-russia.html.

[135] U.S. Department of Defense, *supra* note 49.

[136] Barnes, s*upra* note 134.

[137] U.S. Department of Defense, *supra* note 49.

[138] Barnes, *supra* note 134.

[139] *Id.*

[140] Shannon Vavra, *Cyber Command Deploys Abroad to Fend Off Foreign Hacking Ahead of the 2020 Election,* CYBERSCOOP (Aug. 25, 2020), https://cyberscoop.com/2020-presidential-election-cyber-command-nakasone-deployed-protect-interference-hacking/.

D. Sovereignty Over Software and Data Transmissions From External Sources

The more difficult question is the extent to which a State exercises sovereignty over mere software and data transmissions entering its territory from external sources. The short answer is that it is unsettled under international law.[141] Again, assuming sovereignty is a rule of international law, a State must not conduct cyber operations that violate the sovereignty of another State.[142] There are exceptions to this general rule, of course, such as self-defense or when a breach of sovereignty is authorized by the United Nations Security Council.[143] The Tallinn Manual examines the lawfulness of remote cyber operations that manifest in a State's territory on two grounds. The first is the degree of infringement on the target State's territorial integrity. The second is whether there has been an interference with or usurpation of inherently governmental functions.[144]

1. The Degree of Infringement on the Target State's Territorial Integrity

As to the first ground regarding the degree of the cyber operation's infringement into the target State's territory, the Tallinn experts analyzed three characteristics that include physical damage, the loss of functionality, and the infringement on territorial integrity falling below the threshold of a loss of functionality.[145] Even before the Solarium Commission proposed its layered cyber deterrence strategy, the United States demonstrated its willingness to engage in all three types of cyber activities.

a. Physical Damage

As to the first type of cyber activity, remote U.S. cyber operations resulting in physical injury or property damage within a target State would be a breach of sovereignty absent a valid defense under international law.[146] One of the most violent cyberattacks to date by any State is the Siberian pipeline explosion allegedly perpetrated by the United States. In 1982, Russia sought to build an expansive pipeline linking Siberian gas fields to European markets, however it lacked the

---

[141] TALLINN MANUAL 2.0, *supra* note 34, at 20.
[142] *Id.* at 17.
[143] *Id.*
[144] *Id.* at 20.
[145] *Id.*
[146] *Id.*

sophisticated automated control software to operate the pipeline's valves and compressors.[147] The United States denied Russia's request for the software and later learned that Russia intended to steal it from the Canadians. Responding to a Russian industrial espionage campaign, the U.S. Central Intelligence Agency allegedly worked with the Canadian software designers to install a Trojan horse into the software that, after a period of normal operations, ultimately caused the new pipeline's pumps, turbines, and valves to produce pressure far beyond what they were designed to withstand.[148] The result was an explosion and fire that was visible from space and that the U.S. Air Force rated to be the equivalent of a small nuclear bomb.[149] No injuries or deaths were known to have occurred given the remote location of the explosion.[150] If true, the United States clearly violated Russian sovereignty in carrying out its cyber operation in this case given the extent and severity of physical damage to the pipeline. The case for a breach of sovereignty would have been even stronger had the pipeline explosion resulted in human casualties in addition to the property damage caused.

b. Loss of Functionality

The second characteristic under the Tallinn Manual for analyzing a cyber infringement into a target State is a loss of functionality. The Tallinn experts agreed that a loss of functionality, such as a remote malware attack that causes a nuclear reactor to malfunction, could constitute a violation of sovereignty, but they could not agree on the threshold of precisely when it occurs due to the lack of *opinio juris*.[151] A case in point occurred in approximately 2008 when the United States partnered with Israel to launch a multi-year cyber sabotage operation against Iran's nuclear enrichment program at Natanz.[152] The United States and its allies were wary of a nuclear-empowered Iran in the heart of the Middle East and negotiations with Iran had proven ineffective. Initiating an all-out military campaign was unfeasible for political, military, and economic reasons, so the United States and Israel sought to take control of critical components of Iran's nuclear reactor to slow down

---

[147] NATIONAL SECURITY ARCHIVE, *Update: Agent Farewell and the Siberian Pipeline Explosion* (Apr. 26, 2013), https://unredacted.com/2013/04/26/agent-farewell-and-the-siberian-pipeline-explosion/.
[148] David Hoffman, *Reagan Approved Plan to Sabotage Soviets*, WASH. POST (Feb. 26, 2004), https://www.washingtonpost.com/archive/politics/2004/02/27/reagan-approved-plan-to-sabotage-soviets/a9184eff-47fd-402e-beb2-63970851e130/.
[149] Rid, *supra* note 76, at 10–11.
[150] Hoffman, *supra* note 148.
[151] TALLINN MANUAL 2.0, *supra* note 34, at 20–21.
[152] Brandon Valeriano and Benjamin Jensen, *From Arms and Influence to Data and Manipulation: What Can Thomas Schelling Tell Us About Cyber Coercion?,* LAWFARE (Mar. 16, 2017, 4:09 PM), https://www.lawfareblog.com/arms-and-influence-data-and-manipulation-what-can-thomas-schelling-tell-us-about-cyber-coercion.

or stop its production. Because the reactor's equipment was not connected to the internet, the infection likely occurred through the insertion of a removable drive. By the end of 2010, the worm had infected over one hundred thousand computers in dozens of countries.[153] It was coded to seek out a specific target and, if it did not find the correct configuration, it did nothing.[154] If it did, however, the worm began a sequence to change the output frequencies of specific drivers that caused the reactor's motors to malfunction and physically damage its rotors, turbines, and centrifuges.[155] The cyberattack was designed to slowly cripple the centrifuges over time in order to escape detection by the plant's operators and ultimately destroy or delay Iran's enrichment program.[156] A similar attack today under layered cyber deterrence very likely would constitute a U.S. breach of sovereignty given the significant loss of functionality of a key component of State infrastructure.[157]

c. Infringement Below the Loss of Functionality Threshold

Finally, the Tallinn experts could not reach a consensus on the most challenging analytical scenario: Whether, and if so, when, a remote cyber operation that results in no physical damage or loss of cyber functionality in the target State constitutes a violation of sovereignty.[158] The general consensus seems to be that software that simply resides on a network within another State's territory without its permission, but does nothing, is not a breach of sovereignty. For many experts, the adage "no harm, no foul" applies. And yet, causing infrastructure or programs to operate differently, altering or deleting data, or placing malware on a system that leads to a temporary but significant loss of functionality could result in a sovereignty violation.[159] Software residing within another State's territory that can cause substantial physical or structural harm at some future time arguably is a breach of sovereignty simply because it resides in that State's territory without its consent and against its interests. Even discovering the intrusion can harm the target State as it may be required to expend substantial resources to neutralize its potential effects.[160] The magnitude and duration of the potential harm would, of course, be important considerations.

Russia has had a long and documented history of intrusions into U.S. networks and infrastructure without causing immediate physical

---

[153] Rid, *supra* note 74, at 18.
[154] *Id.* at 18.
[155] *Id.* at 18–19.
[156] *Id.* at 19.
[157] Sanger & Perlroth, *supra* note 125.
[158] TALLINN MANUAL 2.0, *supra* note 34, at 21.
[159] *Id.*
[160] Schmitt, *supra* note 99.

harm. SolarWinds was one example but by no means the only one. It was not until recently, under more aggressive defend forward and now layered cyber deterrence strategies, that the United States finally began taking concerted action in response. For example, during the mid-2010s, Russia engaged in at least three major cyber operations against the United States that were carried out by its Federal Security Service (F.S.B.), its military intelligence agency (G.R.U.), and Russian government contractors.[161] Two cyber operations were well-publicized: one in which documents were stolen from the Democratic National Committee and other political groups, and the other in which Russia's Internet Research Agency used social media to sow dissension leading up to the 2016 presidential election.[162] A third, lesser-known operation involved intrusions into American and European infrastructure, including energy, water, aviation, and critical manufacturing sectors.[163] Russian spies infiltrated the corporate networks of several U.S. nuclear, energy and water plants, including, as mentioned, the Wolf Creek Nuclear Operating Corporation which runs a Kansas nuclear plant. They took screenshots of the machinery and stole details of how the power switches at those plants can be turned off.[164] The Department of Homeland Security eventually released computer screenshot evidence showing how Russia infiltrated the industrial control infrastructure, allowing them to turn the power off or engage in sabotage.[165] Although the intrusion did not result in any immediate physical harm to the United States, the fact that it could eventually cause significant future harm may be sufficient to constitute a breach of U.S. sovereignty.

The United States itself now conducts some of these same types of extraterritorial intrusions that may constitute a violation of international law. Under operation Nitro Zeus, the U.S. planted computer code within Iran's infrastructure allowing it to control power grids, communications networks, command-and-control systems, and other vital components in the event that the 2015 nuclear accord failed and conflict arose.[166] Layered cyber deterrence aims in theory to shift U.S. cyber strategy from defense to greater offense, signaling the United States' willingness to access and, if necessary, harm its adversaries' infrastructure to protect its interests.[167] "[T]he placement of potentially crippling malware inside the

---

[161] Nicole Perlroth & David E. Sanger, *Cyberattacks Put Russian Fingers on the Switch at Power Plants, U.S. Says*, N. Y. TIMES (Mar. 15, 2018), https://www.nytimes.com/2018/03/15/us/politics/russia-cyberattacks.html.

[162] *Id.*

[163] Sanger & Perlroth, *supra* note 125.

[164] Perlroth & Sanger, *supra* note 161.

[165] *Id.*

[166] *Id.*

[167] *Id.* Current U.S. defense policy thus envisions an environment in which the United States military uses technology to exercise global command and control and execute both close and long-range strikes. DEP'T OF DEF., SUMMARY: DEPARTMENT OF DEFENSE CYBER STRATEGY 1 (2018), https://media.defense.gov/2018/Sep/18/2002041658/-1/-

Russian system [occurs] at a depth and with an aggressiveness [that has] never been attempted before. It is intended partly as a warning, and partly to be poised to conduct cyber strikes if a major conflict broke out between Washington and Moscow."[168] As evidence of this shift in policy, new legal authority within the military authorization bill passed by Congress in the summer of 2018 approved clandestine cyberspace military activity and gave the Secretary of Defense authority to defend against cyberattacks without special presidential approval.[169]

The United States has engaged in other tactics below the loss of functionality threshold under layered cyber deterrence that signal a more hopeful offensive posture. One tactic has been to publicly release adversary malware obtained during recent hunt forward missions to allow defensive software to lessen the malware's effectiveness. Another recurring U.S. cyber operation is disrupting and degrading adversary capabilities used to conduct attacks against the United States. For instance, U.S. Cyber Command and the National Security Agency took actions to prevent foreign actors from interfering in the 2020 presidential election, including an operation against Iran two weeks immediately prior to the election. Each of these scenarios involved persistent engagement and incorporeal defend forward operations within the territories of other States that now fall under layered cyber

---

1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF. "Computers and network technologies underpin U.S. military warfighting superiority by enabling the Joint Force to gain the information advantage, strike at long distance, and exercise global command and control." *Id.* The Solarium Commission refines this policy by arguing that, rather than merely reacting and then responding to cyber-attacks, the key to understanding and neutralizing adversaries' cyber threats is gaining and maintaining access to their positions, regardless of where they are located throughout the world. This more offensive approach expands on the defend forward policy of persistent engagement and is a departure from the more neutral and defensive Obama administration stance on operating in cyberspace. The essential tool undergirding the Commission's strategy is the full spectrum of military power needed to accomplish these objectives. The Commission's Report states that:

> [T]he United States must operate in cyberspace to provide early warning; gain situational awareness of evolving adversary tactics, techniques, and procedures (TTPs), capabilities, and personas; and conduct operational preparation of the environment (OPE). The cyber domain is dynamic, opportunities are fleeting, and our adversaries are agile and adaptive. *A prerequisite to keeping pace with them and anticipating their behavior, rather than simply reacting and responding to it, is gaining and maintaining access against defined targets and pursuing adversaries as they maneuver….* The recommendations supporting this pillar focus on *ensuring that the United States protects its ability to employ the military instrument of power, alongside other instruments, across the spectrum of engagement from competition to crisis and conflict.*

U.S. CYBERSPACE SOLARIUM COMM'N, *supra* note 2, at 112 (emphasis added).

[168] Sanger & Perlroth, *supra* note 125.

[169] *Id.*

deterrence but may not have resulted in physical damage or a loss of functionality in the target State.[170] Under this lower threshold then, such actions could still arguably violate State sovereignty depending on which side of the debate one takes.

Thus, more broadly, each of the examples discussed above demonstrates the United States' willingness to infringe on, or at least test the limits of, State sovereignty to protect its cyber interests. Other examples include operations involving U.S. operatives' physical presence in other State territories, such as the teams sent abroad prior to the 2020 elections, or where there is a loss of functionality, such as with the Iran nuclear reactor attack. Yet another example is when there is an infringement on territorial integrity falling below the threshold of a loss of functionality, such as planting computer code within an adversary State's infrastructure allowing it to control power grids and command-and-control systems. Given this new policy that seeks to legitimize more aggressive cyber behavior, the United States must take care to balance the need to lawfully protect its cyber interests with preserving State sovereignty under layered cyber deterrence. In particular, remote cyber operations resulting in actual physical injury or property damage within a target State must be avoided or done so covertly or pursuant to a valid defense, in order to avoid a violation of State sovereignty. Where there is a loss of functionality or an infringement beneath such loss within the target State, the lack of *opinio juris* or even a consensus among States as to the threshold at which it occurs means that there is some latitude for the United States to lawfully conduct its layered cyber deterrence operations extraterritorially.

2. Interference With or Usurpation of Inherently Governmental Functions

The second ground on which a violation of sovereignty could occur under layered cyber deterrence is when one State's cyber operation interferes with or usurps the inherently governmental functions of another State.[171] The Tallinn experts could not reach a consensus on the definition of "inherently governmental functions" but agreed that a cyber-attack violates sovereignty if it interferes with data or services necessary for social services, elections, tax collection, diplomacy, national defense, etc.[172] A majority of experts further agreed that a cyber operation violates sovereignty regardless of where it is launched,[173]

---

[170] Nakasone & Sulmeyer, *supra* note 4.
[171] TALLINN MANUAL 2.0, *supra* note 34, at 21–22.
[172] *Id.* at 22.
[173] *Id.* at 24.

occurs, or manifests, meaning that it need not be initiated or felt within the sovereign territory of that State. For example, the United States blocking Russian citizens' access to welfare support likely would constitute a breach of Russian sovereignty as an interference with the inherently governmental function of providing social services.[174] It is important to note that intent is not a requisite element for a breach of sovereignty.[175] Thus, a breach of sovereignty also could occur if the U.S. launched a cyber operation under layered cyber deterrence that targeted a Russian government office, but had the unintended effect of preventing Russian citizens' access to welfare support or even inadvertently violating a second State's sovereignty.

V. VIOLATION OF THE NONINTERVENTION PRINCIPLE UNDER LAYERED CYBER DETERRENCE

Closely related to the notion of sovereignty, the nonintervention principle is another area in which the United States can run afoul of international law in its pursuit of layered cyber deterrence.

A. The Origins and Definition of the Nonintervention Principle

One of the earliest references to the nonintervention principle is found in the 1928 Organization of American States (OAS) Convention on the Rights and Duties of States in the Event of Civil Strife. Article 1, paragraph 1 of the Convention provides that "[T]he contracting states bind themselves to…*use all means at their disposal to prevent the inhabitants of their territory, nationals or aliens, from* participating in, gathering elements, *crossing the boundary or sailing from their territory* for the purpose of starting or promoting civil strife."[176]

> The International Group of Experts was of the view that a State's cyber operations may constitute a violation of another State's sovereignty, whatever the basis for that violation, irrespective of whether the operations are launched from the acting State's territory, the target State's territory, the territory of a third State, the high seas, international airspace, or outer space. Any damage caused to cyber infrastructure aboard a sovereign platform is similarly a violation of the target State's sovereignty no matter where the platform is located (Rule 5).

Id.

[174] *Id.* at 23.

[175] *Id.* at 24.

[176] Convention on Duties and Rights of States in Event of Civil Strife art. 1, ¶ 1, Feb. 20, 1928 134 L.N.T.S. 45. In *Nicaragua v. United States of America*, the International Court of Justice relied on these earliest documented references to the nonintervention principle in its opinion. *See* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgement, 1986 I.C.J 14 (June 27).

(emphasis added). The nonintervention principle was reaffirmed by the OAS General Assembly in a 1972 resolution.

> The General Assembly Resolves 1. To reiterate solemnly the need for the member states of the Organization to *observe strictly the principles of nonintervention and self-determination of peoples* as a means of ensuring peaceful coexistence among them and to refrain from committing any direct or indirect act that might constitute a violation of those principles.[177] (Emphasis added).

In addition, the 1970 U.N. Declaration on Principles of International Law, Friendly Relations and Co-operation Among States in Accordance With the Charter of the United Nations sets forth the non-intervention principle.[178] Among other related provisions in the Declaration, it states the U.N. General Assembly's position that, "[N]o State or group of States has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State."[179]

It is worth noting that none of the above-quoted provisions define intervention or how States can violate it. One may, therefore, infer that the authors did not intend to restrict the principle of sovereignty to specific realms. Given that the domains of air, sea, and land were known but not explicitly stated in the documents when they were created, it is reasonable to conclude that the nonintervention principle applies broadly to all domains, including cyberspace and intrusions on sovereignty through technology. Rule 66 of the Tallinn Manual entitled "Intervention by States" supports this interpretation by explaining that

---

[177] 1986 I.C.J. 14., at 92.

[178] G.A. Res. 2625 (XXV), 3–8 (Oct. 24, 1970). The relevant portions of the Declaration are as follows:

> Convinced that the strict observance by States of the obligation not to intervene in the affairs of any other State is an essential condition to ensure that nations live together in peace with one another, since *the practice of any form of intervention not only violates the spirit and letter of the Charter, but also leads to the creation of situations which threaten international peace and security…No State or group of States has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State.* Consequently, armed intervention and all other forms of interference or attempted threats against the personality of the State or against its political, economic and cultural elements, are in violation of international law…(c) *States shall conduct their international relations in the economic, social, cultural, technical and trade fields in accordance with the principles of sovereign equality and non-intervention.*

Id. at 3–8 (emphasis added).

[179] *Id.* at 3–8.

"[a] State may not intervene, including by cyber means, in the internal or external affairs of another State."[180]

As the International Court of Justice observed in *Nicaragua v. United States of America*, the nonintervention principle also requires coercion of a target State's *domaine réservé*, or its essential internal functions.[181] One example mentioned earlier is Iran's attempts to influence the U.S. 2020 presidential election by sending threatening emails and posting a video to diminish confidence in the voting process.[182] Similarly, activity under layered cyber deterrence that significantly impacts an adversary State's public transportation system, legislative functions, foreign affairs, electoral infrastructure, or financial operations could violate the nonintervention principle. There is substantial debate, however, on what is required for such a violation.[183] Merely placing malware in another State's infrastructure without activating it, as the United States did in Iran through Nitro Zeus or in Russia to control power grids and command-and-control systems, would not be an intervention because no coercion is involved.[184] Activating it, however, may yield a different result. In a March 2020 speech, Defense Department General Counsel Paul Ney accepts that the prohibition on coercive intervention in the core functions of another State is a rule of international law that applies in cyberspace[185] and he notes that other States have adopted this view. He adds, however, that there is "no international consensus among States on the precise scope or reach" of this rule.[186] Thus, the United States' more aggressive stance under layered cyber deterrence that cyber campaigns like Nitro Zeus might be lawful, even if they only have the mere potential to cripple major State infrastructure, is potentially inconsistent with judicial and scholarly opinion.

B. Intervention, Interference, and Usurpation

Intervention is sometimes used interchangeably with interference and usurpation in the literature. The confusion arises because the definitions of all three overlap to some extent, with each involving one State intruding into some aspect of another State. Written instruments of a majority of States and the United Nations, as well as judgments by the International Court of Justice, use the term "interference" when referring to a State's *noncoercive* intrusion into another State's sovereign

---

[180] TALLINN MANUAL 2.0, *supra* note 34, at 312.
[181] Nicar v. U.S., 1986 I.C.J. at 98.
[182] Nakashima, *supra* note 32.
[183] Simon et al., *supra* note 121; *see also* Ney, Jr., *supra* note 88.
[184] Schmitt, *supra* note 99.
[185] Ney, Jr., *supra* note 88.
[186] *Id.*

affairs.[187] Interference can include suppressing, modifying, adding, transmitting, editing, deleting, or otherwise damaging data, systems, and services.[188] On the other hand, as mentioned, intervention involves *coercive* interference with another State's *domain réservé*.[189] Like interference, usurpation lacks coercion and, unlike intervention, it merely involves inherently governmental functions rather than a State's *domain réservé*.[190]

To illustrate, suppose in the context of layered cyber deterrence, the United States initiates a denial-of-service attack on an adversary government's website that overwhelms its servers with requests and prevents legitimate traffic from accessing the site.[191] This may constitute *interference* because there is no coercion in the State's sovereign affairs. The scenario can change to a *usurpation* if the United States seizes the adversary State's servers without its consent to obtain evidence in an international criminal prosecution.[192] Such seizure becomes a sovereignty violation because the operation usurps an inherently governmental law enforcement function exclusively reserved to the adversary State under international law.[193] If the cyber operation then results in data being changed or deleted that substantially disrupts the adversary State's judicial system, it may constitute a prohibited *intervention* because the coercive conduct affects one of the State's core functions, namely, the adjudication of disputes.[194]

These distinctions are important when analyzing the potential legal effects of the layered cyber deterrence strategy from an offensive perspective. The Report highlights the weaknesses of the current U.S. policy in cyberspace by arguing that its failure to more aggressively respond to major cyber-attacks that fall outside the *domaine réservé* leaves it vulnerable to ongoing threats.

> Adversaries suspect that the U.S. government would retaliate for turning off the power in a major city [*i.e., intervention*] but doubt American resolve to respond to intellectual property theft [*i.e., interference*], the implanting of malware in critical infrastructure [*i.e., usurpation*], and election interference [*i.e., interference*]. They know they can achieve their objectives on the cheap.

---

[187] TALLINN MANUAL 2.0, *supra* note 34, at 313.
[188] *Cybercrime Module 2 Key Issues: Offences Against the Confidentiality, Integrity and Availability of Computer Data and Systems*, U.N. OFF. ON DRUGS AND CRIME (May 2019), https://www.unodc.org/e4j/en/cybercrime/module-2/key-issues/offences-against-the-confidentiality--integrity-and-availability-of-computer-data-and-systems.html (last visited Oct. 6, 2020).
[189] TALLINN MANUAL 2.0, *supra* note 34, at 313.
[190] *Id.* at 24.
[191] MARIE-HELEN MARAS, CYBERCRIMINOLOGY 270–71 (2017).
[192] TALLINN MANUAL 2.0, *supra* note 34, at 21–23.
[193] *Id.*
[194] Ney Jr., *supra* note 88.

> Both state and non-state actors know that in the current environment, new vulnerabilities that they can exploit emerge every day across the private sector while government and private-sector responses will be uncoordinated and sporadic at best."[195] (Emphasis and commentary added).

The Report observes that while U.S. adversaries acknowledge the United States may respond to so-called interventions under current cyber policy, such as a debilitating attack on the nation's power grid, it is neither likely nor expected to respond to mere interference or a usurpation, such as an intellectual property theft or implanted malware that affects critical infrastructure. This distinction lies at the heart of the layered cyber deterrence policy and is why a far more aggressive approach in both defending U.S. interests in cyberspace and proactively shaping adversary behavior is required.[196] It also is why taking some form of consistent and meaningful action to back up the layered cyber deterrence strategy is so critically necessary in defending the U.S. from major cyber-attacks.

VI. DEFENSES TO INTERNATIONAL LAW VIOLATIONS UNDER LAYERED CYBER DETERRENCE

The United States has defenses available to it under layered cyber deterrence if another State alleges it breached that State's sovereignty in

---

[195] U.S. CYBERSPACE SOLARIUM COMM'N, *supra* note 2, at 15.

[196] As the Report itself states:

> [T]he [layered cyber deterrence] strategy builds on the defend forward concept, originally articulated in the Department of Defense (DoD) Cyber Strategy, to include all of the instruments of national power. It integrates defend forward into a whole-of-nation approach for securing American interests in cyberspace. Defend forward is a proactive, rather than reactive, approach to adversary cyber threats. Specifically, it addresses the fact that the United States has not created credible and sufficient costs against malicious adversary behavior below the level of armed attack…*Therefore, defend forward posits that the United States must shift from responding to malicious behavior after it has already occurred to proactively observing, pursuing, and countering adversary operations and imposing costs to change adversary behavior*.

Id. at 24 (emphasis added). *See generally* MICHAEL P. FISCHERKELLER & RICHARD J. HARKNETT, PERSISTENT ENGAGEMENT, AGREED COMPETITION, CYBERSPACE INTERACTION DYNAMICS, AND ESCALATION 11 (INSTITUTE FOR DEFENSE ANALYSES ED. 2018), https://www.ida.org/-/media/feature/publications/p/pe/persistent-engagement-agreed-competition-cyberspace-interaction-dynamics-and-escalation/d-9076.ashx.; Emily Goldman, *History of Persistent Engagement and Defend Forward (Meeting Minutes)* (Sept. 23, 2019).

cyberspace, intervened in its *domaine réservé*, or otherwise violated international law. Consent, necessity, self-defense, countermeasures, and espionage are all potential defenses to an otherwise unlawful cyber act.[197]

A. Consent

Consent is a key rationale underlying the layered cyber deterrence strategy. According to the U.S. Department of Defense, if a non-consensual cyber operation is not a prohibited use of force or intervention, it is not barred under customary international law and is thus permitted.[198] The Department of Defense cites other States' public silence after known cyber intrusions into foreign networks as support for this position.[199] Under layered cyber deterrence then, the United States would be free to engage in any cyber operation in another State's territory that is not explicitly prohibited and does not rise to the level of an unlawful intervention or use of force. Significantly, this legitimizes cyber operations that include espionage, usurpations, certain interventions, countermeasures designed to thwart future attacks against the United States, and similar activities. These types of operations, in turn, support much of the layered cyber deterrence strategy. As the Solarium Commission writes in its Report:

> This [defend forward] approach addresses the set of malicious adversary action that exists on a spectrum between routine activities that states tacitly accept (e.g., espionage) and strategic cyberattacks that would constitute an armed attack. The Commission reimagines and expands the core logic of [the Department of Defense's] concept of defend forward to incorporate both military and non-military instruments of power.
>
> Defend forward follows from the recognition that organizing U.S. cyber forces around simply reacting to adversary activity has been ineffective in preventing adversary cyber campaigns; and initiatives that rely solely on non-military instruments of power have been insufficient to alter adversaries' cost-benefit and risk calculus. Therefore, the United States must ensure that it is organized, resourced, and postured to position and employ forces forward - geographically and virtually - to

---

[197] TALLINN MANUAL 2.0, *supra* note 34, at 104.
[198] Ney Jr., *supra* note 88, at 13.
[199] *Id.* at 12–13.

> counter adversary campaigns, pursue adversaries as they maneuver, and impose costs.[200]

B. Necessity and Self-Defense

The United States also may assert the defense of necessity under the law of State responsibility in response to a cyberattack that poses a grave and imminent peril to an essential U.S. interest when doing so is the only means to protect that interest.[201] Depending on the scale and effects of the initial attack, the United States also can argue self-defense under Article 51 of the United Nations Charter and customary international law if it is the target of a major cyber operation that rises to the level of an armed attack.[202] For example, under layered cyber deterrence, the United States could claim necessity and perhaps self-defense if it responded in kind to an adversary State's cyber operation that crippled a large U.S. electrical grid that provided power to a sizeable number of people.[203] California is a prime target with its vulnerable, aging power system that faces millions of cyber-attacks each month.[204] As one expert described it:

> Never has California's aging electricity infrastructure been more vulnerable, even as the government plans to rely on it more completely with 5 million electric cars and, eventually, to fully operate the world's fifth-largest

---

[200] U.S. CYBERSPACE SOLARIUM COMM'N, *supra* note 2, at 110.
[201] TALLINN MANUAL 2.0, *supra* note 34, at 135.
[202] U.N. Charter, *supra* note 96; *see also* TALLINN MANUAL 2.0, *supra* note 34, at 339.
[203] TALLINN MANUAL 2.0, *supra* note 34, at 136–37. According to the Tallinn Manual:

> A number of examples may serve to illustrate situations in which essential interests are gravely and imminently threatened. Most of the Experts agreed that, for instance, a cyber operation that would debilitate the State's banking system, cause a dramatic loss of confidence in its stock market, ground flights nation-wide, halt all rail traffic, stop national pension and other social benefits, alter national health records in a manner endangering the health of the population, cause a major environmental disaster, shut down a large electrical grid, seriously disrupt the national food distribution network, or shut down the integrated air defence system would provide the basis for the application of this Rule. They concurred that it is most clearly implicated when critical infrastructure is targeted in a manner that may have severe negative impact on a State's security, economy, public health, safety, or environment.

Id.
[204] Rob Nikolewski, *California Operator of Electricity Grid Fends Off Millions of Cyberattacks Each Month,* SAN DIEGO UNION-TRIB. (June 14, 2019), https://www.sandiegouniontribune.com/business/energy-green/story/2019-06-12/california-grid-operator-a-target-for-millions-of.

> economy. A widespread, sustained power outage is frightening to contemplate, with the tools we use to navigate our lives taken from us: no lights, telephone service or charging capacity; no heating or cooling; no computers, working gas pumps or ATMs. 'Think of the internet as a weapon of mass destruction,' says former news anchor Ted Koppel, whose book 'Lights Out' explores threats to U.S. electricity grids.... At [San Diego Gas & Electric], which has 3.6 million electricity customers, 'there's always some type of an intrusion attempt daily,' said Zoraya Griffin, the company's emergency operations manager.[205]

On March 5, 2019, a cyber-attack on the California power grid marked the first time a digital attack actually interfered with electrical grid operations in the United States.[206] In a similar example, hackers widely suspected of working for the Russian government repeatedly targeted Ukraine in a series of escalating cyber operations that eventually sabotaged its physical infrastructure.[207] In December 2015, they attacked Ukraine's power grid, compromising the network systems at three energy distribution companies and disrupting the supply of electricity.[208] Over two-hundred thousand people in Kiev were left without power and heat in frigid temperatures.[209] Fortunately, the systems were restored before pipes started to freeze and people perished from the bitter winter cold.[210] A major cyber-attack on the power grid of a state such as California—with the fifth largest economy in the world and the largest population in the country with nearly forty million people—would have devastating effects on both the California and U.S. economies. It also likely would justify an attack under layered cyber deterrence and the doctrines of necessity and self-defense.

C. The Doctrine of Countermeasures and the Attribution Problem

Countermeasures, or belligerent reprisals in the context of armed conflict,[211] provides the U.S. with another defense against an otherwise unlawful intrusion into another State's territory. A countermeasure is an

---

[205] Julie Cart, *Cyber-Terror, Wildfire, Rodents – How Can California Protect its Vulnerable Power Supply?*, SACRAMENTO BEE (Feb. 1, 2019), https://www.sacbee.com/news/state/california/article225289475.html.
[206] Nikolewski, *supra* note 204.
[207] Greenberg, *supra* note 65.
[208] Nikolewski, *supra* note 204.
[209] Greenberg, *supra* note 65.
[210] *Id.*
[211] TALLINN MANUAL 2.0, *supra* note 34, at 121.

offended State's act or omission against an offending State that otherwise would violate international law but for its characterization as a countermeasure. The International Court of Justice and arbitral tribunals have recognized countermeasures as lawful under international law.[212] In the cyber domain, Rule 20 of the Tallinn Manual provides that, "A State may be entitled to take countermeasures, whether cyber in nature or not, in response to a breach of an international legal obligation that is owed by another state."[213] A countermeasure is thus an appropriate response to another state's coercive intervention in its inherently governmental functions, as long as it is not an unlawful use of force.[214] A key point in implementing layered cyber deterrence then will be the U.S.'s characterization of its cyber-attacks as countermeasures, particularly if sovereignty is regarded as a rule rather than a principle of international law. This is because countermeasures provide the United States with legal protection to launch operations under layered cyber deterrence that otherwise would be deemed illegal.

Countermeasures, however, can be problematic for the United States under layered cyber deterrence that ultimately may cause them to be unlawful. First is the uncertainty under Rule 20 as to whether there has been a sufficient breach of an international legal obligation to lawfully permit the United States to initiate a countermeasure. Since a countermeasure is only available in response to an internationally wrongful act, the U.S. must be reasonably certain that it is justified in engaging in a response under layered cyber deterrence or risk violating international law itself by attacking a State whose conduct was not unlawful.

Second, prior to implementing a countermeasure, the United States may be required to notify the offending State, allow it to cease its unlawful behavior and, under Rule 21 of the Tallinn Manual, offer to negotiate a resolution. Obviously, such a requirement substantially weakens the effectiveness of any subsequent countermeasure because the responsible State can simply deny the allegation or take evasive or defensive measures against a U.S. responsive cyber-attack. The U.S. position on the matter appears to have changed from 2016 when it merely acknowledged the international community's general acceptance of the prior notification rule to now saying there is no international consensus of any kind that prior notice is required in all circumstances.[215] The

---

[212] *Id.* at 111.
[213] *Id.* at 111.
[214] Kosseff, *supra* note 93, at 8–9.
[215] Brian J. Egan, *Remarks on International Law and Stability in Cyberspace,* U.S. DEP'T OF STATE DIPL. IN ACTION (Nov. 10, 2016), https://2009-2017.state.gov/s/l/releases/remarks/264303.htm ("The doctrine of countermeasures also generally requires the injured State to call upon the responsible State to comply with its international obligations before a countermeasure may be taken - in other words, the doctrine generally requires what I will call a 'prior demand.' The … purpose of the requirement … is to give the responsible State notice of the injured

Defense Department's General Counsel, Paul Ney, noted in a March 2020 speech that there are "varying State views on whether notice would be necessary in all cases in the cyber context because of secrecy or urgency." While this change in position is understandable, the consequence of it is clear. It allows the United States to become more aggressive under its layered cyber deterrence strategy in responding to cyber-attacks without prior notice, yet still maintain that its actions were a lawful countermeasure under international law.

Third, the attribution problem, common in cyber operations, can lead to the U.S. striking the wrong target and rendering a responsive cyber-attack unlawful under layered cyber deterrence. Two additional factors complicate the attribution problem in cyberspace. One, as mentioned, is the difficulty the United States may have in determining whether a cyber-attack even rises to the level of a breach of international law to justify a countermeasure. The U.S. attacking another State without sufficient provocation would itself violate international law. Second is the speed at which cyber operations occur. Cyberattacks can occur within seconds or minutes, not hours or days as with conventional strikes.[216] In the time it takes the United States to determine with reasonable certainty who initiated a cyber-attack, the U.S. could be attacked a thousand more times, increasing the urgency of a response and the possibility of misattribution. Rule 20 of the Tallinn Manual requires that a countermeasure be initiated against the offending State, but not knowing who the offending State is places the U.S. in the untenable position under layered cyber deterrence of either retaliating against an innocent State and violating international law or doing nothing at all.

Instead of waiting to be attacked and then potentially retaliating against the wrong target, the U.S. position under layered cyber

---

State's claim and an opportunity to respond."). *But cf.* Hon. Paul C. Ney, Jr.*, DOD General Counsel Remarks at U.S. Cyber Command Legal Conference*, U.S. DEP'T DEFENSE (Mar. 2, 2020), https://www.defense.gov/News/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/ (explaining that in March 2020, Department of Defense General Counsel, Paul Ney, Jr., acknowledged the "traditional view" that notice must precede a countermeasure, but noted that States' views on the matter vary and such notice may not be required if it is unclear whether the attack violated international law, or if there was no intent and the attribution problem and the urgency of the threat make it impracticable to give notice. "In the traditional view, the use of countermeasures must be preceded by notice to the offending State, though we note that there are varying State views on whether notice would be necessary in all cases in the cyber context because of secrecy or urgency. In a particular case it may be unclear whether a particular malicious cyber activity violates international law. And, in other circumstances, it may not be apparent that the act is internationally wrongful and attributable to a State within the timeframe in which the DoD must respond to mitigate the threat. In these circumstances, which we believe are common, countermeasures would not be available.").

[216] *See generally* Adam Meyers, *First-Ever Adversary Ranking in 2019 Global Threat Report Highlights the Importance of Speed,* CROWDSTRIKE BLOG (Feb. 19, 2019), https://www.crowdstrike.com/blog/first-ever-adversary-ranking-in-2019-global-threat-report-highlights-the-importance-of-speed/.

deterrence is to proactively search out and neutralize threats, even if that means breaching sovereignty or engaging in questionable countermeasures. The Solarium Commission Report suggests that the attribution problem, the persistent nature of cyber threats against the U.S., and the speed with which cyber operations occur justify this policy shift.[217]

> Today most cyber actors feel undeterred, if not emboldened, to target our personal data and public infrastructure. In other words, *through our inability or unwillingness to identify* and punish our cyber adversaries, we are signaling that interfering in American elections or stealing billions in U.S. intellectual property is acceptable. The federal government and the private sector must defend themselves and *strike back with speed and agility*.[218] (Emphasis added.)

Fourth, a U.S. countermeasure under layered cyber deterrence is unlawful if it is a use of force or otherwise disproportionate to the harm incurred.[219] In determining the latter, the United States must consider the extent of the harm, the gravity of the wrongful act, its own rights vis-à-vis those of the offending State, and the need to cause the offending State to comply.[220] U.S. countermeasures also must be restricted to ending the offending State's unlawful activity and nothing more.[221] Anything beyond that may constitute an unlawful countermeasure.[222] If in response to North Korea's cyber-attack against Sony Pictures, for example, the United States responded by initiating a cyber-attack that crippled North Korea's telecommunications networks used to communicate with its allies, such a response would be disproportionate to the initial harm and likely an unlawful countermeasure. The coercive conduct affects a core function of North Korea's government, namely, the conduct of its national security and foreign affairs, and thus would constitute a prohibited intervention under layered cyber deterrence. Of course, in light of the continuous nature of cyber threats by North Korea and other States that prompted the layered cyber deterrence strategy, "the United States would have a reasonable argument that positioning

---

[217] U.S. CYBERSPACE SOLARIUM COMM'N, *supra* note 2, at v–vi.
[218] *Id.* at v.
[219] TALLINN MANUAL 2.0, *supra* note 34, at 127.
[220] Int'l Law Comm'n, Draft Art. On Responsibility of States for Internationally Wrongful Acts, With Commentaries, U.N. Doc. A/56/10, 135 (2001).
[221] TALLINN MANUAL 2.0, *supra* note 34, at 116 ("Countermeasures, whether cyber in nature or not, may only be taken to induce a responsible State to comply with the legal obligations it owes an injured State.").
[222] *Id.* at 112 (affirming that such limitations on countermeasures are the reason the term "may be" is used in the Rule instead of "is.").

and degradation are necessary over the long term as this persistent aggression is unlikely to cease."[223]

As discussed, the United States also may choose to employ a layered cyber deterrence strategy in which it covertly plants malware on an adversary State's internal network, waiting to activate it at a later time. On the one hand, the operation may satisfy the proportionality requirement against Russia, for example, given its repeated intrusions into U.S. infrastructure.[224] On the other hand, the United States could not successfully argue that the operation was a lawful countermeasure. Article 49 of the International Law Commission's Articles on State Responsibility is clear that a countermeasure may only be taken to induce the responsible State to cease the wrongful conduct.[225] A State with malware lurking within its cyber infrastructure cannot be induced to alter its behavior if it is unaware that the malware even exists. Moreover, a State may only use a countermeasure in response to a wrongful act.[226] For example, if Iran maintains its nuclear program in compliance with international law, countermeasures are unavailable under layered cyber deterrence regardless of how vehemently the United States and its allies oppose the program.

D. Espionage

Cyber espionage is defined under the Tallinn Manual as "any act undertaken clandestinely or under false pretenses that uses cyber capabilities to gather, or attempt to gather, information."[227] It can involve cyber surveillance, monitoring, capturing, or exfiltrating electronically transmitted or stored communications, data, or other information.[228] The Solarium Commission defines cyber espionage in its Report simply as a "cyber operation whose primary purpose is to steal information for national security or commercial purposes."[229] The Commission considers espionage to be a major threat to U.S. economic, national security, and other interests and thus makes responding to it a key component of its layered cyber deterrence strategy.[230] To understand, anticipate, and counter these cyber threats under layered cyber deterrence, the United States intends to gather information, surveil and monitor adversaries, and capture communications and data by accessing its adversaries' networks.

---

[223] Kosseff, *supra* note 93, at 8.
[224] Int'l Law Comm'n, *supra* note 220, at 134–35.
[225] *Id.* at 129–30.
[226] Schmitt, s*upra* note 99.
[227] TALLINN MANUAL 2.0, s*upra* note 34, at 168.
[228] *Id.*
[229] U.S. CYBERSPACE SOLARIUM COMM'N, *supra* note 2, at 132.
[230] *Id.* at v.

Although a State's peacetime cyber espionage operations are not a *per se* violation of international law, they could be if not properly executed under layered cyber deterrence.[231] The U.S. government's position is that espionage is lawful, even when it involves physical or virtual intrusion into a foreign territory, if it is only to acquire information or conduct counterintelligence activities, such as deploying honeypots.[232] Beyond that, a U.S. cyber espionage operation under layered cyber deterrence could become unlawful if, for example, it inadvertently deleted an adversary government's critical data or caused harm to its vital networks during the espionage operation.[233]

Characterizing cyber activity as espionage is irrelevant, however, according to the Tallinn Manual. What matters is whether the underlying act in question violates international law[234] and several acts of espionage do not, such as when the offended State can claim consent, self-defense, countermeasures, necessity, force majeure, and distress.[235] If the cyber espionage activity does violate international law, for example when it infringes on sovereignty or the nonintervention principle, it may still be a lawful countermeasure if the adversary State violated international law first.[236]

The Solarium Commission Report identifies China as a major U.S. adversary in cyber espionage operations. China is gaining considerable power to surveil its business clients who have a growing reliance on its technology. One of its clients is the United States. Because of this, the Commission notes that China poses a growing attack threat to the United States' core military and critical infrastructure systems.[237] The Report also notes that China is the most active cyber espionage threat to the United States government, its allies, and U.S. corporations.[238] One cyber operation publicly attributed to China is its twelve-year espionage campaign conducted by the alleged State-sponsored hacking group ATP10. Over the twelve-year period, the group stole massive amounts of U.S. intellectual property and compromised computer systems containing personally identifiable information on over one hundred thousand U.S. Navy personnel.[239] Under these circumstances, the

---

[231] TALLINN MANUAL 2.0, *supra* note 34, at 168.
[232] Ney, Jr., *supra* note 88.
[233] Kosseff, *supra* note 93, at 11.
[234] TALLINN MANUAL 2.0, *supra* note 34, at 25.
[235] TALLINN MANUAL 2.0, *supra* note 34, at 104.
[236] Kosseff, *supra* note 93.
[237] Brian Barrett, *How China's Elite APT10 Hackers Stole the World's Secrets,* WIRED (Dec. 20, 2018). https://www.wired.com/story/doj-indictment-chinese-hackers-apt10/ ("'No country poses a broader, more severe long-term threat to our nation's economy and cyber infrastructure than China. China's goal, simply put, is to replace the US as the world's leading superpower, and they're using illegal methods to get there,' FBI director Christopher Wray said.... 'While we welcome fair competition, we cannot and will not tolerate illegal hacking, stealing, or cheating.'").
[238] U.S. CYBERSPACE SOLARIUM COMM'N, *supra* note 2, at 11.
[239] *Id.* at 10.

United States would be entitled to engage in lawful countermeasures against China under layered cyber deterrence, given China's unlawful infringement on U.S. sovereignty and its violation of the nonintervention principle.

CONCLUSION

There is no question that the United States is facing an escalating number of cyberattacks on its critical infrastructure that are increasing in severity. The Cyberspace Solarium Commission's report and layered cyber deterrence propose to address these attacks in a more comprehensive and cohesive fashion than earlier U.S. cyber strategies. At the same time, this paper discussed several ways in which layered cyber deterrence falls short. The whole-of-nation strategy reduces the government's control over the plan, can place critical U.S. infrastructure at increased risk, and may make the United States more vulnerable to international law violations when it fails to exercise due diligence and private cyber misconduct is attributed to it. The layered cyber deterrence strategy lacks a clear definition of what adversary actions will result in retaliation and lacks credibility due to the U.S.'s failure to impose strong, meaningful consequences on cyber attackers. Layered cyber deterrence will only be effective if it leads to swift and punitive measures for the most egregious cyberattacks, not merely a continued over-reliance on deterrence by denial. With proper attribution, the United States also must be prepared to use all instruments of national power, including military threats or force if necessary, to punish and deter critical attacks on U.S. infrastructure. Because layered cyber deterrence incorporates defend forward, the United States also runs the risk of violating State sovereignty and the nonintervention principle. Despite defenses available to it, as the U.S. implements layered cyber deterrence and itself engages in extraterritorial intrusions into other States' networks, it must take steps to avoid such violations, such as by characterizing its actions as lawful countermeasures or espionage. Finally, the success of the layered cyber deterrence strategy depends in large part on the United States' willingness to finally take consistent and concerted action in response to major cyberattacks. Rather than merely rely on deterrence by words, the U.S. also must deter by punishment and prosecution to impact adversaries' cost-benefit calculus and shape their behavior, and finally lead by example in this developing military realm of cyberspace.