University of Miami Inter-American Law Review

Volume 53 | Number 1 Article 4

12-13-2021

Defend Forward & Sovereignty: How America's Cyberwar Strategy Upholds International Law

Elya Taichman
Congresswoman Lori Trahan

Defend Forward & Sovereignty: How America's Cyberwar Strategy Upholds International Law

Elya Taichman*

To thwart a seemingly neve rending bombardment of cyberattacks, the U.S. Department of Defense recently implemented a new strategy – defending forward. This approach demands persistently engaging the enemy on a daily basis to disrupt cyber activity. Rather than waiting to be attacked, the United States is bringing the fight to the enemy. However, this strategy poses fascinating and complex questions of international law. In particular, because most defend forward operations fall within the gray zone of warfare, it remains unclear whether these operations violate the sovereignty of American adversaries or even third party nation states in whose cyberspace U.S. Cyber Command is operating. This paper proposes that defend forward does not violate sovereignty within international law. First, sovereignty is a principle of international law, not a rule the United States can violata. Second, American domestic law has limited defend forward operations to proportional responses to persistent cyber-attacks and threats.

---

* Elya Taichman serves as the Legislative Director for Congresswoman Lori Trahan (D-MA) where he advises her on a range of issues including national security and foreign policy. He is currently obtaining his J.D. at Temple University Beasley School of Law where he is a Beasley Scholar, and a Law and Public Policy Scholar. The views expressed in this article are those of the author and do not necessarily reflect the official policy or position of Congresswoman Trahan.

Finally, America's chief adversaries have fundamentally different understandings of sovereignty, which reinforces the necessity and legality of defend forward. Overall, defend forward should be viewed as fitting squarely in the existing framework of international law. Whether defend forward will succeed, however, is another question.

I. INTRODUCTION

The United States is under perpetual attack and old strategies are not working. The ubiquity of connectivity in the digital age and societal dependence on the Internet for the most basic of actions has rendered cyberspace a critical realm to be defended. The United States' adversaries have shown an insatiable appetite for hacking American cyberspace—whether to steal data, disrupt elections, or merely cause fear—that has yet to be quenched. Regrettably, old Cold War strategies like deterrence have not worked in cyberspace because the costs inflicted on enemies are not severe enough for cyber warfare.[1] As Commander of U.S. Cyber Command, General Paul Nakasone wrote, "a reactive and defensive posture proved inadequate to manage evolving threats."[2] Recognizing this dilemma, in 2018 the Department of Defense (DoD) implemented a new strategy for combatting adversaries in this new arena—defending forward.[3]

Defending forward entails persistently engaging the enemy on a daily basis to "disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict."[4] The goal is to make it harder for adversaries to succeed in their cyber–attacks. It is accomplished through strengthening defenses on government networks, critical infrastructure, and coordinating with private entities.[5] This strategy demands working with American allies and hunting together for adversaries in allied cyberspace.[6] Additionally, defending forward attempts to prevent adversaries from being able to launch an attack in the first place.

---

[1] James Andrew Lewis, Toward a More Coercive Cyber Strategy, CTR. FOR STRATEGIC & INT'L STUD. (March 10, 2021), https://www.csis.org/analysis/toward-more-coercive-cyber-strategy.

[2] Paul M. Nakasone & Michael Sulmeyer, How to Compete in Cyberspace: Cyber Command's New Approach, FOREIGN AFF. (Aug. 25, 2020), https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity.

[3] 3.U.S. DEP'T OF DEFENSE, THE DEPARTMENT OF DEFENSE CYBER STRATEGY (2018).

[4] *Id* at 1.

[5] Nakasone & Sulmeyer, *supra* note 2.

[6] *Id.* (describing the "hunt forward" mission Cyber Command completed in 2019 in Montenegro).

Gathering intelligence ahead of attacks and deploying cyber–weapons to preempt or prevent those attacks is essential.[7]

However, defending forward poses important questions, especially under international law. First, it remains unclear whether defend forward cyber operations amount to a use of force, an armed attack, a prohibited intervention, or a violation of another nation's sovereignty. Ultimately, the bulk of actions under defending forward will largely exist in a gray space that is a level below a use of force.[8] As such, defend forward demands an understanding of whether it violates the target nation's or a third–party nation's sovereignty. Overall, sovereignty and defend forward are compatible because American domestic law has authorized only proportional responses to cyber–attacks and threats. Additionally, under international law, sovereignty, as applied to cyberspace, is a principle that must be considered, but it is not a rule that can be violated. Importantly, Cyber Command has thus far attempted operations that involve only *de minimis* effects on third–party nations' sovereignty. Finally, the adversaries that Cyber Command targets have fundamentally different understandings of sovereignty than the United States and its allies. Russia and China, for example, wield sovereignty as a shield under international law while simultaneously slashing American sovereignty with the sword of cyber–attacks. This reinforces the United States' right to respond in–kind through defend forward, even if it is no longer waiting to be attacked.

II. INTERNATIONAL LAW IN CYBERSPACE

This section begins by discussing how international law classifies different actions in cyberspace and cyberwar, from espionage to an armed attack. While most of these categories are clear under international law, sovereignty violations in cyberspace are not. Next, the section includes a brief discussion on the traditional notions of sovereignty, which demonstrate why cyberspace defies traditional classification. Finally, the section lays out the debate between those who argue sovereignty is a rule that may be violated and those who view it instead as a principle.

---

[7] Nakasone & Sulmeyer, *supra* note 2.

[8] *See id.*

a. How the Structure of International Law Renders Sovereignty Critical for Analyzing Defend Forward's Gray Zone Activities

The United States has recognized that international law governs cyberspace and cyberwar.[9] In a 2012 speech, State Department Legal Advisor Harold Koh made this unambiguous when he explained that cyberspace is not a "law–free zone."[10] For Koh, new technologies in cyberspace have raised new questions in international law, but not whether international law applies to cyberspace.[11] The vast majority of sovereign states ascribe to this viewpoint, as does the Tallinn Manual 1.0 which proclaims, "that general principles of international law appl[y] to cyberspace."[12] This matters because many scholars have argued that the Internet is so fundamentally different from physical space that the normal order would not apply.[13] Recognizing that international law governs cy-

---

[9] Harold Koh, State Department Legal Advisor, International Law in Cyberspace, Address at USCYBERCOM Inter-Agency Legal Conference Ft. Meade, MD (Sept. 18, 2012), https://harvardilj.org/wp-content/uploads/sites/15/2012/12/Koh-Speech-to-Publish1.pdf [hereinafter Koh Speech] (opining, "[T]he United States has made clear our view that established principles of international law do apply in cyberspace."); Brian Egan, State Department Legal Advisor, Remarks on International Law and Stability in Cyberspace, Address at Berkeley Law School, CA, (Nov. 10, 2016), https://2009-2017.state.gov/s/l/releases/remarks/264303.htm [hereinafter Egan Speech] (explaining, "There are three pillars to the U.S. strategic framework, each of which can help to ensure stability in cyberspace by reducing the risks of misperception and escalation. The first is global affirmation of the applicability of existing international law to State activity in cyberspace in both peacetime and during armed conflict.).

[10] Koh Speech, *supra* note 9, at 3

[11] *Id.*

[12] TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 13 (Michael N. Schmitt, gen. ed., 2013). The Tallinn Manual is a non-binding, academic study on the application of international law in cyberspace. The experts who compiled it seek to answer relevant questions on how nations should behave in cyber space. Michael Schmitt led the project. *Id.*

[13] *See* David R. Johnson & David G. Post, *Laws and Borders – The Rise of Law in Cyberspace*, 48 STANFORD LAW REVIEW 1367, 1370 (1996) (explaining that "Cyberspace radically undermines the relationship between legally significant (online) phenomena and physical location . . . The Net thus radically subverts a system of rule-making based on borders between physical spaces, at least with respect to the claim that cyberspace should naturally be governed by territorially defined rule."); John Perry Barlow, *A Declaration of the Independence of Cyberspace*, ELECTRONIC FRONTIER FOUNDATION (1996) (arguing "Governments of the Industrial World . . . You have no sovereignty where we gath-

berspace is a necessary precondition to debating the legalities of defend forward because only sovereign states can make international law.

The United Nations Charter is a useful place to begin an investigation of how international law applies in cyberspace and to cyberwar. Article 2(4) prohibits the "threat or use of force against the territorial integrity or political independence of any State."[14] Coupled with Article 51, sovereign states are permitted to use force in self–defense against an "armed attack."[15] While the United States, unlike most other states, has not recognized a difference between an armed attack and the use of force, many cyber actions may take place below the threshold of an illegal use of force.[16] These activities occur in a realm somewhere between war and peace, which is commonly referred to as the gray zone.[17]

It is, perhaps, easier to define cyber–actions above gray zone activities that would amount to a use of force. American strategic thinking employs an effects test to measure cyberattacks in comparison to physical attacks.[18] Koh explained that any cyber–activities resulting in someone's death would likely constitute a use of force.[19] Koh listed factors to consider: "the context of the event, the actor perpetrating the action (recognizing challenging issues of attribution in cyberspace), the target and location, effects

---

er . . . Your legal concepts of property, expression, identify, movement, and context do not apply to us. They are all based on matter, and there is no matter here).

[14] U.N. Charter art. 2, ¶ 4.

[15] U.N. Charter art. 51.

[16] Koh Speech, *supra* note 9. *compare id. with* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.) (Merits1986 I.C.J. 14, ¶ 191 (June 27) (explaining, "it will be necessary to distinguish the most grave forms of the use of force (those constituting an armed attack) from other less grave forms") *and* ¶ 249 ("[w]hile an armed attack would give rise to an entitlement to collective self-defense, a use of force of a lesser degree of gravity cannot . . . produce any entitlement to take collective countermeasures involving the use of force")).

[17] Gary P. Corn, *Cyber National Security: Navigating Gray Zone Challenges In and Through Cyberspace*, *in* COMPLEX BATTLESPACES: THE L. OF ARMED CONFLICT AND THE DYNAMICS OF MODERN WARFARE 345, 347 (Winston S. Williams & Christopher M. Ford eds., 2018).

[18] Koh Speech, *supra* note 9 at 4.

[19] *Id.*

and intent, among other possible issues."[20] Should a cyber operation trigger a nuclear plant meltdown, that would most likely amount to an illegal use of force against the United States; after all, the intent and target of the perpetrator could only be malicious. Overall, such an attack would be almost indistinguishable in effect from the Russians dropping a KAB–500S–E on that same reactor.[21] However, cyber operations in the gray zone are inherently insufficient in effects to qualify as an armed attack or a use of force. But these cyber–activities are still disruptive and unwelcome for victim states which demand legal responses and an effective means to deter, halt, or thwart such attacks.

The gray zone creates a host of legal issues for the United States because the bulk of cyber operations pursued under the defend forward strategy would most likely occur in the gray zone.[22] This means it will likely fall into one of the three tiers of the gray zone: espionage, a sovereignty violation, or a prohibited intervention. Espionage, which includes cyber espionage, is not prohibited under international law, though it is certainly unwelcome.[23] As the name would suggest, prohibited interventions are illegal under international law and require coercion of one state against another.[24] They also enable the victim state to respond with countermeasures.[25] However, it is unclear whether a defend forward mission that violates another nation's sovereignty in cyberspace also violates international law.

---

[20] *Id.*

[21] *See* KAB-500S / KAB-500S-E, MILITARY, https://www.globalsecurity.org/military/world/russia/kab-500se.htm (A KAB-500S-E is the Russian equivalent of a Joint Direct Attack Munition (JDAM)).

[22] Robert Chesney, The Domestic Legal Framework for U.S. Military Cyber Operations, in NATIONAL SECURITY, TECHNOLOGY, AND LAW, HOOVER INST. (July 29, 2020), https://s3.documentcloud.org/documents/7014455/Chesney-Webreadypdf.pdf

[23] Robert Chesney, *The Pentagon's General Counsel on the Law of Military Operations in Cyberspace*, LAWFARE (March 9, 2020, 12:33 PM), https://www.lawfareblog.com/pentagons-general-counsel-law-military-operations-cyberspace.

[24] *Id.*

[25] *See* Mary Ellen O'Connell, *Attribution and Other Conditions of Lawful Countermeasures to Cyber Misconduct*, 10 NOTRE DAME J. OF INT'L & COMPAR. L. 1, 8 (2020).

Cyber Command successfully blocking Internet access to the Russian Internet Research Agency (IRA) in St. Petersburg in 2018 is an excellent example of the dilemma defend forward faces.[26] The mission lasted for several days until American election results were certified.[27] During the operation, Cyber Command contacted Russian operatives directly to make it clear the United States knew who they were.[28] While this mission helped protect the integrity of American elections, no one has claimed that it amounted to a use of force. Still, as General Paul Nakasone, Commander of Cyber Command and Director of the National Security Agency, offered, disrupting the IRA in 2018 required "operating outside our borders, being outside our networks, to ensure that we understand what our adversaries are doing."[29] The DoD was operating in Russian cyberinfrastructure, or perhaps a third country's cyber infrastructure in order to target the IRA, depending on how the IRA had initially deployed its resources. This demonstrates the paradox in defending forward: because deterrence alone is ineffective, success demands taking action in foreign networks, often to protect the sovereignty of the United States. Does this mean the United States violated another nation's sovereignty in order to defend its own?

b. Sovereignty in Cyberspace

Sovereignty is commonly considered the chief organizing principle of nation–states that arose out of the Peace of Westphalia.[30] Historian F.H. Hinsley defined it as "the idea that there is a final

---

[26] Ellen Nakashima, *U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms*, WASH. POST (Feb. 27, 2019, 8:22 AM) 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. The IRA is infamous as the troll factory that spread propaganda and misinformation in the 2016 election. *Id.*

[27] Julian E. Barner, *Cyber Command Operation Took Down Russian Troll Farm for Midterm Elections*, N.Y. TIMES (Feb. 26, 2019), https://www.nytimes.com/2019/02/26/us/politics/us-cyber-command-russia.html.

[28] *See id.*

[29] *An Interview with Paul M. Nakasone*, JOINT FORCE Q. (2019), https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92_4-9_Nakasone-Interview.pdf.

[30] *See* Derek Croxton, *The Peace of Westphalia and the Origins of Sovereignty*, 21 THE INT'L. HIST. REV. 569, 570 (1999).

and absolute political authority in the political community . . . . . and no final and absolute authority exists elsewhere."[31] In the traditional sense of nation–states this is a simple concept to grasp. When the Third Reich crossed the Polish border on September 1, 1939, it had invaded the sovereignty of Poland because the Polish government was supposed to be the only government that exercised control within its territories. The invasion was intended to coerce Warsaw into having no choice but to surrender. After the Second World War, the U.N. Charter reaffirmed the principle of sovereignty in Article 2(1) stating, "The Organization is based on the principle of the *sovereign* equality of all its Members."[32]

Sovereignty is both an internal and external concept. Internally, it refers to a state's right to control those within the state and the activities that occur within its borders.[33] This also includes a state's ability to control individuals conducting cyber activities as well as its cyber infrastructure.[34] Externally, sovereignty empowers a state to conduct international relations; for example, declaring war or entering into a treaty.[35] But in a world of interconnected cyberspace, where sending an email or doing a Google search often involves traveling through Internet service providers (ISP) and nodes across multiple countries, it is readily apparent that the otherwise tidy geographical lines of sovereignty are muddled.

This presents significant issues for DoD's strategy of defend forward. As General Nakasone elucidated, defending forward demands operating in foreign networks.[36] However, customary international law has recognized that states are prohibited from intervening in the internal or external sovereignty of another state.[37]

---

[31] F.H. HINSLEY, SOVEREIGNTY 26 (2nd ed. 1966).

[32] U.N. Charter art. 2, ¶ 1 (emphasis added).

[33] Michael N. Schmitt, *Grey Zones in the International Law of Cyberspace*, 42 YALE J. OF INT'L L. ONLINE 1, 4 (2018).

[34] *Id.*

[35] *Id;* Channel Case (U.K. v. Alb.) (Merits), 1949 I.C.J. REP. 4, 43 (Apr. 9), (Judge Alvarez explained that sovereignty meant, "the whole body of rights and attributes which a state possesses in its territory, to the exclusion of all other states, and also in its relation with other states.")

[36] Nakasone, *supra* note 29.

[37] *See* Military and Paramilitary Activities in and Against Nicaragua (*Nicar. v. U.S.*) (Merits), 1986 I.C.J. 14, 106, ¶ 202 (June 27) (holding that "[t]he principle of non-intervention involves the right of every sovereign State to conduct

This protects states from intervention below what would otherwise qualify as a use of force.[38] Indeed, the International Court of Justice has recognized non–intervention as "a corollary of the principle of the sovereign equality of States."[39] When the United States shut off the IRA's Internet in 2018, it was operating in Russian cyberspace, and the mission had affected the ability of the Russian government to control the cyber activities within its territory.[40] Whether this mission violated international law is an open debate that revolves around two interpretations of the role of sovereignty in cyberwar and the gray zone.

i. Sovereignty as a Rule

Many states and legal experts view sovereignty as a rule within international law that may be violated through gray zone cyber operations.[41] The Tallinn Manual 2.0 takes this approach when it stated, "[a] State must not conduct cyber operations that violate the sovereignty of another State."[42] That seems easy enough. However, Michael Schmitt, who directed the Tallinn Manual compilation, acknowledged that state practice and *opinio juris*—a sense of legal obligation felt by a state—have not definitively coalesced around an understanding for sovereignty in the gray zone.[43] In fact, some of the Tallinn Manual 2.0 experts proposed that sovereignty violations should be limited to cyber operations that cause physical

---

its affairs without outside interference . . . the Court considers that it is part and parcel of customary international law.").

[38] Corn, *supra* note 17, at 410.

[39] I.C.J., *supra* note 37 at ¶ 202.

[40] After all, the Russians have passed a cyber sovereignty law and want to have a firewall like that of China. *See* Zak Doffman , *Putin Now Has Russia's Internet Kill Switch To Stop U.S. Cyberattacks*, FORBES (Oct 28, 2019, 8:55 PM), https://www.forbes.com/sites/zakdoffman/2019/10/28/putin-now-has-russias-internet-kill-switch-to-stop-us-cyberattacks/?sh=b24c6e031b2b.

[41] Jack Kenny, *France, Cyber Operations and Sovereignty: The 'Purist' Approach to Sovereignty and Contradictory State Practice*, LAWFARE (March 12, 2021, 8:01 AM), https://www.lawfareblog.com/france-cyber-operations-and-sovereignty-purist-approach-sovereignty-and-contradictory-state-practice.

[42] TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 17 (Michael N. Schmitt & Liis Vihul eds., 2017) [hereinafter TALLINN MANUAL 2.0].

[43] Schmitt, *supra* note 33, at 6.

damage.[44] Ultimately, the majority of experts agree that cyber operations that cause non–temporary loss of functionality violate sovereignty even when no physical damage occurs.[45] Still, the experts could not agree on the precise threshold at which this occurs because of a lack of *opinio juris* from states. Additionally, the experts could not decide whether gray zone operations lacking physical effects or causing loss of functionality violated sovereignty, though they offered several possibilities.[46] One of these, " . . . causing a temporary, but significant, loss of functionality, as in the case of a major DDoS operation,"[47] sounds awfully similar to Cyber Command disabling the IRA's Internet for several days.[48] Importantly, the Tallinn Manual also concluded that a cyber operation which "usurps the inherently governmental functions of another State" violates sovereignty.[49] Unfortunately, the experts could not settle on a definition of inherently governmental functions.[50]

On its face, sovereignty, as a rule, is clear–cut. Brightline rules certainly make things simpler. Of the states offering opinions on this debate, most recognize sovereignty as a rule.[51] Regrettably, this rule is not as easy to follow as it appears. While several states have offered a viewpoint, overall, very few states have answered

---

[44] *Id.*

[45] *See* TALLINN MANUAL 2.0, *supra* note 42, at 20.

[46] *Id.* at 21, (The possibilities included, "a cyber operation causing cyber infrastructure or programs to operate differently; altering or deleting data stored in cyber infrastructure without causing physical or functional consequences, as described above; emplacing malware into a system; installing backdoors; and causing a temporary, but significant, loss of functionality, as in the case of a major DDoS operation.").

[47] DDoS means Denial-of-service. *Id.* at 29.

[48] *See* TALLINN MANUAL 2.0, *supra* note 42, at 21.

[49] *Id.*

[50] *Id.* at 22. The experts agreed inherently governmental included "operation that interferes with data or services that are necessary for the exercise of inherently governmental functions is prohibited as a violation of sovereignty," which is rather circular in logic. *Id.* They offered potential examples, "changing or deleting data such that it interferes with the delivery of social services, the conduct of elections, the collection of taxes, the effective conduct of diplomacy, and the performance of key national defence activities." *Id.* Still, the important point is they could ultimately not agree on what inherently governmental functions are. *Id.*

[51] *See infra* text accompanying note 102.

this question.[52] Oddly, the Tallinn experts proclaimed that sovereignty as a rule exists, but then explained that states must define what the rule means.[53] For instance, the experts could not concur on the threshold for violating sovereignty via loss of functionality without physical damage.[54] If such a threshold is indeterminate, it would be hard to describe sovereignty as a rule. Rather, a principle would seem more accurate. Ultimately, state practice and *opinio juris* will crystalize into international law.[55] But, at the moment, the experts are putting the cart before the horse. The Tallinn Manual is a useful jumping–off point for states hoping to answer this question, but it is not law. This is not to say that the Tallinn experts are wrong. They may be right, but their determinations read more as *lex feranda*, as opposed to *lex lata*.[56]

ii. Sovereignty as a Principle

On the other hand, several scholars view sovereignty as a "baseline principle undergirding specific primary norms," such as the prohibition on the use of force.[57] They argue state practice and *opinio juris* have not crystallized into a common understanding that sovereignty is an independent rule of customary international law that gray zone operations violate.[58] Without a clear prohibition, it is ultimately up to states to decide for themselves whether sovereignty is a rule or principle through practice, treaties, or declarations.[59] Currently, the inherent tension between internal and external sovereignty—the right to control cyber activities within a state's territory and the concurrent right of states to execute cyber operations as a form of international affairs—has produced a principle. Under this thinking, the principle of sovereignty should be

---

[52] Harriet Moynihan, *The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention*, CHATHAM HOUSE (Dec. 2, 2019), https://www.chathamhouse.org/2019/12/application-international-law-state-cyberattacks/2-application-sovereignty-cyberspace.

[53] *See* TALLINN MANUAL 2.0, *supra* note 42, at 17-27.

[54] *Id.* at 20-21.

[55] Moynihan, *supra* note 52, at 2

[56] Corn, *supra* note 17, at 419.

[57] *Id.* at 414-15.

[58] *Id.* at 416-7.

[59] *Id.* at 421.

considered before any military operations, but it is not determinative.[60]

Ret. Colonel Gary Corn offers compelling reasons for why sovereignty as a rule is erroneous and why a principle is more accurate. In addition to states not having a consistent practice or stated opinion, experts themselves cannot agree.[61] Corn points to debates among the International Group of Experts who authored the Tallin Manuals on what type of cyber operation would violate sovereignty.[62] Corn is also critical of the Tallinn experts for only considering territorial sovereignty and confusing internal sovereignty with the inviolability of borders under both Article 2(4) and nonintervention.[63] These, Corn contends, demand a higher threshold before violation than cyber operations affecting information and technology infrastructure inside another state's borders.[64] Applying this thinking, Cyber Command shutting the IRA's internet off in 2018 would not rise to the level of prohibited intervention, let alone a use of force. Additionally, Corn points out that espionage, despite violating domestic laws in victims states, does not violate international law.[65] This lends credence to the acceptability of taking actions internally in the territory of a foreign state. Lastly, although sovereignty itself is universal as a principle, its application is unique across different domains. Corn and Robert Taylor, former Principal Deputy General Counsel of the Department of Defense, note the "different regimes to govern the air, space, and maritime domains underscores the fallacy of a universal rule of sovereignty with a clear application to the domain of cyberspace."[66]

---

[60] *Id.*

[61] *Id.*

[62] *See* Corn, *supra* note 17, at 417; *see* Schmitt, *supra* note 33, at 6; *see generally* TALLINN MANUAL 2.0, *supra* note 42, at 17–27; *see* Schmitt, *supra* note 33, at 6 (While the experts debated what would violate sovereignty, Schmitt notes, "a majority of [experts] concluded that remotely causing cyber infrastructure's non-temporary loss of functionality is likewise a sovereignty violation, even if no physical damage occurs.").

[63] Corn, *supra* note 17, at 417.

[64] *Id.*

[65] *Id.*

[66] Gary P. Corn & Robert Taylor, *Sovereignty in the Age of Cyber*, 111 AJIL UNBOUND 207, 210 (2017).

This statement reinforces how state practice will determine the application of sovereignty more than anything else.

Schmitt rebuts Corn's thinking and points out that throughout the seven years of deliberations among Tallinn Manual experts, not once did the sovereignty as a principle idea surface.[67] This is a weak argument. The fact that an idea is new or novel does not inherently disqualify it and the academic and global situation has changed greatly since Tallinn 2.0. To start, a growing consensus of experts agree that traditional deterrence is a fool's errand in the gray zone, and the DoD promulgated defend forward a year after Tallinn 2.0. Significantly, the United States, the world's most powerful cyber power, and its greatest target, has not adopted the "sovereignty as a rule approach." Therefore, an examination of state practice and *opinio juris* of the United States will assist in understanding how the United States is reconciling defend forward and the issue of sovereignty.

III. HOW AMERICAN AND FOREIGN STATE PRACTICE AND *OPINIO JURIS* ON SOVEREIGNTY IN CYBERSPACE DEMONSTRATE THAT SOVEREIGNTY IS A PRINCIPLE, NOT A RULE

This section begins with a discussion of how the United States' position on sovereignty in cyberspace has been articulated with greater clarity since 2012 when Koh first vaguely established the American position that sovereignty is a principle. This includes an analysis of Koh's position as well as that of the subsequent State Department Legal Advisor, Brian Egan, and also of the DoD's General Counsel, Paul C. Ney Jr. Next, the section considers the practice of American allies: France and the United Kingdom. France has taken the view that sovereignty is a rule, whereas Britain is even clearer than the United States that sovereignty is a principle. The section concludes by examining the hypocrisy of American adversaries, Russia and China, in their views on cyberspace. Both nations want to have their cake and eat it too.

---

[67] Schmitt, *supra* note 33, at 5.

a. American State Practice and Opinio Juris on Sovereignty in Cyberspace

Although not explicit, American state practice and *opinio juris* have adopted sovereignty as a principle. In the same 2012 speech in which he declared that international law applied in cyberspace, Harold Koh declared that before conducting cyber operations, including in armed conflict, the "sovereignty of other states needs to be considered."[68] This is because the physical infrastructure of the Internet is located across multiple countries and jurisdictions and because the effects of a single operation in one nation may be felt in many others.[69] Though he did not say so explicitly, it appears Koh did not endorse the sovereignty as a rule approach. After all, a rule is not something to simply be considered, but instead followed. However, Koh's thoughts on sovereignty in cyberspace were a brief paragraph in a lengthy speech.

Four years later, the next State Department Legal Advisor, Brian Egan, built on Koh's initial assertion. Egan clarified that the United States respects the sovereignty of all states to pass laws that govern their territories and operations which violate those laws could be prosecuted in the victim state or have foreign policy consequences.[70] Whether such an operation violated international law was a separate question.[71] Egan acknowledged a cyber operation in another state's territory could violate international law, despite not amounting to a use of force, and that because of the physical design of the Internet this could encroach on another state's sovereignty.[72] Nevertheless, Egan opined, "Precisely when a non–consensual cyber operation violates the sovereignty of another State is a question lawyers within the U.S. government continue to study carefully, and it is one that ultimately will be resolved through the practice and *opinio juris* of States."[73] Egan's statement demonstrates that as of 2016, the United States had not adopted sovereignty as a rule approach. If a rule already existed, it would

---

68 Koh Speech, *supra* note 9.
69 *Id.*
70 Egan Speech, *supra* note 9.
71 *Id.*
72 *Id.*
73 *Id.*

not require additional state practice or *opinio juris*, it would simply exist. Egan would have been able to assert its existence.

Egan next considered nonintervention, the corollary of sovereignty, and coercion intended to affect the victim state's ability to affect an issue it should have exclusive control over because of its sovereign rights.[74] Egan called this a "relatively narrow rule of customary international law."[75] He then cited cyber operations that interfered in a victim state's ability to hold a free election or if those operations actually manipulated the results of that election as an example of a prohibited intervention.[76] So, although Egan did not call sovereignty a rule, nonintervention, a derivative of sovereignty, is a rule. This reinforces the line of thinking that sovereignty is a principle from which other primary rules emanate.[77]

Still, the answer is perhaps more nuanced. Importantly, Egan's speech was made on November 10, 2016, two days after the Presidential election, and long after the upper echelons of the U.S. government knew of Russian interference in the election.[78] In fact, President Obama had already issued a warning to President Putin on October 31, 2016, that "[i]nternational law, including the law for armed conflict, applies to actions in cyberspace."[79] Obama could have told Putin that Russia's actions amounted to an act of war; in fact, at least one senior advisor recommended he assert that interfering in our election was an act of war.[80] Instead, Obama chose a vague warning.

This begs the question of what the Democratic National Committee (DNC) hack was under international law. To start, no one is arguing it amounted to an illegal use of force.[81] Professor William Banks believes it was not even a prohibited intervention or interna-

---

[74] *Id.*

[75] *Id.*

[76] *Id.*

[77] Kenny, *supra* note 41.

[78] William M. Arkin, et al., *What Obama Said to Putin on the Red Phone About the Election Hack*, NBC NEWS (Dec. 19, 2016, 6:30 PM), https://www.nbcnews.com/news/us-news/what-obama-said-putin-red-phone-about-election-hack-n697116.

[79] *Id.*

[80] *Id.*

[81] William Banks, *State Responsibility and Attribution of Cyber Intrusions After Tallinn 2.0*, 95 TEX. L. REV. 1487, 1500 (2017).

tionally wrongful act.[82] Certainly, the Russians stole and published private information, but that was espionage, which is not prohibited under international law. Had the Russians actually used cyber weapons to "tamper with voting machines or change votes" that would be coercion, as it would have limited American ability to have a free and fair election.[83] Nonetheless, few would argue the Russians did not "change votes" through their propaganda and dissemination of fake news – different than the private, but true, emails of Hillary Clinton, John Podesta, and others. In fact, former CIA Director, General Michael Hayden, said Russia had gone further than "honorable state espionage" when it "weaponized" the data it stole.[84] In this sense, the Russian hack was coercive, and that seems to be what Egan was implying in his speech.

Obama's statement to Putin and Egan's speech, made only weeks apart, demonstrate the United States grasping for the correct terminology to describe the Russian election hack while simultaneously providing American forces enough latitude to conduct future cyber operations. Egan made clear that cyber operations on devices in foreign jurisdictions are not a "per se violation of international law. In other words, there is no absolute prohibition on such operations as a matter of international law. This is perhaps most clear where such activities in another State's territory have no effects or de minimis effects."[85] This could mean two things: that cyber operations in foreign states do not violate sovereignty, or that sovereignty violations do not automatically produce international law violations. Either way, sovereignty is not a rule. Therefore, it must be a principle. Moreover, by stating that operations lacking in effects or those with *de minimis* effects do not inherently violate sovereignty, Egan is attempting to resolve what happens if

---

[82] *Id.*

[83] *Id.* at 1501. Fortunately, the Mueller report asserted there was no evidence the Russians directly altered votes or attempted to do so.

[84] Nicole Gaouette, *Ex-CIA Chief: Russian Hackers Trying to 'Mess with Our Heads'*, CNN (Oct. 18, 2016, 6:19 PM), https://www.cnn.com/2016/10/18/politics/hayden-russia-us-cyber-elections. *Compare id.* (Hayden statement), with Quotes FAQ, INT'L CHUTCHILL SOC., https://winstonchurchill.org/resources/quotes/quotes-faq/ (last visited May 8, 2021, at 11:32 AM) (Ed Murrow describing Churchill mobilizing the English language and sending it into battle which used the truth to rally the British people.).

[85] Egan Speech, *supra* note 9.

Cyber Command must operate in third party or neutral nation networks to thwart its adversaries.

Interestingly, Professor Banks notes that under the sovereignty as a rule and the Tallinn 2.0 approach, the Russian election hack would have violated sovereignty. Still, when it came to American state practice, the American response of "relatively nonthreatening self–help retorsion" demonstrated the United States viewed the hack not as "internationally wrongful acts, but instead as a species of espionage that is generally unregulated by international law."[86] This makes sense, though it neglects the possibility that the United States, for strategic and or political reasons, decided against a greater response despite a violation of international law. Regardless, this is incredibly frustrating as it seemingly lets Russia off the hook. But the United States may have responded in kind with proportionate, covert actions within the gray zone. Since Egan's speech, the State Department has not officially weighed in on the subject.

The most recent American pronouncements on sovereignty in cyberspace came from DoD's General Counsel, Paul C. Ney Jr., on March 2, 2020. In his speech, Ney asserted the Pentagon's attorneys take the "principle of sovereignty" into account.[87] Ney clarified that states certainly retain sovereignty over the physical infrastructure in their territories that creates cyberspace, but he acknowledged that "implications of sovereignty for cyberspace are complex."[88] Reading between the lines, this implies that if sovereignty was a binding rule, it would likely bind Cyber Command and prevent a defend forward strategy. And then, in a step Koh and Egan never took, Ney said, "we continue to study this issue and how State practice evolves in this area, even if it does not appear that there exists a *rule* that all infringements on sovereignty in cyberspace necessarily involve violations of international law."[89] To date, Ney is the highest level American official to explicitly argue

---

[86] Banks, *supra* note 81, at 1512.

[87] Hon. Paul C. Ney, Jr., *DOD General Counsel, Remarks, U.S. Cyber Command Legal Conference* , U.S. DEP'T OF DEFENSE (March 2, 2020), https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/.

[88] *Id.*

[89] *Id.* (emphasis added)

that sovereignty is not a rule. Although Ney said attorneys would continue to study the issue,[90] it appears the DoD has determined or is leaning strongly in the direction that sovereignty is a principle and not a rule as applied to cyberspace.

While Ney's speech is useful, it is not as determinative as Koh or Egan's speeches. The State Department speeches occurred only after interagency review with the goal of producing a "whole–of—government position."[91] Ney's speech is a manifestation of only the Pentagon's position.[92] Nevertheless, Ney indicates that the DoD's attorneys vet proposed cyber operations through an espionage lens.[93] Michael Schmitt explains that in this assessment, if a cyber operation resembles intelligence or counterintelligence activities it does not violate sovereignty.[94] However, if the DoD attorneys do not see a congruency then it could violate sovereignty.[95] Schmitt questions why the Pentagon would bother with such an assessment if sovereignty could not be violated.[96] As to Ney's statement on sovereignty itself, Schmitt interprets that some cyber operations in the gray zone could violate international law.[97] The trouble is identifying which ones do and which ones do not. No matter, Schmitt's argument ignores that the State Department and the DoD believe that although sovereignty can be violated, this does not mean international law is automatically violated.[98]

---

[90] *Id.*

[91] Chesney, *supra* note 22.

[92] *See id.*

[93] *See* Ney, *supra* note 81 ("In examining a proposed military cyber operation, we may therefore consider the extent to which the operation resembles or amounts to the type of intelligence or counterintelligence activity for which there is no per se international legal prohibition.").

[94] *See* Michael Schmitt, *The Defense Department's Measured Take on International Law in Cyberspace*, JUST SECURITY (March 11, 2020), https://www.justsecurity.org/69119/the-defense-departments-measured-take-on-international-law-in-cyberspace/.

[95] *See id.*

[96] *See id.*

[97] *See id.*

[98] *See* text accompanying notes 87 and 94.

b. American Allies – France and the United Kingdom Weigh in on Sovereignty

i. France – A Contradiction in Opinio Juris and State Practice

At first glance, France has taken the position that sovereignty is a rule under international law that may be violated.[99] In 2019, France's Ministry of Armed Forces proclaimed, "any cyberattack against French digital systems or any effects produced on French territory by digital means by a State organ . . . constitutes a breach of sovereignty."[100] However, although many commentators concluded that France was articulating that sovereignty is a rule of international law, this was not as clearly articulated as nations, such as Finland.[101] Indeed, Finland recently states "Finland sees sovereignty as a primary norm of public international law, a breach of which amounts to an internationally wrongful act and triggers State responsibility. This norm is fully applicable in cyberspace, too."[102] Many other states, such as Austria, Czech Republic, Germany, the Netherlands and others have taken a similar approach.[103] Furthermore, France's own actions add complexity to its official pronunciation. For example, France recently participated in Operation Ladybird, a global operation to disrupt the Emotet botnets, which have proven to be one of the past decade's greatest cyber threats.[104] The operation occurred in conjunction with the United

---

[99] Kenny, *supra* note 41.

[100] *International Law Applied to Operations in Cyberspace,* FRENCH MINISTRY OF ARMED FORCES, 7 (2019).

[101] *See* Michael Schmitt, *France's Major Statement on International Law and Cyber: An Assessment*, JUST SECURITY (Sept. 16, 2019).

[102] U.N. General Assembly, *Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States Submitted by Participating Governmental Experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security Established Pursuant to General Assembly Resolution 73/266*, U.N. Doc. A/76/136 (July 13, 2021) https://front.un-arm.org/wp-content/uploads/2021/08/A-76-136-EN.pdf.

[103] *Id.*

[104] Andy Greenberg, *Cops Disrupt Emotet, the Internet's 'Most Dangerous Malware'*, WIRED (Jan. 27, 2021, 12:46 PM), https://www.wired.com/story/emotet-botnet-takedown/. Operations against EncroChat in 2020 and Retadup in

States, United Kingdom, the Netherlands, Germany, Canada, and Lithuania.[105] To disrupt the Emotet botnets, France and others took control of three of Emotet's command and control servers, updated its code, and assumed control of an additional 700 command and control servers located across 90 states around the globe.[106] Authorities then disabled and quarantined the Emotet in infected computers.[107] Operation Ladybird also installed a "time–bomb–like code" that will uninstall Emotet from all infected computers on April 25, 2021.[108]

However, France and the other states involved did not request or receive permission from the 90 states whose cyberspace they operated in.[109] Under France's definition of sovereignty, France likely violated the sovereignty of those nations through Operation Ladybird because it operated in third party nations' cyberspace. Some of the other states involved, like Germany and the Netherlands, more affirmatively view sovereignty as a rule. Germany's approach is, "Germany agrees with the view that cyber operations attributable to States which violate the sovereignty of another State are contrary to international law. In this regard, State sovereignty constitutes a legal norm in its own right . . . "[110] Overall, even among the states who profess that sovereignty is a rule under international law, those states lack a coherent understanding of what operations actually violate sovereignty. The Netherlands, Germany and others claim an all or nothing approach, though their actions can contradict their words. The lack of agreement demonstrates

---

2019 are further examples of similar operations that appear to contradict France's own rule of sovereignty. *See* Kenny, *supra* note 41.

105 Press Release, *World's Most Dangerous Malware Emotet Disrupted Through Global Action,* EUROPOL (Jan. 27, 2021), https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action.

106 Catalin Cimpanu, *Authorities Plan to Mass-Uninstall Emotet from Infected Hosts on April 25, 2021*, ZDNET (Jan. 27, 2021, 11:55 AM) https://www.zdnet.com/article/authorities-plan-to-mass-uninstall-emotet-from-infected-hosts-on-april-25-2021/.

107 *Id.*

108 *Id.*

109 *See id.*

110 U.N. General Assembly, *supra* note 102.

that even if sovereignty is a rule, there is no agreement on what the rule is. This discord renders sovereignty a principle in effect.

ii. United Kingdom – Definitively Opposed to Sovereignty as a Rule

The United Kingdom has taken an approach similar to the United States, except it has been more vocal. On May 23, 2018, UK Attorney General, Jeremy Wright, announced, "I am not persuaded that we can currently extrapolate from that general principle a specific rule or additional prohibition for cyber activity beyond that of a prohibited intervention."[111] And then, in bold firmness declared, "The UK Government's position is therefore that there is no such rule as a matter of current international law."[112] This is an unequivocal rejection of the Tallinn Manual 2.0's approach to sovereignty. However, it is worth noting that Wright used the word "currently" in his speech. This leaves open the possibility that with future state practice this could evolve.

The United Kingdom's approach is a double–edged sword. On the one hand, it provides British policymakers complete operational flexibility in the gray zone. On the other hand, the United Kingdom has a limited vocabulary from which to condemn unfriendly cyberactions directed. This presents a dilemma for a nation on the receiving end of roughly ten cyber–attacks each week.[113] Instead, the only principle the United Kingdom may still point to in the gray zone is non–intervention. The difference, of course, between violating sovereignty and engaging in a prohibited intervention is that prohibited intervention demands coercion. Should Russia, China, or another unfriendly actor commit the equivalent of the DNC election hack during a United Kingdom election or spread fake–news and misinformation, that would likely not count as co-

---

[111] Attorney General's Office & The Rt Hon Jeremy Wright QC MP, *Cyber and International Law in the 21st Century*, GOV.UK (May 23, 2018), https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.

[112] *Id.*

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

ercion. If such acts are prohibited under international law as sovereignty violations, then the United Kingdom could respond in kind with countermeasures. But if they are not prohibited, then the United Kingdom cannot declare the perpetrators have violated international law. Notwithstanding, it may respond in kind because those actions still would not violate international law. Ultimately, this approach enables the United Kingdom to engage in gray zone activities beneath prohibited interventions without waiting for an illegal intervention as license. In short, the United Kingdom's National Cyber Force may go on the offensive and hunt cyber foes before they launch their attacks. By definitively answering the question of sovereignty, the United Kingdom may defend forward in cyberspace.

c. American Adversaries – China and Russia – Charlatans of Sovereignty

On sovereignty, China and Russia want to have it both ways. They demand that other states limit their external sovereignty, but they are quick to complain that other states have violated Russian or Chinese sovereignty through cyber operations. Hypocritically, both demonstrate a clear disregard for the sovereignty of other states.

In 2019, Vladimir Putin signed a law to create Russia's "Sovereign Internet," an internal Russian Internet.[114] This law provided Putin a "kill switch" to the world wide web in the event Russia deemed it necessary to operate an *intranet*. Moscow justified the law citing national security threats and fear of cyber–attacks against Russia.[115] While the real impetus behind this law was increasing centralized control and the ability to repress dissent, this law also reveals Russia's belief that the Russian state should retain complete control over its cyber space and that any unauthorized

---

[114] *See* Zak Doffman, *Putin Now Has Russia's Internet Kill Switch To Stop U.S. Cyberattacks*, FORBES (Oct 28, 2019, 8:55 PM), https://www.forbes.com/sites/zakdoffman/2019/10/28/putin-now-has-russias-internet-kill-switch-to-stop-us-cyberattacks/?sh=b24c6e031b2b.

[115] *See* Alexander Tabachnik & Lev Topor, *Russian Cyber Sovereignty: One Step Ahead*, RUSSIAN INT'L AFF.COUNCIL (Sept. 8, 2020), https://russiancouncil.ru/en/analytics-and-comments/analytics/russian-cyber-sovereignty-one-step-ahead/.

intrusions would violate Russia's sovereignty. China has also passed cyber sovereignty legislation to control the flow of information in and out of China.[116] It begins by setting forth its goals and aims. Article 1 of the 2016 Cybersecurity Law proclaims, "This Law is formulated in order to: ensure cybersecurity; safeguard *cyberspace sovereignty* and national security . . . and promote the healthy development of the informatization of the economy and society."[117] Overall, the law reinforces what China calls its "Golden Shield" and what the West refers to as the "Great Firewall."[118]

In June 2017, the UN Group of Governmental Experts (GGE) failed in its mandate to develop a "common understanding" of the proper behavior for states in cyberspace because Russia and China, among others, objected to the final draft.[119] The proposal made clear that use of force and international humanitarian law applied in cyberspace.[120] Subsequently, Russia and China proposed an Open–Ended Working Group (OEWG) to continue where the GGE failed to achieve consensus.[121] In their 2019 opening statement before the OEWG, China proclaimed, "It is widely endorsed by the international community that the principle of sovereignty applies in cyberspace."[122] This statement sounds like an endorsement of sov-

---

[116] *See* Rogier Creemers et al., *Translation: Cybersecurity Law of the People's Republic of China*, NEW AMERICA (June 29, 2018), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/.

[117] *Id.* (emphasis added).

[118] Simon Denyer, *China's Scary Lesson to the World: Censoring the Internet Works*, WASH. POST (May 23, 2016), https://www.washingtonpost.com/world/asia_pacific/chinas-scary-lesson-to-the-world-censoring-the-internet-works/2016/05/23/413afe78-fff3-11e5-8bb1-f124a43f84dc_story.html.

[119] *See* Arun M. Sukumar, *The UN GGE Failed. Is International Law in Cyberspace Doomed As Well?*, LAWFARE (July 4, 2017, 1:51 PM), https://www.lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well.

[120] *Id.*

[121] Valentin Weber, *The Sinicization of Russia's Cyber Sovereignty Model*, COUNCIL ON FOREIGN RELATIONS (April 1, 2020 3:16 PM), https://www.cfr.org/blog/sinicization-russias-cyber-sovereignty-model; Adam Segal, China's Alternative Cyber Governance Regime, COUNCIL ON FOREIGN RELATIONS (March 13, 2020), https://www.uscc.gov/sites/default/files/testimonies/March%2013%20Hearing_Panel%203_Adam%20Segal%20CFR.pdf.

[122] *China's Submissions to the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of*

ereignty as a principle instead of a rule. However, such an interpretation would misunderstand Chinese, and for that matter, Russian interpretations of sovereignty.

China and Russia have strongly promoted the idea of cyber sovereignty as a means of absolute control over their internal cyberspaces. They intend and claim the right to balkanize the Internet through the right of sovereignty.[123] Thus, any action that inhibited their ability to be the sole power that could, for example, turn the Internet on or off, slow it down, or manipulate data—all within their territorial cyberspace (for lack of a better word)—would violate state sovereignty. The Deputy Director of the People's Liberation Army (PLA) National Defense University, Colonel Li Minghai, equates controlling cyberspace in the 21st century with controlling the seas and air in prior centuries.[124] It is a domain that, for national security purposes, must be controlled or China will once again face Western colonial dominance .[125] Russia sees cyberspace similarly.[126] Threats to sovereignty—to Russia and China—are a matter of national security. It is not just a rule, it is the goal. Any actions that reduce state control hinder and violate sovereignty.[127]

International Security, UN OPEN-ENDED WORKING GROUP (OEWG) (Sept. 9, 2019), https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/09/china-submissions-oewg-en.pdf.

[123] Adam Segal, *Peering into the Future of Sino-Russian Cyber Security*, WAR ON THE ROCKS (Aug. 10, 2020), https://warontherocks.com/2020/08/peering-into-the-future-of-sino-russian-cyber-security-cooperation/

[124] Major Michael Kolton, *Interpreting China's Pursuit of Cyber Sovereignty and its Views on Cyber Deterrence*, 2 The Cyber Defense Review 119, 121 (2017), https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/Interpreting%20Chinas%20Pursuit%20of%20Cyber%20Sovereignty_Kolton.pdf?ver=2018-07-31-093726-797.

[125] *Id.*

[126] Moynihan, *supra* note 112.

[127] It is worth noting that China views sovereignty violations in cyberspace as much graver and serious threats than United States does. *Compare* Ministry of Foreign Affairs & the Cyberspace Administration of China, INTERNATIONAL STRATEGY OF COOPERATION ON CYBERSPACE (Mar. 1, 2017), http://www.xinhuanet.com//english/china/2017-03/01/c_136094371_2.htm *with* U.S. DEP'T OF DEFENSE, THE DEP'T OF DEFENSE CYBER STRATEGY (2018). An operation the United States undertakes, which it may believe is defensive in nature, may threaten and offend China far more than it would if China directed the same action against the United States. *Id.* This misunderstanding risks dra-

Russia and China view defending forward, which entails operating in foreign cyberspace, as a violation of their sovereignty. Of course, the great irony is that both Russia and China are notorious for their cyber–attacks against the United States.[128] But if the United States dared to reciprocate those attacks, both Russia and China would claim the United States had violated their inherent right to cyber sovereignty. This demonstrates the potential for weaponizing sovereignty to prevent nations that value international law from engaging in strategies like defend forward. As Koh put it in his 2012 speech, "If we succeed in promoting a culture of compliance, we will reap the benefits. And if we earn a reputation for compliance, the actions we do take will earn enhanced legitimacy worldwide for their adherence to the rule of law." Koh is right, the United States should always set the right example, and reputation matters. Balancing this admirable goal without being caught flat–footed, however, will never be easy.

IV. RECONCILING DEFEND FORWARD AND SOVEREIGNTY

If deterrence was working in cyberspace, then defend forward would not be necessary. Unfortunately, deterrence has not proven effective in making American adversaries recalculate their cyberattacks against the United States in the gray zone. These adversaries have no qualms about wielding international law as a shield to protect their so–called cyber sovereignty while simultaneously slashing through another nation's sovereignty with the sword of offensive cyber operations. The United States, however, is better than that. International law is the touchstone of international affairs. Therefore, defend forward should fit within the legal structures in place.

Defend forward originated because the United States recognized that a stationary defense was impractical. No matter the quality of American defenses, an adversary would find a way through.

---

matic escalation that could culminate in war—all because neither side properly understood the other. *Id.*

[128] *See*, *e.g.*, Scott Neuman, *Intelligence Chiefs Say China, Russia Are Biggest Threats To U.S.*, NPR (April 14, 2021, 2:50 PM), https://www.npr.org/2021/04/14/987132385/intelligence-chiefs-say-china-russia-are-biggest-threats-to-u-s.

The strategy of defend forward rests on the assumption that American adversaries are determined to infiltrate American cyber networks. No one would dispute this assumption, and there is no reason to think this is about to change. But understanding that defend forward is anticipating hostile attacks is helpful because it places the strategy on firmer legal footing. Disabling the IRA's Internet for several days should be seen as an in–kind response in *anticipation* of the IRA intending to violate American sovereignty or committing a prohibited intervention. Further, Cyber Command is not launching cyber operations at random. The Intelligence Community assists in developing the targets for its missions.

Congress has also legalized defend forward. Against our chief adversaries, Russia, China, North Korea, and Iran, the 2019 NDAA authorized what Robert Chesney described as a mini–AUMF for cyber operations.[129] The NDAA authorized cyber operations in the event DoD determined these foes are "conducting an active, systematic, and ongoing campaign of attacks against the Government or people of the United States in cyberspace . . . "[130] Note the word *ongoing*. Congress likely inserted this language recognizing that these four adversaries would continue the perpetual cyber–attacks against the United States. Next, Cyber Command may "take appropriate and proportional action in foreign cyberspace to disrupt, defeat, and deter such attacks."[131] The NDAA broadly spoke of *foreign cyberspace*, not Russian, Chinese, North Korean, or Iranian.[132] This appears to permit operations in the cyberspace of third–party nations that are not the ultimate target. Had Congress wanted to limit operations in those four countries, it could have specified such. Instead, it recognized that cyberwar has no fixed sovereignty when it comes to the battlefield. Overall, the NDAA legalizes persistent engagement and defend forward.

However, the 2019 NDAA only authorized cyber operations against four adversaries and did not explicitly authorize operations

---

[129] Robert Chesney, *The Law of Military Cyber Operations and the New NDAA*, LAWFARE (July 26, 2018, 2:07 PM), https://www.lawfareblog.com/law-military-cyber-operations-and-new-ndaa.

[130] National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, – § 1642 (2018).

[131] *Id.*

[132] *Id.*

in the cyber space of other threats or third–party nations.[133] And foreign cyberspace could be interpreted as only that of Russia, China, North Korea, or Iran. The 2020 NDAA went a step further and authorized military operations "short of hostilities and in areas outside of areas of active hostilities for the purpose of preparation of the environment, influence, force protection, and deterrence of hostilities."[134] *Short of hostilities* is more certainly a license for gray zone operations. Additionally, the 2020 NDAA granted the Secretary of Defense authority to conduct cyber operations against a "foreign power."[135] *Areas outside of areas of active hostilities* removed any existing ambiguity about whether Cyber Command could launch missions in a neutral nation's cyberspace. *Foreign power* is more than just Russia, China, North Korea, or Iran. The language is broad and allows actions against non–state actors. But domestic authorization does not guarantee that Cyber Command's actions are legal under international law, particularly if these actions violate another nation's sovereignty.

When Cyber Command executed defend forward under the 2019 and 2020 NDAAs, it did not violate international law regardless of whether they violated another nation's sovereignty. To start, the 2019 NDAA limited cyber operations to *proportional* actions. This means any action Cyber Command takes is necessarily in response to either a prior attack or a perceived threat. Russia hacked the 2016 election, and American intelligence likely determined that Russia intended to do the same in 2018. Hence, Cyber Command was acting on the belief of an imminent attack when it shut off the IRA's Internet just before the 2018 elections.

Because the 2019 NDAA required proportional responses, Cyber Command will not be able to violate sovereignty under domestic law, even if sovereignty was an international rule of law that could be violated. For instance, if Russia's SolarWinds attack violated American sovereignty and an international rule of law, then the United States could legally resort to countermeasures and respond in–kind through proportionate means—cyber or not. If SolarWinds violated sovereignty, but did not violate international

---

[133] National Defense Authorization Act for Fiscal Year 2020, Pub. L. No. 116-92, § 1631 (2019).

[134] *Id.*

[135] *Id.*

law, then a proportionate American response would be unlikely to violate international law, even if it violated Russian sovereignty.[136] In the latter example, the American response would be classified as a retorsion.[137]

Michael Schmitt refers to this as "in–kind" responses.[138] Schmitt elaborates that those in–kind responses may not be punitive, but may only be intended to stop the hostile actor or to secure reparations.[139] Schmitt lists proportionality as a requirement for in–kind responses, though this seems a bit redundant. For Schmitt, the key is intent. He explains, "[an]in–kind response that itself would otherwise be unlawful is only justified if its primary purpose is permissible."[140] Even so, discerning intent is arduous without a long history of state practice and because of this there are significant issues of attribution. Calculating a proportional response and, perhaps most importantly, foreseeing how an adversary will classify that response are equally challenging. A miscalculated response, even if the actor sincerely believes and intends the response to be proportional or in–kind, could be received as an escalation.

As state practice and *opinio juris* around gray zone cyber activities and sovereignty continue to evolve, nation states will likely engage in tacit bargaining to create these norms.[141] Explicit bargaining is actual negotiation between states to achieve an understanding. Tacit bargaining involves actions, statements, and declarations that form a recognizable pattern defining limits, restraints, and predictable responses.[142] Overtime, each side comes to recognize what is acceptable and unacceptable behavior, which increas-

---

[136] *See* Michael N. Schmitt & Durward E. Johnson, *Responding to Hostile Cyber Operations: The "In-Kind" Option*, 97 INT'L L. STUDIES 95, 99 (2021).

[137] U.S. DEP'T OF DEFENSE OFFICE OF GEN. COUNSEL, DEPARTMENT OF DEFENSE LAW OF WAR MANUAL 1110 (updated Dec. 2016), The definition of retorsion is "unfriendly conduct, (1) which is not inconsistent with any international obligation of the State engaging in it, and (2) which is done in response to an internationally wrongful act."

[138] Schmitt & Johnson, *supra* note 139, at 101.

[139] *See id.* at 116.

[140] *Id.* at 120.

[141] Michael P. Fischerkeller & Richard J. Harknett, *Persistent Engagement and Tacit Bargaining: A Path Toward Constructing Norms in Cyberspace*, LAWFARE (Nov. 9, 2018, 7:00 AM), https://www.lawfareblog.com/persistent-engagement-and-tacit-bargaining-path-toward-constructing-norms-cyberspace.

[142] *Id.*

es stability. Michael Fischerkeller and Richard Harknett argue that defending forward and persistent engagement align with tacit bargaining, but stress it is critical for each side to clearly communicate what they are doing.[143]

This still does not answer the question of third–party or neutral nation sovereignty under international law. Fortunately, from the limited amount of non–classified information available, it seems Cyber Command has limited its operations in third–party nations' networks to those that create only a *de minimis* effect. This avoids the sovereignty issue entirely. For example, to take ISIS offline in Operation Glowing Symphony, Cyber Command had to access data on nodes around the world, not just in Syria and Iraq.[144] ISIS's data was often stored on the same server as civilian data.[145] Before launching an attack in these foreign nodes, Joint Task Force ARES had to prove to DoD officials and Members of Congress that the operation would only affect ISIS's data.[146] Although Cyber Command would be operating in a third–party nation's network, essentially trespassing on its network, the effects would be minimal. Without naming it, Cyber Command employed a *de minimis* effects standard when carrying out Operation Glowing Symphony.

Of course, questions will remain should Cyber Command not be able to leave civilian data untouched or if the effects on a third–party nation would be greater than *de minimis*. Over time, as more operations like Glowing Symphony are conducted, the American confidence will grow both in how precise Cyber Command's strikes can be and what constitutes acceptable practice. Operation Glowing Symphony is an important and early example of state

---

143 *See id.*

144 *See* Elena Chachko & Ashley Deeks, *Which States Support the 'Unwilling and Unable' Test?*, LAWFARE (Oct. 10, 2016, 1:55 PM), https://www.lawfareblog.com/which-states-support-unwilling-and-unable-test (explaining that the AUMF did not authorize cyber operations against either Iraq or Syria, this would not present a problem under international law because both states had failed to contain and control an international terrorist group. The United States had the ability under international law to defend itself because the governments or Syria and Iraq had both failed to contain and control ISIS and, because of state sovereignty, were responsible for all internal actions within their borders).

145 Dina Temple-Raston, *How The U.S. Hacked ISIS*, NPR (Sept. 26, 2019, 5:00 AM), https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis.

146 *Id.*

practice defining the strategy of defend forward. Additionally, America's position that sovereignty is a principle will inform future state practice in future missions. Cyber Command will carefully consider the consequences of its actions vis–à–vis sovereignty, but not necessarily stop because of it.

Ultimately, it seems that in practice the effect of sovereignty as a rule and sovereignty as a principle will be nearly identical. As Schmitt points out, even if sovereignty is a rule, actions and responses are not limited so long as the intent of defending forward is to stop adversaries from attacking the United States instead of being punitive.[147] Since the 2019 AUMF authorized Cyber Command to engage in proportional cyber operations, those operations must always be in response to prior acts or anticipated acts. And because sovereignty is a principle that should be considered, but is not determinative in cyberspace, defend forward operations that violate sovereignty are not inherently internationally wrongful acts—they are legal retorsions against enemies.

V. CONCLUSION

This paper has focused on the question of whether defend forward operations that violate other nations' sovereignty also violate international law. Because sovereignty in cyberspace is a principle and not a rule, and because American domestic law authorizes defend forward as a response to ongoing attacks against the United States, defend forward does not violate international law. However, this does not answer the question of whether defend forward will work. Defend forward is worth trying because deterrence has not been working.[148] In that same vein, asking whether defend forward will work while maintaining the goal posts of deterrence sets defend forward up for failure. The goal is not deterrence so

---

[147] This seems like a contradiction of his original position that sovereignty is a hard and fast rule and, at minimum, weakens the sovereignty as a rule argument. This latest argument was only published in 2021 and is relatively new for Schmitt. Perhaps he recognized the need to adapt to defend forward, lest his approach to sovereignty become obsolete. Schmitt and Johnson, *supra* note 139, at 120.

[148] As President Franklin D. Roosevelt justified, "It is common sense to take a method and try it. If it fails, admit it frankly and try another. But above all, try something."

much as it is disruption. In the long run, perhaps, defend forward may deter adversaries if the costs of attacking the United States become too high. In the meantime, defend forward will likely work because it provides the United States the operational flexibility necessary to confront its foes who have remained defiant without waiting for them to attack. The United States can engage on its own terms and bring the fight to the enemy.

Defend forward is not without risk. Many critics fear trading cyber responses will quickly and unpredictably escalate out of the gray zone and into use of force and armed attacks, whether cyber or not.[149] This means Cyber Command must carefully consider how China, Russia, Iran, North Korea, and others will perceive its missions. Crucially, despite defend forward being inherently responsive under American law, adversaries will likely never view American actions as responsive. They will label the United States as the perpetrator and aggressor. Understanding "the realities of the mentalities or the localities" is paramount for conducting shrewd and successful international affairs.[150]

General Nakasone and others must therefore take gradual and calculated actions while defending forward. Missions should slowly and barely escalate, if at all, while also leaving a calling card demonstrating America's resolve, capabilities, and the rule going forward. Over time, tacit bargaining will crystalize norms that provide nations with firmer footing of what is acceptable and unacceptable behavior in the gray zone. Without defend forward, this would not be possible, or at least not as effective, as the United States would be at the mercy of its enemies as they set the norms. Time will tell whether defend forward works. The thwarting of the IRA ahead of the 2018 elections and Operation Glowing Sympho-

---

[149] Lyu Jinghua, *A Chinese Perspective on the Pentagon's Cyber Strategy: From 'Active Cyber Defense' to 'Defending Forward'*, LAWFARE (Oct. 19, 2018, 9:30 AM), https://www.lawfareblog.com/chinese-perspective-pentagons-cyber-strategy-active-cyber-defense-defending-forward ("[D]efending forward should be understood as something more proactive and potentially escalatory than active cyber defense."); Jason Healey & Robert Jervis, *The Escalation Inversion and Other Oddities of Situational Cyber Stability*, 3 TEX. NAT'L SEC. REV. 31 (2020).

[150] Walter A. McDougall, *Kissinger's World Order*, FOREIGN POLICY RESEARCH INSTITUTE (Oct. 13, 2014), https://www.fpri.org/2014/10/kissingers-world-order/ (quoting James Kurth).

ny are reasons for optimism. Of course, anything can happen—even a Pearl Harbor level cyber event—despite Cyber Command's best efforts. But this will not be because Cyber Command was sitting behind a computer idly waiting for an attack to come. The war is already here. Defend forward recognizes this new reality and brings the war to the enemy's doorstep.