IT'S THE PRINCIPLE: DEFINING SOVEREIGNTY IN THE CONTEXT OF CYBER OPERATIONS

Corey Pray *

As a relatively new and unique operational domain, cyberspace presents novel questions about the application of international law principles. One such question focuses on sovereignty. Although the concept of territorial sovereignty has existed for centuries, it is much less defined in cyberspace, where data can be stored across multiple locations. Scholarly debate in this area has led to two schools of thought. The first views sovereignty as its own, enforceable rule of international law, with strict application of territorial inviolability in the cyber realm. The second frames sovereignty as a principle founded upon several international law rules, meaning only certain operations, such as those rising to the level of a use of force, would violate international norms. This Comment analyzes the merits of these two approaches and concludes that the sovereignty-as-principle view is consistent with state practice and the reality of cyber operations.

* Antonin Scalia Law School at George Mason University, J.D., 2020; Boston University, B.A., Chemistry and Political Science, 2017. Many thanks to the members of the National Security Law Journal for their suggestions and edits to this Comment.

INTRODUCTION

In late 2016, the United States commenced Operation Glowing Symphony, a secret operation designed to infiltrate the Islamic State's cyber infrastructure and target terrorist propaganda.[1] U.S. Cyber Command (Cybercom) successfully accessed Islamic State administrator accounts, changed passwords, deleted battlefield footage, and prevented propaganda specialists from accessing information.[2] The targeted cyber infrastructure was located in approximately 35 nations, several of which were U.S. allies.[3] The U.S. took action in at least five nations.[4]

Originally, Cybercom planned to execute the operation without notifying U.S. allies.[5] Behind the scenes, however, a disagreement took place. In one group, Secretary of State John Kerry,

[1] Ellen Nakashima, *U.S. Military Operation to Attack ISIS Last Year Sparked Heated Debate Over Alerting Allies,* WASH. POST (May 9, 2017), https://www.washingtonpost.com/world/national-security/us-military-cyber-operation-to-attack-isis-last-year-sparked-heated-debate-over-alerting-allies/2017/05/08/93a120a2-30d5-11e7-9dec-764dc781686f_story.html?utm_term=.44fe121aa9b1.
[2] *Id.*
[3] Joe Uchill, *Anti-ISIS Cyber Op Struggled with Issue of Notifying Allies*, THE HILL (May 9, 2017), https://thehill.com/policy/cybersecurity/332491-anti-isis-cyber-op-struggled-with-issue-of-notifying-allies.
[4] Nakashima, *supra* note 1.
[5] *Id.*

CIA Director John Brennan, FBI Director James Comey, and Director of National Intelligence James Clapper argued in favor of notification.[6] Opposing them were Secretary of Defense Ash Carter, Cybercom Commander Admiral Michael Rogers, and Joint Chiefs Chairman Joseph Dunford.[7] They promoted the original plan, arguing legal authority did not mandate notification and alerting allies might result in a leak.[8] Ultimately, several countries were notified.[9] While Operation Glowing Symphony succeeded in removing propaganda and locking out terrorist accounts, military officials and the intelligence community differed on the long-term impact of the operation.[10]

The debate that took place during Operation Glowing Symphony likely included discussions about whether failing to notify host countries that their cyber infrastructure would be targeted might undermine the territorial sovereignty of those countries.[11] Sovereignty is a complex and fluid area of international law, and its application to cyberspace has been met with uncertainty. Some contend sovereignty is an independent *rule* of international law that serves as an absolute guarantee of territorial inviolability, subject to exceptions or consent.[12] Under this view, many trans-border cyber operations would violate international law even if they fell below the thresholds of other prohibited actions such as a use of force, prohibited intervention, or armed attack. Others characterize sovereignty as a *principle* limited to the force it has in existing international law and customary norms.[13] According to this sovereignty-as-principle view, cyber operations only infringe on sovereignty if they violate another rule of international law.

---

[6] *Id.*
[7] *Id.*
[8] *Id.*
[9] Uchill, *supra* note 3.
[10] Nakashima, *supra* note 1.
[11] Sean Watts & Theodore Richard, *Baseline Territorial Sovereignty and Cyberspace*, 22 LEWIS & CLARK L. R. 803, 805 (2018).
[12] *See* Michael N. Schmitt & Liis Vihul, *Respect for Sovereignty in Cyberspace*, 95 TEX. L. R. 1639, 1640 (2017).
[13] *See* Gary P. Corn & Robert Taylor, *Sovereignty in the Age of Cyber*, 111 AM, J. INT'L. L. UNBOUND 207, 210 (2017).

The proposed operations in Operation Glowing Symphony did not involve physical harm to people or infrastructure and thus fell below the threshold of a use of force or an armed attack.[14] But the operations resulted in more than *de minimis* effects; they involved data deletion and manipulation.[15] Under the sovereignty-as-rule view, U.S. officials would risk violating international law by proceeding with the operation without notifying and obtaining consent from the targeted countries. This result is undesirable for nation-states (states) needing to take immediate, necessary action to prevent further infringements on their own territorial sovereignty.

This Comment supports the view that, although sovereignty is a fundamental principle that should weigh heavily in decision-making for cyber operations, it is not its own enforceable legal rule. In coming to this conclusion, this Comment analyzes recent state practice and *opinio juris*, and determines that both are consistent with the sovereignty-as-principle approach. Further, this Comment argues the sovereignty-as-principle approach better provides victim states with an adequate means of responding to cyber threats from state and non-state actors.

Part I of this Comment discusses the importance of cyberspace in national security discussions, provides an overview of early views on the principle of sovereignty as it applies in cyberspace, and introduces competing theories of cyber sovereignty while also highlighting areas of agreement. Part II details why sovereignty should be viewed as a baseline principle in cyberspace rather than as an enforceable rule of international law, as well as how state practice and *opinio juris* fit into this context. Finally, Part III argues the sovereignty-as-principle view provides states with a better framework for conducting and responding to cyber operations that do not qualify as a use of force, as well as responding to cyber operations against non-state actors.

[14] Watts & Richard, *supra* note 11, at 829.
[15] Nakashima, *supra* note 1.

I. BACKGROUND

A. The Importance of Cyberspace in National Security Discussions

Cyberspace poses one of the greatest national security challenges for the United States and nations around the world. As populations, businesses, and governments rely more heavily on cyber infrastructure to perform critical functions, the consequences of cyber conflict increase in severity.[16] The most harmful cyber attacks can cause physical damage or total destruction to water lines, power plants, or banking institutions.[17] Most hostile cyber activity, however, does not amount to a use of force with physical consequences; instead, cyber activity may come in the form of data manipulation or "influence campaigns," such as Russia's extensive attempts to influence U.S. elections.[18]

Real-world instances have previewed the potentially devastating effects of hostile cyber activity. For example, in 2007, Estonia experienced an unprecedented cyber attack with destructive proximate effects.[19] After the Estonian government removed a statue depicting a Red Army soldier from the center of Tallinn, the Estonian capital, Russian sympathizers took to the streets in protest.[20] In the weeks following the protests, Estonia experienced major cyber attacks, likely orchestrated by the Russian government or Russian agents.[21]

---

[16] *See, e.g.*, Natasha Turak, *The Next 9/11 will be a Cyberattack, Security Expert Warns*, CNBC, (June 1, 2018, ^;14 PM), https://www.cnbc.com/2018/06/01/the-next-911-will-be-a-cyberattack-security-expert-warns.html.
[17] David W. Opderbeck, *Cybersecurity and Executive Power*, 89 WASH. U. L. REV. 795, 797-98 (2012).
[18] *See* Tim Maurer, Ariel E. Levite & George Perkovich, *Toward a Global Norm Against Manipulating the Integrity of Financial Data*, LAWFARE, (Mar. 28, 2017,10:14 AM), https://www.lawfareblog.com/toward-global-norm-against-manipulating-integrity-financial-data; David Shepardson, *U.S. Officials Warn Congress on 2018 Election Hacking Threats,* REUTERS, (May 22, 2018, 11:35 AM), https://www.reuters.com/article/us-usa-election-security/us-officials-warn-congress-on-election-hacking-threats-idUSKCN1IN25H.
[19] Damien McGuinness, *How a Cyber Attack Transformed Estonia*, BBC NEWS, (Apr. 27, 2017), https://www.bbc.com/news/39655415.
[20] *Id.*
[21] *Id.*

The event paralyzed networks of banks, the media, and the government; citizens found themselves unable to use cash machines, news organizations were prevented from reporting, and government employees lost communication with each other.[22] In some cases, the effects of the attacks lasted weeks.[23]

More recently, the Stuxnet virus made its way through international networks and did extensive physical damage to its target, an Iranian nuclear power plant.[24] Stuxnet was "carefully designed to disrupt the sort of systems that help control equipment at nuclear power plants."[25] Stuxnet's sophistication suggested it was created by a state actor, in this case probably the United States or Israel.[26] The virus appeared to significantly affect Iran's output of refined uranium.[27]

The potential for a large-scale cyber-attack targeting the United States is escalating. As then-Director of National Intelligence, Dan Coats, remarked in 2018, "It was in the months prior to September 2001 when, according to then-CIA Director George Tenet, the system is blinking red. And here we are nearly two decades later, and I'm here to say, the warning lights are blinking red again."[28] In addition to this pre-9/11 mentality, Coats also emphasized that U.S. adversaries are already undermining U.S. interests in cyberspace by "penetrating our digital infrastructure and conducting a range of cyber intrusions and attacks against targets in the United States."[29]

---

[22] *Id.*
[23] *Id.*
[24] Opderbeck, *supra* note 17, at 799.
[25] *Id.*
[26] *Id.*
[27] *See The Stuxnet Worm: Yet to Turn*, THE ECONOMIST (Dec. 18, 2010), http://www.economist.com/node/17730556?story_id=17730556&CFID=158391401&CFTOKEN=34182131.
[28] Veronica Stracqualursi, *US Intelligence Chief: 'The Warning Lights are Blinking Red Again on Cyberattacks'*, CNN (Jul. 14, 2018), https://www.cnn.com/2018/07/14/politics/director-of-national-intelligence-dan-coats-cyberattacks-russia/index.html.
[29] *Id.*

B. Historical Views of Sovereignty and Early Application to Cyberspace

Sovereignty has always been understood to have an internal and an external component.[30] Internal sovereignty refers to the authority and exclusivity that states enjoy over their own territories.[31] "The internal aspects of sovereignty carry with them the problems of submission of subjects to the sovereign, limits on the authority of the sovereign, and the need to determine a sovereign representative."[32] External sovereignty refers to the legal equality of all states in the international system.[33]

Territorial sovereignty is not comprehensively defined in a single treaty or other source of international law.[34] Rather, history and state practice have clarified the meaning of sovereignty as a customary international principle.[35] Territorial sovereignty is commonly referred to as Westphalian sovereignty, named after the Peace of Westphalia.[36] The Peace of Westphalia ended the Thirty Years War and created a system of legally equal states that relied heavily on shared legal norms.[37] The treaty of the Peace of Westphalia maintained that states were prohibited from interfering with one another or "jeopardiz[ing] the general peace without cause."[38] Subsequently, Westphalian sovereignty has been defined as a "political organization based on the exclusion of actors from authority structures within a given territory."[39]

---

[30] Ronald A. Brand, *External Sovereignty and International Law*, 18 FORDHAM INT'L L. J. 1685, 1689 (1995).
[31] Theodore Richard & Sean Watts, *Baseline Territorial Sovereignty and Cyberspace*, 22 LEWIS & CLARK L. REV. 708, 830 (2018) (citing Memorandum from Jennifer M. O'Connor, Gen. Counsel of the Dep't of Def., International Law Framework for Employing Cyber Capabilities in Military Operations (Jan. 19, 2017)).
[32] Brand, *supra* note 30, at 1689.
[33] Watts & Richard, *supra* note 11, at 860-61.
[34] *Id.* at 826.
[35] *Id.*
[36] *Id.* at 828.
[37] *Id.* at 827-28.
[38] *Id.* at 829.
[39] STEPHEN D. KRASNER, SOVEREIGNTY: ORGANIZED HYPOCRISY 3-4 (1999).

Modern notions of territorial sovereignty are based on the international structure that emerged after World War II and are particularly rooted in the principles of the United Nations Charter.[40] Notably, however, there are few direct references to sovereignty in the Charter.[41] The Charter affirms "the principle of the sovereign equality of all its members."[42] Elsewhere, the Charter states that relationships among Member States "shall be based on respect for the principle of sovereign equality."[43] The Charter's strongest support for territorial sovereignty is found in Article 2(4), which states, "[a]ll 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."[44]

The basic framework of the Charter was supplemented by decisions of the International Court of Justice (ICJ) that applied sovereignty principles to factual situations. For example, in the *Corfu Channel* case, the ICJ found that the United Kingdom violated Albanian sovereignty by conducting a minesweeping operation in Albanian territorial waters.[45] The ICJ held that "[b]etween independent states, respect for territorial sovereignty is an essential foundation of international relations."[46] Subsequently, in *Case Concerning Military and Paramilitary Activities in and Against Nicaragua*, the ICJ held that U.S. support of the Contras in their rebellion against the Nicaraguan government violated the principle of non-intervention, amounted to an unlawful use of force, and violated Nicaraguan sovereignty.[47]

When cyberspace was a relatively new concept, many envisioned it as a space free from sovereignty, legal constraints, and

[40] Watts & Richard, *supra* note 11, at 839.
[41] *Id.*
[42] U.N. Charter art. 2, ¶ 1.
[43] U.N. Charter art. 78.
[44] U.N. Charter art. 2, ¶ 4.
[45] Corfu Channel Case (U.K. v. Alb.), Judgment, 1949 I.C.J. 4, at 35 (Apr. 9).
[46] *Id.*
[47] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, at ¶ 242 (June 27).

extensive regulation.[48] Some viewed cyberspace as a "global commons," where claims of sovereignty gave way to universal access.[49]

Practical considerations soon demonstrated that cyberspace is not a lawless place. Cyberspace can be separated into three layers: the physical layer, the logical layer, and the social layer.[50] In the physical layer, the components of cyberspace such as hardware, servers, cables, and transmitters are located in places where sovereign entities may exercise control over such components.[51] The logical layer consists of data and applications, which, if stored in the physical components, are also subject to sovereign control.[52] The social layer "encompasses individuals and groups engaged in cyber activities."[53] Further, states have demonstrated a strong stake in enforcing domestic laws in cyberspace, including those relating to intellectual property, national security, contract enforcement, gambling, and speech content.[54]

C. Competing Theories of Sovereignty in Cyberspace

As cyberspace became more accessible and complex, state actors eventually acknowledged the applicability of customary international law to cyberspace.[55] An early assessment from the Office of General Counsel of the U.S. Department of Defense in 1999 alluded to the principle of sovereignty in cyberspace but did not take any affirmative stances, only suggesting that "[a]n unauthorized electronic

---

[48] *See e.g.* John Perry Barlow, *A Declaration of the Independence of Cyberspace*, ELEC. FRONTIER FOUND. (Feb. 8, 1996), https://www.eff.org/cyberspace-independence ("Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.").

[49] Watts & Richard, *supra* note 11, at 811.

[50] *Id.* at 856; *see also* TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 12 (Michael N. Schmitt ed., 2d ed. 2017) [hereinafter Tallinn Manual 2.0] ("For purposes of this Manual, the physical, logical, and social layers of cyberspace are encompassed in the principle of sovereignty.").

[51] Watts & Richard, *supra* note 11, at 856.

[52] *Id.*

[53] Tallinn Manual 2.0, *supra* note 50, at 12.

[54] *Id.* at 813; *see also* JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET?: ILLUSIONS OF A BORDERLESS WORLD 150 (2006).

[55] Watts & Richard, *supra* note 11, at 851.

intrusion into another nation's computer systems may very well end up being regarded as a violation of the victim's sovereignty."[56] The assessment also stressed that understandings of sovereignty are contextual.[57] For example, unauthorized intrusions into airspace are considered serious violations of territorial sovereignty, while objects in orbit in outer space are "beyond the territorial claims of any nation."[58] In the time since the assessment, states have been reluctant to clarify customary international norms in cyberspace, while private commentators have offered several proposed solutions.[59]

In 2012, Harold Koh, the Legal Advisor to the U.S. Department of State, delivered a famous speech in which he recognized the applicability of international law principles to cyberspace, including the right to self defense against armed attack, guidelines for determining whether cyber operations qualify as a use of force, and *jus in bello* rules.[60] Koh also described the role of sovereignty in cyberspace, explaining that "[w]henever a state contemplates conducting activities in cyberspace, the sovereignty of other states needs to be considered."[61] In the time since Koh's speech, new ideas about cyber sovereignty have developed but have created uncertainty. This section details two competing views currently dominating the conversation about sovereignty in cyberspace: the sovereignty-as-rule view advanced by the Tallinn Manuals and the sovereignty-as-principle view held by several scholars and state actors.

1. The Tallinn Manuals and the Sovereignty-as-Rule View

The Tallinn Manuals on the International Law Applicable to Cyber Operations are an important contribution to the development

[56] Off. of Gen. Couns., Dep't of Def., AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS 1, 19 (1999).
[57] *Id.* at 2.
[58] *Id.*
[59] *See generally* Michael N. Schmitt & Sean Watts, *The Decline of International Humanitarian Law Opinio Juris and the Law of Cyber Warfare*, 50 TEX. INT'L L.J. 189, 222 (2015).
[60] *See generally* Harold Koh, *International Law in Cyberspace*, 54 HARV. INT'L L.J. ONLINE 1, 4 (2012).
[61] *Id.* at 6.

of comprehensive international law on cyber operations. The first Tallinn Manual (Tallinn 1.0) was an international effort designed to articulate how *jus ad bellum* and international humanitarian law apply in cyber conflicts and cyber operations.[62] Between 2009 and 2012, a group of approximately twenty international experts gathered to write Tallinn 1.0 by invitation of the North Atlantic Treaty Organization (NATO) Cooperative Cyber Defense Centre of Excellence.[63] The manual was not intended to be binding but was rather an attempt to clarify legal issues that remained largely abstract.[64] Tallinn 1.0, published in 2013, focused mostly on cyber conflict and its relation to the law of armed conflict. A second edition (Tallinn 2.0) was published in 2017.[65] Tallinn 2.0 focused more broadly on the law applying to cyber operations, including operations that fall below the threshold of a use of force.[66]

Tallinn 2.0 is not meant to serve as a means for states to fill in gaps in areas of cyber law that have yet to be addressed.[67] Tallinn 2.0 is filled with ambiguities, and the experts who wrote it did not shy away from expressing when they disagreed with each other or recognized the existence of multiple viewpoints. Tallinn 2.0 is an interpretive tool, not an authoritative force, and is "intended as an objective restatement of the *lex lata*."[68] Thus, the "rules" promulgated by the Manual are starting points of conversation and are open to interpretation.

Tallinn 2.0 addresses sovereignty up front.[69] Rule 1 of Tallinn 2.0 recognizes that sovereignty applies in cyberspace and that sovereign powers exercise control over cyber infrastructure and activities within their sovereign territory.[70] Rules 2 and 3 recognize

[62] TALLINN MANUAL 2.0, *supra* note 50, at 1.
[63] Eric T. Jensen, *The Tallinn Manual 2.0: Highlights and Insights*, 48 GEO. J. INT'L L. 735, 738 (2017).
[64] *Id.*
[65] *Id.* (this Comment analyzes only TALLINN 2.0 as it is the most recent version).
[66] *Id.*
[67] TALLINN MANUAL 2.0, *supra* note 50, at 2.
[68] *Id.* at 3.
[69] *See id.* at 11.
[70] *Id.*

that the principles of internal and external sovereignty, discussed above, apply in cyberspace.[71]

Rule 4 is the boldest of Tallinn 2.0's "rules" on sovereignty and provides that "[a] State must not conduct cyber operations that violate the sovereignty of another State."[72] Further, the Commentary to Rule 4 states, "[in] the cyber context, therefore, it is a violation of territorial sovereignty for an organ of a State, or others whose conduct may be attributed to the State, to conduct cyber operations while physically present on another State's territory against that State or entities or persons located there."[73] Clearly, the experts who wrote the Manual favor the view that sovereignty can be enforced as a rule of international law.[74] Professor Michael Schmitt, the Director of the Tallinn Manual projects, acknowledges, however, that not all cyber operations taking place on another state's cyber infrastructure violate territorial sovereignty.[75]

Schmitt and Liis Vihul, the latter of whom served as the managing editor of Tallinn 2.0, point to judicial treatment and state practice as supporting evidence of the sovereignty-as-rule view. They argue the holdings in the *Corfu Channel* and *Nicaragua* cases treat violations of sovereignty with the same level of significance as the principles of non-intervention and use of force.[76] They then reference a 2015 ICJ case in which Costa Rica and Nicaragua accused each other of violating territorial sovereignty.[77] The ICJ explained that "it is

[71] *Id.* at 13-16 ("A state enjoys sovereign authority with regard to the cyber infrastructure, persons, and cyber activities located within its territory, subject to its international legal obligations."); *id.* at 16-17 ("A State is free to conduct cyber activities in its international relations, subject to any contrary rule of international law binding on it.")

[72] *Id.* at 17.

[73] *Id.* at 19.

[74] Jensen, *supra* note 63, at at 741; *see also* Schmitt & Vihul, *supra* note 12, at 1640-41.

[75] *See* Schmitt & Vihul, *supra* note 12, at 1648.

[76] *See id.* at 1653-54.

[77] *Id.* at 1654; *see also* Certain Activities Carried out by Nicaragua in the Border Area (Costa Rica v. Nicar.) and Construction of a Road in Costa Rica Along the San Juan River (Nicar. v. Costa Rica), Judgment, 2015 I.C.J. 665, ¶ 2-4, 9 (Dec. 16) (Costa Rica alleged that Nicaraguan armed forces dug a channel on Costa Rican territory;

necessary, in order to establish whether there was a breach of Costa Rica's territorial sovereignty, to determine which State has sovereignty over that territory."[78] Schmitt and Vihul argue that because the court used terms such as "breach," territorial sovereignty is recognized as a legally binding rule.[79]

Next, Schmitt and Vihul point to historical instances where questions of territorial sovereignty have been front and center. For example, in 1960, a Soviet rocket shot down Francis Gary Powers while he was flying his U-2 spyplane over the Soviet Union.[80] The U.S. did not condemn the U-2 shoot-down.[81] In another incident occurring during the same year, the United States protested when Soviet fighters shot down an RB-47 aircraft.[82] Schmitt and Vihul contend the plausible explanation for this difference is that the U-2 was shot down over Soviet airspace while the RB-47 was shot down over supposedly international airspace; accordingly, the former incident was not a violation of territorial sovereignty while the latter was.[83]

2. The Sovereignty-as-Principle View

The sovereignty-as-rule view is not shared by all. As stated by the U.S. Cyber Command Legal Advisor, Colonel Gary Corn:

> An opposing view holds that sovereignty is a baseline principle of the Westphalian international order undergirding binding norms such as the prohibition against the use of force in Article 2(4) of the UN Charter, or the customary international law rule of non-

Nicaragua alleged that Costa Rica built a road on a contested area, causing environmental damage in Nicaragua).

[78] *Id.* ¶ 69.

[79] Schmitt & Vihul, *supra* note 12, at 1655.

[80] Oliver J. Lissitzyn, *Some Legal Implications of the U-2 and RB-47 Incidents*, 56 AM. J. INT'L L. 130, 135 (1962).

[81] Schmitt & Vihul, *supra* note 12, at 1656.

[82] *Id.*

[83] *Id.* at 1656-57.

> intervention, which States have assented to as an exercise of their sovereign equality.[84]

Corn acknowledges international law establishes a general rule of non-intervention and rules against the unlawful use of force.[85] Below the threshold of prohibited intervention, however, Corn and Robert Taylor argue "there is insufficient evidence of either state practice or *opinio juris* to support assertions that the principle of sovereignty operates as an independent rule of customary international law that regulates states' actions in cyberspace."[86] In their view, while respect for territorial sovereignty is an important consideration for conducting cyber operations, it does not completely preclude operations against *all* cyber infrastructure within other sovereign territories.[87]

Corn and Taylor's view is supported by the fact that applications of sovereignty principles vary based on customary practices in different domains. Cyber norms on land are different from cyber norms in outer space, in the air, or on the seas.[88] For example, outer space is open to peaceful exploitation by all nations.[89] Meanwhile, territorial intrusions into airspace are considered serious violations of international law absent consent or pursuant to exceptions.[90] While cyberspace has been recognized as a separate domain, sovereignty principles often apply on a fact-specific basis, taking into account practical considerations.[91] Corn and Taylor conclude that, although the principle of sovereignty is universal, a

---

[84] Gary Corn, *Tallinn Manual 2.0 –Advancing the Conversation*, JUST SECURITY (Oct. 18, 2018), https://www.justsecurity.org/37812/tallinn-manual-2-0-advancing-conversation/#more 37812.
[85] *Id.*
[86] Corn & Taylor, *supra* note 13, at 208.
[87] This is especially the case when the cyber infrastructure is controlled by non-state actors such as terrorists. *Id.* at 211.
[88] *See* Jensen, *supra* note 63, at 742-43.
[89] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, Jan. 27, 1967, 18 U.S.T. 2410, 610 U.N.T.S. 205.
[90] Corn & Taylor, *supra* note 13, at 210.
[91] *See* Jensen, *supra* note 63, at 741-42.

sovereignty-as-rule view is too restrictive considering the diversity of sovereignty applications across different domains.[92]

II. THE SOVEREIGNTY-AS-PRINCIPLE APPROACH IS CONSISTENT WITH RECENT STATE PRACTICE AND *OPINIO JURIS*

Both the sovereignty-as-rule and sovereignty-as-principle approaches make valid attempts to clarify the application of sovereignty to cyberspace. State practice and *opinio juris* in this area are mixed, but there is significant support of the sovereignty-as-principle view.[93]

The best argument put forth by those who support the sovereignty-as-rule approach is that prior judicial treatment has acknowledged sovereignty as a rule of international law. But the relevant examples, including the *Corfu Channel* and *Nicaragua* cases, address different activities in different domains.[94] Cyberspace is a unique domain requiring customized, fact-specific approaches to international law principles. Thus, the rules discussed by earlier ICJ cases are nearly impossible to apply in cyberspace and should not automatically govern cyber operations.

Additionally, Corn points out that the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE), the body tasked with examining how international law applies to states' cyber operations, has never taken a position consistent with the sovereignty-as-rule view.[95] Instead, the 2015 UNGGE consensus report provides that "[s]tate sovereignty and international norms and principles that *flow from sovereignty* apply to the conduct by States of [information and communications

[92] Corn & Taylor, *supra* note 13, at 210.
[93] *See, e.g.,* UK Attorney General Jeremy Wright, Cyber and International Law in the 21st Century (May 23, 2018), (transcript available at https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century); Sean Watts & Theodore Richard, *supra* note 31.
[94] *See* Gary P. Corn & Robert Taylor, *Concluding Observations on Sovereignty in Cyberspace*, 111 AJIL UNBOUND 282, 282-83 (2017).
[95] *See id.*

technologies]-related activities."[96] Here, the UNGGE appears to characterize sovereignty as a baseline principle on which international norms are based rather than its own rule. Subsequently, in 2017, the UNGGE failed to agree on the applicability of international law in cyberspace.[97]

State practice in the cyber realm, though still developing, indicates significant embrace of the sovereignty-as-principle view. On the last day of President Barack Obama's presidency, the Department of Defense General Counsel issued a memorandum that discussed military operations and sovereignty in cyberspace.[98] While the memo acknowledged the applicability of international law and the non-intervention principle to cyber operations, it went on to state: "military cyber activities that are neither a use of force, nor that violate the principle of non-intervention are largely unregulated by international law at this time . . . "[99] Further, the memo concluded that contemporary state practice and *opinio juris* do not conclusively indicate the existence of sovereignty as a binding legal norm.[100]

In May 2018, British Attorney General Jeremy Wright echoed strong support for the sovereignty-as-principle view when he said, "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. The UK Government's position is therefore that there is no such rule as a matter of current international law."[101] Wright's explicit affirmation of this view was an

[96] Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2015), transmitted by Letter dated 26 June 2015 from the Chair of the Group. Established pursuant to ¶ 4 of General Assembly Resolution 68/243 (2013), ¶ 27 U.N. Doc. A/70/174 (2015) (emphasis added).
[97] Dan Efrony & Yuval Shany, *A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice*, 112 AM. J. INT'L L. 583, 653 (2018).
[98] Watts & Richard, *supra* note 31.
[99] *Id.*
[100] *Id.*
[101] Wright, *supra* note 93.

important step in filling interpretive gaps with regard to international law in cyberspace.[102]

Since Wright's speech, a few additional states have released statements on the applicability of international law in cyberspace, with some coming out in favor of the sovereignty-as-rule view. For example, in September 2019 the French Ministère des Armées released a publication in which it stated, "Any cyberattack against French digital systems or any effects produced on French territory by digital means by a State organ, a person or an entity exercising elements of governmental authority or by a person or persons acting on the instructions of or under the direction or control of a State constitutes a breach of sovereignty."[103] However, it is unclear whether this statement reflects the position of the French government as a whole.[104] Similarly, the Netherlands released a statement in July 2019, pointing to the ICJ's *Nicaragua* case as an authority supporting a separate rule of sovereignty.[105]

In March 2020, Department of Defense General Counsel Paul Ney delivered a keynote address with the purpose of clarifying U.S. views on cyberspace issues. Ney directly addressed sovereignty:

---

[102] *See* Matthew Waxman, *U.K. Outlines Position on Cyberattacks and International Law*, LAWFARE (May 23, 2018, 9:57 AM), https://www.lawfareblog.com/uk-outlines-position-cyberattacks-and-international-law.

[103] MINISTÈRE DES ARMÉES, INTERNATIONAL LAW APPLIED TO OPERATIONS IN CYBERSPACE 7 (2019).

[104] Gary Corn, *Punching on the Edges of the Grey Zone: Iranian Cyber Threats and State Cyber Responses*, JUST SECURITY (Feb. 11, 2020), https://www.justsecurity.org/68622/punching-on-the-edges-of-the-grey-zone-iranian-cyber-threats-and-state-cyber-responses/ ("[The document] was written and published by the French Ministère des Armées (MdA), in the same vain [sic] as the DoD Law of War Manual which does not necessarily reflect the views of the U.S. government as a whole.").

[105] Letter from Dutch Minister of Foreign Affairs to the President of the House of Representatives 2 (Jul. 5, 2019), available at https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace; *see also* Michael Schmitt, *The Netherlands Releases a Tour de Force on International Law in Cyberspace*, JUST SECURITY (Oct. 14, 2019), https://www.justsecurity.org/66562/the-netherlands-releases-a-tour-de-force-on-international-law-in-cyberspace-analysis/.

> The DoD OGC view, which we have applied in legal reviews of military cyber operations to date, shares similarities with the view expressed by the U.K. Government in 2018 . . . many States' public silence in the face of countless publicly known cyber intrusions into foreign networks precludes a conclusion that States have coalesced around a common view that there is an international prohibition against all such operations (regardless of whatever penalties may be imposed under domestic law).[106]

While true that states' failure to condemn certain cyber operations is not indicative of whether a violation of international law occurred, Ney's observation highlights the lack of consistent state practice necessary for inferring that sovereignty exists as a separate rule. The views of France and the Netherlands, while significant, do not reflect the views of all states, and certainly not the United Kingdom or the United States. The sovereignty-as-principle approach remains a significant and plausible approach to international law in cyberspace.

III. THE SOVEREIGNTY-AS-PRINCIPLE APPROACH IS NECESSARY TO PROVIDE STATES WITH SUITABLE CYBER REMEDIES IN RESPONSE TO THREATS

As customary international norms in cyberspace are refined, states must have adequate means of responding to cyber and non-cyber threats from both state and non-state actors. The sovereignty-as-rule approach suggested by the Tallinn Manual does not offer states a suitable remedy for addressing such threats. On the other hand, the sovereignty-as-principle approach gives states far more options for responding to and engaging in cyber operations that are below the level of a use of force, and permits the principle of sovereignty in cyberspace to be further refined by future state practice.

---

[106] Paul C. Ney, Jr., DOD General Counsel Remarks at U.S. Cyber Command Legal Conference (Mar. 2, 2020), https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/.

A. Responses to State Actors Falling Below the Threshold of a Use of Force

One of the most pressing questions in the law applying to cyber operations is how states should approach operations that fall below the threshold of a use of force.[107] Tallinn 2.0 contains a narrow definition for the term "use of force." According to Rule 69, "[a] cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force."[108] This "scale and effects" test was originally articulated by the ICJ in the *Nicaragua* case as a tool for determining whether certain actions rise to the level of an "armed attack."[109] The authors of Tallinn 2.0 determined that the "scale and effects" test is equally helpful for distinguishing operations that amount to a use of force from those that do not.[110] However, the effects of cyber operations are not always analogous to the types of effects caused by non-cyber operations.

Many cyber operations result in severe consequences without causing any physical destruction.[111] This is precisely what occurred several years ago when the United States became the victim of a series of cyber operations targeting financial institutions. Over the course of 176 days between 2011 and 2013, attackers conducted distributed denial of service (DDoS) operations against financial institutions such as the Bank of America, Wells Fargo, the New York Stock Exchange, Nasdaq, and several others.[112] The Ababil operation, as it came it be known, caused tens of millions of dollars in economic harm and denied account access to several hundreds of thousands of

---

[107] *See* Michael N. Schmitt, *The Law of Cyber Warfare: Quo Vadis?*, 25 STAN. L. & POL'Y REV. 269, 279 (2014) ("The interpretive dilemma lies in application of the norm to cyber operations that, while not unleashing destructive or injurious force, nevertheless produce severe non-physical consequences.").
[108] TALLINN MANUAL 2.0, *supra* note 50, at 330.
[109] *Id.*
[110] *Id.* at 331 (listing factors to assist in distinguishing a use of force from other acts, including: severity, immediacy, directness, invasiveness, measurability of effects, military character, state involvement, and presumptive legality); Schmitt, *supra* note 105, at 280.
[111] Schmitt, *supra* note 105, at 279.
[112] Efrony & Shany, *supra* note 96, at 598.

customers.[113] Hackers also gained access to the control systems of a dam located in New York, although no physical destruction resulted from this specific breach.[114] The attack can most likely be attributed to Iran, as evidenced by an indictment brought against seven Iranian nationals in relation to the event.[115]

The U.S. responded softly, and evidence suggests that this is because the Obama administration feared the possible consequences of a counter-operation.[116] The administration rejected a proposal by Keith Alexander, the National Security Agency Director, to execute a cyber operation against those responsible for the Ababil operation because U.S. officials were uncertain "that the action could be so precise and expressed concern that affecting a server in Iran – even in self-defense – would represent a violation of its sovereignty."[117] This is a case where the sovereignty-as-rule view, which the U.S. officials here seemed to be relying on, created "unworkable hurdles" for for a state wishing to conduct cyber operations necessary to support a national security interest.[118] States in similar situations have little to no means of responding without risking a violation of the supposed sovereignty rule. Although Tallinn 2.0 includes a section that sets out a process for implementing countermeasures in cases such as the Ababil operation, the rules set out contain similar "unworkable hurdles," namely a strict notice requirement, that fail to take into account the nature of cyberspace.[119]

In contrast, an application of the sovereignty-as-principle view would have allowed U.S. officials to conduct certain cyber operations in response to the Abibal operation without violating Iran's territorial sovereignty. Again, under that standard, an infringement on

---

[113] *Id.*
[114] *See id.* at 598.
[115] *Id.* at 599.
[116] *See id.* at 600.
[117] Ellen Nakashima, *US Rallied Multinational Response to 2012 Cyberattack on American Banks*, WASH. POST (Apr. 11, 2014), https://www.washingtonpost.com/world/national-security/us-rallied-multi-nation-responseto-2012-cyberattack-on-american-banks/2014/04/11/7c1fbb12-b45c-11e3-8cb6-284052554d74_story.html? utm_term=.ba23ea798108.
[118] Corn, *supra* note 84.
[119] *Id.*

territorial sovereignty only occurs when another international law is violated.[120] In response to the Abibal hackers' operations, the sovereignty-as-principle view would have permitted the United States to conduct a wide range of targeted, limited operations without requiring the notification or consent of the target country.[121] Such operations would not be permitted to amount to a use of force or prohibited intervention. Nonetheless, states would be less burdened by unnecessary restrictions on defensive cyber operations.

B. Operations Against Non-State Actors

The sovereignty-as-principle view is better applied to contemporary national security needs, particularly defending against operations by non-state actors intent on causing harm. The Islamic State (ISIS) is a helpful case study. ISIS formed its own hacking division, known as the Cyber Caliphate, and successfully orchestrated a series of hacks in 2015.[122] In one instance, ISIS hackers gained access to social media accounts belonging to U.S. Central Command and posted propaganda material.[123] These hackers and propaganda specialists were not necessarily located in ISIS-controlled territory.[124] Rather, they operated on servers and cyber infrastructure located across the globe.[125] The states with sovereign authority over this physical infrastructure may not have been aware of its use by the ISIS cyber network, or may have lacked the ability to respond to cyber threats.[126] Importantly, as non-state actors, ISIS adherents do not violate sovereignty when conducting cyber operations because, even in the sovereignty-as-rule view, only states can violate sovereignty

[120] Corn & Taylor, *supra* note 13, at 210.
[121] *See* Corn, *supra* note 84.
[122] Paul Szoldra, *Inside the Hacker Underworld of ISIS*, BUSINESS INSIDER (June 16, 2016, 9:54 AM), https://www.businessinsider.com/isis-hacking-division-operates-2016-6.
[123] *Id.*
[124] Corn & Taylor, *supra* note 13, at 211.
[125] *Id.*
[126] *Id.*

principles.[127] Moreover, "countermeasures cannot be invoked as as a justification for actions taken against non-state actors."[128]

Under the sovereignty-as-principle view, states wishing to conduct cyber operations against non-state actors may begin countermeasures against associated cyber infrastructure without soliciting the consent of the host state, so long as no other principles of international law are violated.[129] As Corn and Taylor explain, "[w]here the proposed cyber action is focused solely against the individual accounts or facilities of terrorists or terrorist organizations widely recognized as such, and when the cyber actions will generate only *de minimis* effects on non-terrorist infrastructure within the host state, international law does not preclude those cyber actions."[130] In short, this view reaches a middle ground where states can pursue crucial national security interests while respecting international law. Further, states are free to prohibit certain cyber actions in domestic law, but such prohibitions do not necessarily implicate international law.[131] For example, states have an absolute authority to criminalize cyber espionage in their domestic laws, but espionage by itself is not widely viewed as a violation of international law.[132] Accordingly, the sovereignty-as-principle view permits states to retain ample authority for deterring cyber intrusions within their own territories while enabling them to conduct cyber operations necessary for national security.

Those favoring the sovereignty-as-rule view agree with Corn and Taylor that "not all cyber operations that manifest, either partially or totally, on another State's cyber infrastructure infringe that State's territorial inviolability."[133] They might nevertheless argue that certain instances of conduct falling short of an infringement on sovereignty do not refute the existence of an enforceable rule; rather, these instances are evidence the rule requires further development.

---

[127] TALLINN MANUAL 2.0, *supra* note 50, at 17-18.
[128] Corn, *supra* note 84.
[129] Corn & Taylor, *supra* note 13, at 211.
[130] *Id.*
[131] *Id.* at 212.
[132] *Id.* at 209.
[133] Schmitt & Vihul, *supra* note 12, at 1648.

However, the very fact that violations of sovereignty cannot be determined without analyzing contextual criteria, such as the domain in which the violation occurred, suggests that such a clear-cut rule does not exist.

CONCLUSION

Territorial sovereignty has always been a difficult and abstract concept, even before the introduction of cyberspace as an operational domain. Cyberspace is becoming a more dangerous place, with the consequences of harmful cyber operations ranging from minor manipulations of data to physical damage to people and critical infrastructure. Comprehensive principles on which states may rely when operating in cyberspace are necessary in this new reality.

Tallinn 2.0 is a noteworthy contribution to the widespread effort to clarify international law principles in cyberspace. However, international norms and principles applying to cyberspace are still widely open to interpretation. Interpretations of territorial sovereignty that apply in other domains may apply differently or not at all in cyberspace. State practice and the acceptance of customary cyber norms will ultimately determine the international legal landscape in cyberspace.

Recent state practice indicates that states are acknowledging problems with Tallinn 2.0's proposition that sovereignty is its own enforceable legal rule. The United Kingdom has explicitly voiced its support for the sovereignty-as-principle view in which sovereignty is not itself a separate rule, but rather serves as a basis for many international law rules and norms. Although a few states subscribe to the sovereignty-as-rule view, ongoing disagreements between states about the status of sovereignty in cyberspace suggest the absence of a settled rule.

Lastly, the sovereignty-as-principle view better aligns with states' goals of effectively responding to threats with cyber tools. The sovereignty-as-rule view creates complications for states wishing to conduct various types of cyber operations below the use of force threshold. This view is impractical considering the nature of

cyberspace, particularly the growing level of malicious cyber activity that justifies more liberal mechanisms for responding. Additionally, the sovereignty-as-rule view inhibits cyber operations against malicious non-state actors, who often exploit cyber infrastructure located across the globe and do not abide by international law principles. In contrast, the sovereignty-as-principle view allows states to deter cyber operations harmful to their own territory through domestic law, while at the same time permitting them to conduct necessary cyber operations, subject to other rules of international law.