BASELINE TERRITORIAL SOVEREIGNTY AND CYBERSPACE

by
Sean Watts[*] *& Theodore Richard*[**]

The question of how territorial sovereignty operates in the novel yet ubiquitous realm of cyberspace has proved enormously contentious. State practice in cyberspace presents a confusing array of behavior and justifications for conduct that runs along the enduring legal fault lines of territorial sovereignty. This Article examines the legal history of sovereignty, emerging State cyber practice, and early legal views taken with respect to the application of sovereignty to cyberspace.

We argue that based on historical origins, legal evolution, international litigation, and recent State expressions concerning applicability of international law to cyberspace, the baseline rules of territorial sovereignty should be currently understood as a rule of conduct that generally prohibits States' nonconsensual interference with the integrity of cyber infrastructure on the territory of other States.

We acknowledge that States may soon adapt sovereignty to operate differently in cyberspace, as they have in other contexts of international relations. However, in the absence of a lex specialis *of cyber sovereignty and until States resort to deliberate international lawmaking, the baseline guarantee of territorial integrity provides a principled and normatively desirable understanding of sovereignty and how it relates to cyberspace. We urge States to act quickly to reaffirm their commitment to baseline Westphalian norms of territorial sovereignty in cyberspace while crafting, through accepted means of international legal development, a nuanced and effective doctrine of territorial sovereignty in cyberspace. A sound approach will acknowledge the binding legal character of territorial sovereignty as a limit on foreign interference but offer an emerging cyber-specific understanding much like that developed for other domains that have challenged national security and peaceful interactions between States.*

[*] Professor of Law, Creighton University School of Law; Lieutenant Colonel, United States Army Reserve.

[**] Lieutenant Colonel, United States Air Force.

I. INTRODUCTION

In late 2016, in an operation code-named Glowing Symphony, the United States Cyber Command reportedly acquired administrator passwords to Islamic State (IS) websites. The passwords enabled deletion of digital content, including videos used for recruitment, from cyber infrastructure located in at least five countries outside actively hostile areas of Iraq and Syria.[1] Similar digital content reportedly resided on cyber infrastructure in as many as 30 other States.[2] Changing the passwords reportedly locked IS administrators out of the websites.[3]

It is unclear whether the United States notified the States in whose territory the affected cyber infrastructure resided in advance of the operations. A media account of the operation relates,

> CIA Director John Brennan, Secretary of State John F. Kerry, FBI Director James B. Comey and Director of National Intelligence James R. Clapper Jr. argued that notice was necessary—especially to allied countries—to preserve relationships. [Secretary of Defense Ashton] Carter, Cybercom commander Adm. Michael S. Rogers and Gen. Joseph F. Dunford Jr., the chairman of the Joint Chiefs of Staff, countered that existing authority did not require it, particularly as the Pentagon insisted there would be no harmful collateral effects.

[1] Ellen Nakashima, *U.S. Military Cyber 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=.bc276ae54a1f; Joe Uchill, *Anti-ISIS Cyber Op Struggled with Issue of Notifying Allies*, The Hill (May 9, 2017), http://thehill.com/policy/cybersecurity/332491-anti-isis-cyber-op-struggled-with-issue-of-notifying-allies. Although both authors are assigned at the time of writing to a command responsible for U.S. Department of Defense cyber operations, neither author contributed to legal reviews of an operation reported publicly as Glowing Symphony. Nor did the authors' access to non-publicly available information on U.S. cyber operations form any part of this Article.

[2] Nakashima, *supra* note 1.

[3] *See* Uchill, *supra* note 1.

> They also argued that if notice is given, word of the operation could leak. That could tip off the target and enable other adversaries to discover the command's cyber capabilities.[4]

In addition to the political and operational calculations involved in the operation, legal considerations surely formed part of the deliberations that preceded these operations. Legal analyses are an integral part of U.S. Department of Defense operations, especially operations subject to the laws of war.[5] However, because the deletions did not involve physical destruction of infrastructure or physical harm to persons, it is unlikely U.S. Cyber Command planners and policymakers devoted significant attention to whether the operation involved a use of force or armed attack under *ius ad bellum*, the international law of conflict management between States, or an attack for purposes of *ius in bello*, the international law on the conduct of hostilities.[6]

Instead, legal attention preceding the operation likely focused on the general peacetime restraints found in public international law. And because the operation involved action taking place or with effects manifesting in foreign territory, it is further likely the lawyers advising the operation against IS considered the extent to which these operations would violate, *inter alia*, the sovereignty of the States on whose territory the affected cyber infrastructure was located. If so, these lawyers found themselves addressing one of the most difficult and pressing issues of the ongoing effort to apply international law to emerging domains of international relations, the question of how territorial sovereignty operates in the interconnected yet diffuse, virtual yet material, and novel yet ubiquitous realm of cyberspace.

Even divorced from the unique and legally challenging context of cyberspace, territorial sovereignty is an enormously complex and arcane subject of international law. While it is axiomatically foundational to nearly every subject and rule of international law, the precise legal import of territorial sovereignty is frustratingly complicated, contextual, and elusive. It has been conceived variously and simultaneously as a concept,

---

[4] Nakashima, *supra* note 1.

[5] As a component of the U.S. Department of Defense (DoD), United States Cyber Command is bound by DoD legal policy including its Law of War Program. U.S. DEP'T OF DEF., DIR. 2311.01E, DOD LAW OF WAR PROGRAM ¶¶ 2, 5.7.3 (May 9, 2006). The DoD Law of War Program requires all DoD components, "[m]ake qualified legal advisers at all levels of command available to provide advice about law of war compliance during planning and execution of exercises and operations . . . ." *Id.* at ¶ 5.7.3. The legal advice provided by DoD legal advisers is not limited to the law of war but rather incorporates the full spectrum of legal obligations applicable to U.S. military operations, including domestic and international law. *See id.* at ¶ 2.

[6] U.S. DEP'T OF DEF., LAW OF WAR MANUAL ¶¶ 1.11, 16.3 (2016) (addressing *ius ad bellum*); ¶¶ 3.4, 16.5 (addressing *ius in bello*); and ¶ 3.5 (describing the relationship between the concepts).

a sentiment, a status, a principle, and a rule of conduct. Add to these complications, the fact that the concept of sovereignty seems to exist in a perpetual state of flux—a moving target for jurists.

As sovereignty has evolved to meet the demands of increasingly complex State relations, commentators have detected a "declining intelligibility of the concept . . . ."[7] Therefore, putting sovereignty to work in a coherent and principled manner has proved immensely difficult. That difficulty has been compounded in contexts lacking deeply-rooted or established patterns of State practice. Cyberspace presents such a context. States offer a confusing array of behavior and justifications for conduct that runs along the enduring legal fault lines of territorial sovereignty.

Various strains of thought have emerged in response to questions concerning the fit between sovereignty and cyberspace. Early academic attention addressed the fundamental question of the general relevance of sovereignty to cyberspace, especially whether cyberspace might present a post-Westphalian domain.[8] This work focused on issues of compatibility, especially the extent to which States could actually assert control over widely dispersed, seemingly virtual cyber infrastructure and actions divorced from the physical, territorial world of classic sovereignty.[9] Jurisdictional inquiries dominated, especially questions concerning the legitimacy of prescriptive and enforcement jurisdiction over infrastructure in other States' territory.[10]

Later work usefully characterized competing visions of governance in cyberspace thought to flow from sovereignty.[11] One model has prioritized

[7] Nicholas Greenwood Onuf, *Sovereignty: Outline of a Conceptual History*, 16 ALTERNATIVES 425, 428 (1991).

[8] *See* David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace,* 48 STAN. L. REV. 1367, 1370–71 (1996) (conceiving cyberspace as a legally distinct domain of interaction, apart from the physical world). *But see* Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199, 1245–46 (1998) (emphasizing the physical manifestations of cyberspace as subject to existing legal regimes).

[9] *See generally* Johnson & Post, *supra* note 8.

[10] William P. Barr, *Authority of the Federal Bureau of Investigation to Override International Law in Extraterritorial Law Enforcement Activities*, Jun. 21, 1989, *in* 13 OPINIONS OF THE OFFICE OF LEGAL COUNSEL OF THE UNITED STATES DEPARTMENT OF JUSTICE 163 (1996); Robert G. Dixon, Jr., *Constitutionality of Legislation to Establish a Program to Prevent Aircraft Piracy*, Mar. 23, 1973, in 1 SUPPLEMENTAL OPINIONS OF THE OFFICE OF LEGAL COUNSEL OF THE UNITED STATES DEPARTMENT OF JUSTICE, 356–57 (Nathan A. Forrester ed., 2013); Jack L. Goldsmith, *The Internet and the Abiding Significance of Territorial Sovereignty*, 5 GLOBAL LEGAL STUD. J. 475, 476 (1998); John M. Harmon, *Extraterritorial Apprehension by the Federal Bureau of Investigation*, 1980, *in* 4B OPINIONS OF THE OFFICE OF LEGAL COUNSEL OF THE UNITED STATES DEPARTMENT OF JUSTICE 543 (Margaret Colgate Love ed., 1985); Henry H. Perritt, Jr., *Jurisdiction in Cyberspace,* 41 VILL. L. REV. 1, 3 (1996).

[11] *See* Kristen E. Eichensehr, *The Cyber-Law of Nations*, 103 GEO. L.J. 317, 329 (2015).

State control, especially over domestic features and functioning of cyber infrastructure. Authoritarian States have claimed that cyber sovereignty guarantees complete insulation from outside regulation or international interference with the controls and restrictions they place on cyberinfrastructure in their territory.[12] For China and Russia, the exercise of sovereignty in cyberspace involves not only efforts to secure the integrity of information and information systems but also to control the flow and character of content accessed on territorial cyber infrastructure.[13] Meanwhile, a competing model, most often advanced by liberal democracies, has argued for a more limited notion of cyber sovereignty, conditioned by pluralistic, multi-stakeholder control based on coordination and cooperation regulated by practice-based norms.[14]

Further dialogue has inquired whether cyberspace and its ability to connect broadly dispersed populations and interests has rendered sovereignty obsolete and whether many aspects of sovereignty should be surrendered to supranational institutions.[15] Such proposals join previous dialogues considering alternatives to sovereignty as means of governance.[16] These discussions join broader inquiries into the extent to which preservation of sovereignty helps or hinders security and peaceful coexistence between States.[17] At the core of each of these dilemmas is a dispute about sovereignty, its history, its legal weight, and its import in new domains of State action such as cyberspace.

Meanwhile, a seemingly more basic issue related to sovereignty has arisen. As Operation Glowing Symphony illustrates,[18] cyberspace greatly expands opportunities for States to violate the independence and exclu-

[12] *See generally* Adam Segal, *Chinese Cyber Diplomacy in a New Era of Uncertainty*, HOOVER INSTITUTION 3 (June 2, 2017), https://www.hoover.org/research/chinese-cyber-diplomacy-new-era-uncertainty (discussing China and Russia's approach to cyber security).

[13] *See* Keir Giles, *Russia's Public Stance on Cyberspace Issues*, *in* 4TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT 63, 65 (C. Czosseck et al. eds., 2012), https://ccdcoe.org/sites/default/files/multimedia/pdf/2_1_Giles_RussiasPublicStanceOnCyberInformationWarfare.pdf; Segal, *supra* note 12, at 3.

[14] Eichensehr, *supra* note 11, at 320–21, 329–32.

[15] *See generally* Walter B. Wriston, *Technology and Sovereignty*, 67 FOREIGN AFF. 63 (1988).

[16] *See* PROBLEMATIC SOVEREIGNTY: CONTESTED RULES AND POLITICAL POSSIBILITIES viii (Stephen D. Krasner ed., 2001).

[17] *See* ABRAM CHAYES & ANTONIA HANDLER CHAYES, THE NEW SOVEREIGNTY: COMPLIANCE WITH INTERNATIONAL REGULATORY AGREEMENTS 1 (1995) (advocating a "new sovereignty" based on the capacity to participate in collective actions previously reserved to single States); Anne-Marie Slaughter, *Sovereignty and Power in a Networked World Order*, 40 STAN. J. INT'L L. 283, 285 (2004) (observing "states can no longer govern effectively by being left alone and by leaving other states alone" and identifying a "new sovereignty" of cooperative "government networks").

[18] Nakashima, *supra* note 1.

sivity traditionally attendant to sovereignty. By means of its interconnected framework, cyberspace presents States unprecedented access to information and objects on the territory of other States. Cyberspace frees States from many of the geographic and physical restraints that might have previously prevented access. Because of their potential to compromise territorial integrity without significant impact to physical property or immediately proximate impact on persons, cyber operations bring into sharp focus the question whether mere intrusions into territorial property amount to internationally wrongful acts.

General international law has not devoted to these low-intensity intrusions the significant attention it has dedicated to high-intensity and coercive interactions between States. Where the latter events implicate a somewhat rich vocabulary of customary and codified norms and doctrine, such as *ius ad bellum* and *ius in bello*, the former are governed chiefly by the comparatively underdeveloped and vague framework of sovereignty. To be sure, States have refined their notions of sovereignty in several specific domains of international relations such as the seas and outer space. Through customs and treaties, States have both reinforced and conditioned the legal import of sovereignty. However, the extent to which these domain-specific refinements should be transposed to cyberspace or whether more general, baseline restraints should prevail is unclear. And if the baseline restraints of territorial sovereignty are to apply, the precise content and extent of these rules, or whether any such rules exist, has been shockingly neglected.

We begin this Article with a brief account of the extent and nature of emerging State interactions in cyberspace. We devote particular attention to increasingly common instances of competitive, even destructive, cyber operations undertaken by States against cyber infrastructure located in other States' territory. We then survey the history, development, and regulatory content of territorial sovereignty to evaluate its past and current legal import as a rule of conduct. Although we concede contextual variations and exceptions have evolved for specialized domains of interaction such as the seas, we identify in territorial sovereignty a baseline rule of conduct and a corresponding duty on the part of States to refrain from interference with the integrity of conditions in other States' territory. We then examine and evaluate public and private legal analyses of how territorial sovereignty operates in cyber contexts. We argue that based on historical origins, legal evolution, and recent State expressions concerning applicability of international law to cyberspace, the baseline rules of territorial sovereignty should be currently understood as a rule of conduct that generally prohibits States' nonconsensual interference with the integrity of cyber infrastructure on the territory of other States.[19]

[19] In 2012, the State Department Legal Adviser, Harold Koh, explained that international law principles applied to cyberspace and that "States conducting

This view may not hold forever, or even for long. State practice and emerging legal statements suggest States may soon adapt sovereignty to operate differently in cyberspace, as they have in other contexts of international relations. However, in the absence of a *lex specialis* of cyber sovereignty and until States resort to deliberate international lawmaking, the baseline guarantee of territorial integrity provides a principled and desirable understanding of sovereignty and how it relates to cyberspace.

II. CYBERSPACE AND INTERNATIONAL RELATIONS

States now widely recognize cyberspace as a vital domain of international relations and competition. Their policies and plans warn of increasing use of cyberattacks as political instruments.[20] The United Kingdom has acknowledged that it regularly suffers "attempts by states and state-sponsored groups to penetrate UK networks for political, diplomatic, technological, commercial and strategic advantage, with a principal focus on the government, defence, finance, energy and telecommunications sectors."[21] Russia's recently declared cybersecurity posture focuses on establishing an international legal regime aimed at creating conditions for international information security.[22] Russian strategy recognizes

activities in cyberspace must take into account the sovereignty of other States, including outside the context of armed conflict." U.S. DEP'T OF STATE OFF. OF THE LEGAL ADVISOR, DIGEST OF THE UNITED STATES PRACTICE IN INTERNATIONAL LAW 596 (CarrieLyn D. Guymon ed., 2012), https://www.state.gov/documents/organization/211955.pdf. More recently, the leaders of the G20 nations, including the United States, affirmed "international law, and in particular the UN Charter, is applicable to state conduct in the use of [information and communication technologies (ICTs)] and [we] commit ourselves to the view that all states should abide by norms of responsible state behaviour in the use of ICTs . . . ." G20 LEADERS' COMMUNIQUÉ, ANTAYLA SUMMIT 6 (Nov. 15–16, 2015), http://www.mofa.go.jp/files/000111117.pdf. They also endorsed a 2015 report by the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. *Id.* This report clearly stated, "State sovereignty and international norms and principles that flow from sovereignty apply to the conduct by States of ICT-related activities and to their jurisdiction over ICT infrastructure within their territory" and that "States have jurisdiction over the ICT infrastructure located within their territory." U.N. Secretary-General, *Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, ¶ 11, U.N. Doc. A/70/174 (July 22, 2015) [hereinafter U.N. Doc. A/70/174].

[20] U.S. DEP'T OF DEF., THE DEPARTMENT OF DEFENSE CYBER STRATEGY 2 (2015).

[21] HM GOV'T, NATIONAL CYBER STRATEGY 2016–2021 18 (2016), https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national_cyber_security_strategy_2016.pdf.

[22] COOPERATIVE CYBER DEFENCE CTR. OF EXCELLENCE, BASIC PRINCIPLES FOR STATE POLICY OF THE RUSSIAN FEDERATION IN THE FIELD OF INTERNATIONAL INFORMATION SECURITY TO 2020, 3 (2013), https://ccdcoe.org/sites/default/files/strategy/RU_state-policy.pdf.

the threat of information and communications technology used for terroristic, criminal, military, or political purposes inconsistent with international law and for interference into the internal affairs of sovereign States to violate the public order.[23] The United States cyber strategy also recognizes threats to economic security from extortion, fraud, identity theft and child exploitation, while noting, "[c]ybersecurity threats can even endanger international peace and security more broadly, as traditional forms of conflict are extended into cyberspace."[24] For its part, the Chinese People's Liberation Army has speculated that the entire Internet may simply be a Western ploy to undermine Chinese sovereignty.[25]

While States lament intrusions and disruptions of their own cyber infrastructure by outside agents, a survey of publicly-available accounts of State conduct in cyberspace shows a simultaneous willingness to engage in unfriendly cyber conduct dating to early stages of cyberspace. States regularly engage in nefarious or hostile cyber operations and increasingly resort to cyber means to deny other States effective use of cyberspace. The disruptive and destructive potential of military operations in cyberspace was clear to the United States over a decade ago. The 2006 U.S. National Military Strategy boldly stated, "[t]he United States must have cyberspace superiority to ensure our freedom of action and deny the same to our adversaries through the integration of network defense, exploitation, and attack."[26] Similarly, the 2008 strategy for the U.S. Air Force Cyber Command aimed to "provide decision-makers flexible options to deter, deny, disrupt, deceive, dissuade, and defeat adversaries through a variety of destructive and non-destructive, and lethal and non-lethal means."[27]

The extent to which the early architects of cyberspace anticipated these hostile conditions is unclear. Its designers initially conceived cyberspace as a communications platform. In the 1960s, the U.S. Advanced Projects Research Agency, known as "ARPA," sponsored studies to enable computers to communicate with each other at distant locations or

[23] *Id.* at 2–3.

[24] EXEC. OFF. OF THE PRESIDENT, INTERNATIONAL STRATEGIES FOR CYBERSPACE: PROSPERITY, SECURITY AND OPENNESS IN A NETWORKED WORLD 4 (May 2011).

[25] ADAM SEGAL, THE HACKED WORLD ORDER: HOW NATIONS FIGHT, TRADE, MANEUVER, AND MANIPULATE IN THE DIGITAL AGE 29 (2016) (citing *Army Newspaper: We Can Absolutely Not Allow the Internet Become a Lost Territory of People's Minds*, CHINA COPYRIGHT & MEDIA (May 13, 2015), https://chinacopyrightandmedia.wordpress.com/2015/05/13/army-newspaper-we-can-absolutely-not-allow-the-internet-become-a-list-territory-of-peoples-minds/).

[26] PETER PACE, CHAIRMAN OF THE JOINT CHIEFS OF STAFF, THE NATIONAL MILITARY STRATEGY FOR CYBERSPACE OPERATIONS 1 (2006), http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-023.pdf.

[27] MAJ. GEN. WILLIAM T. LORD, AIR FORCE CYBER COMMAND STRATEGIC VISION, USAF II (Feb. 2008), www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA479060.

nodes.[28] In 1973, ARPA established its first international cyber nodes in Kjeller, Norway[29] and at the University College of London.[30] Whether anticipated or not, hostile conduct soon surfaced; the same year these nodes became operational, ARPA discovered malicious behavior involving systems compromised and intentionally crashed by anonymous users.[31]

On January 1, 1983, an improved communication protocol enabled multiple computer networks to communicate with each other, forming a network of networks, ARPANET or the early Internet.[32] Mindful of its power for both good and mischief, early cyber philosophers declared the Internet a realm free from sovereignty and State authority.[33] Many thought an unregulated, decentralized Internet would make government control and censorship impossible.[34] These accounts emphasized the seemingly virtual qualities of electronic storage and exchange.[35] Others characterized the Internet as a "global commons," analogous to the high seas.[36] As a global commons, cyberspace might be a domain outside the

[28] Robert H. Zakon, *Hobbes' Internet Timeline 25*, ZAKON.ORG, https://www.zakon.org/robert/internet/timeline/.

[29] *ARPANET: NORSAR Becomes the First Non-US Node on ARPANET, the Predecessor to Today's Internet*, NORSAR, https://www.norsar.no/about-us/history/arpanet-article774-270.html.

[30] *30 Years of the International Internet*, BRIT. BROADCASTING CORP. (Nov. 19, 2003), http://news.bbc.co.uk/2/hi/technology/3280897.stm.

[31] *See RFC 602 - "The Stockings Were Hung by the Chimney with Care,"* FAQS.ORG, http://www.faqs.org/rfcs/rfc602.html.

[32] MITCH WALDROP, DARPA AND THE INTERNET REVOLUTION 85 (2015), http://www.darpa.mil/attachments/(2O15)%20Global%20Nav%20-%20About%20Us%20-%20History%20-%20Resources%20-%2050th%20-%20Internet%20(Approved).pdf.

[33] John Perry Barlow, *A Declaration of the Independence of Cyberspace*, ELEC. FRONTIER FOUND. (Feb. 8, 1996), https://www.eff.org/cyberspace-independence. Later legal analyses refined the argument somewhat noting differences in the scale and effect of cyber interactions to justify departure from legacy legal frameworks including international law. *See* David G. Post, *Against "Against Cyberanarchy,"* 17 BERKELEY TECH. L.J. 1365, 1366 (2002).

[34] Katherine Maher, *The New Westphalian Web*, FOREIGN POLICY (Feb. 25, 2013), http://foreignpolicy.com/2013/02/25/the-new-westphalian-web/.

[35] Johnson & Post, *supra* note 8, at 1370–71.

[36] U.S. DEP'T OF DEF., STRATEGY FOR HOMELAND DEFENSE & CIVIL SUPPORT 1 (2005); Elena Bojinova, *Cyberlaw: Jurisdiction and Choice of Law*, 7 NEW ENG. INT'L & COMP. L. ANN. 217, 217 (2001); Anupam Chander, *The New, New Property*, 81 TEX. L. REV. 715, 720 (2003); Roger Hurwitz, *Depleted Trust in the Cyber Commons*, 6 STRATEGIC STUD. Q. 20, 23 (2012); Lowell E. Jacoby, *Global Commons and the Role for Intelligence*, 83 INT'L L. STUD. 51, 52 (2007); Charles D. Siegal, *Rule Formation in Non-Hierarchical Systems*, 16 TEMP. ENVTL. L. & TECH. J. 173, 216 (1998); Bill Davidow, *The Tragedy of the Internet Commons*, THE ATLANTIC (May 18, 2012), https://www.theatlantic.com/technology/archive/2012/05/the-tragedy-of-the-internet-commons/257290/; MAJ. GEN. MARK BARRETT ET AL., SUPREME ALLIED COMMAND TRANSFORMATION, NORTH

political control of any single State's sovereignty, offering universal access.[37]

However, the Internet soon proved to be neither a global commons nor a virtual or sovereignty-free realm. It manifested instead as a collection of linked but distinct, concrete, and physically identifiable infrastructure.[38] Today, most of the components of cyberspace are located on territory fully subject to territorial sovereignty. The inner workings of its functions and protocols often seem ethereal and remain, for most, clouded in mystery. Yet cyberspace clearly reveals itself in a physical architecture, including tangible hardware, connecting structures, cables, and transmitters. With these material conceptions in mind, debates concerning international cyberspace governance quickly turned toward traditional regulatory models, including domestic and Westphalian-based[39] international law.

Social, practical, and political considerations explain the embrace of the State-centric, Westphalian system in cyberspace. Professors Jack Goldsmith and Tim Wu offer three explanations why the State-centric system of governance has been transposed to cyberspace. First, end users prefer local linguistic and cultural content.[40] Despite its worldwide reach and early dominance by English language sites, Internet use and content has become more parochial, and therefore territorial, in many respects over time. Second, technological developments have enabled State-imposed controls, such as firewalls and closed networks.[41] Notwithstanding its technical capacity to operate in an entirely borderless fashion, the Inter-

ATLANTIC TREATY ORG., ASSURED ACCESS TO THE GLOBAL COMMONS xi (Apr. 3, 2011), http://www.act.nato.int/images/stories/events/2010/gc/aagc_finalreport.pdf.

[37] UN SYSTEM TASK TEAM ON THE POST-2015 UN DEVELOPMENT AGENDA, GLOBAL GOVERNANCE AND GOVERNANCE OF THE GLOBAL COMMONS IN THE GLOBAL PARTNERSHIP FOR DEVELOPMENT BEYOND 2015 3 (2013), http://www.un.org/en/development/desa/policy/untaskteam_undf/thinkpieces/24_thinkpiece_global_governance.pdf; Michael Chertoff, *The Strategic Significance of the Internet Commons*, 8 STRATEGIC STUD. Q. 10, 10 (2014).

[38] JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET?: ILLUSIONS OF A BORDERLESS WORLD 68 (2008). *See also* Patrick W. Franzese, *Sovereignty in Cyberspace: Can it Exist?*, 64 A.F. L. REV. 1, 17 (2009) (arguing that it is problematic to characterize cyberspace as a global commons because it lacks prerequisite characteristics, such as a global governing treaty with specific and identifiable uses and prohibitions, common and definable boundaries, consensus by States to forgo sovereignty claims, and lack of state ability to control); Mark Raymond, *Puncturing the Myth of the Internet as a Commons*, 3 GEO. J. INT'L AFF. 53, 57–58 (2014) (characterizing the internet as a set of nested clubs). *But see* Wolff Heintschel von Heinegg, *Territorial Sovereignty and Neutrality in Cyberspace*, 89 INT'L L. STUD. 123, 126 (2013) (asserting that cyberspace is properly classified as *res communis omnium*, while its components are subject to territorial sovereignty rules).

[39] Leo Gross, *The Peace of Westphalia, 1648–1948*, 42 AM. J. INT'L L. 20, 20 (1948).

[40] GOLDSMITH & WU, *supra* note 38, at 149.

[41] *Id.* at 149–50.

net has been to some extent Balkanized by security controls erected and maintained by States. Finally, States have felt compelled to enforce legacy laws, especially those regulating national security, intellectual property, contract enforcement, libel and slander, gambling, and content of speech.[42] From a sovereignty-minded perspective, States have demonstrated a strong commitment to enforce their laws over Internet activities within their territories.

It is not surprising that once States conceived of cyberspace as a domain commensurate with the competitive Westphalian system of international relations, that cyberspace would share the latter's faults and security challenges. Cyberspace has proved to reflect, rather than to deviate from, the contentious environment of international relations. Even before international cyber relations became common place, States recognized the potential for code to secure strategic advantage. During the Cold War, the U.S. Central Intelligence Agency (CIA) tracked Soviet efforts to acquire Western technology by surreptitious means. The CIA reportedly worked with American industry to modify and allow Soviet agents to steal defective technology.[43] In one case, a covert operation deliberately slipped flawed natural gas pipeline software code to the Soviets.[44] Months later a Soviet natural gas pipeline exploded, giving perhaps the first literal effect to a "logic bomb."[45]

As cyberspace matured, campaigns ranging from small-scale, individual hacks to coordinated State practice proliferated rapidly. In 1986, West German hackers broke into the Lawrence Berkley National Laboratories, the ARPANET/MILNET,[46] and other U.S. networks. Searches for keywords like "nuclear," "sdi" (the Strategic Defense Initiative), "norad" (the joint Canadian-U.S. North American Aerospace Defense Command), and "kh-11" (a reconnaissance satellite) revealed an effort to locate sensitive national security information either on behalf of U.S. Cold War adversaries or for transfer to them.[47] Breaches traced to the Nether-

[42] *Id.* at 150.

[43] Gus. W. Weiss, *Duping the Soviets: The Farewell Dossier*, 39 STUD. IN INTELLIGENCE 121, 125 (1996).

[44] THOMAS C. REED, AT THE ABYSS: AN INSIDER'S HISTORY OF THE COLD WAR 268–69 (2004); David E. Hoffman, *Reagan Approved Plan to Sabotage Soviets*, WASH. POST, (Feb. 27, 2004), https://www.washingtonpost.com/archive/politics/2004/02/27/reagan-approved-plan-to-sabotage-soviets/a9184eff-47fd-402e-beb2-63970851e130/?utm_term=.2582b0bd3829.

[45] REED, *supra* note 44, at 269.

[46] MILNET was created for operational military traffic in 1983 due to heavy use of the ARPANET. U.S. GEN. ACCOUNTING OFFICE, GAO/IMTEC-89-57, COMPUTER SECURITY: VIRUS HIGHLIGHTS NEED FOR IMPROVED INTERNET MANAGEMENT 8–9 (1989) [hereinafter GAO/IMTEC-89-57].

[47] Clifford Stoll, *Stalking the Wily Hacker*, 31 COMM. OF THE ACM 484, 489 (1988). *See also* Jason Healey, *A Brief History of U.S. Cyber Conflict*, *in* A FIERCE DOMAIN: CONFLICT

lands similarly accessed U.S. military networks searching for information on Patriot missiles, nuclear weapons, and Operation Desert Storm from 1990 to 1991.[48] The Dutch hackers reportedly offered to sell the information to the Iraqi government, which considered the offer a hoax.[49] In 1994, British hackers gained unauthorized access to computer networks at U.S Air Force laboratories in Rome, New York. They soon downloaded sensitive research on air tasking orders, the messages used by military commanders to convey orders to pilots relating to wartime tactics and targeting.[50] In 1998, teenagers from California and an Israeli citizen accessed U.S. and Israeli national security computer networks in the most organized and systematic infiltration discovered to that point.[51]

State responses to each of these incidents focused on domestic criminal processes.[52] Little publicly-available information indicates the extent to which the victim States regarded these incidents as international in

IN CYBERSPACE, 1986 TO 2012, 29 (Jason Healey ed., 2013); CLIFF STOLL, THE CUCKOO'S EGG: TRACKING A SPY THROUGH THE MAZE OF COMPUTER ESPIONAGE 364–69 (2005).

[48] U.S. GEN. ACCOUNTING OFF., GAO/T-IMTEC-92-5, COMPUTER SECURITY: HACKERS PENETRATE DOD COMPUTER SYSTEMS 1–2 (1991) (statement of Jack L. Brock, Jr., Director, Government Information and Financial Management, Information Management and Technology Division); Healey, *supra* note 47, at 36.

[49] *Computer Security Experts: Dutch Hackers Stole Gulf War Secrets*, ASSOCIATED PRESS (Mar. 24, 1997), http://www.apnewsarchive.com/1997/Computer-security-experts-Dutch-hackers-stole-Gulf-War-secrets/id-9bdfd653327fc9c17e643090f08d1d04.

[50] Healy, *supra* note 47, at 37; U.S. GEN. ACCOUNTING OFF., GAO/T-AIMD-96-92, COMPUTER SECURITY: COMPUTER ATTACKS AT DEPARTMENT OF DEFENSE POSE INCREASING RISKS 3–4 (1996) [hereinafter GAO/T-AIMD-96-92] (statement of Jack L. Brock, Director, Defense Information and Financial Management Systems, Accounting and Information Management Division).

[51] *Five Teens Suspected of Hacking into Pentagon Computers*, WASH. POST (Mar. 20, 1998), https://www.washingtonpost.com/archive/politics/1998/03/20/five-teens-suspected-of-hacking-into-pentagon-computers/abc8a0bc-9741-43dd-aaa9-a57ff873975a/?utm_term=.a2fa8e4469ee; Doug Struck, *'Rites of Youth': Hacking in the '90s*, WASH. POST (Mar. 21, 1998), https://www.washingtonpost.com/archive/politics/1998/03/21/rites-of-youth-hacking-in-the-90s/4d17d284-b58f-47c9-b8e3-d3b16a3ef731/?utm_term=.58768745d178.

[52] The German hackers were arrested. John Markoff, *West Germans Raid Spy Ring That Violated U.S. Computers*, N.Y. TIMES (Mar. 3, 1989), http://www.nytimes.com/1989/03/03/world/west-germans-raid-spy-ring-that-violated-us-computers.html. Although the Dutch hackers were filmed by a television news team, they were not prosecuted because the Netherlands had no laws prohibiting computer hacking at the time. *Computer Security Experts*, *supra* note 49; John Markoff, *Dutch Computer Rogues Infiltrate American Systems with Impunity*, N.Y. TIMES (Apr. 21, 1991), http://www.nytimes.com/1991/04/21/us/dutch-computer-rogues-infiltrate-american-systems-with-impunity.html. The Dutch Parliament enacted a Computer Crime Act in 1993 to prevent further hacking. Bert-Jaap Koops, *Cybercrime Legislation in the Netherlands*, 4 CYBERCRIME & SECURITY 1 (2005), http://www.cyberlawdb.com/docs/netherlands/cybercrime.pdf. One British hacker, codenamed "Datastream Cowboy," was caught, while the other, codenamed "Kuji," was not. GAO/T-AIMD-96-92, *supra* note 50, at 4. Datastream Cowboy, who was 16 years old in 1994, was fined over £1,200 for the intrusions. *Id.*

character. While these cases were concerning, they represented a mere prelude to later events as malicious cyber operations between State actors became paramount.

It soon became clear that State cyber operations no longer operated on an *ad hoc* basis. Rather, States had developed complex, deliberate, and systematic cyber exploitation agendas and actively cultivated the personnel and means to carry them out. By the late 1990s, the United States and other Western powers surmised that the Russian government ran an organized and well-resourced operation to infiltrate computer systems from defense ministries, space agencies, other government departments and universities.[53] Publicly-available information on these programs and the extent of Western awareness of them is still limited. In an incident that received extensive after-the-fact coverage, Russia is reported to have infiltrated classified U.S. government systems using thumb drives scattered near U.S. overseas military bases.[54] Buoyed by these successes, Russian cyber infiltration and manipulation campaigns have proliferated since.[55]

In 2005, the United States confirmed an extensive cyber campaign by China.[56] A decade later, Chinese hackers managed to breach the United States Office of Personnel Management and steal sensitive information on U.S. Government personnel.[57] China denied the charges, then

[53] Adam Elkus, *Moonlight Maze*, *in* A FIERCE DOMAIN: CONFLICT IN CYBERSPACE, 1986 TO 2012, 152 (Jason Healey ed., 2013).

[54] Karl Grindal, *Operation BUCKSHOT YANKEE*, *in* A FIERCE DOMAIN: CONFLICT IN CYBERSPACE, 1986 TO 2012 205–7 (Jason Healey ed., 2013). While the virus sent a beacon over the internet, it was disabled before any instructions were received. *Id.* at 205.

[55] Andy Greenberg, *Russian Hackers Have Used the Same Backdoor for Two Decades*, WIRED (Apr. 3, 2017), https://www.wired.com/2017/04/russian-hackers-used-backdoor-two-decades/. *See also* Craig Whitlock & Missy Ryan, *U.S. Suspects Russia in Hack of Pentagon Computer Network*, WASH. POST (Aug. 6, 2015), https://www.washingtonpost.com/world/national-security/us-suspects-russia-in-hack-of-pentagon-computer-network/2015/08/06/b80e1644-3c7a-11e5-9c2d-ed991d848c48_story.html?utm_term=.4792c856dd65 (describing Russian infiltration of the U.S. Joint Chiefs of Staff email system); Kim Zetter, *Russian 'Sandworm' Hack Has Been Spying on Foreign Governments For Years*, WIRED (Oct. 14, 2014), https://www.wired.com/2014/10/russian-sandworm-hack-isight/ (describing how Russians exploited vulnerabilities in the Windows operating system since 2009 to collect intelligence and diplomatic information on Ukraine); Kim Zetter, *Russian Spy Gang Hijacks Satellite Links to Steal Data*, WIRED (Sept. 9, 2015), https://www.wired.com/2015/09/turla-russian-espionage-gang-hijacks-satellite-connections-to-steal-data/ (describing how the Russian state-sponsored "Turla" gang covertly hacked satellite IP addresses between 2007 and the article's publication in 2015).

[56] Adam Segal, *From TITAN RAIN to BYZANTINE HADES: Chinese Cyber Espionage*, *in* A FIERCE DOMAIN: CONFLICT IN CYBERSPACE, 1986 TO 2012 166 (Jason Healey ed., 2013).

[57] Brendan I. Koerner, *Inside the Cyberattack That Shocked the US Government*, WIRED (Oct. 23, 2016), https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/; *OPM to Notify Employees of Cybersecurity Incident*, U.S. OFF. OF PERSONNEL

publicly accused the U.S. of cyber espionage relying on revelations from Edward Snowden, a U.S. National Security Agency contractor who disclosed top-secret information, including accounts of sensitive and threatening U.S. cyber capabilities.[58] The United States eventually indicted five Chinese military personnel for commercial espionage under domestic criminal law.[59]

Although serious, China's allegations against the U.S. were not especially scandalous given that the U.S. had already publicly admitted to engaging in cyber intelligence collection.[60] A number of specific cyber espionage events have been attributed to the U.S. and its allies. In 2012, for example, the Russian antivirus firm Kaspersky Lab discovered spyware dubbed "Flame" on computers primarily located in the Middle East and attributed it to contractors hired by the United States and Israel.[61]

Of course, cyber espionage is not limited to large, powerful nations. In fact, given the modest means required to carry out cyber espionage, cyberspace has proved something of a leveler between strong and weak States. North Korea, for example, reportedly hacked the operator of South Korean nuclear reactors and threatened to sell the information to other States.[62] Similarly, researchers from Palo Alto Networks discovered

MGMT. (June 4, 2015), https://www.opm.gov/news/releases/2015/06/opm-to-notify-employees-of-cybersecurity-incident/.

[58] James T. Areddy, *China Says U.S. also Engages in Hacking*, WALL ST. J. (May 27, 2014), https://www.wsj.com/articles/china-issues-its-own-allegations-on-u-s-cyberespionage-1401162497; Siobhan Gorman, *Defense Secretary Says U.S. Not Seeking to 'Militarize' Cyberspace*, WALL ST. J. (Mar. 28, 2014), https://www.wsj.com/articles/defense-secretary-says-u-s-not-seeking-to-militarize-cyberspace-1396036239.

[59] Press Release, U.S. Dep't of Justice, U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage (May 19, 2014), https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor. *See generally* Press Release, The White House, FACT SHEET: President Xi Jinping's State Visit to the United States (Sept. 25, 2015), https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states (noting that following the indictment, the United States and China have agreed that "neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property").

[60] Andy Greenberg, *Cyberespionage Is a Top Priority for CIA's New Directorate*, WIRED (Mar. 9, 2015), https://www.wired.com/2015/03/cias-new-directorate-makes-cyber espionage-top-priority/; Gorman, *supra* note 58.

[61] Kim Zetter, *Meet 'Flame,' The Massive Spy Malware Infiltrating Iranian Computers*, WIRED (May 28, 2012), https://www.wired.com/2012/05/flame/.

[62] Ju-min Park & Meeyoung Cho, *South Korea Blames North Korea for December Hack on Nuclear Operator*, REUTERS (Mar. 17, 2015), http://www.reuters.com/article/us-nuclear-southkorea-northkorea-idUSKBN0MD0GR20150317.

Iranian spyware on 326 computers in 35 countries thought to have been in place from 2007 until discovery in 2016.[63]

While the mere collection of intelligence information is evident in longstanding and widespread State conduct and has perhaps established itself as an exception to sovereignty-based duties prohibiting interference, a relatively new practice appears to be developing. In recent cases, information has been extracted from cyber infrastructure and then selectively released to influence or corrupt policymaking and potentially the political processes of victim States.

Disclosures of electronically-stored State secrets gained notoriety with high-profile cases involving individuals like Snowden and U.S. Army Private First Class Bradley (now Chelsea) Manning. Each independently obtained classified information from U.S. classified networks, then released it to media outlets to inform the public of questionable U.S. government behavior.[64] In 2016, 2.6 terabytes of confidential emails and files from a Panamanian law firm were released to the press.[65] These "Panama Papers" implicated world leaders and others in massive tax avoidance schemes.[66] Although the documents did not name Russian President Vladimir Putin, they demonstrated how his close associates made billions of dollars from his influence.[67] Putin responded by citing a WikiLeaks tweet connecting the funding of one of the media organizations reporting on the Panama Papers to the U.S., and declared, "WikiLeaks has showed us that official people and official organs of the US are behind this."[68] The

[63] Lucian Constantin, *Researchers Dismantle Decade-Long Iranian Cyberespionage Operation*, PCWORLD (June 29, 2016), http://www.pcworld.com/article/3089878/researchers-dismantle-decade-long-iranian-cyberespionage-operation.html.

[64] Mark Norris, *Bad "Leaker" or Good "Whistleblower"? A Test*, 64 CASE W. RES. L. REV. 693, 696–98 (2013).

[65] Andy Greenberg, *How Reporters Pulled Off the Panama Papers, the Biggest Leak in Whistleblower History*, WIRED (Apr. 4, 2016), https://www.wired.com/2016/04/reporters-pulled-off-panama-papers-biggest-leak-whistleblower-history/.

[66] Luke Harding, *What are the Panama Papers? A Guide to History's Biggest Data Leak*, THE GUARDIAN (Apr. 5, 2016), https://www.theguardian.com/news/2016/apr/03/what-you-need-to-know-about-the-panama-papers.

[67] Roman Anin, *Russia: Banking on Influence*, ORGANIZED CRIME & CORRUPTION REPORTING PROJECT (OCCRP) (June 9, 2016), https://www.occrp.org/en/panamapapers/rossiya-putins-bank/; Luke Harding, *Revealed: The $2Bn Offshore Trail that Leads to Vladimir Putin*, THE GUARDIAN (Apr. 3, 2016), https://www.theguardian.com/news/2016/apr/03/panama-papers-money-hidden-offshore.

[68] Alec Luhn & Luke Harding, *Putin Dismisses Panama Papers as an Attempt to Destabilise Russia,* THE GUARDIAN (Apr. 7, 2016), https://www.theguardian.com/news/2016/apr/07/putin-dismisses-panama-papers-as-an-attempt-to-destabilise-russia; *Panama Papers: Putin Rejects Corruption Allegations*, BRIT. BROADCASTING CORP. (Apr. 7, 2016), http://www.bbc.com/news/world-europe-35989560. While Wikileaks pointed to U.S. funding of a media outlet, Wikileaks later tweeted, "[c]laims that #PanamaPapers themselves are a 'plot' against Russia are nonsense." Neil MacFarquhar & Stephen Castle, *Panama Papers Continue to Shake Leaders, Including*

whistleblower behind the Panama Papers has not been revealed, but denied working for any government or intelligence agency, and claims the motivation was to reveal injustice.[69]

Regardless who leaked the Panama Papers, Russia selectively released information collected by its intelligence sources to the media to generate political effects in other countries. By 2016, the world learned that Russia's intelligence services had used cyber means to collect information on targets associated with both major U.S. political parties.[70] Russia then leaked victim data to media outlets and WikiLeaks to influence U.S. elections.[71] Russian hackers are accused of similar behavior in French elections.[72] Experts believe Russia was not simply releasing selective information collected through cyber means, but also altering it to create disinformation, creating confusion and undermining the credibility of foreign media.[73]

Cameron and Putin, N.Y. TIMES (Apr. 7, 2016), https://www.nytimes.com/2016/04/08/world/europe/vladimir-putin-panama-papers-american-plot.html.

[69] Caroline Mortimer, *Panama Papers: Whistleblower Breaks Silence to Explain Why They Leaked the 11.5M Files*, INDEP. (May 6, 2016), http://www.independent.co.uk/news/world/politics/panama-papers-whistleblower-breaks-silence-to-explain-why-he-leaked-the-115m-files-a7017691.html.

[70] OFFICE OF THE DIR. OF NAT. INTELLIGENCE, BACKGROUND TO "ASSESSING RUSSIAN ACTIVITIES AND INTENTIONS IN RECENT US ELECTIONS": THE ANALYTIC PROCESS AND CYBER INCIDENT ATTRIBUTION (2017), https://www.dni.gov/files/documents/ICA_2017_01.pdf.

[71] *Id.*

[72] Andy Greenberg, *The NSA Confirms It: Russia Hacked French Election 'Infrastructure,'* WIRED (May 9, 2017), https://www.wired.com/2017/05/nsa-director-confirms-russia-hacked-french-election-infrastructure/. Earlier Russian cyber election inference consisted of taking unfavorable websites off the internet, slowing down access to them, or changing them. Andy Greenberg, *Everything We Know About Russia's Election-Hacking Playbook*, WIRED (June 9, 2017), https://www.wired.com/story/russia-election-hacking-playbook/.

[73] Andy Greenberg, *Russian Hackers Are Using 'Tainted' Leaks to Sow Disinformation*, WIRED (May 25, 2017), https://www.wired.com/2017/05/russian-hackers-using-tainted-leaks-sow-disinformation/. During the Cold War, the Soviet Union made considerable use of "active measures," which a senior KGB official described as "clandestine actions designed to affect foreign governments, groups, and influential individuals in ways that favored the objectives of Soviet policy and weakened the opposition to them." TENNENT H. BAGLEY, SPYMASTER: STARTLING COLD WAR REVELATIONS OF A SOVIET KGB CHIEF 170 (2013). Active measures consisted of releasing public documents or facts embarrassing to Western governments or officials. *Id.* They also involved disinformation, where facts were distorted, concealed, invented, or forged. *Id. See also* CHRISTOPHER ANDREW & VASILI MITROKHIN, THE SWORD AND THE SHIELD: THE MITROKHIN ARCHIVE AND THE SECRET HISTORY OF THE KGB 234–46 (1999) (describing active measures against J. Edgar Hoover, the FBI, U.S. Senator Henry "Scoop" Jackson, National Security Adviser Zbigniew Brzezinski, and Ronald Reagan, as well as other similar operations); DECEPTION OPERATIONS: STUDIES IN THE EAST-WEST CONTEXT 1 (David A. Charters & Maurice A. J. Tugwell eds., 1990) (detailing the Soviet deception operation designed to falsely blame the AIDS

A survey of State practice reveals States also use cyber means to deny access to information. In 1988, a college student created one of the earliest computer viruses, the Morris Worm, to replicate itself on infected machines, slowing systems to a virtual halt until the virus could be removed.[74] More recent cyber denial techniques consist of denial of service (DOS) and distributed denial of service (DDOS) operations to generate more traffic than service providers, networks, or nodes can handle.[75] Service is restored easily when the operation ends, and effects can be averted with firewalls and sufficient bandwidth, but the political effects can be enormous and lasting. Although these events may be thought of as temporary and reversible, they can still be costly in terms of lost productivity and clean-up. For example, a researcher estimated that the Morris Worm caused between $100,000 and $10 million in losses even though no permanent hardware damage occurred.[76] More difficult to estimate are the political costs of a public's loss of confidence in government capacity to safeguard cyber infrastructure and guarantee free and functioning communications and information storage.

As in early cyber espionage cases, individual hackers were responsible for early Internet DOS events. The first notable events occurred in 1999, as pro-Serbian "patriotic hackers" denied access to U.S. whitehouse.gov sites as well as U.S. Navy and NATO websites during operation Allied Force.[77] Chinese patriotic hackers similarly responded to the bombing of the Chinese embassy and later EP-3 collision.[78] 1999 also saw patriotic hackers intervene to deny access to and deface websites dur-

epidemic on biological weapons experiments carried out by the United States). Western powers also leveraged deception and information operations, but the KGB had considerably more freedom to tell lies, allowing it to create propaganda quantitatively and qualitatively superior to the West. BAGLEY at 171; U.S. DEP'T OF STATE, CONTEMPORARY SOVIET PROPAGANDA AND DISINFORMATION: A CONFERENCE REPORT (1985) (released Mar. 1987). The West, with its more open society, was also more vulnerable to these active measures. DECEPTION OPERATIONS at 405.

[74] GORDON CORERA, INTERCEPT: THE SECRET HISTORY OF COMPUTERS AND SPIES 135–40 (2015).

[75] Large scale DDOS attacks frequently leverage botnets, which are networks of hijacked, remotely controlled computers. *See* LIIS VIHUL ET AL., COOPERATIVE CYBER DEFENCE CTR. OF EXCELLENCE, LEGAL IMPLICATIONS OF COUNTERING BOTNETS 2 (2012), https://ccdcoe.org/sites/default/files/multimedia/pdf/VihulCzosseckZiolikowskiAasmannIvanovBr%C3%BCggemann2012_LegalImplicationsOfCounteringBotnets.pdf.

[76] GAO/IMTEC-89-57, *supra* note 46, at 17.

[77] Jonathan Diamond, *Early Patriotic Hacking*, *in* A FIERCE DOMAIN: CONFLICT IN CYBERSPACE, 1986 TO 2012, 137–38 (Jason Healey ed., 2013). Hackers had been blocking DoD and NATO sites and defacing websites intermittently since 1994. *Id.* at 140.

[78] *Id.* at 138–39. KENNETH GEERS, NATO SCI. & TECH. ORG., CYBERSPACE AND THE CHANGING NATURE OF WARFARE 7, https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/RTO-MP-IST-076/$MP-IST-076-KN.pdf.

ing Israeli-Palestinian and India-Pakistan conflicts.[79] In 2007, Estonia fell victim to DDOS attacks when it began efforts to move a Soviet-era war memorial.[80] A pro-Kremlin youth group claimed responsibility for the Estonian incident as a "cyber defense" measure. The group had originally been created by the Kremlin and received occasional funding from it, but it remained nominally independent because most of its funding came from business leaders in the private sector looking to ingratiate themselves with the government.[81] Russian hacker groups are also thought to be responsible for 300 defaced websites in Lithuania following the adoption of a new law prohibiting the public display of Soviet and Nazi insignia, as well as playing their respective anthems at public gatherings in 2008.[82] In these examples, States used—or at least acquiesced to—private citizens denying Internet services in other countries often to serious political effect.

Difficulties arising from efforts to identify the sources of these incidents frustrate legal analysis and political responses. For example, Kyrgyzstan faced a country-wide DDOS attack generated from Russia in 2009, but experts are unsure whether the attack was directed by the Russian government to motivate the Kyrgyz to close a U.S. airbase quickly, or if the Kyrgyzstan government itself was trying to silence opponents to the base closure.[83] More recently, a group calling itself "Izz ad-Din al-Qassam

[79] Diamond, *supra* note 77, at 145–49. KENNETH GEERS, COOPERATIVE CYBER DEFENCE CTR. OF EXCELLENCE, 1 PANDEMONIUM: NATION STATES, NATIONAL SECURITY, AND THE INTERNET 7, 10 (2014), https://ccdcoe.org/publications/TP_Vol1No1_Geers.pdf.

[80] ENEKEN TIKK ET AL., COOPERATIVE CYBER DEFENCE CTR. OF EXCELLENCE, INTERNATIONAL CYBER INCIDENTS: LEGAL CONSIDERATIONS 16 (2010), https://ccdcoe.org/publications/books/legalconsiderations.pdf; Andreas Schmidt, *The Estonian Cyber Attacks*, *in* A FIERCE DOMAIN: CONFLICT IN CYBERSPACE, 1986 TO 2012, 174 (Jason Healey ed., 2013).

[81] Noah Shachtman, *Kremlin Kids: We Launched the Estonian Cyber War*, WIRED (Mar. 11, 2009), https://www.wired.com/2009/03/pro-kremlin-gro/; Steven Lee Myers, *Youth Groups Created by Kremlin Serve Putin's Cause*, N.Y. TIMES (July 8, 2007), http://www.nytimes.com/2007/07/08/world/europe/08moscow.html. Russia defines "net NGOs" as "internet combatants who as a rule declare the absence of any link with State bodies but which as a rule are financed by them, or by other entities." KEIR GILES, "INFORMATION TROOPS" – A RUSSIAN CYBER COMMAND?, (COOPERATIVE CYBER DEFENCE CTR. OF EXCELLENCE) 54 (Christian Czosseck, Enn Tyugu, & Tom Wingfield eds., 2011), https://ccdcoe.org/sites/default/files/multimedia/pdf/InformationTroopsARussianCyberCommand-Giles.pdf.

[82] TIKK ET AL., *supra* note 80, at 53–54.

[83] Ward Carroll, *Russia Now 3 and 0 in Cyber Warfare*, MILITARY.COM (Jan. 30, 2009), https://www.defensetech.org/2009/01/30/russia-now-3-and-0-in-cyber-warfare/#ixzz2kC8saBkH+; Nathan Hodge, *Russian 'Cyber Militia' Takes Kyrgyzstan Offline?*, WIRED (Jan. 28, 2009), https://www.wired.com/2009/01/cyber-militia-t/; Andrzej Kozlowski, *Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan*, 3 EUR. SCI. J. 237, 240–41 (2014); JOSE NAZARIO, COOPERATIVE CYBER DEFENCE CTR. OF EXCELLENCE, POLITICALLY MOTIVATED DENIAL OF SERVICE ATTACKS 8–9 (2009),

Cyber Fighters" claimed responsibility for launching DOS operations against U.S. banks in 2013.[84] United States government officials, however, believe the group to be a cover for the Iranian government.[85] Iran has denied responsibility, citing its respect for international law and legal prohibitions on targeting economic and financial institutions.[86] Similarly, when the Syrian Electronic Army claimed responsibility for DOS attacks and a spear-phishing campaign to compromise the computer systems of the U.S. government and other entities in support of the Syrian Government and President Bashar al-Assad, U.S. officials were reported to believe that they were actually Iranian.[87] The U.S. later indicted individuals residing in Syria and Germany for the Syrian Electronic Army's activities.[88] Still, absent reliable attribution, the full custom and practice of nations in cyberspace is relatively unknown in public circles.

To the degree attribution is possible, States appear to have resorted to temporary and reversible cyber measures in conjunction with use of force. In 2007, for example, Israel is thought to have used cyber technology to suppress Syrian air defense systems during an airstrike on a suspected nuclear reactor.[89] When Russia and Georgia went to war in August

https://ccdcoe.org/sites/default/files/multimedia/pdf/12_NAZARIO%20Politically%20Motivated%20DDoS.pdf.

[84] Nicole Perlroth & Quentin Hardy, *Bank Hacking Was the Work of Iranians, Officials Say*, N.Y. TIMES (Jan. 8, 2013), http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html.

[85] *Id.*

[86] *Id.* For more on the legal issues involved in the targeting of economic and "war sustaining" entities, see WILLIAM BOOTHBY, THE LAW OF TARGETING 106 (2012); Burrus M. Carnahan, *The Law of Air Bombardment in its Historical Context*, 17 A.F. L. REV. 39, 42 (1975); Janina Dill, *The 21st-Century Belligerent's Trilemma*, 26 EUR. J. INT'L L. 83, 95 (2015); Yoram Dinstein, *Legitimate Military Objectives Under the Current* Jus in Bello, 78 INT'L L. STUD. 139, 145 (2002); Ryan Goodman, Comment, *Targeting 'War-Sustaining' Objects in Non-International Armed Conflict*, 110 AM. J. INT'L L. 663 (2016); Theodore T. Richard, *Nuclear Weapons Targeting: The Evolution of Law and U.S. Policy*, 224 MIL. L. REV. 862, 954–61 (2016).

[87] David E. Sanger, *Syria War Stirs New U.S. Debate on Cyberattacks*, N.Y. TIMES (Feb. 24, 2014), https://www.nytimes.com/2014/02/25/world/middleeast/obama-worried-about-effects-of-waging-cyberwar-in-syria.html.

[88] Press Release, U.S. Dep't of Justice, Computer Hacking Conspiracy Charges Unsealed Against Members of Syrian Electronic Army (Mar. 22, 2016), https://www.justice.gov/opa/pr/computer-hacking-conspiracy-charges-unsealed-against-members-syrian-electronic-army. The hacker residing in Germany was a Syrian National who was later extradited to the U.S. and pleaded guilty to felony charges of conspiring to receive extortion proceeds and conspiring to unlawfully access computers. Press Release, U.S. Dep't of Justice, Syrian Man Affiliated with Syrian Electronic Army Pleads Guilty (Sept. 28, 2016), https://www.justice.gov/usao-edva/pr/syrian-man-affiliated-syrian-electronic-army-pleads-guilty.

[89] Lewis Page, *Israeli Sky-Hack Switched Off Syrian Radars Countrywide*, THE REGISTER (Nov. 22, 2007), https://www.theregister.co.uk/2007/11/22/israel_air_raid_syria_hack_network_vuln_intrusion/; Sharon Weinberger, *How Israel Spoofed Syria's*

2008, Russia not only defaced Georgian websites, but also blocked Georgia's ability to communicate through the Internet and shut down its banking sector.[90] The Russian hackers were not State government employees, but the Kremlin was thought to have actively coordinated them.[91] Sporadic DDOS attacks and website defacements have been attributed to patriotic hackers from Russia and the Ukraine after Ukrainian protestors drove out a pro-Russia president, Russia's occupation of the Crimean Peninsula, and the beginning of armed conflict in eastern Ukraine.[92] The Russo-Ukrainian conflict also saw deployment of advanced cyber espionage tools, selective leaking of stolen confidential information, cutting of internet cables, attempted interference in the Ukrainian election result reporting, and Russian employment of hundreds of "trolls"—operatives posting pro-Russian propaganda on social media to influence domestic and international audiences.[93]

The gravity of cyber operations in the Russo-Ukrainian conflict was significantly elevated on December 23, 2015, when hackers denied electrical power to a significant segment of Ukraine.[94] As part of this effort, hackers rewrote code on servers to render the devices permanently useless.[95] During the conflict, hackers also permanently erased terabytes of data from the Ukrainian finance ministry.[96] In 2017, the NotPetya cyber attack became the most costly in history as malware, which permanently encrypted computer systems, spilled over from financial and energy sector targets in Ukraine to computers in 60 countries.[97] These represent the

Air Defense System, WIRED (Oct. 4, 2007), https://www.wired.com/2007/10/how-israel-spoo/; Ward Carroll, *Israel's Cyber Shot at Syria*, MILITARY.COM (Nov. 26, 2007), https://www.military.com/defensetech/2007/11/26/israels-cyber-shot-at-syria.

[90] Andreas Hagen, *The Russo-Georgian War 2008*, *in* A FIERCE DOMAIN: CONFLICT IN CYBERSPACE, 1986 TO 2012, 196–98 (Jason Healey ed. 2013); TIKK ET AL., *supra* note 80, at 69–71.

[91] TIKK ET AL., *supra* note 80, at 75; Jason Healey, *How to Beat a Russian Cyber Assault on Ukraine*, NEW ATLANTICIST (Mar. 3, 2014), http://www.atlanticcouncil.org/blogs/new-atlanticist/how-to-beat-a-russian-cyber-assault-on-ukraine. Russian writers perceived that their cyber, or information, campaign in the conflict performed poorly and was in need of improvement. Giles, *supra* note 13, at 46.

[92] NATO COOPERATIVE CYBER DEFENCE CTR. OF EXCELLENCE, CYBER WAR IN PERSPECTIVE: RUSSIAN AGGRESSION AGAINST UKRAINE 8 (Kenneth Geers ed., 2015).

[93] *Id.* at 11.

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

[95] *Id.* More recently, the malware used to destroy Ukrainian electrical power generating systems was found on similar infrastructure in the U.S. *Id.*

[96] *Id.*

[97] NATO Cooperative Cyber Defence Ctr. of Excellence, *NotPetya and WannaCry Call for a Joint Response from International Community* (June 20, 2017) https://ccdcoe.org/notpetya-and-wannacry-call-joint-response-international-community.html. Andy Greenberg, *Petya Ransomware Epidemic May Be Spillover From Cyberwar*, WIRED

final broad category of unfriendly multinational cyber relations: destructive cyber operations.

State cyber operations have now matured beyond mere espionage and temporary disruptions of service. State actions intended to destroy systems and wipe data from cyber infrastructure located on other States' territory have been uncovered in the last decade. Destructive cyber operations often involve "application-level attacks" where an attacker takes over a compromised machine from a remote location.[98] Apart from the Russo-Ukrainian conflict, these destructive attacks have not been associated with a conventional armed conflict. In 2010, researchers discovered a highly complex worm, later code named Stuxnet. Allegedly an American and Israeli creation, Stuxnet caused permanent physical damage to Iranian uranium enrichment gas centrifuges.[99] The worm ultimately rendered nearly a thousand Iranian centrifuges useless. Later, in spring of 2012, Iran's oil production was targeted by the "Wiper" virus. Wiper systematically scrubbed hard drives clean, deleting the malware's code along with it.[100] Subsequently, Iran has been suspected of destructive

(June 28, 2017) https://www.wired.com/story/petya-ransomware-ukraine/. The United States, United Kingdom, and Denmark recently attributed the attack to the Russian military. The White House, Statement from the Press Secretary, (Feb. 15, 2018) https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/; Andy Greenberg, *The White House Blames Russia for NotPetya, the 'Most Costly Cyberattack In History'*, WIRED (Feb. 15, 2018) https://www.wired.com/story/white-house-russia-notpetya-attribution/.

[98] KARLIS PODINS & PABLO ANDREU BARASOAIN, NATO COOPERATIVE CYBER DEFENCE CTR. OF EXCELLENCE, APPLICATION LEVEL ATTACKS STUDY, 4, 19 (2012), https://ccdcoe.org/sites/default/files/multimedia/pdf/PodinsBarasoain2012_ApplicationLevelAttacksStudy.pdf.

[99] Ellen Nakashima & Joby Warrick, *Stuxnet Was Work of U.S. and Israeli Experts, Officials Say*, WASH. POST (June 2, 2012), https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html?utm_term=.6a619d322841. Stuxnet was two distinct computer worms. Ralph Langner, *Stuxnet's Secret Twin*, FOREIGN POL'Y (Nov. 19, 2013), http://foreignpolicy.com/2013/11/19/stuxnets-secret-twin/. It was also part of a larger effort against Iran's nuclear weapon program. Chris Morton, *Stuxnet, Flame, and Duqu – the Olympic Games*, *in* A FIERCE DOMAIN: CONFLICT IN CYBERSPACE, 1986 TO 2012 212 (Jason Healey ed. 2013).

[100] Thomas Erdbrink, *Facing Cyberattack, Iranian Officials Disconnect Some Oil Terminals From Internet*, N.Y. TIMES (Apr. 23, 2012), http://www.nytimes.com/2012/04/24/world/middleeast/iranian-oil-sites-go-offline-amid-cyberattack.html; Kim Zetter, *Wiper Malware That Hit Iran Left Possible Clues of its Origins*, WIRED (Aug. 29, 2012), https://www.wired.com/2012/08/wiper-possible-origins/.

cyber operations against Aramco, a Saudi state oil company,[101] RasGas, a Qatari natural gas firm,[102] and the U.S.-based Sands Casino.[103]

As with cyber espionage, cyber sabotage and attacks are not the exclusive province of strong States. North Korea is thought to have launched several destructive cyber assaults. It is considered responsible for destructive attacks on South Korean banks and television broadcasters in 2013.[104] A year later, North Korea reportedly used cyber means to damage Sony computers and destroy data located within the United States after the company refused to pull *The Interview*, a film that ridiculed the North Korean leader.[105] In 2017, North Korea allegedly deployed the WannaCry computer worm affecting as many as 300,000 people, businesses, and organizations in 150 countries, encrypting their computers and demanding ransom payments to unlock them.[106] North Korea may not reflect prevailing ideals of international relations or legal

[101] Nicole Perlroth, *In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back*, N.Y. TIMES (Oct. 23, 2012), http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html.

[102] Doha News Team, *US Officials: Cyberattacks on Aramco, RasGas May Have Come From Iran*, DOHA NEWS (Oct. 14, 2012), https://dohanews.co/us-officials-cyberattacks-on-aramco-rasgas-may-have/; Kim Zetter, *Qatari Gas Company Hit with Virus in Wave of Attacks on Energy Companies*, WIRED (Aug. 30, 2012), https://www.wired.com/2012/08/hack-attack-strikes-rasgas/.

[103] Jose Pagliery, *Iran Hacked an American Casino, U.S. Says*, CNN (Feb. 27, 2015), http://money.cnn.com/2015/02/27/technology/security/iran-hack-casino/index.html; BARBARA SLAVIN & JASON HEALEY, BRENT SCOWCROFT CTR. ON INT'L SECURITY S. ASIA CTR, IRAN: HOW A THIRD TIER CYBER POWER CAN STILL THREATEN THE UNITED STATES, ATLANTIC COUNSEL, 2 (2013), http://www.atlanticcouncil.org/images/publications/iran_third_tier_cyber_power.pdf.

[104] Symantec Security Response, *Four Years of DarkSeoul Cyberattacks Against South Korea Continue on Anniversary of Korean War*, SYMANTEC OFFICIAL BLOG (June 26, 2013), https://www.symantec.com/connect/blogs/four-years-darkseoul-cyberattacks-against-south-korea-continue-anniversary-korean-war.

[105] Peter Elkind, *Sony Pictures: Inside the Hack of the Century, Part I*, FORTUNE.COM (June 25, 2015), http://fortune.com/sony-hack-part-1/; Jim Finkle, *Exclusive: FBI Warns of 'Destructive' Malware in Wake of Sony Attack*, REUTERS (Dec. 1, 2014), http://www.reuters.com/article/us-sony-cybersecurity-malware-idUSKCN0JF3FE20141202; Kim Zetter, *Sony Got Hacked Hard: What We Know and Don't Know So Far*, WIRED (Dec 3, 2014), https://www.wired.com/2014/12/sony-hack-what-we-know/.

[106] Ellen Nakashima, *The NSA Has Linked the WannaCry Computer Worm to North Korea*, WASH. POST (June 14, 2017), https://www.washingtonpost.com/world/national-security/the-nsa-has-linked-the-wannacry-computer-worm-to-north-korea/2017/06/14/101395a2-508e-11e7-be25-3a519335381c_story.html?tid=ss_tw&utm_term=.26286673bc39. According to the computer security firm Kasperski Lab, Russia suffered the most attacks from the WannaCry attack, followed by computers in Ukraine, India, and Taiwan. Andrew E. Kramer, *Russia, This Time the Victim of a Cyberattack, Voices Outrage*, N.Y. TIMES (May 14, 2017), https://www.nytimes.com/2017/05/14/world/europe/russia-cyberattack-wannacry-ransomware.html; Alex Perekalin, *WannaCry: Are You Safe?*, KASPERSKY LAB DAILY (May 13, 2017), https://www.kaspersky.com/blog/wannacry-ransomware/16518/.

behavior. State responses to its behavior, however, may be indicative of the present and future international legal climate.

States have made nascent efforts to rein in these cyber operations. The United States and China concluded a framework agreement to refrain from "cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors."[107] A 2015 Communiqué issued by world leaders attending the 20 Antalya Summit similarly proclaimed, "no country should conduct or support ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors" and "all states should abide by norms of responsible state behavior" in using information and communication technologies.[108] Despite the apparent détente relating to commercial espionage, malicious and exploitive cyber operations are a prominent and persistent feature of twenty-first-century international relations.

Based on State practice over several decades, examples of malicious cyber activities appear to fall into three broad categories: (1) espionage and information release, (2) connectivity disruption and information denial, and (3) data and hardware destruction. Apart from interception of or interference with wireless transmissions, malicious cyber activities generally take place on routers, servers, computers, and associated equipment located on territory within the jurisdiction of a State. Spyware, malware, or other programming tools must be inserted on this equipment and either disable it or change its intended function. These practices increasingly challenge traditional understandings of the limits on State activity attendant to territorial sovereignty during times of peace. An examination of the history, development, and current state of territorial sovereignty illuminates both the legal context for emerging cyber operations and suggests that States are rapidly approaching a critical crossroads in the relationship between cyberspace and international law.

III. THE INTERNATIONAL LAW OF TERRITORIAL SOVEREIGNTY

It is widely acknowledged that State cyber operations have potential to amount to grave violations of international law. Popular attention to cyber conflict has long focused on catastrophic events—so-called cyber Pearl Harbors—sudden, broad-scale, and debilitating attacks on critical

[107] Press Release, The White House, FACT SHEET: President Xi Jinping's State Visit to the United States (Sept. 25, 2015), https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

[108] G20 LEADERS' COMMUNIQUÉ, *supra* note 19, at 6.

infrastructure perhaps resulting in human casualties.[109] However, as the preceding accounts perhaps indicate, the far more prevalent form of State-sponsored cyber exploitation involves consequences below the thresholds of use of force or even the coercive element required by the principle of non-intervention.[110] Despite their comparatively slight impact, these operations do not take place in a legal vacuum. Low-intensity cyber operations implicate important and long-standing international-law norms. And despite predating cyberspace by, in some cases, centuries, extant norms of public international law bear directly on State conduct. One such example is the principle and associated rule respecting territorial sovereignty.

No treaty comprehensively defines territorial sovereignty or expresses it as a stand-alone international legal concept. It is chiefly a creature of customary international law derived from the general and consistent practices of States, carried out from a sense of legal duty or obligation.[111] All the same, territorial sovereignty has deep roots in international law and violations of those rules have long been regarded as breaches of legal obligations. Although often expressed as a vague principle, guideline, or framework, the legal history of sovereignty clearly establishes territorial sovereignty as a legally binding rule of conduct between States.

Attempting to express the customary law of territorial sovereignty, the American Law Institute's *Third Restatement of Foreign Relations Law* observes that sovereignty "implies a state's lawful control over its territory generally to the exclusion of other states, authority to govern in that territory, and authority to apply law there."[112] The comment's resort to the qualifying terms "implies" and "generally" indicates some of the equivocation that surrounds expressions of territorial sovereignty. The *Restatement* echoes somewhat stronger phrasing in a 1928 international arbitration decision by Max Huber:

---

[109] *See, e.g.*, SEGAL, *supra* note 25, at 6 (recounting warnings by then-Secretary of Defense Leon Panetta concerning the threat of sudden, debilitating cyber operations against critical U.S. infrastructure).

[110] *See* Terry D. Gill, *Non-Intervention in the Cyber Context*, *in* PEACETIME REGIME FOR STATE ACTIVITIES IN CYBERSPACE: INTERNATIONAL LAW, INTERNATIONAL RELATIONS AND DIPLOMACY 218 (Katharina Ziolkowski ed., 2013); Catherine Lotrionte, *Countering State-Sponsored Cyber Economic Espionage Under International Law*, 40 N.C. J. INT'L L. & COM. REG. 443, 492–509 (2015); Sean Watts, *Low-Intensity Cyber Operations and the Principle of Non-Intervention*, *in* CYBERWAR: LAW AND ETHICS FOR VIRTUAL CONFLICTS 250 (Jens David Ohlin et al. eds., 2015).

[111] *See* Statute of the International Court of Justice, art. 38(1)(b), June 26, 1945, 59 Stat. 1055, 33 U.N.T.S. 993; North Sea Continental Shelf Cases, 1969 I.C.J. Rep. 3, 22, ¶ 19; RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 102 (1987).

[112] RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 206 cmt. b (1987).

> Sovereignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State. The development of the national organisation of States during the last few centuries and, as a corollary, the development of international law, have established this principle of the exclusive competence of the State in regard to its own territory in such a way as to make it the point of departure in settling most questions that concern international relations.[113]

The international relations scholar Stephen Krasner echoes the emphasis on exclusivity. He defines "Westphalian sovereignty" as a "political organization based on the exclusion of external actors from authority structures within a given territory."[114] Krasner explains, "Westphalian sovereignty is violated when external actors influence or determine domestic authority structures."[115] Krasner and others have questioned the historical accuracy of associating this norm of State behavior with the 1648 Peace of Westphalia.[116] He concedes Westphalian or, more precisely, territorial sovereignty has origins in the sixteenth and seventeenth centuries, but emphasizes that the concept has evolved considerably, both in practice and in law. A brief look at this historical development illustrates not only its origins, but also how sovereignty matured into a primary rule of international law.[117]

The series of treaties that formed the Peace of Westphalia, which ended the Thirty Years War, is regarded as the starting point for the

[113] Island of Palmas (U.S. v. Neth.), 2 R.I.A.A. 829, 838 (Perm. Ct. Arb. 1928).

[114] STEPHEN D. KRASNER, SOVEREIGNTY: ORGANIZED HYPOCRISY 3–4 (1999). Krasner identifies three other uses of the term sovereignty: international legal sovereignty, which deals with recognition between states; domestic sovereignty, which deals with the formal organization of political authority within a state; and interdependence sovereignty, which deals with "the ability of public authorities to regulate the flow of information, ideas, goods, people, pollutants, or capital across the borders of their state." *Id.*

[115] *Id.* at 20.

[116] *Id.*; Michael Axworthy & Patrick Milton, *The Myth of Westphalia*, FOREIGN AFF. (Dec. 22, 2016), https://www.foreignaffairs.com/articles/europe/2016-12-22/myth-westphalia; Andreas Osiander, *Sovereignty, International Relations, and the Westphalian Myth*, 55 INT'L ORG. 251, 261 (2001).

[117] Primary rules of international law establish obligations for a State, while secondary rules are "the general conditions under international law for the State to be considered responsible for wrongful actions or omissions, and the legal consequences which flow therefrom." INT'L L. COMM'N, DRAFT ARTICLES ON RESPONSIBILITY OF STATES FOR INTERNATIONALLY WRONGFUL ACTS, WITH COMMENTARIES 31 (2001), http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf.

modern system of international relations and law.[118] The Peace of Westphalia created a system of legally equal States, reliant principally on a balance of political, diplomatic, and military power to maintain stability but also based on observance of international legal norms.[119] The Peace of Westphalia was not entirely novel. It built on foundations of sovereignty introduced by the 1555 Peace of Augsburg, which recognized distinct States wherein sovereign rulers determined State religion—*cuius region eius religio*.[120] Ultimately, the religious settlement of the Peace of Augsburg, and the notion that political unity relied on religious unity, collapsed under political and sectarian dissent.[121] The Westphalian solution, addressing in large part the States within the Holy Roman Empire, clarified contentious religious rights and adjusted territorial arrangements with a view toward a more durable peace. For legal purposes and for purposes of understanding its contribution to the modern system of States, Westphalia formalized the rights of the States, declaring:

> [T]o prevent for the future any Differences arising in the Politick State, all and every one of the Electors, Princes and States of the Roman Empire, are so establish'd and confirm'd in their antient Rights, Prerogatives, Libertys, Privileges, free exercise of Territorial Right, as well Ecclesiastick, as Politick Lordships, Regales, by virtue of this present Transaction: that they never can or ought to be molested therein by any whomsoever upon any manner of pretence.[122]

---

[118] HENRY WHEATON, HISTORY OF THE LAW OF NATIONS IN EUROPE AND AMERICA; FROM THE EARLIEST TIMES TO THE TREATY OF WASHINGTON, 1842 69 (1845); Gross, *supra* note 39, at 21; HENRY KISSINGER, WORLD ORDER 2–3 (2014).

[119] Gross, *supra* note 39, at 29. The "equal states" were those within the territory of the Holy Roman Empire which were equally granted legal rights within the Empire, including, "political autonomy . . . , [the] right of participating in decisions on major Imperial policy areas, concluding alliances with other Imperial Estates and foreign powers, maintaining armies, waging war, and making peace." Michael Axworthy et al., *Series Report: Report on Phase One of the Seminar Series and Project "A Westphalia for the Middle East,"* UNIVERSITY OF CAMBRIDGE, DEPARTMENT OF POLITICS AND INTERNATIONAL STUDIES FORUM ON GEOPOLITICS (Oct. 13, 2016), https://www.coggs.polis.cam.ac.uk/news/westphalia-report. The Swiss Confederation and the United Provinces of the Netherlands were recognized as independent States within Europe. PHILLIP BOBBITT, THE SHIELD OF ACHILLES: WAR, PEACE, AND THE COURSE OF HISTORY 507 (2002).

[120] BOBBIT, *supra* note 119, at 487.

[121] *See* Gordon A. Christenson, "*Liberty of the Exercise of Religion*" *in the Peace of Westphalia*, 21 TRANSNAT'L L. & CONTEMP. PROBS. 721, 736 (2013).

[122] *Treaty of Westphalia: Peace Treaty Between the Holy Roman Emperor and the King of France and Their Respective Allies*, YALE LAW SCH. AVALON PROJECT art. LXIV, http://avalon.law.yale.edu/17th_century/westphal.asp. The Emperor retained the authority to intervene within the German states, who were not fully sovereign in the modern sense, but the Emperor could not act arbitrarily because France and Sweden guaranteed the rights of Catholics and Protestants, respectively. BRENDAN SIMMS, EUROPE: THE STRUGGLE FOR SUPREMACY FROM 1453 TO THE PRESENT 43 (2013).

and,

> the free Towns, and other States of the Empire, shall have decisive Votes; they shall, without molestation, keep their Regales, Customs, annual Revenues, Libertys, Privileges to confiscate, to raise Taxes, and other Rights, lawfully obtain'd from the Emperor and Empire, or enjoy'd long before these Commotions, with a full Jurisdiction within the inclosure of their Walls, and their Territorys . . . .[123]

Territorial sovereignty within the Empire recognized States with equal rights for individual and collective security, so long as "[a]lliances be not against the Emperor, and the Empire, nor against the Publick Peace."[124] The Peace of Westphalia also established common restrictions on these States. Under its terms, they were forbidden to interfere with or "molest[]" one another, nor could they legally jeopardize the general peace without cause.[125]

The rudimentary legal foundation laid by the Peace of Westphalia soon matured into a far more intricate system of relationships and rules between States, including firm notions of territorial sovereignty. No jurist's description of this burgeoning legal system was more influential than that of the seventeenth-century Dutch legal scholar, Hugo Grotius.[126] His account of international law, based on an underlying "natural law," drew on a comprehensive study of the customs and practices of nations, supported and explained by opinions of philosophers and other experts.[127] Grotius envisioned a juridical order of State entities possessing fundamental rights and freedoms, but lacking a higher or centralized authority.[128] Grotius described the sovereign State as one "whose Acts are not subject to another's Power, so they cannot be made void by any other human Will."[129] At the same time, he noted that every State had the duty to serve interests of the wider community of States as a whole in accordance with rules they could agree upon: the "Law of Nations."[130]

The first article of the Treaty of Westphalia reflected this duty when it observed, "each Party shall endeavour to procure the Benefit, Honour and Advantage of the other; that thus on all sides they may see this Peace

---

[123] *Treaty of Westphalia*, *supra* note 122, at art. LXVII.

[124] *Id.* at art. LXV.

[125] *Id.* at art. LXVII.

[126] Ove Bring, *The Westphalian Peace Tradition in International Law: From* Jus ad Bellum *to* Jus contra Bellum, 75 INT'L L. STUD. 57, 58 (2000). King Gustavus Adolphus of Sweden, one of the major combatants in the Thirty Years War, is reported to have carried a volume of Grotius everywhere. CICELY V. WEDGWOOD, THE THIRTY YEARS WAR 261 (1938).

[127] BOBBIT, *supra* note 119, at 513–14; Bring, *supra* note 126, at 58–59.

[128] BOBBIT, *supra* note 119, at 508; Bring, *supra* note 126, at 58–59.

[129] HUGO GROTIUS, THE RIGHTS OF WAR AND PEACE, BOOK I 259 (Richard Tuck ed., 2005).

[130] *Id.* at 94; BOBBIT, *supra* note 119, at 517.

and Friendship in the Roman Empire, and the Kingdom of France flourish, by entertaining a good and faithful Neighbourhood."[131] In support of their duty to the collective body of States, Grotius deduced States should refrain from interfering with the territorial dominion of other States. Although the Peace of Westphalia hardly prevented such interferences, or even war (in fact, the Grotian system licensed warfare to enforce State rights), the international, legal, and political concepts it created endured.[132]

Admittedly, the Westphalian model and the supporting Grotian legal framework did not secure universal support. Notably, Arman Jean du Plessis, Cardinal de Richelieu, the First Minister of France from 1624 to 1642, promulgated the concept of *raison d'état*: that the well-being of a State justified whatever means were employed to further it; national security interests supplanted morality.[133] Another contemporary of Grotius, the political philosopher Thomas Hobbes, denied that States owed any international duties to one another. Hobbes insisted States had only a duty to obey the "law of nature" and to tend to the safety and best interests of their own people.[134] Hobbes's descriptive characterization of international relations has been associated with present-day international relations "realism."[135] In legal terms, a purely Hobbesian world views skeptically any legal duty to refrain from interfering with another State inside its territorial jurisdiction.[136] To the extent any such norm existed, it would yield entirely to the perceived needs of the sovereign.

The German legal scholar Samuel Pufendorf bridged some of the differences between Hobbesian, self-interested realism and the coopera-

[131] *Treaty of Westphalia*, *supra* note 122, at art. I.

[132] Bring, *supra* note 126, at 65.

[133] HENRY KISSINGER, DIPLOMACY 58–59 (1994). When Grotius faced financial hardships, Richelieu presented him with tempting employment opportunities if Grotius would agree to completely serve French interests. HAMILTON VREELAND, JR., HUGO GROTIUS: THE FATHER OF THE MODERN SCIENCE OF INTERNATIONAL LAW 178–79 (1917). Grotius declined, explaining, "I must adhere to my former way of thinking." *Id.* at 179. Richelieu is considered the father of the modern state system while Grotius is considered the father of international law.

[134] THOMAS HOBBES, THE ESSENTIAL LEVIATHAN 188–89 (Nancy A. Stanlick ed., 2016).

[135] EDWARD HALLETT CARR, THE TWENTY YEARS' CRISIS 1919–1939: AN INTRODUCTION TO THE STUDY OF INTERNATIONAL RELATIONS 153 (1949); W. Julian Korab-Karpowicz, *Political Realism in International Relations*, STANFORD ENCYCLOPEDIA OF PHILOSOPHY (July 26, 2010), https://plato.stanford.edu/entries/realism-intl-relations/.

[136] Hans J. Morgenthau, *To Intervene or Not to Intervene*, 45 FOREIGN AFF. 425, 425–26 (1967); Hans J. Morgenthau, *Positivism, Functionalism, and International Law*, 34 AM. J. INT'L L. 260, 264–65 (1940); KENNETH H. WALTZ, THEORY OF INTERNATIONAL POLITICS 103 (1979); Stephen D. Krasner, *Realist Views of International Law*, 96 AM. SOC'Y INT'L L. PROC. 265, 268 (2002); Kenneth N. Waltz, *Structural Realism after the Cold War*, 25 INT'L SECURITY 5, 13, 27 (2000).

tive, Grotian society of nations.[137] Like Hobbes, Pufendorf found no difference between the law of nations and law of nature. However, he viewed Hobbes's characterization of the law of nature as unreasonably harsh. Pufendorf expressed a duty to institute a broader political society for collective security.[138] As for the concept of sovereignty, Pufendorf detected frequent misuse of the term. In Pufendorf's view, sovereignty should properly apply almost exclusively to people. Sovereignty, to the extent it applied to territory at all, merely signified a requirement of consent to persons residing within the sovereign's dominion. He explained, "and they who come to sojourn there only for a time, are, during that Space, obliged to acknowledge his Jurisdiction."[139] To Pufendorf's mind, no entity had power to interfere with a sovereign's rights to a place under his dominion.[140] He may not have embraced the term "territorial sovereignty," but Pufendorf clearly articulated the State's authority to control and set rules for its territory and its broader duty not to molest another State's rights within its dominion.

Grotius and Pufendorf remained highly influential in these nascent and formative stages of international law. However, the most important contributor to early understandings of territorial sovereignty may have been the eighteenth-century Swiss Diplomat Emer de Vattel.[141] A widely read and acknowledged authority on international law, Vattel offered a cosmopolitan vision of international law.[142] Where some of his Swiss contemporaries favored independent, Hobbesian approaches to international relations and law, Vattel described a collective, even collaborative community of States. Although he explained, "[e]very nation that governs itself . . . without dependence on any foreign power, is a *sovereign state*,"[143] he emphasized each State is obligated to cultivate peace with other States and avoid disturbing that peace.[144] Vattel further detailed rights and obligations of States relating to the national domain, which he defined as the State's territories and rights.[145] He explained:

---

[137] David Boucher, *Resurrecting Pufendorf and Capturing the Westphalian Moment*, 27 REV. OF INT'L STUD. 557, 565 (2001).

[138] SAMUEL PUFENDORF, OF THE LAW OF NATURE AND NATIONS 632 (Basil Kennett trans., 4th ed. 1729); Boucher, *supra* note 137, at 565–66.

[139] PUFENDORF, *supra* note 138, at 396.

[140] *Id.*

[141] Jesse S. Reeves, *The Influence of the Law of Nature Upon International Law in the United States*, 3 AM. J. INT'L L. 547, 549 (1909).

[142] *Id.*; Charles G. Fenwick, *The Authority of Vattel*, 7 AM. POL. SCI. REV. 395, 395 (1913); Brian Richardson, *The Use of Vattel in the American Law of Nations*, 106 AM. J. INT'L L., 547, 570 (2012).

[143] EMER DE VATTEL, THE LAW OF NATIONS 83 (Béla Kapossy & Richard Whatmore eds., 2008) (emphasis in original).

[144] *Id.* at 652–53.

[145] *Id.* at 302.

> The sovereignty united to the domain establishes the jurisdiction of the nation in her territories, or the country that belongs to her. It is her province, or that of her sovereign, to exercise justice in all the places under her jurisdiction, to take cognisance of the crimes committed, and the differences that arise in the country.
>
> Other nations ought to respect this right.[146]

Vattel expanded on the importance of territorial sovereignty and described the resemblance of a primary rule prohibiting violations of sovereignty:

> We should not only refrain from usurping the territory of others; we should also respect it, and abstain from every act contrary to the rights of the sovereign: for a foreign nation can claim no right in it. We cannot then, without doing an injury to a state, enter its territories with force and arms in pursuit of a criminal, and take him from thence. This would at once be a violation of the safety of the state, and a trespass on the rights of empire or supreme authority vested in the sovereign. This is what is called *a violation of territory*; and among nations there is nothing more generally acknowledged as an injury that ought to be vigorously repelled by every state that would not suffer itself to be oppressed. We shall make use of this principle in speaking of war, which gives occasion for many questions on the rights of territory.
>
> The sovereign may forbid the entrance of his territory either to foreigners in general, or in particular cases, or to certain persons, or for certain particular purposes, according as he may think it advantageous to the state. There is nothing in all this, that does not flow from the rights of domain and sovereignty: every one is obliged to pay respect to the prohibition; and whoever dares to violate it, incurs the penalty decreed to render it effectual.[147]

Thus, the writings of Grotius, Pufendorf, and Vattel established an early framework regulating how nations ought to interact with one another. Based on studies of history and religion, they documented rules for interactions between sovereign States, each the supreme authorities over their own territories and within their respective jurisdictions. These rules amounted to the foundation of international law in Europe and North America. They also identified early legal doctrine for rules of conduct, including insistence on nearly absolute respect for States' exclusive and independent control of territory. This doctrine would be tested by evolving customs and the future practices of nations. But legal support

[146] *Id.* at 303–04. Supreme Court Justice and author Joseph Story characterized this passage from Vattel as laying "down the true doctrine, in clear terms." JOSEPH STORY, COMMENTARIES ON THE CONFLICT OF LAWS 787 (2d ed. 1841).

[147] VATTEL, *supra* note 143, at 308–09 (emphasis added) (internal citation omitted).

for territorial sovereignty rules persisted through the eighteenth and into the nineteenth century, although observance and the force of the law were often significantly diminished in the political and military interests of maintaining a balance of power.

Indeed, efforts to settle territorial, political, and military scores presented a significant challenge to territorial sovereignty. At the conclusion of the Napoleonic Wars, European powers sent diplomatic representatives to Vienna to redraw political borders and to revise rules for future relations.[148] In a secret clause added to the First Treaty of Paris, the great power victors of the wars, Austria, Great Britain, Prussia, and Russia, granted themselves a status superior to other European powers thinking they might maintain peace through selective interventions in the name of balance.[149] They agreed to meet periodically and to reach agreements on emerging crises.[150] Within three years, France joined the great powers in this balancing function.[151] Not only did the great powers agree to maintain an equilibrium of resources and people, they also agreed to act in the common interests of Europe as a whole.[152] The resulting Vienna system, known as the Concert of Vienna or Concert of Europe, appeared to reflect two important concepts for the future of international relations. First, the Concert was an early resort to positivism as a means to better express and secure compliance with behavioral norms. Second, it reflected further investment in the notion of territorial sovereignty as a means to ensure peaceful relations between States.[153]

State practice from the early years of the Concert of Europe illustrates how positivism and territorial sovereignty operated in tandem. When Austria, Russia, and Prussia adopted measures to give the great powers a "perpetual pretext" for interfering in the concerns of different

[148] KYLE LASCURETTES, RAND CORP. PERSPECTIVE, THE CONCERT OF EUROPE AND GREAT-POWER GOVERNANCE TODAY 4 (2017), http://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE226/RAND_PE226.pdf.

[149] *Id.* at 5–6. To the foreign ministers of Austria, Great Britain, and France, the balance of power meant maintaining an equilibrium of forces between the great powers to discourage unilateral aggression by any of them. GORDON A. CRAIG, EUROPE SINCE 1815 18 (2d ed. 1966). In 1961, the U.S. Department of Justice argued that this balance of power system lacked long-term, "enduring relationships" between States, which "had to be free to change their alignment any time the balance was threatened, and free to use force whenever the system required it. Checks on the use of force were, therefore, political ones rather than legal ones, and war was not formally outlawed." Nicholas deB. Katzenbach, *Intervention by States and Private Groups in the Internal Affairs of Another State*, Apr. 12, 1961, *in* 1 SUPPLEMENTAL OPINIONS OF THE OFFICE OF LEGAL COUNSEL OF THE UNITED STATES DEPARTMENT OF JUSTICE 226 (Nathan A. Forrester ed., 2013).

[150] LASCURETTES, *supra* note 148, at 6; KISSINGER, *supra* note 118, at 3.

[151] KISSINGER, *supra* note 118, at 60.

[152] BOBBITT, *supra* note 119, at 551–53 (2002).

[153] *Id.* at 565.

States based on the Neapolitan revolution of 1820, the British government balked. Britain dissented "not only upon the ground of their being, if reciprocally acted on, contrary to the fundamental laws of Great Britain, but such as could not safely be admitted as part of a system of international law."[154] The British foreign minister wrote that international law would only allow intervention to be justified "by the strongest necessity" and would not admit a general exception to deal with revolutionary movements.[155] In 1822, Britain threatened hostilities with France over its potential interference in the Spanish revolution because there was no "direct and imminent danger to the safety and interests of other states, which might justify a forcible interference."[156] Both Great Britain and the United States warned Spain and its allies against interventions in the revolutionary contests taking place in South and Central America.[157] In the United States, insistence on non-interference by European powers took political form in the 1823 Monroe Doctrine.[158] Great Britain's position, upholding international law norms against interference in the absence of justification, opened a rift among European great-power States.[159] Austria, Russia, and Prussia continued to justify anti-revolutionary interferences

[154] WHEATON, *supra* note 118, at 518.

[155] *Id.*

[156] *Id.* at 519.

[157] *Id.* at 520.

[158] Arnulf Becker Lorca, *Universal International Law: Nineteenth-Century Histories of Imposition and Appropriation*, 51 HARV. INT'L L.J. 475, 515 (2010). With the Monroe Doctrine, the United States asserted the right to take all necessary action to prevent any non-American power from obtaining control over territory in the Western Hemisphere. Norbert A. Schlei, *Authority Under International Law to Take Action if the Soviet Union Establishes Missile Bases in Cuba*, Aug. 30, 1962, *in* 1 SUPPLEMENTAL OPINIONS OF THE OFFICE OF LEGAL COUNSEL OF THE UNITED STATES DEPARTMENT OF JUSTICE 255 (Nathan A. Forrester ed., 2013). In 1846, the "Polk Corollary" of the Doctrine was added to assert this right regardless of whether the inhabitants of the area affected consented to the foreign intervention. *Id.* During the Cuban Missile Crisis, the Department of Justice explained that the legal justifications for the Monroe Doctrine and Polk Corollary were still valid because the rights asserted were based on regional self-defense. *Id.*

[159] LASCURETTES, *supra* note 148, at 13. The British appeared to have viewed international law as a law-abiding sentiment for the society of advanced nations, rather than as strict obligations imposed by a universal sovereign authority. MARTTI KOSKENNIEMI, THE GENTLE CIVILIZER OF NATIONS: THE RISE AND FALL OF INTERNATIONAL LAW 1870–1960, at 48–49 (2004). The Prime Minister responded to an 1887 proposal in the House of Lords to create a court of international arbitration by explaining, "International law has not any existence in the sense in which the term 'law' is usually understood. It depends generally upon the prejudices of writers of text-books. It can be enforced by no tribunal, and therefore to apply it to the phrase 'law' is to some extent misleading . . . ." THOMAS ALFRED WALKER, THE SCIENCE OF INTERNATIONAL LAW 1 (1893) (emphasis omitted).

based on maintaining stability in Europe, while Great Britain generally protested their actions, frequently on international legal grounds.[160]

The period also introduced a new voice in international law, the English philosopher Jeremy Bentham. Bentham is reputed to have coined the term "international" and applied it to law.[161] He posited, contrary to the elitist arrangement of the Concert of Europe, that the objective for a universal international code would be universal, equal utility of all nations.[162] Bentham also proposed the concept of an international court or "common tribunal" to adjudicate disputes.[163] Students of Bentham spread his ideas to newly independent States during the nineteenth century as a counterweight to the cynical positivism of the Concert of Europe.[164] Meanwhile, other nineteenth-century international lawyers equivocated, embracing equality but with limits or conditions. Some went so far as to rank States based on a standard of civilization, with the European model on top, allowing States to articulate a legal justification for colonialism.[165] In doing so, these lawyers rejected the indiscriminate universalism of Bentham, denying benefits of European international law to the rest of the world and reserving full sovereignty to a civilized, elite community of States.[166]

---

[160] LASCURETTES, *supra* note 148, at 14. France tried to establish the Hapsburg Archduke Maximilian in Mexico while the United States was preoccupied with its Civil War. SIMMS, *supra* note 122, at 230.

[161] MARK MAZOWER, GOVERNING THE WORLD: THE HISTORY OF AN IDEA, 1815 TO THE PRESENT 19 (2012). Bentham wrote early manuscripts on international law from 1786–89. *See generally* JEREMY BENTHAM, THE WORKS OF JEREMY BENTHAM (John Bowring ed., 1843).

[162] BENTHAM, *supra* note 161, at 537.

[163] *Id.* at 552.

[164] MAZOWER, *supra* note 161, at 21–22.

[165] *Id.* at 71–74; L. OPPENHEIM, 1 INTERNATIONAL LAW: A TREATISE 148 (2d ed. 1905). Other legal writers of the age, like Frantz Despargnet and Charles Salomon, warned against these justifications. *Id.* at 81.

[166] KOSKENNIEMI, *supra* note 159, at 142. Turkey, for example, was not part of the Concert of Europe until after the Crimean War. ORLANDO FIGES, THE CRIMEAN WAR: A HISTORY 423 (2010). That mid-nineteenth century conflict presents an interesting case study of the era's interventions and balance of power politics. It resulted from the Russian invasion of the Ottoman Empire to enforce its perceived legal rights to protect the Orthodox Christians within Ottoman territories. *Id.* at 104–16; IAN FLETCHER & NATALIA ISHCHENKO, THE CRIMEAN WAR: A CLASH OF EMPIRES 12–16 (2004). Fearing a Russian takeover of the Straits of Bosporus and Dardanelles, Great Britain and France responded to defend Turkey's sovereignty. COLEMAN PHILLIPSON, WHEATON'S ELEMENTS OF INTERNATIONAL LAW 108 (5th ed. 1916). Yet it would be wrong to assert the Crimean War was merely about resolving legal disputes; religion, national pride, and national strategies played significant roles in the decision to go to War. FIGES at 123–25, 157–58. The war left the Ottoman Empire indebted to the Allies. *Id.* at 427–28. Repayment loans were conditioned on the Ottomans issuing a decree for religious equality. *Id.* This type of lawful cultural intervention was disruptive to the social fabric within the Ottoman Empire, causing significant anti-

At the end of the century, the British international law scholar Lassa Oppenheim explained that sovereignty contained three fundamental qualities: independence of State action, internally and externally; territorial supremacy over all persons and things within the State's boundaries; and personal supremacy over the State's citizens at home and abroad.[167] The territorial sovereignty rule reflected these qualities:

> The protection granted to these qualities by the Law of Nations finds its expression in the right of every State to demand that other States abstain themselves, and prevent their organs and subjects, from committing any act which contains a violation of its independence and its territorial as well as personal supremacy.[168]

The duty of non-interference was clear:

> It is impossible to enumerate all such actions as might contain a violation of this duty. But it is of value to give some illustrative examples. Thus, in the interest of the independence of other States, a State is not allowed to interfere in the management of their international affairs nor to prevent them from doing or to compel them to do certain acts in their international intercourse. Further, in the interest of the territorial supremacy of other States, a State is not allowed to send its troops, its men-of-war, and its police forces into or through foreign territory, or to exercise an act of administration or jurisdiction on foreign territory, without permission.[169]

Oppenheim acknowledged, however, that State custom and practice allowed for broad exceptions for interferences based on self-defense, maintenance of the balance of power, and the interests of humanity.[170] While these exceptions were expansive, Oppenheim cautioned against their abuse because "any unjustifiable intervention by one State in the affairs of another gives a right of intervention to all other States."[171]

Some of the period's international law experts expressed even less tolerance for practices of interference. The British legal scholar Thomas Walker wrote that international law rested on territorial sovereignty, meaning that all States were formally equal and the only justification for

Christian violence. *Id.* at 430–32. The Ottomans ultimately failed to enforce religious equality reforms, which in turn had consequences in the Balkans where the Christian majority began rising up against Muslim landlords and generated nationalist movements that later ignited the First World War. *Id.* at 432. In retrospect, the interventions of the nineteenth century demonstrate the inadequate ability of the period's international law to constrain the forces of *raison d'état*, national pride, and religious affiliations.

[167] OPPENHEIM, *supra* note 165, at 170–71.

[168] *Id.* at 171.

[169] *Id.* at 173.

[170] *Id.* at 182–91. *See also* PHILLIPSON, *supra* note 166, at 91–92.

[171] OPPENHEIM, *supra* note 165, at 188.

an interference was "the imperative necessity of self-protection."[172] In Walker's view, the intrusions of European powers were examples falling short of the ideal; the progress of history showed that the rule of noninterference was strengthening.[173]

Henry Halleck, a lawyer who would become the United States Army Chief of Staff during the American Civil War, published a leading international law treatise in 1861. Addressing the nature and effect of territorial sovereignty, he emphasized the significance of non-interference with a sovereign State:

> No writer of authority, on international law, advocates any general right of one sovereign and independent state to interfere with the domestic concerns and internal government of another sovereign and independent state. Some, however, make numerous exceptions to the general rule, and attempt to justify interference by one state, in the internal affairs of another, in particular cases and for certain specified objects. The principal grounds upon which such interference has been justified are: first, self defence; second, the obligations of treaty stipulations; third, humanity; and fourth, the invitation of the contending parties in a civil war.[174]

Halleck recognized that States had interfered in the internal affairs of other States based on pretexts, but declared that the noninterference rule was "the fundamental principle of international jurisprudence" and therefore "usage, and custom, cannot make it justifiable or lawful, for no length of usage can justify a wrong."[175] Halleck also explained that a State could not transgress upon the territory of a peaceful neighboring State in pursuit of hostile rebels or other belligerents, but allowed for one exception: "If the neighboring state, from the want either of the will or of the ability, neglects to prevent such excursions, or to suppress such organizations, the threatened state may cross the frontier and attack or destroy the threatened danger."[176]

---

[172] WALKER, *supra* note 159, at 57, 112.

[173] *Id.* at 151.

[174] H.W. HALLECK, INTERNATIONAL LAW; OR, RULES REGULATING THE INTERCOURSE OF STATES IN PEACE AND WAR 83 (1861). *See generally* A.G. HEFFTER, LE DROIT INTERNATIONAL PUBLIC DE L'EUROPE §§ 44–46 (Jules Bergson trans., 1866); ROBERT PHILLIMORE, COMMENTARIES UPON INTERNATIONAL LAW 204–05 (1854); WILLIAM OKE MANNING, COMMENTARIES ON THE LAW OF NATIONS 98 (1839); ANTONIO RIQUELME, ELEMENTOS DE DERECHO PÚBLICO INTERNACIONAL, lib. 1, tit. 2, cap. 14 (1849); FRIEDRICH AUGUST WILHELM WENCK, CODEX JURIS GENTIUM RECENTISSIMI, tit. 1, 8 (1781).

[175] HALLECK, *supra* note 174, at 84.

[176] *Id.* at 95–96. The debate concerning the "unwilling or unable" standard observed by Halleck persists today. *See, e.g.*, Dawood I. Ahmed, *Defending Weak States Against the "Unwilling or Unable" Doctrine of Self-Defense*, 9 J. INT'L L. & INT'L REL. 1 (2013); Ashley S. Deeks, *"Unwilling or Unable": Toward a Normative Framework for Extraterritorial Self Defense*, 52 VA. J. INT'L L. 483 (2012); Kevin Jon Heller, *The Absence of*

The end of the nineteenth century saw the final fragmentation of the Concert of Europe. As much as any other factor, Britain's adherence to international law principles of sovereignty and territorial integrity ultimately carried it into armed conflict with Germany in the twentieth century. Germany's invasion of Belgium, which had been guaranteed neutrality by a treaty with the great-powers, brought the British into the First World War.[177] Likewise, President Wilson's fourteen-point plan, upon which the United States based its actions during the war, called for an association of nations to afford "mutual guarantees of political independence and territorial integrity to great and small states alike."[178]

Wilson's vision of an association of nations, much like the earlier Concert of Europe and Grotius's community of States before that, found life in the form of positive international law. Following the First World War, States drafted the Covenant of the League of Nations, a multilateral treaty creating an international body to promote cooperation, as well as peace and security. One of its declared purposes was to firmly establish "international law as the actual rule of conduct among Governments . . . ."[179] The Covenant required State parties to "respect and preserve as against external aggression the territorial integrity and existing political independence of all Members of the League."[180] Some hoped the new League would provide a mechanism to preserve sovereign rights and values over the unchecked power of foreign States.[181] The effort foundered, however, especially after the United States Senate declined to consent to the Covenant, in part because it appeared to strengthen political alliances rather than international law.[182]

In the interwar period, territorial sovereignty was the focus of seminal litigation at the Permanent Court of International Justice. In the *S.S. Lotus* case, France claimed Turkey had violated its sovereignty by subjecting to its criminal jurisdiction the watch officer of a French vessel involved in a collision with a Turkish ship on the high seas which killed 8 Turkish sailors. France characterized the ship as sovereign territory, argu-

Practice Supporting the "Unwilling or Unable" Test, OPINIO JURIS (Feb. 17, 2015), http://opiniojuris.org/2015/02/17/unable-unwilling-test-unstoppable-scholarly-imagination/.

[177] ISABEL V. HULL, A SCRAP OF PAPER: BREAKING AND MAKING INTERNATIONAL LAW DURING THE GREAT WAR 41–43 (2014).

[178] *President Woodrow Wilson's Fourteen Points*, YALE L. SCH. AVALON PROJECT, http://avalon.law.yale.edu/20th_century/wilson14.asp. Fifty years later the U.S. Department of Justice explained that international law changed after World War I to prohibit armed interventions. Katzenbach, *supra* note 149, at 226.

[179] *The Covenant of the League of Nations*, YALE L. SCH. AVALON PROJECT, http://avalon.law.yale.edu/20th_century/leagcov.asp.

[180] *Id.* at art. 10.

[181] Sir Geoffrey Butler, *Sovereignty and the League of Nations*, 1 BRIT. Y.B. INT'L L. 35, 41 (1920–21).

[182] MAZOWER, *supra* note 161, at 138.

ing the officer's wrongful act fell outside Turkish jurisdiction.[183] The Court stated, "the first and foremost restriction imposed by international law upon a State is that—failing the existence of a permissive rule to the contrary—*it may not exercise its power in any form in the territory of another State*."[184] The Court, however, explained that international law permitted a victim State to exercise criminal jurisdiction over an offense that occurred in another State when the effects take place within the victim State.[185] Both France, on whose territory the watch officer's act occurred, and Turkey, on whose territory the effects occurred, had concurrent legal authority to take action.[186]

The League of Nations infamously collapsed prior to the Second World War but was soon succeeded by the United Nations in 1945, which adopted many of the League's expectations with respect to territorial inviolability.[187] The United Nations Charter lies at the structural core of modern international relations but refers to sovereignty only twice. First, the Charter notes that the United Nations "is based on the principle of the sovereign equality of all its Members."[188] Second, the Charter explains that when a territory under a trusteeship becomes a Member State, it ceases to be a trustee because the relationship among Member of the United Nations "shall be based on respect for the principle of sovereign equality."[189] The Charter does not define sovereignty. However, the drafting conference that produced it understood that sovereign equality included the following elements:

> (1) that states are juridically equal;
>
> (2) that each state enjoys the right inherent in full sovereignty;
>
> (3) that the personality of the state is respected, as well as its territorial integrity and political independence;
>
> (4) that the state should, under international order, comply faithfully with its international duties and obligations.[190]

---

[183] S.S. Lotus (Fr. v. Turk.), Judgment, 1927 P.C.I.J. (ser. A) No. 10, 6–7 (Sept. 7).

[184] *Id.* at 18 (emphasis added).

[185] *Id.* at 25–27.

[186] *Id.* at 31.

[187] Charles Townshend, *The League of Nations and the United Nations*, BBC (Feb. 17, 2011), http://www.bbc.co.uk/history/worldwars/wwone/league_nations_01.shtml.

[188] U.N. Charter, art. 2, ¶ 1.

[189] *Id.* at art. 78.

[190] LELAND M. GOODRICH & EDVARD HAMBRO, CHARTER OF THE UNITED NATIONS: COMMENTARY AND DOCUMENTS 66 (1946) (quoting UNCIO, *Report of Rapporteur of Committee 1 to Commission I,* Doc. 944, I/1/34(1), p. 12; *Verbatim Minutes of Second Meeting of Commission I,* Jun. 15, 1945, Doc. 1123, I/8, p. 5–7; and *Verbatim Minutes of the Ninth Plenary Session*, Jun. 25, 1945, Doc. 1210, P/20, p. 3).

Members of the U.S. delegation negotiating the Charter resisted defining "sovereign equality" because they feared undermining the strength of the rule. Mr. Leo Pasvolsky, the Special Assistant to the U.S. Secretary of State, explained, "an enumeration of what is included under the term 'sovereign equality' would weaken the concept which, stated in general terms, covers a very broad field."[191] For example, as the negotiations addressed terms to protect the territory of States from external aggression, Mr. Harley A. Notter, an advisor to the U.S. delegation, objected to detailing such rules, stating, "[w]e interpret sovereign equality as embodying the principle of respect for territorial integrity. We consider the principle implicit so that it is difficult to answer the question why we object to spelling it out."[192] Thus, Mr. Pasvolsky proposed language for the Charter that would not "involve a guarantee of territorial integrity" because it risked objections from the Soviet bloc.[193] The language he preferred, "[a]ll members of the *United Nations* shall refrain in their international relations, from the threat or use of force *against the territorial integrity or political independence of any member or state*, or in any other manner inconsistent with the purposes of the United Nations[,]" was subsequently included in the Charter, with slight modification, in Article 2(4).[194] The Charter's use of force provisions were included at the request of smaller nations as to preserve them against external aggression.[195] Thus, while the Charter's legal obligation to refrain from the use of force is treaty-based and somewhat qualified, it is evident the obligation is derived from customary law understandings of sovereignty far broader in scope.[196]

Since the Charter entered force, judgments of the International Court of Justice have addressed territorial sovereignty, especially post-war customary law notions of noninterference. In its *Corfu Channel* judgment, the Court held the United Kingdom violated Albania's sovereignty by routing warships and conducting demining operations in Albania's terri-

[191] *Minutes of the Fourteenth Meeting of the United States Delegation, Held at San Francisco, Tuesday, April 24, 1945, 9:30 a.m.*, *reprinted at* FOREIGN RELATIONS OF THE UNITED STATES: DIPLOMATIC PAPERS, 1945, GENERAL: THE UNITED NATIONS, VOL. I, 375 (1972).

[192] *Minutes of the Thirty-Ninth Meeting of the United States Delegation, Held at San Francisco, Tuesday, May 15, 1945, 9 a.m., reprinted at* FOREIGN RELATIONS OF THE UNITED STATES: DIPLOMATIC PAPERS, 1945, GENERAL: THE UNITED NATIONS, VOL. I, 726 (1972) (emphasis in original).

[193] *Id.*

[194] *Id.* (emphasis in original).

[195] GOODRICH & HAMBRO, *supra* note 190, at 68.

[196] Although some perceive treaty obligations as undermining sovereignty, a State enters such obligations based on its authority and plenary prerogative to deal with other States. *See* Thomas C. Heller & Abraham D. Sofaer, *Sovereignty: The Practioners' Perspective*, *in* PROBLEMATIC SOVEREIGNTY: CONTESTED RULES AND POLITICAL POSSIBILITIES 24, 45 (Stephen D. Krasner, ed., 2001).

torial waters without its consent.[197] The United Kingdom sought to justify the operations to secure its freedom of navigation rights through international straits.[198] The Court characterized the U.K. demining operations as an exercise of an "alleged right of intervention as the manifestation of a policy of force, such as has, in the past, given rise to most serious abuses and such as cannot . . . find a place in international law."[199] The *Corfu Channel* Judgment clearly stands for the proposition that one State's nonconsensual operations in the territory of another—a violation of sovereignty—cannot be justified based on general security concerns.

Later, in the 1986 *Case Concerning Military and Paramilitary Activities in and Against Nicaragua*, the International Court of Justice offered now widely-cited elaborations on the principle of non-intervention and the prohibition on the use of force. But the Court also offered significant and underappreciated observations on territorial sovereignty.[200] The case arose from claims related to United States support of armed groups allegedly responsible for attacks in Nicaragua and for alleged U.S. operations undertaken in Nicaraguan territorial waters and airspace.[201] The Court applied the customary law principle of nonintervention and determined that U.S. financial and other support for rebels in Nicaragua amounted to a coercive intervention in matters committed to the exclusive prerogative of the Nicaraguan government.[202] Elaborating on the link

[197] Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. Rep. 4 ¶¶ 69–70 (Apr. 9).

[198] *Id.* at 64–65.

[199] *Id.* at 35. While the Court held the British action violated Albania's sovereignty, it allowed no redress apart from the declaration of the violation. *Id.* at 47.

[200] Military and Paramilitary Activities in and Against Nicaragua (hereinafter, Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep. 14, ¶ 251 (June 27).

[201] *Id.* at ¶¶ 21, 250. Aspects of this case are viewed skeptically by U.S. government attorneys. Davis Robinson, the U.S. State Department Legal Adviser from 1981–1985, expressed "disquiet" over this decision because, "[a]fter the fact, events have confirmed, as we then believed, that Nicaragua's application [to the International Court of Justice] was based on a fraudulent affidavit." Davis R. Robinson, *The Reagan Administration – Davis R. Robinson (1981-1985)*, *in* SHAPING FOREIGN POLICY IN TIME OF CRISIS: THE ROLE OF INTERNATIONAL LAW AND THE STATE DEPARTMENT LEGAL ADVISER 62 (Michael P. Scarf & Paul R. Williams eds., 2010). Robison also points out that Nicaragua's lead attorney on the case admitted to communicating with an ICJ judge before filing the case. *Id.* In assessing earlier support to anti-communist groups, the Department of Justice had opined that a neutral State could not support an organized armed attack upon another State, but explained "there would appear to be no violation of this precedent by the mere provision of arms by private parties, even the stockpiling of arms, as long as they remain within the control of private groups rather than belligerent parties, or by permitting volunteers to be recruited, assembled, and perhaps even trained so long as this did not approach the point of an organized military force." Katzenbach, *supra* note 149, at 225.

[202] *Nicar. v. U.S.*, 1986 I.C.J. at ¶ 242. The Court based much of its legal findings on the use of force and non-intervention on the 1970 U.N. General Assembly

between territorial sovereignty and the principle of non-intervention, the Court observed,

> The principle of non-intervention involves the right of every sovereign State to conduct its affairs without outside interference; though examples of trespass against this principle are not infrequent, the Court considers that it is part and parcel of customary international law. As the Court has observed: "Between independent States, respect for territorial sovereignty is an essential foundation of international relations . . .", and international law requires political integrity also to be respected.[203]

The Court also held, somewhat controversially, that U.S. logistical support to the Nicaraguan rebels, including arming and training, amounted itself to a prohibited use of force.[204] Understandably, these two holdings attracted the lion's share of attention following the case. They surely represented the gravest breaches of international law involved in the case. However, the *Paramilitaries* judgment also included important observations on territorial sovereignty, independent from its holdings on the principles related to use of force and intervention.

A limit on the parties' consent to its jurisdiction prevented the Court from directly applying the United Nations Charter to the litigation, including the Article 2, paragraph 4 prohibition on the threat or use of

Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States. *Id.* (citing G.A. Res. A/RES/25/2625, Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations (Oct. 24, 1970), http://www.un-documents.net/a25r2625.htm). The Court acknowledged the non-binding nature of General Assembly instruments, however it also noted the United States voted in favor of the Declaration without reservations and had accepted similar statements of principles in other settings. *Id.* at ¶ 188.

[203] *Nicar. v. U.S.*, 1986 I.C.J. at ¶ 202 (quoting Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. Rep. 4 ¶ 35 (Apr. 9)).

[204] *Nicar. v. U.S.*, 1986 I.C.J. at ¶ 228. This decision proved to be so controversial to the United States that it led to the revocation of its consent to the Court's compulsory jurisdiction. *See* U.S. DEP'T OF STATE, LETTER AND STATEMENT CONCERNING TERMINATION OF ACCEPTANCE OF ICJ COMPULSORY JURISDICTION, 24 I.L.M. 1742 (1985). The focus of the controversies involved the Court's acceptance of jurisdiction, the right of El Salvador to intervene in the litigation, and the Court's finding that Nicaragua's claims were justiciable. *U.S. Terminates Acceptance of ICJ Compulsory Jurisdiction: Hearing Before the Senate Foreign Relations Committee* (Dec. 4, 1985) (statement of Abraham D. Sofaer, Legal Advisor, U.S. Dep't of State), *reprinted in* 86 Dep't of State Bull. 67 (Jan. 1986); Sean D. Murphy, *The United States and the International Court of Justice: Coping with Antinomies in* THE SWORD & THE SCALES: UNITED STATES AND INTERNATIONAL COURTS AND TRIBUNALS 83 (Cesare Romano ed., 2009). United States legal advisors also criticized the Court's distinctions between an armed attack and the use of force in this case. *See* Abraham D. Sofaer, *Terrorism, the Law, and the National Defense*, 126 MIL. L. REV. 89, 92–93 (1989); William H. Taft IV, *Self-Defense and the Oil Platforms Decision*, 29 YALE J. INT'L L. 295, 300–01 (2004).

force.[205] However, the Court frequently resorted to the Charter for evidence of the customary international law it applied to the case.[206] With respect to territorial sovereignty, the Court cited, *inter alia*, Article 2, paragraph 1 of the Charter, which recites "the sovereign equality of all its Members."[207] The Court supplemented its findings on territorial sovereignty and extended them to airspace and territorial seas with citations to the 1944 Chicago Aviation Convention and the 1958 Geneva Convention on Territorial Sea.[208] The Court easily concluded that these treaties offered clear support for a customary duty on the part of States to refrain from violating the exclusive control enjoyed by sovereigns over their territory, including seas and air space.[209]

The Court also relied pointedly on its own decisions in its examination of territorial sovereignty. The Court quoted and reaffirmed its *Corfu Channel* case repeatedly for the legal effect of sovereignty, observing, "[b]etween independent States, respect for territorial sovereignty is an essential foundation of international relations."[210] Discussing the related principle of nonintervention, the Court identified a compelling parallel between U.S. intermeddling in Nicaragua and the United Kingdom's effort "to secure evidence in the territory of another State" in *Corfu Channel*.[211] Returning to the issue of territorial sovereignty, the Court examined whether U.S., "attacks on Nicaraguan territory, incursions into its territorial sea, and overflights" were violations of Nicaraguan sovereignty.[212] The Court held that the attacks, "not only amount to an unlawful use of force, but also constitute *infringements of the territorial sovereignty* of Nicaragua."[213] The Court made a similar determination with respect to U.S. maritime and overflight operations ruling, "they constitute a violation of Nicaragua's sovereignty."[214]

---

[205] *Nicar. v. U.S.*, 1986 I.C.J. at ¶¶ 56, 172.

[206] *Id.* at ¶ 182.

[207] U.N. Charter, art. 2, ¶ 1.

[208] United Nations Convention on the Law of the Sea, Dec. 10, 1982, 1833 U.N.T.S. 397, [hereinafter UNCLOS]; Geneva Convention on the Territorial Sea, Apr. 29, 1958, 516 U.N.T.S. 205; Convention on International Civil Aviation, Dec. 7, 1944, 15 U.N.T.S. 295 [hereinafter Chicago Convention].

[209] *Nicar. v. U.S.*, 198 I.C.J. at ¶¶ 212–13.

[210] *Id.* at ¶ 202 (quoting Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. Rep. 4 ¶ 35 (Apr. 9)).

[211] *Id.*

[212] *Id.* at ¶ 250.

[213] *Id.* at ¶ 251 (emphasis added).

[214] *Id.*

The importance of territorial integrity as an aspect of sovereignty has also been vigorously emphasized by States.[215] In 1989, not long after the *Paramilitaries* case, United States State Department Legal Adviser Abraham Sofaer explained, "'[t]erritorial integrity' is a cornerstone of international law; control over territory is one of the most fundamental attributes of sovereignty."[216] Thus it should be no surprise that Presidents of the United States and other senior government officials frequently invoke the need to respect sovereignty.[217] Accordingly, the United States

[215] Michael N. Schmitt & Liis Vihul, *Respect for Sovereignty in Cyberspace*, 95 TEX. L. REV. 1639, 1657–59 (2017) (recounting State reactions to violations of territorial sovereignty).

[216] Digest of United States Practice in International Law 1989–1990, at 93–96 (Margaret S. Pickering et al. eds., 2003) (quoting Hearing Before Subcommittee on Civil Constitutional Rights of House Committee on the Judiciary (Nov. 8, 1989) (statement of Abraham D. Sofaer, Legal Advisor, U.S. Dep't of State)).

[217] *See, e.g.*, *Dwight D. Eisenhower, Special Message to the Congress on the Situation in the Middle East*, AM. PRESIDENCY PROJECT, http://www.presidency.ucsb.edu/ws/?pid=11007 ("Our country supports without reservation the full sovereignty and independence of each and every nation of the Middle East."); *Richard Nixon, Fourth Annual Report to the Congress on United States Foreign Policy*, AM. PRESIDENCY PROJECT, http://www.presidency.ucsb.edu/ws/?pid=3832 ("These are principles which the United States has sought to engage the other great powers in observing[:] Coexistence, negotiated solutions, avoiding the use or threat of force, great power restraint, noninterference, respect for the sovereignty and territorial integrity of states, renunciation of hegemony or unilateral advantage . . . . They are not new principles; every member state of the United Nations has subscribed to their essential elements."); *Jimmy Carter, Vienna Summit Meeting Joint U.S.-U.S.S.R. Communiqué*, AM. PRESIDENCY PROJECT, http://www.presidency.ucsb.edu/ws/?pid=32497 ("The two sides stressed the importance of peaceful resolution of disputes, respect for the sovereignty and territorial integrity of states, and of efforts so that conflicts or situations would not arise which could serve to increase international tensions."); *William J. Clinton, United States-European Union Summit Statement on Chechnya*, AM. PRESIDENCY PROJECT, http://www.presidency.ucsb.edu/ws/?pid=57087 ("We stress that the respect for the territorial integrity and sovereignty of neighboring states is a fundamental principle of the international system."); *George W. Bush, Joint Statement by President George W. Bush and President Vladimir V. Putin of Russia on a New Relationship Between the United States and Russia*, AM. PRESIDENCY PROJECT, http://www.presidency.ucsb.edu/ws/?pid=63384 ("We support the building of a European-Atlantic community whole, free, and at peace, excluding no one, and respecting the independence, sovereignty and territorial integrity of all nations."); *United States and India: Prosperity Through Partnership*, WHITE HOUSE (Jun. 26, 2017), https://www.whitehouse.gov/the-press-office/2017/06/26/united-states-and-india-prosperity-through-partnership (declaring support for "ensuring respect for sovereignty and territorial integrity, the rule of law, and the environment"). *See also* Schmitt & Vihul, *supra* note 215, at 1662–63 (summarizing similar statements by President Barak Obama and officials in his administration); *Joint Statement for Enhancing the Comprehensive Partnership between the United States of America and the Socialist Republic of Vietnam*, WHITE HOUSE (May 31, 2017), https://www.whitehouse.gov/briefings-statements/joint-statement-enhancing-comprehensive-partnership-united-states-america-socialist-republic-vietnam/ (jointly committing to an enhanced Comprehensive Partnership "grounded in respect for the United Nations Charter

has found that a State's agents have no arrest authority in a foreign State without the consent of the foreign State (absent a situation involving self-defense).[218] The United States expressed its "grave[] concern[s]" to Canada after Canadian authorities arrested an American citizen 200 yards on the United States' side of the border.[219] U.S. objections to a foreign State official acting within U.S. territory is in line with a series of similar cases, perhaps the most notorious of which involved Israeli Mossad agents abducting the Nazi war criminal Adolph Eichmann from Argentina for trial in Israel without first obtaining Argentina's consent.[220] Argentina referred Eichmann's case to the United Nations Security Council, which agreed that the transfer of Eichmann from Argentina to Israel constituted a violation of Argentina's sovereignty that was incompatible with the U.N. Charter and risked undermining international peace and security.[221] Although the Security Council did not order Eichmann released, it did request Israel make reparations to Argentina.[222] These examples underscore sovereignty's place as a primary rule of international law clearly prohibiting a State from taking acts associated with jurisdiction in a foreign territory without consent.[223]

Sovereignty rules do not merely prohibit a State's unilateral law enforcement activities in a foreign territory; they prohibit officials and agents from nonconsensual entry into the territory of a foreign State. For example, in accord with the International Court of Justice's rulings, airspace over a State is considered sovereign; consequently, aircraft are not generally entitled to enter the airspace above the territory of a foreign State without permission.[224] This is a significant part of the basis for Pakistan's objections to U.S. unmanned vehicles conducting operations over Pakistani territory.[225] Similar sovereignty rules apply to a State's territorial waters, with many States asserting their sovereignty by seizing trespassing foreign military vessels.[226] As noted scholar Quincy Wright explained,

and international law, each other's independence, sovereignty, territorial integrity, and respective political systems.").

[218] Sofaer Testimony, *supra* note 216, at 93 (citing 1 INTERNATIONAL LAW: BEING THE COLLECTED PAPERS OF HERSCH LAUTERPACHT, 487–88 (Elihu Lauterpacht ed., 1970)); RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 433 (1987).

[219] DIGEST OF UNITED STATES PRACTICE IN INTERNATIONAL LAW 1991–1999, at 445–46 (Sally J. Cummins & David P. Stewart eds., 2005).

[220] L.C. Green, *The Eichmann Case*, 23 MODERN L. REV. 507, 508–10 (1960).

[221] S.C. Res. S/4349 (June 23, 1960).

[222] *Id.* at ¶ 2.

[223] RESTATEMENT (THIRD) OF FOREIGN RELATIONS §§ 432(2), 433.

[224] Chicago Convention, *supra* note 208, ¶¶ 1, 6; Oliver J. Lissitzyn, *The Treatment of Aerial Intruders in Recent Practice and International Law*, 47 AM. J. INT'L L. 559 (1953).

[225] Schmitt & Vihul, *supra* note 215, at 1657.

[226] *Id.* at 1657–58 (detailing the 2007 seizure of the British crew from the HMS Cornwall and the 2016 capture of U.S. riverine craft by Iranian Islamic Revolutionary

States have habitually protested "against private military expeditions proceeding from foreign territory with complicity or negligence of the government of that territory; and even against injuries to persons or property in their territory originating from acts in foreign territory without hostile intent or negligence by the government of that state."[227] Based on this precedent, State sovereignty protections extend well beyond prohibitions on the use of force and non-intervention into another State's political, economic, social and cultural system, or the formulation of its foreign policy; each State has the exclusive right to control activities within its borders and to refrain from undertaking nonconsensual activities within the borders of foreign States.

Outside of the threshold for wartime hostilities, States have agreed to specific innocent transit regimes for the air and sea domains. In the maritime environment, a treaty, the United Nations Convention of the Law of the Sea (UNCLOS), established rules for the innocent passage of other States' military vessels. The treaty grants that ships of all States are allowed continuous and expeditious passage through the territorial sea of a foreign State so long as the movement is innocent, meaning that it does not prejudice the peace, good order, or security of the coastal State.[228] To avoid confusion, UNCLOS lists activities considered to be prejudicial, to include: the threat of use of force; weapons use, practice, or exercise; information collection; propaganda broadcasting; launching or landing aircraft or devices; loading or unloading cargo; fishing; polluting; research and surveys; or interference with communications of facilities in the coastal State.[229] UNCLOS also allows coastal states to adopt necessary safety regulations relating to maritime navigation and traffic.[230] Coastal states, however, do not have the authority to require advance permission or notification of a foreign warship's transit, nor may a coastal state close off or otherwise impose arbitrary limits on the passage through its territorial seas during peacetime.[231] The UNCLOS innocent passage rules were agreed upon by States to balance their collective interests in maintaining the oceans as a common resource for transportation and com-

Guard forces, as well as U.S. and Chinese conduct over disputed waters in the South China Sea).

[227] Quincy Wright, *Legal Aspects of the U-2 Incident*, 54 AM. J. INT'L L. 836, 844 (1960). *See also* Schmitt & Vihul, *supra* note 215, at 1652–55, 1660–61 (discussing Australia's assertion of sovereignty at the ICJ to stop France from atmospheric nuclear weapons testing where effects manifested in Australia; assertions of sovereignty by Nicaragua and Costa Rica over transboundary environmental damage; and Canadian assertions of sovereignty in response to damage by a Soviet spacecraft crash).

[228] UNCLOS, *supra* note 208, at arts. 17–18, 24.

[229] *Id.* at art. 19.

[230] *Id.* at arts. 21–22, 25.

[231] Ronald D. Neubauer, *The Right of Innocent Passage for Warships in the Territorial Sea: A Response to the Soviet Union*, 68 NAVAL WAR C. REV. 189, 191 (1988).

munication with the interests of coastal States in protecting their interests and especially their territorial sovereignty.[232]

Overflight of foreign territory is also governed by treaties and international agreements. The 1919 Convention Relating to the Regulation of Aerial Navigation recognized that every State "has complete and exclusive sovereignty over the air space above its territory."[233] This was understood to reflect the unilateral and absolute right of each nation to permit or deny entry into its territory and to control all movements therein.[234] The primacy of sovereignty was repeated in the 1944 treaty governing aviation, the Convention on International Civil Aviation (Chicago Convention).[235] This treaty is a primary modern source of law for State obligations for all aircraft (although it applies exclusively to civil aircraft, it has provisions applicable to State aircraft).[236] Unlike the UNCLOS regime, the Chicago Convention prohibits a State's military aircraft from flying over or landing in the territory of a foreign state without special authorization.[237] State charter flights over foreign territory may be required to obtain permission and provide information relating to flight plans and stopovers.[238] The Chicago Convention does have a mechanism for aircraft in distress to make emergency landings in a foreign State without advance notice.[239] These rules for aircraft were at the center of an international dispute in 2001, when a U.S. Navy EP-3 aircraft was forced to make an emergency landing in territory belonging to the People's Republic of China following a midair collision with a Chinese F-8 aircraft.[240] In that case, the Chinese argued the U.S. violated their sovereignty with an unannounced entry and landing, while the U.S. argued that it's aircraft in distress committed no wrong and that its sovereignty was violated by subsequent Chinese actions.[241]

---

[232] Karin M. Burke and Deborah A. DeLeo, *Innocent Passage and Transit Passage in the United Nations Convention on the Law of the Sea*, 9 YALE J. WORLD PUB. ORD. 389, 391 (1983).

[233] Convention Relating to the Regulation of Aerial Navigation, Oct. 13, 1919, art. 1, 11 L.N.T.S. 173.

[234] PAUL S. DEMPSEY, PUBLIC INTERNATIONAL AIR LAW 43 (2008); Christopher M. Petras, *The Law of Air Mobility—The International Legal Principles Behind the U.S. Mobility Air Forces' Mission*, 66 A. F. L. REV. 1, 10–11 (2010) (citing John Cobb Cooper, *Backgrounds of International Public Air Law*, 1 Y.B. AIR & SPACE L. 3 (1967)).

[235] Chicago Convention, *supra* note 208, art. 1.

[236] *Id.* at art. 3.

[237] *Id.*

[238] Petras, *supra* note 234, at 10–11.

[239] Chicago Convention, *supra* note 208, at art 25; 2 Y.B. OF THE INT'L L. COMMISSION 102 (1978).

[240] DIGEST OF THE UNITED STATES PRACTICE IN INTERNATIONAL LAW 2001, at 703 (Sally J. Cummins & David P. Stewart eds., 2002).

[241] *Id.* at 707–10.

Not every potential exception to sovereignty can be found in international treaties. Whether an exception exists for espionage in the form of information and intelligence gathering in the territory of a foreign State appears to be unresolved. A notable modern case study looks at the U.S. overflight program of the Soviet Union by U-2 reconnaissance aircraft from 1956 until 1960.[242] On May 1, 1960, the Soviets shot down the U-2 flown by Francis Powers.[243] Contemporary legal experts examining the United States' U-2 reconnaissance overflights of the Soviet Union in 1960 conclude they probably violated international law, despite the argument that the flights were necessary to protect against surprise attack.[244] Similar prohibitions against espionage in another State's territori-

[242] President Truman officially authorized reconnaissance overflights of the Soviet Union starting in 1950. R. Cargill Hall, *The Truth About Overflights: Military Reconnaissance Missions Over Russia Before the U-2 Are One of the Cold War's Best Kept Secrets*, 9 MIL. HIST. Q. 24, 28 (1997). The British Royal Air Force began a similar program in 1951. *Id.* at 29. The U-2 overflights started in 1956. *Id.* at 39.

[243] Wright, *supra* note 227, at 836.

[244] *Id.* at 838, 846–47. *See also* Eleanor H. Finch, Comment, *Lester H. Woolsey 1877–1961*, 56 AM. J. INT'L L.130, 139 (1962) (noting that after the U-2 was shot down, the United States complained about the numerous acts of espionage committed by Soviet agents in the United States, but "refrained from claiming a legal right to overfly the Soviet Union for reconnaissance purposes, and some representatives attached importance to the announcement of the United States that the U-2 flights over the U.S.S.R. had been discontinued."); Quincy Wright, *Espionage and the Doctrine of Non-Intervention in Internal Affairs*, *in* ESSAYS ON ESPIONAGE AND INTERNATIONAL LAW 18 (Roland J. Stanger, ed., 1962) (noting that self-defense is only permitted in cases of armed attack or the threat thereof, but the U.S. justifications for the U-2 flights were based on ascertaining Soviet policy and intent, not from an immediate threat of attack). Thomas Reed, a Secretary of the Air Force during the Ford administration, stated, "[t]he aerial overflights of the Soviet Union had no justification in international law. They were espionage, pure and simple." REED, *supra* note 44, at 37. Professor Schmitt and Ms. Vihul argue that the U.S. failure to protest the U-2 shoot down was an acknowledgement of Soviet sovereignty over its airspace, especially when the U.S. protested the shoot down of another aircraft over the high seas earlier in that year. Schmitt & Vihul, *supra* note 215, at 1656–57. The relevant issue is not whether the Soviets had sovereignty over their airspace (they clearly did), but whether the U.S. violated international law by sending the spy craft over Soviet territory in the first place. W. Hays Parks emphasizes this point: "Penetration of a state's airspace for purposes of collection of intelligence, while often vaguely characterized as a 'violation of international law,' more correctly may be regarded as a violation of the sovereignty of that state as recognized by international law. The remedy generally lies with the state whose airspace has been violated rather than in international law as such." W. Hays Parks, *The International Law of Intelligence Collection*, *in* NATIONAL SECURITY LAW 439 (John Norton Moore et al. eds., 1990). Due to the domestic law remedy, Parks asserts that the U-2 overflights did not constitute a *per se* violation of international law, even though the Soviets were justified in resorting to proportional levels of force to defend their sovereignty. *Id.* Self-help, however, is a typical mechanism for dealing with international law violations due to the absence of

al waters may exist.[245] Land-based espionage involving territorial trespass by agents would be similarly prohibited. In fact, one expert found that "national territory has a stricter national legal regime than the territorial sea and national airspace" and found that espionage involving territorial incursions did, in fact, violate international law.[246] Despite its potential peacetime illegality, States have long engaged in peacetime espionage, but rarely acknowledge doing so.[247]

This longstanding international relations reality has led to a *tu quoque* argument (i.e., everybody spies), where many conclude that international law does not address espionage.[248] As a former General Counsel to

a central authority for enforcement of rules. L. OPPENHEIM, 1 INTERNATIONAL LAW 13–14 (photo Reprint 1962) (H. Lauterpacht ed., 8th ed. 1955).

[245] JOHN KISH, INTERNATIONAL LAW AND ESPIONAGE 89 (David Turns ed., 1995); James Kraska, *Putting Your Head in the Tiger's Mouth: Submarine Espionage in Territorial Waters*, 54 COLUM. J. TRANSNAT'L L. 164, 181 (2015).

[246] KISH, *supra* note 245, at 83.

[247] Wright, *supra* note 227, at 849.

[248] Hugo Grotius stated, "sending [spies] is beyond doubt permitted by the law of nations"—although the context of his discussion on sending spies dealt with wartime practice. HUGO GROTIUS, DE BELLI AC PACIS, BOOK III, CH. IV 655 (1925). Wartime espionage is permissible because belligerents are not obligated to respect each other's territory or government, while peacetime espionage arguably violates a State's duty to respect another's territorial integrity and political independence. Wright, *supra* note 244, at 12. Other legal scholars have found espionage to be legal. *See, e.g.*, Christopher D. Baker, *Tolerance of International Espionage: A Functional Approach*, 19 AM. U. INT'L REV. 1091, 1092 (2004) ("[I]nternational law neither endorses nor prohibits espionage, but rather preserves the practice as a tool by which to facilitate international cooperation."); Ashley Deeks, *An International Legal Framework for Surveillance*, 55 VA. J. INT'L L. 291, 300 (2015) (observing that "[w]ith a few exceptions . . . , most scholars agree that international law either fails to regulate spying or affirmatively permits it."); Craig Forcese, *International Law and Intelligence Collection*, 5 J. NAT'L SEC. L. & POL'Y 179, 204-05 (2011) (observing that "there is no clear answer on the international legality of extraterritorial espionage, assessed from the sovereignty perspective, and the international community seems content with an artful ambiguity on the question."); OPPENHEIM, *supra* note 165, at 491 (observing that "[a]lthough all States constantly or occasionally send spies abroad, and although it is neither morally nor politically and legally considered wrong to send spies, such agents have, of course, no recognised position whatever according to International Law, since they are not agents of States for their international relations."); Parks, *supra* note 244, at 433–34 ("Intelligence collection as such does not violate international law. However, some aspects of international law affect the means to be utilized in collection. A leading example is the sovereign right of each nation to control access to its territory, coastal waters, and the airspace above each; and to limit activities within each."); A. John Radsan, *The Unresolved Equation of Espionage and International Law*, 28 MICH. J. INT'L L. 595, 596 (2007) (observing that "espionage is neither legal nor illegal under international law."); Glenn Sulmasy & John Yoo, *Counterintuitive: Intelligence Operations and International Law*, 28 Mich. J. Int'l L. 625, 637 (2007) (observing that "[i]nternational law has never prohibited intelligence collection, in peacetime or wartime. State practice has always supported the principle

the Central Intelligence Agency explained, "espionage is such a fixture in international affairs, it is fair to say that the practice of states recognizes espionage as a legitimate function of the state, and therefore it is legal as a matter of customary international law."[249] Indeed, after the aforementioned U-2 shoot down, the Soviet Foreign Minister response was not to dispute the lawfulness of espionage when confronted with Soviet behavior, but to distinguish ordinary espionage from aerial reconnaissance, with the later presumably having a greater capacity to carry destructive weapons than a trespassing agent.[250] States, however, generally do not discuss their espionage programs, let alone attempt to make public assertions of their legality. The lack of *opinio juris* from States on espionage suggests that its international law status is indeterminate at best.[251]

In sum, history and practice make a strong case for recognition of territorial sovereignty as a standing rule of conduct between States. While originally conceived to reorganize and balance volatile political relations, territorial sovereignty soon developed into both the basis for an entire juridical order and a primary rule of conduct comprising that order. Sovereignty matured into a clear, albeit frequently compromised and contextually conditioned, rule of conduct between States promising exclusive and independent control of territory and the persons and property located on it. Alongside the widely recognized authority of sovereigns to exercise dominion over territory, a complementary duty to refrain from interfering with other States' authority in that respect emerged, including expectations of near inviolability of political borders. By the end of the nineteenth century, the duty to refrain from interference with territorial sovereignty was clear, though conditioned by exceptions such as cases of self-defense. By the twentieth century, interactions between States in domains such as the seas called for further compromises concerning inviolability. And while the conflict-plagued twentieth century offered sufficiently frequent and grave breaches of territorial sovereignty to perhaps call the rule of non-interference into question, tribunals, publicists, and States, in their construction of collective security arrange-

that such activity, although it can affect the territorial sovereignty of the target, is nevertheless critical to maintaining peace and international security.").

[249] Jeffrey H. Smith, *Keynote Address*, 28 MICH. J. INT'L L. 543, 544 (2007).

[250] Wright, *supra* note 227, at 849. Wright, however, argues that both aerial reconnaissance over foreign territory and secret agents on foreign territory amount to illegitimate enterprises. *Id.*

[251] State practice, without *opinio juris*, cannot create a customary international law rule. Schmitt & Vihul, *supra* note 215, at 1645. The United States and other nations may be establishing *opinio juris* relating to espionage, where it would be limited to gaining information necessary for national security decisions. Martin Libicki, *The Coming of Cyber Espionage Norms*, 9TH INT'L CONFERENCE ON CYBER CONFLICT 3 (2017), https://ccdcoe.org/sites/default/files/multimedia/pdf/Art%2001%20The%20Coming%20of%20Cyber%20Espionage%20Norms.pdf.

ments, offered unwavering support for territorial sovereignty as a rule of conduct.[252]

IV. EMERGENT VIEWS ON TERRITORIAL SOVEREIGNTY IN CYBERSPACE

As illustrated above, States quickly perceived cyberspace as a critical domain of international relations. Nearly as quickly, they understood the importance of developing international legal theories and doctrine to justify their actions in this new realm. Yet for a variety of political reasons, State expressions of applicable legal doctrine have been sporadic.[253] In the case of the United States, initial enthusiasm for expressing cyber legal doctrine soon gave way to a sustained silence on the subject, broken only recently and selectively. Meanwhile, private opinions, chiefly from the academy and nongovernmental efforts, have proliferated and, in the wake of relative State silence, have assumed perhaps outsized influence. Both State and private sources have tackled the question of territorial sovereignty in cyberspace. While consensus that territorial sovereignty operated as a limit on cyber intrusion held for nearly two decades, that consensus has recently vanished. This section showcases and evaluates the merits of these somewhat fragmented views on territorial sovereignty in cyberspace.

In 1999, the Office of General Counsel of the U.S. Department of Defense issued an assessment of international legal issues raised by the Department's increasing resort to information operations, including cyber operations.[254] A ground-breaking study, the assessment surveyed an extraordinarily broad range of international law disciplines, including the law of war, space law, communications law, and other peacetime regimes regulating relations between States.[255] Although no section of the assessment addresses territorial sovereignty exclusively or comprehensively, the subject pervades the entire work. While it reserves judgment on many doctrinal details, the assessment repeatedly characterizes sovereign-

[252] Eli Lauterpacht, *Sovereignty—Myth or Reality?*, 73 INT'L AFF. 137, 139–40 (1997) (characterizing territorial aspects of sovereignty as clear and involving comparatively little difficulty in comparison with other aspects).

[253] *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); Michael N. Schmitt & Sean Watts, *State* Opinio Juris *and International Humanitarian Law Pluralism*, 91 INT'L L. STUD. 171, 174 (2015) (noting and critiquing significantly reduced State expressions of international law opinions).

[254] *See* Office of Gen. Counsel, Dep't of Def., An Assessment of International Legal Issues in Information Operations (1999).

[255] *Id.* at i.

ty not only as a recurring theme of international law but also as a rule of conduct with potential to limit State operations in cyberspace.[256]

The assessment's first observations concerning territorial sovereignty survey the concept broadly. The assessment's characterizations of territorial sovereignty emphasize the independence and exclusivity attendant in history and practice. Acknowledging the contextual nature of sovereignty, the assessment contrasts State treatment of the subject in space law with that of air law, two regimes of international law developed in response to novel domains of international relations. The assessment notes that while overflights of air space are "regarded as a serious violation of sovereignty and territorial integrity," orbits in outer space above territorial boundaries are not.[257] The assessment does not set out to explain the difference.[258] However, it in no way calls into question the general normative character of territorial sovereignty as a rule of conduct. Instead, the assessment surmises that outer space was regarded by States as "beyond the territorial claims of any nation."[259]

Expressing similar support for a rule of conduct related to territorial sovereignty, the assessment cites the International Court of Justice *Corfu Channel Case*.[260] The assessment relates the Court's conclusion that British warships' entry into Albanian waters "constituted a violation of Albania's territorial sovereignty."[261] The assessment concludes that the judgment supports "recognition of a general international law of trespass" but quickly notes that remedies for such breaches are limited and may simply amount to a declaration of wrongfulness.[262] The important point, however, is that the assessment clearly expresses the guarantee of exclusivity, the duty to refrain from violations, and the unlawful character of breaches of territorial integrity.

After significant attention to the question whether cyber operations could amount to uses of force or armed attacks under the UN Charter regimes, the assessment briefly and presciently considers the legal signifi-

[256] *Id.* at 2, 19–20.

[257] *Id.* at 2.

[258] *Id.* The lack of sovereignty in outer space orbit presumably flows from the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, art. 2, *opened for signature* Jan. 27, 1967, 18 U.S.T. 2410, T.I.A.S. No. 6347, 610 U.N.T.S. 205 (entered into force Oct. 10, 1967). Furthermore, no formal record of any State objecting to being over-flown by another State's satellite exists, thus there appears to be no persistent objectors to the lack of sovereignty in space orbits in general. FRANCIS LYALL & PAUL B. LARSEN, SPACE LAW: A TREATISE 161 (2009). Some equatorial States asserted rights over geostationary orbits above their territories, but no spacefaring State has accepted or respected this claim. *Id.* at 255.

[259] Office of Gen. Counsel, *supra* note 254, at 2.

[260] *Id.* at 16–17.

[261] *Id.* at 16.

[262] *Id.* at 17.

cance of unauthorized intrusions into another State's cyber infrastructure. The assessment unequivocally supports resort to self-help to expel or counter such intrusions. Turning to the legal characterization of such an event, the assessment observes,

> An unauthorized electronic intrusion into another nation's computer systems may very well end up being regarded as a violation of the victim's sovereignty. It may even be regarded as equivalent to a physical trespass into a nation's territory, but such issues have yet to be addressed in the international community. Furthermore, the act of obtaining unauthorized access to a nation's computer system creates a vulnerability, since the intruder will have had access to the information in the system and he may have been able to corrupt data or degrade the operating system. Accordingly, the discovery that an intrusion has occurred may call into question the reliability of the data and the operating system and thus reduce its utility. If an unauthorized computer intrusion can be reliably characterized as intentional and it can be attributed to the agents of another nation, the victim nation will at least have the right to protest, probably with some confidence of obtaining a sympathetic hearing in the world community.[263]

While the assessment appears to reserve final judgment on whether all nonconsensual cyber intrusions amount to violations of sovereignty, it offers compelling arguments in favor of such a conclusion. Support for resort to self-help suggests support for a conclusion that unauthorized cyber intrusions may constitute the sorts of unlawful activities giving rise to international law counter-measures. More significantly, the quoted passage again offers clear support for a general rule of conduct prohibiting nonconsensual cyber interferences.

The 1999 assessment stood for nearly two decades as the most comprehensive and authoritative U.S. statement on how international law applies to cyber operations. Although several of its passages suggest that legal analysis and doctrine would mature as the U.S. gained experience with operating in cyberspace, the U.S. did not offer a substantial update to or replacement of the assessment. Public statements, such as a 2010 State Department Legal Adviser's remarks, intervened but paled in terms of breadth and depth of analysis and cannot be regarded as a replacement of the 1999 assessment in any sense.[264] The assessment is a rare example of a State undertaking and expressing publicly an early, deliberate, and thorough evaluation of international law in an emergent area of international relations. Meanwhile, private efforts to identify the legal obligations applicable to cyberspace proliferated quickly.

---

[263] *Id.* at 19–20.

[264] DIGEST OF THE UNITED STATES PRACTICE IN INTERNATIONAL LAW, *supra* note 19, at 594–96.

The earliest private commentators to consider the question of non-consensual cyber intrusions concluded easily that territorial sovereignty constitutes a rule of conduct applicable to cyberspace. Taking up the cyber questions left open by the 1999 legal assessment, two early commentators concluded that even low-intensity cyber interference with the integrity or exclusivity of cyber infrastructure amounts to an unlawful violation of sovereignty.[265] Since these early opinions, others have taken up the question and confirmed the general proposition but with somewhat more circumspect conclusions.

A leading effort in this respect is *The Tallinn Manual 2.0 on International Law Applicable to Cyber Operations* (the *Manual*).[266] Sponsored and produced under the auspices of the North Atlantic Treaty Organization's Cooperative Cyber Defence Centre of Excellence, the *Manual* reflects the personal assessments of a group of international law specialists drawn from a wide variety of regions and legal traditions.[267] Like the 1999 DoD assessment, the *Manual* addresses an extraordinarily broad range of international law subjects including many of the peacetime regimes of public international law. Also, like the assessment, sovereignty in cyberspace is among the first subjects addressed.

Four rules and their associated commentaries express the *Manual*'s views on sovereignty.[268] The first three sovereignty rules address, respectively, general application of sovereignty to cyberspace,[269] exercises of internal sovereignty over cyber activity and infrastructure,[270] and exercises

[265] Benedikt Pirker, *Territorial Sovereignty and Integrity and the Challenges of Cyberspace*, *in* PEACETIME REGIME FOR STATE ACTIVITIES IN CYBERSPACE 199–203 (Katharina Ziolkowski ed., 2013); Wolff Heintschel von Heinegg, *Legal Implications of Territorial Sovereignty in Cyberspace*, *in* FOURTH INTERNATIONAL CONFERENCE ON CYBER CONFLICT 11 (C. Czosseck et al. eds., 2012) (observing "any activity attributable to another State, e.g. because it constitutes an exercise of that State's jurisdiction, is to be considered a violation of the sovereignty of the territorial State").

[266] TALLINN MANUAL 2.0 ON INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (Michael N. Schmitt ed., 2017). The *Tallinn Manual 2.0* is an expansion of a previous legal manual, the *Tallinn Manual on International Law Applicable to Cyber Warfare*, that had addressed legal considerations arising in cyber operations related to uses of force and armed conflict. *See* TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt ed., 2013). Professor Watts, one of the authors of this Article, was a member of the international group of experts that authored the *Manual*.

[267] *See* TALLINN MANUAL 2.0, *supra* note 266, at xxvi–xxvii.

[268] *Id.* at 11, 13, 16, 17 (reflecting the consensus of the authors while commentaries develop practical applications of rules and express the various opinions of the authors, including majority and minority views, on rule interpretation and other issues).

[269] TALLINN MANUAL 2.0, *supra* note 266, at 11.

[270] *Id.* at 13.

of external sovereignty over the same.[271] These rules recognize sovereignty as "a foundational principle of international law."[272]

In addition to traditional sources, the *Manual* cites a pair of recent reports from a United Nations-convened Group of Government Experts (GGE) to support application of sovereignty to cyberspace.[273] In the 2013 and 2015 meetings, the GGE, comprised respectively of fifteen[274] and twenty[275] States' representatives including each of the permanent members of the UN Security Council, confirmed, "[i]nternational law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT [information and communications technologies] environment."[276] The 2013 report observed with respect to sovereignty, "State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory."[277]

An earlier UN GGE report produced in 2010 did not include a clear conclusion that international law is applicable to cyberspace.[278] Accounts of the 2010 process indicate China and Russia withheld consent from any conclusion that international law applied fully.[279] The 2010 Report merely recommended dialogue to develop cyber-specific "norms" and to increase cooperation and "[c]onfidence-building . . . measures" between States.[280] Against this backdrop of initial reluctance by two major powers to concede international regulation, the 2013 and 2015 conclusions take on added weight.

---

[271] *Id.* at 16.

[272] *Id.* at 11.

[273] *Id.* at 11 n.4.

[274] Members of the 2013 UN GGE included Argentina, Australia, Belarus, Canada, China, Egypt, Estonia, France, Germany, India, Indonesia, Japan, the Russian Federation, the United Kingdom of Great Britain and Northern Ireland, and the United States of America. U.N. Secretary-General, *Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, at 12–13, U.N. Doc. A/68/98 (June 24, 2013).

[275] Members of the 2015 UN GGE included Belarus, Brazil, China, Colombia, Egypt, Estonia, France, Germany, Ghana, Israel, Japan, Kenya, Malaysia, Mexico, Pakistan, the Republic of Korea, the Russian Federation, Spain, the United Kingdom of Great Britain and Northern Ireland, and the United States of America. U.N. Doc. A/70/174, *supra* note 19, at ¶¶ 15–17.

[276] U.N. Doc. A/68/98, *supra* note 274, at ¶ 19.

[277] *Id.* at ¶ 20.

[278] U.N. Secretary General, *Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, at 4, U.N. Doc. A/65/201 (July 30, 2010).

[279] *See generally,* Eichensehr, *supra* note 11, at 362.

[280] U.N. Doc. A/65/201, *supra* note 278, at ¶ 18.

The *Manual* summarizes its understanding of sovereignty in cyberspace when it observes that a State's resort to cyberinfrastructure and connection to the Internet or any other outlet of cyberspace is not "a waiver of its sovereignty."[281] It concludes that sovereignty relates to each aspect of cyberspace—the physical, logical, and social layers.[282] The infrastructure, the code, and the users that comprise cyberspace are each in some way encompassed by State sovereignty. The *Manual* observes that most often territorial presence gives rise to the rights and obligations attendant to sovereignty. Thus servers, cables, routers, and processors present on a State's territory are associated with its sovereignty like other physical property.[283] Similarly, data and programs can be conceived as residing on infrastructure which has territorial presence and, therefore protection.[284] And finally, persons conducting activities in cyberspace—programmers, technicians, and computer engineers—are generally subject to the sovereignty of the territorial State in which they are located.

While the *Manual* maintains consensus on issues of applicability, questions regarding implementation of the law in cyberspace frequently break consensus. For instance, commentary presents split opinions on extraterritorial expectations and exercises of sovereignty in cyberspace. A small number of contributors extend their view of State sovereignty to national infrastructure and data stored abroad as well as to nationals located in another State's territory.[285] Yet the prevailing view of the *Manual* limits the scope of sovereignty to territorial property and activities, apart from provisions made by specialized regimes of international law such as sovereign immunity.[286]

The preceding observations culminate in a rule of conduct for sovereignty. The rule states, "[a] State must not conduct cyber operations that violate the sovereignty of another State."[287] The rule's importance lies chiefly in its characterization of violations of sovereignty as internationally wrongful conduct. The rule's commentary is significant as an illustration of the range of cyber activities that run afoul of the independence and exclusivity associated with sovereignty.[288]

Like the 1999 DoD assessment before it, the *Manual* confronts gaps in State practice that complicate its legal conclusions. In these cases, it

[281] TALLINN MANUAL 2.0, *supra* note 266, at 12–13.

[282] *Id.* at 12, 14.

[283] *See* Yochai Benkler, *Constitutional Bounds of Database Protection: The Role of Judicial Review in the Creation and Definition of Private Rights in Information*, 15 BERKELEY TECH. L.J. 535, 562–63 (2000) (describing a physical layer of the information environment).

[284] *See id.* (describing a logical layer of the information environment).

[285] TALLINN MANUAL 2.0, *supra* note 266, at 15–16.

[286] *Id.* at 16.

[287] *Id.* at 17.

[288] *Id.* at 17–24.

resorts to a series of hypothetical examples to illustrate the relationship between cyber activities and the protection afforded by sovereignty—efforts to address mixed questions of law and fact.[289] In some cases, factual analogies to non-cyber examples facilitate the analysis. For instance, cyber operations involving physical intrusion by a State into another State's territory are unanimously regarded as violations of sovereignty.[290] To illustrate the point, the *Manual* relates the example of a State's agent physically entering foreign territory to introduce malware by inserting a USB storage device into cyber infrastructure present on that territory.[291] As victim of an internationally wrongful act, a State that suffered such an intrusion could resort to countermeasures as a means of self-help in response.

Not all cyber scenarios considered by the *Manual*, however, offer such helpful factual analogies. For instance, the commentary to Rule 4 presents split opinions concerning remote access cyber operations.[292] Many authors hesitate to conclude that introduction of code by electronic means amounted to a violation of sovereignty in every case.[293] Consequently, the *Manual* offers a wide range of views on the legal status of remote access operations. Some contributors express a maximally protective approach. These authors conclude that even slight alteration of a system, for example installation of a backdoor or other access mechanism or emplacement of code such as malware, is sufficient to establish a violation of sovereignty.[294] These contributors ground their view in the object and purpose of sovereignty, namely a legal guarantee of "full control over access to and activities on their territory."[295]

Other contributors are unable to conclude that mere nonconsensual access violates sovereignty. These authors adopt an effects-based approach to remote access cyber operations. For many of these authors remote access *simpliciter* is not meaningfully intrusive or does not sufficiently compromise independence and exclusivity to conclude a violation of sovereignty is involved.[296] However, remote access operations that result in physical damage, loss of functionality, or compromise of inherently governmental functions amount to violations of sovereignty in these authors' view.[297]

[289] *Id.* at 14–15.
[290] *Id.* at 14.
[291] *Id.* at 19.
[292] *Id.* at 19–20.
[293] *Id.* at 20–21.
[294] *Id.* at 21.
[295] *Id.*
[296] *Id.* at 20–21.
[297] *Id.*

Still other authors do not consider remote access cyber operations as categorical violations of sovereignty, even when resulting in physical damage or loss of functionality or compromise of governmental functions.[298] These authors describe a more holistic approach to evaluating a violation of sovereignty, wherein damage or loss of functionality are but one of many considerations.[299]

A further form of effect-based analysis considers the extent to which a cyber activity interferes with a State's governmental functions. Tracing sovereignty to a legal right to govern exclusively, this view concludes that cyber operations by States that disrupt or impede "inherently governmental functions" amount to violations of sovereignty.[300] This view does not measure effects in cyber terms—by integrity, functionality, or damage to cyber infrastructure—but rather by governance. The *Manual* identifies essential social services, elections, law enforcement, national defense activities, and diplomacy as consensus examples of inherently governmental functions.[301] While State interference with other States' governmental functions recalls the principle of non-intervention, the *Manual* clarifies that where an intervention requires coercion, a mere violation of sovereignty does not.[302] Further, the *Manual* observes that while the concept of *domaine reserve* associated with intervention—matters committed exclusively to the prerogative of a State—overlaps with inherently governmental affairs, the concepts are not identical.[303]

The *Manual* presents split conclusions on the question of cyber operations conducted as part of peacetime espionage. A majority expresses the view that the purpose of information gathering associated with espionage does not excuse or exempt the physical intrusion from constituting a violation of sovereignty.[304] In this view, although espionage is not itself proscribed by international law, the constitutive acts of espionage, such as a non-consensual physical intrusion may be.[305] A small number of the authors, however, considers State practice to support a narrow exception that permits what might otherwise amount to a violation of sovereignty when carried out as part of espionage.[306]

Of course, the *Manual* concedes that sovereignty is not absolute. International lawyers as well as international relations specialists characterize States as surrendering sovereignty to international regulatory regimes

[298] *Id.* at 20.
[299] *Id.*
[300] *Id.* at 22.
[301] *Id.*
[302] *Id.* at 24.
[303] *Id.*
[304] *Id.* at 20.
[305] *Id.*
[306] *Id.* at 19.

and institutions.[307] The *Manual* emphasizes repeatedly that States have made exceptions to their independence by adopting international legal regimes that limit their freedom of action or that grant other States access to their territory, such as the regimes applicable to air and seas.[308] Still, the *Manual* declines to apply such exceptions to cyberspace, applying instead the baseline rule of territorial sovereignty from general international law.[309]

In sum, the *Manual* offers a highly orthodox understanding of sovereignty in cyberspace that is fully substantive in nature. Relying heavily on recent State expressions of support for application of international law to cyberspace, the *Manual*, like the 1999 DoD assessment, identifies sovereignty as both a source of law and a rule of conduct itself. In this view, States do not waive sovereignty in any significant respect by resorting to cyber means or by hosting cyber infrastructure on their territory. Nor does development of State cyber capabilities that make accessible other States' infrastructures excuse the territorial interferences involved in remote access operations. Limited to descriptive work and careful to account for States' limited, publicly-available legal conclusions, the *Manual*'s conclusions with respect to territorial sovereignty in cyberspace would not seem at first blush to be a significant or likely point of contention. Experience soon proved otherwise.

On January 19, 2017, the last day of President Barak Obama's Administration, the outgoing General Counsel of the U.S. Department of Defense issued to U.S. Combatant Commands a memorandum titled "International Law Framework for Employing Cyber Capabilities in Military Operations" ("the memo").[310] Like its 1999 predecessor, the memo addresses a broad range of international legal issues associated with military operations in cyberspace. The memo is significant not merely for its timing and its guidance on a pressing operational issue but also for its clear rejection of the outlook on sovereignty captured by the *Tallinn Manual 2.0*.

Overall, the memo offers a greatly constrained view of the legal effect of sovereignty. At its essence, the memo expresses territorial sovereignty as an organizing principle of international law, foundational, yet lacking independent or substantive legal effect.[311] In many respects, the

[307] Heller & Sofaer, *supra* note 196, at 25. In fact, Heller and Sofaer reject consent to international law as a surrender of sovereignty, preferring to regard treaty ratification and accession and consent to be bound by custom as "exercise[s]" of sovereignty. *Id.* at 45.

[308] TALLINN MANUAL 2.0, *supra* note 266, at 13, 15–17.

[309] *Id.* at 11.

[310] 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).

[311] *Id.* at 4.

memo portrays territorial sovereignty in cyberspace as nominal, concluding States are sovereigns over cyber infrastructure in name only.[312] Accordingly, its legal conclusions legitimize an extraordinarily broad range of intrusive cyber operations and thus it merits careful attention.

Much of the memo's general guidance replicates or elaborates only slightly on existing legal doctrine. For instance, the memo confirms that military cyber operations must comply with international law including the law of war.[313] Department of Defense lawyers received identical guidance in the *2015 Department of Defense Law of War Manual*.[314] The memo also recites the principle of non-intervention.[315] It notes that precisely how the non-intervention principle operates in cyberspace is still unclear but confirms its relevance to cyber operations and predicts that State practice will refine how it applies over time.[316] Neither of these observations is unprecedented or unexpected.

However, shortly after these routine observations the memo takes a provocative turn when it observes, "[m]ilitary 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 . . . ."[317] The memo does not go so far as to conclude that such cyber operations take place in a lawless zone. It concludes that the domestic law of the State in which a cyber operation takes place or where its effects manifest may be relevant.[318] But in the realm of low-intensity cyber operations—operations short of the use of force or prohibited intervention—the memo identifies no generally applicable international law restraints.[319]

The memo's direct treatment of territorial sovereignty begins with observations that align with widely-held understandings. It cautions that "[s]overeignty may impact the conduct of military cyber operations and requires careful legal analysis."[320] It formulates sovereignty as "a fundamental principle of international law."[321] And, like the *Manual*, the memo confirms that sovereignty features both internal and external aspects. Internal aspects of sovereignty capture the independence and exclusivity States enjoy in the control of their territory.[322] External sovereignty refers to States' relationships with one another, especially their equality and in-

[312] *Id.* at 3–4.
[313] *Id.* at 1.
[314] U.S. DEP'T OF DEF., LAW OF WAR MANUAL ¶ 16.2 (2015).
[315] Memorandum from Jennifer M. O'Connor, *supra* note 310, at 1–2.
[316] *Id.* at 2.
[317] *Id.* at 1.
[318] *Id.* at 2.
[319] *Id.*
[320] *Id.* at 3.
[321] *Id.*
[322] *Id.*

dependence from other States and their general freedom from restraints, citing the familiar *Lotus* principle especially for the latter proposition.[323]

Also like the *Manual*, the memo emphasizes that sovereignty is not absolute. It characterizes international law as a series of limitations on sovereignty.[324] In this respect, it cites the United Nations Charter, the right of self-defense, the law of war, and international human rights law.[325] Each of these regimes in its own way replaces the sovereignty-based *Lotus* presumption in favor of freedom of action with meaningful limits on State action.[326]

But in its concluding paragraphs, the memo concludes that sovereignty is not itself an independent restraint on State action. Although it acknowledges sovereignty as a foundational principle that supports and informs *other* rules that restrain State conduct, the memo concludes, "there is insufficient evidence of state practice or *opinio juris* to support the assertion that sovereignty acts as a binding legal norm, proscribing cyber actions by one State that result in effects occurring on the infrastructure located in another State, or that are manifest in another State."[327] Adding operational context, the memo opines that sovereignty does not prevent States from undertaking a cyber operation against cyber infrastructure used by terrorists in other States even without the consent of the latter State so long as the operation is short of the use of force or intervention.[328] Though not explicit, the connection to nonconsensual, remote access cyber operations such as Glowing Symphony is easily implied.

The memo observes that States suffering unwanted cyber intrusions below the threshold of intervention are not without remedies. The memo recites diplomatic exchanges and retorsion as options available to such States.[329] Protests and *démarches* are commonplace means of diplomacy by which States express disapproval.[330] Retorsion, unfriendly though not unlawful acts by States undertaken in response to unwelcome or even unlawful acts by other States, also seem to represent a warranted response according to the memo.[331] Examples of retorsion include withdrawal of favorable, though not legally compelled treatment such as advantageous

[323] *Id.*

[324] *Id.* at 1.

[325] *Id.* at 3.

[326] S.S. Lotus (Fr. v. Turk.), Judgment, 1927 P.C.I.J. (ser. A) No. 10, 7 (Sept. 7).

[327] Memorandum from Jennifer M. O'Connor, *supra* note 310, at 3.

[328] *Id.* at 4.

[329] *Id.* at 2.

[330] *Id.*

[331] U.N. INT'L LAW COMM'N, *Draft Articles on State Responsibility of States for Internationally Wrongful Acts, with Commentaries*, *in* 2 Y.B. OF THE INT'L L. COMMISSION 128 (2001); Memorandum from Jennifer M. O'Connor, *supra* note 310, at 2.

trade practices.[332] The usual purpose of retorsion is to induce an offending State to cease unwanted conduct. But because acts undertaken as retorsion may not involve unlawful conduct, the memo's analysis seems to preclude resort to countermeasures in response to noncoercive but nonconsensual State cyber intrusions. Countermeasures involve self-help measures that involve otherwise unlawful conduct by a victim State. Thus, under the DoD guidance, a State could not resort to an act amounting to intervention in response to a cyber operation that did not itself amount to intervention or use of force.

In sum, the memo confirms the applicability of international law to States' cyber operations, confirms the prohibitions on the use of force and intervention as meaningful limits relevant to cyber operations, but concludes that these limits reflect something of a floor of internationally wrongful conduct in cyberspace. While the memo identifies territorial sovereignty as the source of a right on the part of States to control territory to the exclusion of other States (internal sovereignty), it does not deduce an obligation on the part of a State to consider itself legally excluded from nonconsensual operations within the territory of another State. According to the memo, State cyber operations that interfere with the integrity of cyber infrastructure without the consent of a territorial State, that intrude into such cyber infrastructure, or perhaps even that alter such systems or their data without effects amounting to force or intervention do not amount to internationally wrongful acts.[333] Such operations and their effects reflect accepted practice between States in the cyber context.

It is unclear what precisely provoked the memo. Its release not long after revelation of Operation Glowing Symphony raises the possibility it was produced to instruct DoD components of the legal analysis that supported the operation. DoD lawyers familiar with the 1999 DoD assessment might have found it difficult to reconcile Glowing Symphony and other reports of invasive remote access cyber operations. Thus, the memo may also have been intended to notify the DoD community of U.S. resolve to continue such operations and to signal support for proposal by subordinate commands to plan for and execute similar operations. It is also possible the memo was prepared in advance of publication of the *Manual* to caution DoD lawyers. Drafts of the *Manual*, including the chapter on sovereignty, were circulated widely to governments, thus it is likely the memo's authors were aware of the *Manual*'s position.[334]

It is also unclear whether the memo reflects views of the U.S. government outside the Department of Defense. Department of State and Department of Justice views seem to be especially important in the inter-

[332] *See* 2 Y.B. OF THE INT'L L. COMMISSION, *supra* note 331, at 128.

[333] Memorandum from Jennifer M. O'Connor, *supra* note 310, at 2–3.

[334] Schmitt & Vihul, *supra* note 215, at 1649.

connected and fast-moving realm of cyberspace. Thus, the memo leaves U.S. legal advisors, allies, and adversaries in an uncertain position with respect to predicting future U.S. conduct in cyberspace, especially the extent to which it will regard nonconsensual intrusions as justified and how the U.S. will react to nonconsensual intrusions into its own territorial cyber infrastructure. A clear-minded adjudication of the contrasting positions of the 1999 DoD assessment and the *Manual* on the one hand and the 2017 memo on the other is essential.

V. BASELINE TERRITORIAL SOVEREIGNTY

It would be easy to minimize the significance of the disagreement between the memo and the *Manual* as a minor difference of interpretation in an evolving area of law in a dynamic realm of State relations. After all, the *Manual* itself presents contrasting views on exactly these sorts of questions. But it is important to realize that disagreement between the *Manual* and the memo is far more significant. They disagree on a fundamental question of law. Namely, they disagree whether violations of sovereignty are internationally wrongful acts. There is common ground between the two sources in that both regard sovereignty as a principle of international law.[335] Moreover, both agree that principles of international law apply to cyberspace. However, where the *Manual* concludes that violations of principles of international law are wrongful, the memo distinguishes principles of law from rules of conduct, limiting wrongfulness to breaches of the latter. On balance, the *Manual* offers the more persuasive view.

It is true that States have reduced many regimes of international law to clear treaty law and offered refined, clearly-stated rules of conduct. There may be a view that principles are not themselves rules of conduct but rather, form the bases of such rules. Under this view, principles of international law are not viewed as self-executing. Like the dualist view of international law in domestic systems, principles might be understood to

[335] Principles of international law should be distinguished from general principles of law or, as termed by the Statute of the International Court of Justice, "general principles of law recognized by civilized nations." Statute of the International Court of Justice, *supra* note 111, at art. 38(1)(c). The former refers to regulatory provisions of a broad character that form part of the corpus of public international law itself, whereas the latter are not peculiar to the public international legal system but rather form part of all legal systems, including municipal regimes and private law. *See* Cherif Bassiouni, *A Functional Approach to "General Principles of International Law,"* 11 MICH. J. INT'L L. 768, 770–71 (1990); Rudolf B. Schlesinger, *Research on the General Principles of Law Recognized by Civilized Nations*, 51 AM. J. INT'L L. 734, 739 (1957). Professor Bassiouni identifies four functions of general principles of law including: a source of interpretation; a means for developing new norms; a supplemental source to international law; and a modifier of international law. Bassiouni, *supra* note 335, at 775–76.

require implementing legislation in the form of international rules.[336] But failure to reduce rules to treaty form and even failure to refine principles to specifically proscribed conduct do not prevent the conclusion that acts inconsistent with such principles amount to wrongful behavior. In fact, some treaties give full legal effect to international law principles, authorizing their application to adjudications.[337]

And it is unlikely in this respect that a principle-rule distinction is either firmly established or particularly useful in practice. Professor Crawford, for instance, is skeptical of rigid distinctions between principles and rules.[338] He observes, "[t]he rubric 'general principles of international law' may alternatively refer to rules of customary international law, to general principles of law as in Article 38(1)(c) [of the Statute of the International Court of Justice], or to certain logical propositions underlying judicial reasoning on the basis of existing international law."[339] Others, more accepting of a distinction, simply maintain that like rules, principles of international law can entail rights and obligations.[340] Just as violations of the *ius in bello* principle of distinction are wrongful on the part of States, it is possible to regard violation of the principle of sovereignty as wrongful. It is true that the *ius-in-bello* principle of distinction found refined expression in twentieth-century treaties more clearly expressed as rules. But this evolution has not necessarily prevented violation of the preexisting principle itself from constituting wrongful conduct during armed conflict.[341]

The character of the principle of non-intervention further illustrates the point. No widely-ratified treaty, including the UN Charter, codifies that principle. Yet few States reject its status as binding law and the International Court of Justice has confirmed as much. Admittedly, in a brief to the International Court of Justice during the Nicaragua case, the U.S. argued momentarily that Article 2(4) of the UN Charter reflected the floor of internationally wrongful interferences between States.[342] But the Court

[336] DEP'T OF THE ARMY, LAW OF PEACE 1 (1979).

[337] *See, e.g.*, Rome Statute of the International Criminal Court, art. 21(1)(b), *opened for signature* July 17 1998, 2187 U.N.T.S. 3 (entered into force July 1, 2002). Article 21 of the Rome Statute provides in relevant part: "The Court shall apply: . . . applicable treaties and the principles and rules of international law, including the established principles of the international law of armed conflict . . . ." *Id.* at art. 21(1).

[338] JAMES CRAWFORD, BROWNLIE'S PRINCIPLES OF INTERNATIONAL LAW 37 (8th ed. 2012).

[339] *Id.*

[340] Rüdiger Wolfrum, *Sources of International Law*, *in* MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW 6 (Rüdiger Wolfrum ed., 2011).

[341] *See e.g* Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. Rep. 226, ¶ 30 (July 8) (addressing law-of-war principles of necessity and proportionality).

[342] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep. 14, ¶ 174 (June 27) (rejecting U.S. arguments that lower

abruptly dismissed the idea that the UN Charter reflects the complete universe of internationally wrongful intrusions.[343] The Court also rejected the argument that codification of a rule necessarily precludes wrongfulness of any conduct below, short of, or not meeting the legal elements of that rule.[344]

A second basis to reject the memo's position concerns States' now widespread agreement that public international law applies to cyberspace. It is true, Russia and China fitfully offered a variation of the "cyber as sovereign" view at various stages of the ongoing United Nations Group of Government Experts (UN GGE) proceedings.[345] A more emphatic characterization of their view might be that of "cyber as legal void." During the UN GGE proceedings, Russia and China suggested that cyberspace presents circumstances too different from preexisting interactions between States to concede application of the legacy rules of international law.[346] Each contended its cyber operations might be free from existing legal restraints.[347] There were, however, doubts concerning the authenticity of the Russian and Chinese view. Skepticism formed whether this view reflected considered legal analysis. Some preferred to brand their "cyber as legal void" position as a negotiating position developed specifically for the UN GGE process—a position they were willing to abandon in exchange for more robust approval of authoritarian control over domestic cyber infrastructure. Whatever the truth, Russia and China have both abandoned the public international law void view in the last two rounds

forms of interference had been subsumed by the UN Charter prohibition on the threat or use of force).

[343] *Id.* at ¶ 175.

[344] *Id.*

[345] *See* Eichensehr, *supra* note 11, at 326–27 (terming a regulatory approach to cyber that rejects traditional, Westphalian governance as "cyber as sovereign").

[346] Eneken Tikk-Ringas, *Developments in the Field of Information and Telecommunication in the Context of International Security: Work of the UN First Committee 1998-2012*, ICT4PEACE PUBLISHING pp. 5–6 (2012), available at http://www.ict4peace.org/wp-content/uploads/2012/08/Eneken-GGE-2012-Brief.pdf.

[347] *See* Alex Grigsby, *Overview of Cyber Diplomatic Initiatives*, *in* BRIEFINGS TO THE GLOBAL COMMISSION OF THE STABILITY OF CYBERSPACE FOR THE FULL COMMISSION MEETING, NEW DELHI, at 14 (Nov. 2017), available at https://cyberstability.org/wp-content/uploads/2017/12/GCSC-Briefings-from-the-Research-Advisory-Group_New-Delhi-2017.pdf, ("China takes the position that there are no 'general international rules in cyberspace that . . . govern the behavior' of states.") (omission in original); *Eneken Tikk-Ringas, International Cyber Norms Dialogue as an Exercise of Normative Power*, GEORGETOWN J. INT'L AFFAIRS (2017), available at http://ict4peace.org/wp-content/uploads/2017/02/Tikk-Normative-Power.pdf ("During the 15-year GGE process, Russia has remained skeptical about the efficacy of international law in cyberspace, taking the view that not all legal norms 'automatically' extend to interstate relations in the field of ICTs and relevant criteria need to be specified.").

of UN GGE statements.[348] The extent to which they will abide by the current position in practice is another question altogether on which there are compelling opinions.

At first blush, States' concession that international law applies to cyberspace may seem merely prosaic or even trivial. But it is crucial—especially on matters of legal interpretation and application. It is an essential signal of the starting point or baseline for legal evaluation of States' cyber operations. By consenting to the operation of international law in the domain of cyberspace (if domain-by-domain consent by States was ever really required), States accept as binding a massive and growing collection of rules of conduct as relevant. Existing general international law then forms the legal baseline of limits on cyber conduct by States. Describing what this baseline looks like and how it operates in practical terms is precisely what the *Manual* set out to do.

With respect to the baseline rule of territorial sovereignty, it is easy to conclude that international law guarantees a degree of independence and exclusivity to States. It is also clear that independence from outside interference and exclusivity as to control are never more clearly guaranteed by international law than with respect to a State's own territory and property thereon. The previously-mentioned *Island of Palmas* arbitration and the *Corfu Channel* judgments were important supplemental sources of this understanding, but only as expressions of what seemed clearly to be State views on what sovereignty meant in practice. It is true that neither proceeding awarded significant relief based on violations of sovereignty nor produced significant analysis of sovereignty itself (nor did the *Nicaragua* Court for that matter). But this was not because of doubts as to the wrongfulness of violations, rather it is attributable to the minimal damages caused and, especially in the cases of *Corfu Channel* and *Nicaragua*, the attention these tribunals devoted to more specific rules and regimes of international law (i.e. a duty to warn of mines and use of force, respectively).

If one accepts that sovereignty is an aspect of the existing international law that States have conceded applies to cyberspace and if one accepts that sovereignty, at minimum, protects States from interference with the independent and exclusive control of their territory by other States, the conclusion that interferences with cyber infrastructure violate sovereignty is not an especially difficult one to reach. Exclusion of external interference has been a foundation of the Westphalian system at least since the seventeenth century.[349] A rough syllogism helps illustrate the

[348] Michael Schmitt & Luis Vihul, *International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms*, JUST SECURITY (June 30, 2017), https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/.

[349] Samantha Besson, *Sovereignty, in* MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW ¶ 13 (Rüdiger Wolfrum ed., 2011).

point. A major premise would state, 'sovereignty prohibits interference with States' independent and exclusive management of territorial property.' A minor premise might state, 'cyber infrastructure is property located on State territory.' A conclusion follows, 'cyber operations that interfere with a sovereign's independent and exclusive control of territorial cyber infrastructure are prohibited.' Although the syllogism's cyber context involves still somewhat novel circumstances, the legal baseline it employs and its factual assumptions seem entirely reasonable.

Returning to the UN GGE statements, application of international law to cyberspace involves applying a clear norm of integrity with respect to territorial property to cyber infrastructure. The syllogism leaves unanswered the mixed question of fact and law involving what exactly constitutes an interference in cyber context. But this ambiguity does not undermine the conclusion of law that violations of sovereignty involving cyber infrastructure and cyberspace are wrongful.

To be sure, territorial sovereignty has never been an absolute restraint on foreign interference.[350] As related above, State and academic commentary on sovereignty have emphasized its indeterminate status and contextual meaning in international law.[351] But because of the fundamental character of territorial sovereignty, exceptions to its attendant State duties should not be taken lightly or be haphazardly formed. Great caution must be exercised in identifying or exercising them. The maritime innocent passage and aerial transit exceptions to sovereignty cannot be applied to cyberspace by simple analogy. First, the two regimes are very different. One allows nonthreatening transit without advance notice or coordination. The other requires special authorization. Second, both are codified by treaties agreed upon by States involving years of careful negotiation.

Thus, the default or baseline rule of sovereignty remains one of inviolability. Territory and property located on a State's territory, not subject to a firmly-established exception, remain legally protected from molestation by other States. Operational logic—States' pressing need to remain competitive and secure in the domain of cyberspace—may have supported a conclusion on the part of the 2017 U.S. DoD memo authors that cyber infrastructure ought to be subject to a regime of exceptions like that applicable to territorial sea, a cyber variation of innocent passage if one prefers.[352] But legal logic and analysis do not support such a conclusion at present. In the absence of a fully-developed *lex specialis* of cyber-

[350] *See* Barr, *supra* note 10, at 163.

[351] Heller & Sofaer, *supra* note 196, at 25–28; Onuf, *supra* note 7, at 428.

[352] A defense of the 2017 DoD position and arguments against sovereignty as a rule of international law can be found in Gary P. Corn & Robert Taylor, *Sovereignty in the Age of Cyber*, 111 AJIL UNBOUND 207, 208 (2017); Robert S. Taylor, *Cyber, Sovereignty, and North Korea–And the Risk of Inaction*, JUST SECURITY (Oct. 31, 2017), https://www.justsecurity.org/46531/cyber-sovereignty-north-korea-risk-inaction/.

space like that applicable to seas, the legally correct conclusion with respect to sovereignty and cyberspace resorts to the baseline rule of sovereign inviolability.

Of course, the independence and exclusivity guaranteed by sovereignty are not absolute. Sovereignty has been limited by States in innumerable respects. The chief logical limit on sovereignty might derive from the fact of multiple sovereigns. Because States exercise sovereignty simultaneously with other States, the logical limit of a State's own sovereignty—where its sovereignty ends—is where another State's sovereignty begins. This notion of sovereign equality—the idea that no State's sovereignty is superior to that of any other State—is a fundamental, if sometimes theoretical, precept. Thus, even in the absence of an international system of rules of conduct, sovereignty itself would operate as at least a logical limit on the legitimate conduct of States.

A second, perhaps less esoteric and more tangible limit on sovereign independence and exclusivity is, of course, the international legal system. As a collection of prohibitions and limits on State conduct, international law supports a concept of ordered, rather than absolute, sovereignty. The treaty regimes most universally associated with rules of conduct and primary rules include elaborate exceptions to the baseline freedom of action attendant to sovereignty. Sovereignty might represent a "default law" in this respect. The *Lotus* decision and its underlying legal framework are an illustration of the mechanics of this system of positivist limits on ordered sovereignty. For example, where the *Lotus* framework and absolute sovereignty would permit arrest of diplomatic representatives present on a State's territory, the international legal system has clearly restrained sovereignty in this and many other respects.

But just as sovereign freedom of action is subject to exceptions in the form of international legal prohibitions, international law prohibitions themselves are subject to exceptions. That is, while sovereignty permits freedom of action and finely-wrought prohibitions developed by States in the form of international law restrain exercises of sovereignty by States, States have also afforded themselves exceptions that excuse what would otherwise be violations of international law prohibitions. For example, the U.N. Charter acknowledges the legal right of self-defense against uses of force and armed attacks.[353]

Thus, through centuries of practice and codification, States have developed an international legal regime that specifically clarifies and limits the meaning of sovereignty on the seas. Where sovereignty and the *Lotus* framework would initially suggest freedom of action on the seas, the law of the sea, in recognition of territorial sovereignty, restrains States' use of other States' territorial seas.

[353] U.N. Charter art. 2, ¶ 4; U.N. Charter art. 51.

To credit the DoD memo's position, recent experience is rife with State cyber practice inconsistent with respect to sovereignty. State cyber practice is brimming with examples of what the *Manual* would consider violations of sovereignty. However, it was not the prerogative of the authors to craft or to fabricate any sort of exception to or legal departure from the baseline rule of sovereignty based on such practice. In fact, in extensive consultations with States, none objected to the *Manual*'s formulation of sovereignty, none suggested such a departure was warranted, and none characterized State practice as inconsistent with the rule. In these circumstances, recognition of a cyber-specific exception to territorial exclusivity would have been recognition of a rationalization or *lex ferenda* rather than legislation by States, *lex lata*.

In truth, the legal significance of the fact of State intrusions into other States' cyber infrastructure is still unclear. A possible explanation is that States infringe cyber sovereignty because they think such acts are not prohibited by international law. But expressions of *opinio juris* to that effect are not prevalent. The memo appears to offer such a view on cyber sovereignty.[354] Some might regard the memo as a rare expression of *opinio juris*. But exactly what account should an international lawyer, an academic, a judge, or another State's operational legal advisor give the memorandum? It offers a thoroughly reasoned view and has the feeling of a binding directive from a senior government attorney to subordinate attorneys. But it is an isolated view of a single, though influential, State's agency. And it is not yet clear it even reflects the view of any U.S. government agency other than the Department of Defense. To be sure, it may in the future constitute an early stage of the sort of *opinio juris* that eventually gives rise to a new understanding of international law, but for now that conclusion seems dubious and premature.

There are other explanations for seemingly rampant State practice. For instance, it is possible that States conduct these intrusions and interferences simply because they think they won't be caught or held accountable. The notorious difficulty of attribution in cyberspace certainly reinforces the possibility. States seem to invest significant resources to cover their cyber tracks and States seem persistently to deny involvement in malicious cyber operations even long after the technical community purports to have definitively resolved attribution.

In a somewhat related sense, it is possible that States judge that such operations, to borrow a concept from contract law, amount to efficient breach. That is, perhaps States conclude frequently that the benefits of nonconsensual intrusions outweigh the costs. The reluctance of tribunals to award significant damages or reparations for simple breaches of sovereignty, as in the *Corfu Channel* case,[355] would support such logic. More

[354] Memorandum from Jennifer M. O'Connor, *supra* note 310, at 4.

[355] *See, e.g.*, Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. Rep. 4 (Apr. 9).

likely, both the minimal consequences of simple breaches of cyber sovereignty and the low likelihood of being caught—in other words the risk associated with intrusive cyber operations—is low enough to make them worth undertaking.

And admittedly, not all States complain when other States violate their cyber sovereignty. The United States, for instance, has remained conspicuously silent with respect to allegations of international wrongfulness following recent cyber breaches. But explanations other than lawfulness of those events are available. First, protest as to unlawfulness is not an element of wrongfulness. States need not allege wrongfulness publicly or with any level of intensity or vigor for State conduct to be wrongful. Second, although not a defense in criminal proceedings, the *tu quoque* retort may give some States, and especially cyber-active States like the U.S., pause with respect to alleging violations by other States.

Finally, the litany of State practice involving apparent cyber interferences should not be taken as the final word on State practice. A complete picture of State practice must surely account for forbearance as well as indulgence. Flaunting a catalog of intrusions as representative of State practice ignores the significant likelihood that States just as often, or perhaps more frequently, decline to interfere with other States' cyber infrastructure as they interfere with it. Such duels of accumulated State practice tend not to adequately account for negative practice, instances in which States decline to engage in or never even seriously entertain operations involving violations of sovereignty. Accordingly, and for the reasons offered above, State practice as evidence of law must be treated with great caution.

Until States develop a cyber-specific regime of exceptions to the baseline rule of sovereignty respecting territorial property, the best conclusion regarding interferences with independent and exclusive control of territorial cyber infrastructure is that they violate sovereignty and are internationally wrongful. A contrary conclusion would involve a lawmaking function reserved exclusively to the community of States. It would fly in the face of States' clear indication that international law applies to operations in cyberspace. It would have rendered essentially a nullity, the momentous conclusion that international law applies to cyberspace. Thus, conclusions with respect to most cyber-specific sovereignty exceptions are for now premature. But this could change.

A final consideration commending application of territorial sovereignty to cyberspace is consequentialist in nature. A world that does not prohibit violations of sovereignty not only renders the concept of sovereignty somewhat meaningless, it yields a dangerous and even Hobbesian world. One of the more effective passages of the *Manual* is the observation that connection to cyberspace is not a waiver of sovereignty.[356] The

[356] TALLINN MANUAL 2.0, *supra* note 266, at 12–13.

thought might be expanded to say resort to electronic media and cyber infrastructure is not a waiver of sovereignty. The fact that cyber infrastructure is vulnerable to interference by other States does not render such interference lawful, just as a porous territorial border does not render violations of that border lawful.

VI. CONCLUSION

If substantiated, reports of Operation Glowing Symphony stand as a compelling glimpse of the growing and daunting cyber capabilities of States, the contentious environment of international relations in cyberspace, and the extent to which longstanding norms against foreign interference are under growing pressure. As a testament to the gravity of this pressure, the current state of cyber relations led the highest placed legal authorities of the largest agency of the U.S. government to abandon a long-held position on the sanctity of territorial sovereignty.

Early in the life of cyberspace, States appreciated that such adjustments to norms of international law might be called for. In its 1999 legal assessment of international law in cyberspace, the U.S. Department of Defense observed,

> [W]e can make some educated guesses as to how the international legal system will respond to information operations, but the direction that response actually ends up taking may depend a great deal on the nature of the events that draw the nations' attention to the issue. If information operations techniques are seen as just another new technology that does not greatly threaten the nations' interests, no dramatic legal developments may occur. If they are seen as a revolutionary threat to the security of nations and the welfare of their citizens, it will be much more likely that efforts will be made to restrict or prohibit information operations by legal means.[357]

Given its revolutionary technical, strategic, economic, and political character, it is not unreasonable to expect cyberspace to exact comparably revolutionary changes to international law. In developments like the U.S. Department of Defense memo on territorial sovereignty, we may be witnessing the opening rounds of a struggle for the legal soul of cyberspace. Will cyberspace operate as a Hobbesian free-for-all where sovereignty exists only in a nominal sense? Or will the Grotian community of States survive with its imperfect, though foundational baseline guarantees of territorial integrity and exclusivity? While the latter view is promisingly, if vaguely and haltingly, evident in the work of the United Nations Group of Government Experts, Hobbesian tendencies have surfaced in State practice and have been seemingly memorialized in the memo. With its

[357] Dep't of Def., *supra* note 254, at 2.

low-entry costs, near-ubiquity, and potential to wreak anonymous havoc, cyberspace feels in many respects a Hobbesian domain.

But the history, purpose and fundamental character of territorial sovereignty make clear its role as an essential organizing concept of international relations and as a rule of conduct that has tamed destructive Hobbesian tendencies. To be sure, sovereignty has not been a static concept.[358] Despite its fundamental character, sovereignty has been "a vague formula, with shifting components and uses."[359] Conventional rules have been ignored in some contexts, new rules have been written for specialized domains of international relations.[360] And entire reconceptualizations, such as the proposal for a "new sovereignty," have been proposed (and seemingly rejected) as recently as the late twentieth century.[361] But absent clear and rigorous adoption of such innovations, the historical baseline of territorial sovereignty, including a prohibition on territorial interferences, persists as important guarantor of peaceful relations between States.

The U.S. Department of Defense should act quickly to reaffirm its commitment to baseline Westphalian norms of territorial sovereignty in cyberspace while crafting, through accepted means of international legal development, a nuanced and effective doctrine of territorial sovereignty in cyberspace. A sound approach would acknowledge the binding legal character of territorial sovereignty as a limit on foreign interference but offer an emerging cyber-specific understanding much like that developed for other domains that have challenged national security and peaceful interactions between States.

[358] Besson, *supra* note 349, at ¶ 8 (citing Richard Falk, *Sovereignty*, *in* THE OXFORD COMPANION TO POLITICS IN THE WORLD 789 (Joel Krieger ed., 2d ed. 2001)).

[359] Heller & Sofaer, *supra* note 196, at 24.

[360] PROBLEMATIC SOVEREIGNTY: CONTESTED RULES AND POLITICAL POSSIBILITIES, *supra* note 16, at viii.

[361] *See* CHAYES & CHAYES, *supra* note 17, at 22.