In Defense of Pure Sovereignty in Cyberspace

Kevin Jon Heller

97 Int’l L. Stud. 1432 (2021)

Volume 97

Published by the Stockton Center for International Law
ISSN 2375-2831
In Defense of Pure Sovereignty in Cyberspace

Kevin Jon Heller*

CONTENTS

I. Introduction ........................................................................................... 1433

II. Is Sovereignty a Principle or a Rule? .................................................. 1438
   A. Sovereignty Defined ................................................................. 1438
   B. Sovereignty as a Principle or a Rule ....................................... 1439

III. Does Sovereignty Apply in Cyberspace as a Rule? .......................... 1444
   A. State Positions ............................................................................. 1444
   B. Legal Analysis ............................................................................ 1450

IV. What Does Sovereignty Prohibit in Cyberspace? ............................ 1454
   A. Tallinn Manual 2.0 ...................................................................... 1455
   B. State Positions ............................................................................. 1458
   C. Legal Analysis ............................................................................ 1464

V. The Question of Espionage ................................................................ 1474
   A. Is Espionage Lawful? ................................................................. 1475
   B. Is Espionage Unregulated? ....................................................... 1478
   C. Remote vs. Close Access Cyber Espionage .............................. 1480
   D. Cyber Espionage and Inherently Governmental Functions 1482

VI. Policy Considerations ........................................................................... 1486
   A. Sovereignty as a Principle .......................................................... 1486
   B. Sovereignty as a Rule ................................................................. 1489
   C. The Problem of Ambiguity ....................................................... 1494

VII. Conclusion ............................................................................................. 1498

* Professor of International Law and Security, Centre for Military Studies, University of Copenhagen; Professor of Law, Australian National University. My thanks to Luke Chircop, Russell Buchan, Przemyslaw Roguski, and Harriet Moynihan for their comments on earlier drafts of the article.

The thoughts and opinions expressed are those of the author and not necessarily those of the U.S. government, the U.S. Department of the Navy, or the U.S. Naval War College.
I. Introduction

The final report of the United Nations Open-Ended Working Group (OEWG), adopted by consensus in March 2021, affirms that international law applies to cyberspace and calls upon States “to avoid and refrain from taking any measures not in accordance with international law.” Reaching consensus on that critical issue is a major achievement, given that the OEWG was open to all interested Member States of the United Nations, unlike its much smaller predecessor, the Group of Governmental Experts (GGE). Significant differences nevertheless remain concerning how international law applies to cyberspace, because States have been unable to agree on what kinds of cyber operations international law prohibits. Instead, the OEWG’s final report simply—and rather tepidly—articulates eleven “voluntary, non-binding norms of responsible State behaviour.”

To be sure, some types of cyber operations are clearly internationally wrongful. Nearly all States agree that a cyber operation can qualify as a use of force that violates Article 2(4) of the U.N. Charter or even, depending on its “scale and effects,” as an armed attack that triggers the territorial State’s right of self-defense. Similarly, there is widespread agreement that a cyber operation intended to coerce a State with regard to matters that fall

---


2. This article uses “cyber operation” in accordance with the definition offered by Germany, as the “employment of cyber capabilities to achieve objectives in or through cyberspace.” Federal Government, On the Application of International Law in Cyberspace 2 (Mar. 2021), https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204e54665bd0f/on-the-application-of-international-law-in-cyberspace-data.pdf [hereinafter Statement of Germany].

3. OEWG Final Report, supra note 1, ¶ 8, at 2.

4. See, e.g., Przemysław Roguski, Application of International Law to Cyber Operations: A Comparative Analysis of States’ Views 9 (The Hague Program for Cyber Norms Policy Brief 9, 2020) (“All States endorse the applicability of the prohibition of the use or threat of force under Article 2(4) UN Charter to cyber operations.”).

5. Id. at 21 (“All analysed States acknowledge the right of a State to individual or collective self-defence against cyber operations amounting to an armed attack under Article 51 UN Charter.”).
within its domaine réservé, such as the conduct of elections, violates the customary principle of non-intervention.6

States are deeply divided, however, over the international wrongfulness of a fourth category of cyber operation: those that penetrate computer systems located on the territory of another State but do not rise to the level of a use of force or prohibited intervention—what are often referred to as “low intensity” cyber operations.7 As Michael Schmitt and Liis Vihul have noted, because the prohibition of the use of force and the principle of non-intervention “contain thresholds that are seldom reached,” the “vast majority of hostile cyber operations attributable to States” fall into this category.8 Indeed, according to the Council on Foreign Relations, thirty-four States have engaged in low-intensity cyber operations since 2005, with seventy-six such operations taking place in 2019 alone.9 Low-intensity cyber operations are also likely to continue to become even more common over time, given that they are “an inexpensive and potentially anonymous way of degrading adversaries during conflict or peacetime.”10

Low-intensity cyber operations take a variety of forms. Extraterritorial law enforcement is almost always low intensity because such cyber operations generally aim at obtaining digital evidence from computer systems located abroad, not at harming the territorial State or coercing its government

6. Id. at 7 (noting that “[n]early all analysed States share a widespread consensus that the principle of non-intervention applies to State conduct in cyberspace”). There are some minor disagreements, of course, over how to apply the principle of non-intervention to cyberspace.


8. Michael N. Schmitt & Liis Vihul, Sovereignty in Cyberspace: Lex Lata Vel Non?, 111 AMERICAN JOURNAL OF INTERNATIONAL LAW UNBOUND 213, 213–14 (2017); see also Watts & Richard, supra note 7, at 794 (“[T]he 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.”); Harriet Moynihan, The Application of International Law to State Cyberattacks: Sovereignty and Non-intervention (Chatham House Research Paper 3, 2020) (“[I]n practice, the vast majority of cyber operations by states take place below the threshold of use of force, instead consisting of persistent, low-level intrusions that cause harm in the victim state but often without discernible physical effects.”).


with regard to its *domaine réserve*.\(^\text{11}\) That is true even for law enforcement cyber operations that have a counterterrorism purpose, which are normally less concerned with damaging foreign computer systems than with preventing terrorists from accessing them or removing terrorist content.\(^\text{12}\) A striking example is Operation Glowing Symphony, in which U.S. Cyber Command hacked into computer systems used by ISIS in as many as thirty different States,\(^\text{13}\) making it “the largest and longest offensive cyber operation in US military history.”\(^\text{14}\)

Cyber espionage operations, both public and private, are also normally low intensity. The *Tallinn Manual* provides the following, generally representative, definition of cyber espionage:

> [T]he term “cyber espionage” refers to any act undertaken clandestinely or under false pretences that uses cyber capabilities to gather, or attempt to gather, information. Cyber espionage involves, but is not limited to, the use of cyber capabilities to surveil, monitor, capture, or exfiltrate electronically transmitted or stored communications, data, or other information.\(^\text{15}\)

As this list of functions indicates, successful cyber espionage is the antithesis of the kind of cyber operation that would rise to the level of a use of force or prohibited intervention. The non-damaging, non-coercive nature of cyber espionage is most obvious with espionage that targets private corporations, such as China’s theft of intellectual property from Lockheed-Martin in 2009\(^\text{16}\) and Google in 2010\(^\text{17}\) or Iran’s hacking of universities in the United States, United Kingdom, Australia, and elsewhere between 2016 and 2019.\(^\text{18}\) But it is equally true of espionage that is directed at governmental organs and agencies, such as the theft of massive amounts of personal data from the

---


\(^\text{12}\) Roguski, *Comparative Analysis*, supra note 4, at 4.

\(^\text{13}\) See Watts & Richard, supra note 7, at 772.


\(^\text{15}\) *Tallinn Manual 2.0*, supra note 11, at 168.

\(^\text{16}\) Russell Buchan, *Cyber Espionage and International Law* 179 (2019).


\(^\text{18}\) See, e.g., Moynihan, supra note 8, at 3.
U.S. Office of Personnel Management between May 2014 and June 2015, which was likely the work of China and has been described as America’s “Cyber Pearl Harbor.”

States have adopted three very different positions concerning whether low-intensity cyber operations violate State sovereignty. The first position, endorsed by the United Kingdom and until recently by the United States, is that low-intensity cyber operations are never wrongful because sovereignty is a principle of international law, not a primary rule that can be independently violated. The second position, defended most vigorously by France, is that low-intensity cyber operations are always wrongful because sovereignty is a primary rule of international law that is violated by any non-consensual penetration of a computer system located on the territory of another State—what has been called the “pure sovereigntist” approach. And the third position, adopted by States such as the Netherlands and the Czech Republic, is that although sovereignty is a primary rule of international law, only low-intensity cyber operations that cause physical damage to the territorial State or render its cyber infrastructure inoperable are wrongful—what has been called the “relative sovereigntist” approach.

This dissensus over how sovereignty functions in cyberspace undermines the ability of States to formulate cyber policy. States obviously have no right to engage in cyber operations that violate international law; when they do, they bear State responsibility for their internationally wrongful act. Moreover, a State targeted by a cyber operation that violates international law is entitled to engage in countermeasures against the responsible State.

21. *Id* at 45.
23. Countermeasures are “State actions, or omissions, directed at another State that would otherwise violate an obligation owed to that State and that are conducted by the former in order to compel or convince the latter to desist in its own internationally wrongful acts or omissions.” Michael N. Schmitt, *Below the Threshold Cyber Operations: The Countermeasures Response Option and International Law*, 54 Virginia Journal of International Law 698, 700 (2014).
24. ARSIWA, *supra* note 22, art. 49(1).
The lack of a settled understanding concerning which kinds of low-intensity cyber operations are internationally wrongful thus means that actual operations are very likely to cause conflict—legal, political, and perhaps even military—between the perpetrator State and the territorial State. Indeed, at present, a State contemplating an offensive low-intensity cyber operation can be certain that it will not be viewed as internationally wrongful and met with countermeasures only in one situation: where both States have the same understanding of sovereignty and have articulated their understanding publicly. Such situations are likely to be rare indeed.

This article has two purposes: to explain the different positions that States have taken on whether low-intensity cyber operations violate sovereignty and to provide a comprehensive analysis of which position is the strongest legally and in terms of cyber policy. The article is divided into five parts. Part II briefly explains why sovereignty is a primary rule of international law, not simply a principle from which specific primary rules can be derived. Part III asks whether sovereignty applies in cyberspace, as a rule, and agrees with the vast majority of States that it does. Part IV explains and assesses the two positions that those States have taken concerning how sovereignty applies in cyberspace as a rule: pure sovereignty and relative sovereignty. It concludes that the pure-sovereignist position has a much stronger foundation in general international law than the relative-sovereignist position. Part V then analyses and rejects the most common legal objection to that conclusion: the supposed permissibility of espionage. Finally, Part VI argues that a variety of policy considerations also favor pure sovereignty over relative sovereignty.

Before proceeding, it is important to acknowledge that the analysis below has two important limits. First, the article excludes from consideration low-intensity cyber operations that take place in the context of armed conflict, whether international or non-international. The legality of such operations is determined by international humanitarian law as the lex specialis and requires a separate and quite different legal analysis. Second, the article addresses only low-intensity cyber operations that are attributable to a State pursuant to the Articles on the Responsibility of States for Internationally Wrongful Acts. Such attribution is necessary both for the perpetrator State to be internationally responsible for a particular low-intensity cyber operation and for the territorial State to engage in countermeasures.
II. IS SOVEREIGNTY A PRINCIPLE OR A RULE?

A. Sovereignty Defined

Sovereignty is the essential feature of statehood. The seminal definition of sovereignty was provided by the Permanent Court of Arbitration in the Island of Palmas case:

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.25

Thus understood, sovereignty has both an external and an internal dimension. The external dimension refers to the equality of States under international law, which guarantees their independence and ensures that they possess the same rights and duties as every other State.26 The internal dimension of sovereignty, in turn, has both a territorial aspect and a governmental aspect. Territorial sovereignty refers to a State’s right “to exercise supreme authority over all persons and things within its territory”27 without “any form of interference” by other States.28 Governmental sovereignty refers to the right of each State to freely choose its “political, economic, social, and cultural system” and determine its own foreign policy.29

28. Wolff Heintschel von Heinegg, Legal Implications of Territorial Sovereignty in Cyberspace, in 4TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT 1, 8 (Christian Czosseck et al. eds., 2012).
B. Sovereignty as a Principle or a Rule

The internal sovereignty of States is reflected in, and is the source of, fundamental rules of international law such as the prohibition of the use of force and the principle of non-intervention. The former captures both aspects of internal sovereignty, prohibiting “the threat or use of force against the territorial integrity or political independence of any state.” The latter focuses specifically on the governmental aspect, prohibiting States—as noted above—from coercing a State concerning matters that fall within its domain.

But is sovereignty nothing more than a general principle of international law from which specific rules like the prohibition of the use of force and the principle of non-intervention are derived? Or does it exist as a primary rule in its own right? This is a threshold question concerning whether certain kinds of low-intensity cyber operations are internationally wrongful: if sovereignty is merely a principle under general international law, it cannot be a specific rule in cyberspace.

In fact, the idea that sovereignty is a primary rule of international law is supported by a vast amount of State practice and opinio juris, as well as by judicial decisions and the writings of highly qualified publicists.

1. State Practice and Opinio Juris

As Schmitt and Vihul have observed, States have routinely invoked sovereignty in a manner that makes clear they view it as a primary rule distinguishable from the prohibition of the use of force and the principle of non-intervention. An example on land is Israel’s abduction of Adolph Eichmann.
which Argentina denounced to the Security Council as a violation of its sovereignty.\textsuperscript{34} The Security Council responded by adopting Resolution 138, which affirmed that “violation of the sovereignty of a Member State is incompatible with the Charter of the United Nations.”\textsuperscript{35} In the air, notable examples include China’s claim in 2003 that the distressed landing of a U.S. reconnaissance plane on a Chinese island violated its territorial sovereignty (a claim the United States implicitly accepted)\textsuperscript{36} and Pakistan’s repeated denunciation of U.S. drone operations as “a violation of Pakistani sovereignty and territorial integrity.”\textsuperscript{37} Finally, at sea, two incidents in which Iran detained sailors they believed had violated the State’s “sovereign boundaries” are particularly worth mentioning: the capture of personnel from Britain’s HMS Cornwall in 2007\textsuperscript{38} and the (unprotested) detention of two U.S. Navy vessels that had mistakenly entered Iran’s territorial waters.\textsuperscript{39} In all of these situations, the actions in question could at least arguably\textsuperscript{40} have been characterized as uses of force, yet the States in question debated them using the language of sovereignty.

States have also affirmed the primary rule status of sovereignty through General Assembly resolutions and in treaties. The most notable example of the former is the Friendly Relations Declaration, adopted by consensus in 1970, which specifically distinguishes between the prohibition of the use of force, the principle of non-intervention, and sovereignty when itemizing the rules of international law that govern cooperation between States.\textsuperscript{41} Notable examples of the latter include the U.N. Convention Against Transnational Organized Crime, which provides that “States Parties shall carry out their obligations under this Convention in a manner consistent with the principles

\textsuperscript{34} Id. at 1659.
\textsuperscript{35} S.C. Res. 138 (June 30, 1960).
\textsuperscript{36} Schmitt & Vihul, Respect for Sovereignty, supra note 33, at 1657.
\textsuperscript{37} Id.
\textsuperscript{38} Id. at 1658.
\textsuperscript{39} Id.
\textsuperscript{40} There is considerable debate about whether Article 2(4) contains a de minimis test for the use of force, although Ruys has argued persuasively that it does not. See generally Tom Ruys, The Meaning of “Force” and the Boundaries of the Jus Ad Bellum: Are “Minimal” Uses of Force Excluded From UN Charter Article 2(4)?, 108 AMERICAN JOURNAL OF INTERNATIONAL LAW 159 (2014).
\textsuperscript{41} Friendly Relations Declaration, supra note 32, at 4.
of sovereign equality and territorial integrity of States and that of noninter-
vention in the domestic affairs of other States\footnote{42} and the Helsinki Accords,
which contain separate provisions on sovereignty, the use of force, and in-
tervention.\footnote{43}

Finally, a number of States have explicitly affirmed that sovereignty is a
primary rule of general international law when offering statements about
how international law applies in cyberspace. To mention only three: the
Netherlands “believes that respect for the sovereignty of other countries is
an obligation in its own right, the violation of which may, in turn, constitute
an internationally wrongful act”;\footnote{44} Finland “sees sovereignty as a primary rule
of international law, a breach of which amounts to an internationally wrong-
ful act and triggers State responsibility”;\footnote{45} and New Zealand says that “[t]he
principle of sovereignty prohibits the interference by one state in the inher-
ently governmental functions of another and prohibits the exercise of state
power or authority on the territory of another state.”\footnote{46}

2. Judicial Decisions

The International Court of Justice (ICJ) has consistently held that sover-
ignty is a primary rule of international law, not merely a principle from
which primary rules can be derived. Although the decisions of international

\begin{footnotes}
\footnote{42. United Nations Convention Against Transnational Organized Crime art. 4, Nov.
  15, 2000, 2225 U.N.T.S. 209.}
\footnote{43. \textit{See} Final Act of the Conference on Security and Cooperation in Europe arts. 1, 2,
  6 (Aug. 1, 1975), 14 \textit{INTERNATIONAL LEGAL MATERIALS} 1292 (1975).}
\footnote{44. Government of the Netherlands, Letter from the Minister of Foreign Affairs to the
  President of the House of Representatives on the International Legal Order in Cyberspace,
  app. at 2 (July 5, 2019), https://www.government.nl/documents/parliamentary-docu-
  ments/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyber-
  space [hereinafter Statement of the Netherlands].}
\footnote{45. Ministry of Foreign Affairs, Government of Finland, International Law and Cyber-
  space: Finland’s National Positions 3, https://um.fi/documents/35732/0/Kyberkan-
  natPDF_EN.pdf/12bbbdbe-623b-9f86-b254-07d5af3c6d85t=160309752272 (last visited
  Oct. 1, 2021) [hereinafter Statement of Finland].}
\footnote{46. Ministry of Foreign Affairs and Trade, Government of New Zealand, The Appli-
  cation of International Law to State Activity in Cyberspace ¶ 11 (Dec. 1, 2020),
  https://www.mfat.govt.nz/assets/Peace-Rights-and-Security/International-security/Inter-
  national-Cyber-statement.pdf [hereinafter Statement of New Zealand].}
\end{footnotes}
The ICJ’s very first case, *Corfu Channel*, addressed issues of sovereignty. Alb. claimed that the United Kingdom had violated its territorial sovereignty by sending warships through an Albanian strait and conducting minesweeping operations in Albania’s territorial sea without its consent. The Court rejected the former claim, holding that Albania’s sovereignty had not been violated by the transit of the warships because the innocent passage exception applied. But it accepted the latter claim because no similar exception applied to the minesweeping operations. “Between independent States,” the Court noted, “respect for territorial sovereignty is an essential foundation of international relations.” In the absence of an exception like innocent passage, therefore, “to ensure respect for international law, of which it is the organ, the Court must declare that the action of the British Navy constituted a violation of Albanian sovereignty.”

The ICJ identified sovereignty as a primary rule of international law even more explicitly in the landmark *Nicaragua* case, which involved the legality of various U.S. actions designed to overthrow Nicaragua’s Sandinista government. The Court’s analysis of Nicaragua’s claims famously focused on the prohibition of the use of force and the principle of non-intervention. But the Court made clear that although “[t]he effects of the principle of respect for territorial sovereignty inevitably overlap with those of the principles of the prohibition of the use of force and of nonintervention,” sovereignty remains an independent rule. The Court then relied on the inviolability of Nicaragua’s territorial sovereignty to hold the United States internationally responsible for providing assistance to the contras, for directly attacking ports and oil installations, for mining harbors, and for conducting unauthorized overflights.

---

49. *Id.* at 27.
50. *Id.* at 35.
52. *Id.*
More recently, the ICJ reaffirmed that sovereignty is a primary rule in *Costa Rica v. Nicaragua*, in which Costa Rica claimed that Nicaragua had violated both its territorial sovereignty and the prohibition of the use of force by using its military to dredge a river on Costa Rican territory without consent.\footnote{Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v. Nicaragua) and Construction of a Road in Costa Rica along the San Juan River (Nicar. v. Costa Rica), Judgment, 2015 I.C.J. 665, ¶ 66 (Dec. 16, 2015).} The Court held that Nicaragua’s actions “violated the territorial sovereignty of Costa Rica”\footnote{Id. ¶ 229.} and thus did not find it necessary to reach Costa Rica’s claim concerning the use of force.

3. Highly Qualified Publicists

The teachings of the most highly qualified publicists are another subsidiary means for identifying rules of customary international law.\footnote{ICJ Statute, supra note 47, art. 38(1)(b).} Such publicists have long taught that sovereignty is a primary rule. Some affirmed the inviolability of a State’s territory prior to the adoption of the U.N. Charter—and thus prior to the prohibition of the use of force and the principle of non-intervention. Henry Halleck, for example, argued in 1861 that exclusivity of territorial authority is a “perfect right” of a sovereign State, and “[w]hatever one State can claim as its perfect right, it is the absolute duty of every other to concede. To refuse it, under whatsoever pretext, would be a violation of the positive rule and fundamental principle of international jurisprudence.”\footnote{HENRY W. HALLECK, INTERNATIONAL LAW 270 (1861).}

Similarly, in the first edition of his seminal treatise *International Law: Peace*, published in 1905, Lassa Oppenheim wrote that “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.”\footnote{LASSA OPPENHEIM, 1 INTERNATIONAL LAW: PEACE 172–73 (1905).}

Highly qualified publicists continued to insist on sovereignty’s status as a primary rule after the adoption of the U.N. Charter. In the 1955 edition of Oppenheim’s treatise, for example, Hersch Lauterpacht stated matter-of-factly that “the exercise of a state’s sovereign authority” on the territory of
another State is an internationally wrongful act. More recently, Malcolm Shaw has specifically distinguished sovereignty from the principle of non-intervention, writing that “[t]he principle of respect for the territorial integrity of states is well-founded as one of the linchpins of the international system, as is the norm prohibiting interference in the internal affairs of other states.”

III. DOES SOVEREIGNTY APPLY IN CYBERSPACE AS A RULE?

Sovereignty, in short, is a primary rule of international law, not merely a principle from which specific primary rules are derived. The question then becomes: does sovereignty also apply as a rule in cyberspace? The overwhelming consensus of scholars is that it does. Most notably, the International Group of Experts (IGE) responsible for Tallinn Manual 2.0, which consisted of nearly forty scholars—many of whom no doubt qualify as “highly qualified publicists”—unanimously agreed that “[c]yber operations that prevent or disregard another State’s exercise of its sovereign prerogatives constitute a violation of such sovereignty and are prohibited by international law.”

A. State Positions

Nearly all of the States that have publicly commented on sovereignty share the IGE’s view. Indeed, the idea that sovereignty applies in cyberspace as a rule was initially uncontroversial: the U.N. Group of Governmental Experts, representing twenty States, asserted by consensus in 2013 that “state sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT [information and communication technology] related activities, and to their jurisdiction over ICT infrastructure within their

60. Indeed, the only notable dissenters are Corn and Taylor. See generally Gary P. Corn & Robert Taylor, Sovereignty in the Age of Cyber, 111 AMERICAN JOURNAL OF INTERNATIONAL LAW UNBOUND 207 (2017).
61. Schmitt & Vihul, Respect for Sovereignty, supra note 33, at 1650.
62. TALLINN MANUAL 2.0, supra note 11, at 17.
In Defense of Pure Sovereignty in Cyberspace  Vol. 97

territory.”63 In 2015, the GGE—then consisting of twenty-five States—reaffirmed that “[i]n their use of ICTs, States must observe, among other principles of international law, State sovereignty, sovereign equality, the settlement of disputes by peaceful means and non-intervention in the internal affairs of other States.”64 The General Assembly adopted the GGE’s 2015 report by consensus.65

A few years later, however, the international consensus began to fray. The United Kingdom was a member of the GGE that produced both the 2013 and the 2015 reports. Nevertheless, in 2018, the United Kingdom’s then-Attorney General, Jeremy Wright, publicly rejected the GGE report. According to Wright, the UK’s official position is that sovereignty is a principle, not a rule, and thus cannot be directly violated:

[A] further contested area amongst those engaged in the application of international law to cyber space is the regulation of activities that fall below the threshold of a prohibited intervention, but nonetheless may be perceived as affecting the territorial sovereignty of another state without that state’s prior consent. Some have sought to argue for the existence of a cyber specific rule of a “violation of territorial sovereignty” in relation to interference in the computer networks of another state without its consent. Sovereignty is of course fundamental to the international rules-based system. But I am not persuaded that we can currently extrapolate from that general principle a specific rule or additional prohibition for cyber activity beyond that of a prohibited intervention. The UK Government’s position


65. GA Res. 70/237, ¶ 1–2(a) (Dec. 30, 2015).
is therefore that there is no such rule as a matter of current international law.\textsuperscript{66}

To date, States have almost uniformly rejected the UK’s position. Most strikingly, NATO’s Allied Joint Doctrine for Cyberspace clearly endorses the idea that sovereignty applies in cyberspace as a rule\textsuperscript{67}—a position that forced the United Kingdom to issue a specific reservation to the contrary.\textsuperscript{68} Moreover, nearly every State that has issued a public statement concerning international law and cyberspace since Wright’s speech has taken the same position as NATO. Three of those States—Brazil,\textsuperscript{69} France,\textsuperscript{70} and Germany—\textsuperscript{71} were part of the 2015 GGE, making their affirmation unsurprising. But most


\textsuperscript{68} Id. at v (“The AJP refers to cyberspace operations as being, dependent on the context, potential violations of international law as a breach of sovereignty. . . . [T]he UK government does not consider that the current state of international law allows for a specific rule or additional prohibition for cyberspace operations beyond that of a prohibited intervention.”).

\textsuperscript{69} See Buchan, supra note 17, at 184 (noting the president of Brazil’s statement that U.S. cyber espionage is “an affront to the principles that must guide the relations among them, especially among friendly nations. A country’s sovereignty can never affirm itself to the detriment of another country’s sovereignty.”).


\textsuperscript{71} Statement of Germany, supra note 2, at 2.
are not, including Austria, Bolivia, the Czech Republic, Finland, Guatemala, Guyana, Iran, New Zealand, and Switzerland. The Czech Republic, for example, “firmly believes” that under the principle of sovereignty “States may freely exercise without interference in any form by another State both aspects of sovereignty in cyberspace, be it an internal one . . . or the external one.” New Zealand is more concise, insisting that “the standalone rule of territorial sovereignty also applies in the cyber context.” And Guyana flatly rejects the idea that international law protects a State only against
cyber operations “amounting to an unjustified use of force, to an armed attack, or to a prohibited intervention,” insisting that States “must not conduct cyber operations that violate the sovereignty of another State.”

The U.S. position, it is important to note, has oscillated over time. At first, the United States seemed squarely in the sovereignty-as-a-rule camp. President Obama’s 2011 International Strategy for Cyberspace affirmed that the “development of norms for State conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete. Long-standing international norms guiding State behavior—in times of peace and conflict—also apply in cyberspace.”

The United States also endorsed the 2013 and 2015 reports of the GGE, both of which endorsed the idea that sovereignty functions in cyberspace as a rule.

In March 2020, however, the General Counsel of the Department of Defense (DoD) explicitly rejected the idea that sovereignty functions as a primary rule of international law in cyberspace, thus effectively endorsing the UK position:

For cyber operations that would not constitute a prohibited intervention or use-of-force, the Department believes there is not sufficiently widespread and consistent State practice resulting from a sense of legal obligation to conclude that customary international law generally prohibits such non-consensual cyber operations in another State’s territory.

The DoD OGC view, which we have applied in legal reviews of military cyber operations to date, shares similarities with the view expressed by the U.K. Government in 2018. We recognize that there are differences of opinion among States, which suggests that State practice and opinio juris are presently not settled on this issue. Indeed, many States’ public silence in the face of countless publicly known cyber intrusions into foreign networks precludes a conclusion that States have coalesced around a common view

---

80. *Quoted in* Hollis, *supra* note 73, at 30. It is also worth noting that the IGE conducted consultations with more than “50 states and international organizations” over an early draft of the *Tallinn Manual*, and not a single State objected to the idea, reflected in Rule 4, that sovereignty applies in cyberspace as a rule. *See* Schmitt & Vihul, *Respect for Sovereignty*, *supra* note 33, at 1649.

that there is an international prohibition against all such operations (regardless of whatever penalties may be imposed under domestic law). 82

Many States hoped that the OEWG, which was created in 2019 and was open— unlike the GGE—to “all interested States,” would help clarify this and other important international-law issues. Such an outcome seemed possible when the OEWG issued its “Pre-Draft” Final Report in 2020 because the Pre-Draft specifically affirmed that “[e]xisting obligations under international law, in particular the Charter of the United Nations in its entirety, are applicable to State use of ICT”—a category that included, according to the OEWG, “State sovereignty [and] sovereign equality.” 83 Unfortunately, that optimism proved short-lived: because States were ultimately unable to reach consensus, the OEWG’s Final Report simply affirms the applicability of international law in cyberspace without explaining how it applies. 84


84. See OEWG Final Report, supra note 1, ¶ 25 (“States reaffirmed that norms do not replace or alter States’ obligations or rights under international law, which are binding, but rather provide additional specific guidance on what constitutes responsible State behaviour in the use of ICTs. Norms do not seek to limit or prohibit action that is otherwise consistent with international law.”). For its part, the GGE reaffirms in its Final Report “the commitments of States to the following principles of the Charter and other international law [including] sovereign equality.” See Report of the Group of Governmental Experts on Advancing State Behaviour in the Context of International Security, Advance Copy, annex, ¶ 71(b) (May 28, 2021), https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf [hereinafter 2021 GGE Report].
Muddying the waters still further, the United States appears to have changed its position once again as a result of the 2020 presidential election. In marked contrast to the DoD General Counsel’s dismissal of sovereignty as a rule in March 2020, the U.S.’s comments on the GGE’s 2021 Final Report include the assertion that “[i]n certain circumstances, one State’s non-consensual cyber operation in another State’s territory, even if it falls below the threshold of a use of force or nonintervention, could also violate international law.”85 That assertion implies that sovereignty can indeed function as a rule in cyberspace—at least sometimes.

B. Legal Analysis

The UK position on whether sovereignty is a primary rule of international law in cyberspace is predicated on the idea that—to quote the 2020 DoD statement—“there is not sufficiently widespread and consistent State practice resulting from a sense of legal obligation to conclude that customary international law generally prohibits . . . non-consensual cyber operations in another State’s territory.”86 There are two problems with that idea. The first is the most obvious: State practice and opinio juris are actually remarkably


86. Ney, supra note 82, at 11; cf. Corn & Taylor, supra note 60, at 208 (arguing that, below the thresholds for the use of force and intervention, “there is insufficient evidence of either state practice or opinio juris to support assertions that the principle of sovereignty operates as an independent rule of customary international law that regulates states’ actions in cyberspace”). Israel has questioned the idea that sovereignty necessarily applies in cyberspace in the same way that it does in the physical world, though it has refrained from concluding that sovereignty is a principle and not a rule in cyberspace. See Roy Schoëndorf, Israel’s Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations, 97 INTERNATIONAL LAW STUDIES 396, 397 (2021) (“It cannot be automatically presumed that a customary rule applicable in any of the physical domains is also applicable to the cyber domain. The key question in identifying State practice is whether the practice which arose in other domains is closely related to the activity envisaged in the cyber domain. Additionally, it must be ascertained that the opinio juris which gave rise to the customary rules applicable in other domains was not domain-specific.”).
consistent. As we have seen, no other State currently adopts the UK position, and at least two dozen States have explicitly rejected it.

The second and more important problem is that there is actually no need to find a rule of customary international law that “extends” sovereignty into cyberspace. To understand why, we need to distinguish between specific and general customary rules. When a rule of customary international law is specific to a particular legal or factual context, it is true that we cannot assume the rule applies in other contexts as well—even if extending the rule by analogy would make logical sense. On the contrary, to apply the rule more broadly, we must be able to identify sufficient State practice and opinio juris supporting the extension. Freedom of navigation on the high seas is an example. That customary rule, Dapo Akande and his co-authors note, is specific to the high seas; it “does not guarantee freedom of navigation throughout the seas, nor does it oblige States to guarantee freedom of movement elsewhere.” That does not mean freedom of navigation could not apply elsewhere. But we cannot simply extend freedom of navigation beyond the high seas by fiat; State practice and opinio juris would have to justify recognizing that freedom in a new context.

The analysis is very different, however, when a rule of customary international law is general, designed to prohibit a particular kind of action regardless of how or where that action is carried out. Here we need only identify State practice and opinio juris sufficient to justify the general rule itself; we do not have to find additional State practice and opinio juris for each specific application of the general rule, even if the rule is being applied to a situation that States never contemplated when they created it.

87. As noted above, at the time the UK adopted the sovereignty-as-a-principle position, few States had weighed in on the sovereignty debate. Later rejections of the UK position, however, have not led the UK to rethink it. On the contrary, in its 2021 submission to the GGE, the UK again insisted that it “does not consider that the general concept of sovereignty by itself provides a sufficient or clear basis for extrapolating a specific rule or additional prohibition for cyber conduct going beyond that of non-intervention”). See U.K. Foreign, Commonwealth & Development Office, Application of International Law to States’ Conduct in Cyberspace, ¶ 10 (June 3, 2021), https://www.gov.uk/government/publications/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement.

Consider, for example, the principle of distinction in IHL, a general customary rule that prohibits directly attacking civilians.\footnote{International Committee of the Red Cross, Rule 1. The Principle of Distinction between Civilians and Combatants, IHL DATABASE CUSTOMARY IHL, https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule1 (last visited Oct. 1, 2021).} That rule is means-neutral: directly attacking civilians is prohibited regardless of whether the attacker uses a rifle, a bomb, or a chemical weapon.\footnote{Akande et al., supra note 88.} There is thus no need to find State practice and \textit{opinio juris} for each kind of attack. It is enough that the general rule itself is supported by State practice and \textit{opinio juris}. Moreover, because the customary rule is general, no additional showing of State practice and \textit{opinio juris} would be necessary for it to apply to a weapon that has not yet been invented. If the weapon were used to directly attack civilians after it was invented, it would violate the rule.

The ICJ has explicitly endorsed this understanding of general rules of customary international law. In the landmark \textit{Legality of the Threat or Use of Nuclear Weapons} case, the Court rejected the view—held only by a “small minority” of States—that general IHL rules like the principle of distinction could not be applied to nuclear weapons because such weapons did not exist at the time the rules were created:

\begin{quote}
Indeed, nuclear weapons were invented after most of the principles and rules of humanitarian law applicable in armed conflict had already come into existence; the Conferences of 1949 and 1974–1977 left these weapons aside, and there is a qualitative as well as quantitative difference between nuclear weapons and all conventional arms. However, it cannot be concluded from this that the established principles and rules of humanitarian law applicable in armed conflict did not apply to nuclear weapons. Such a conclusion would be incompatible with the intrinsically humanitarian character of the legal principles in question which permeates the entire law of armed conflict and applies to all forms of warfare and to all kinds of weapons, those of the past, those of the present and those of the future.\footnote{Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J 226, ¶ 86 (July 8).}
\end{quote}

\begin{quote}
The Court reached a similar conclusion, it is worth noting, concerning three conventional rules of the \textit{jus ad bellum}—the prohibition of the use of force, the right of self-defense against an armed attack, and the power of the Security Council to authorize military action in response to a breach of the
\end{quote}
peace or an act of aggression. “These provisions,” the Court noted, “do not refer to specific weapons.” The Court thus held that, as general rules, they apply “to any use of force, regardless of the weapons employed.”

The idea that it is unnecessary to find sufficient State practice and opinio juris for specific applications of a general rule of international law should not be controversial—even in the context of cyberspace. After all, States overwhelmingly agree that the basic rules of IHL, including the principle of distinction, apply equally to cyber and kinetic attacks. That position has been taken, inter alia, by the GGE, North Atlantic Treaty Organization, European Union, and by nearly the entirety of the Organization of American States. Those rules long predated the cyber era, yet no State suggested in those fora—or has suggested since—that sufficient cyber-specific State practice and opinio juris is required to extend them to cyberattacks.

The UK position on sovereignty in cyberspace makes sense, in short, only if the primary rule of sovereignty in international law is limited to kinetic activities. Applying the rule to cyberspace would then require sufficient State practice and opinio juris to justify the extension. But that is not the case: like the basic rules of the jus in bello and jus ad bellum, sovereignty is a general rule that is not limited to particular means of interfering with a State’s exclusive right to control its territory and determine its foreign policy. As the Permanent Court of International Justice (PCIJ) said in the seminal *Lotus* case:

---

92. *Id.* ¶ 38.
93. 2021 GGE Report, *supra* note 84, ¶ 71(f) (noting the applicability in cyberspace of “established international legal principles, including, where applicable, the principles of humanity, necessity, proportionality and distinction”).
94. Statement of NATO, *supra* note 67, at 19 (“NATO COs must be conducted in accordance with international law, including the United Nations (UN) Charter, Law of Armed Conflict (LOAC) and human rights law, as applicable.”).
95. See Council of the European Union, Draft Council Conclusions 11357/13, annex at 4 (June 25, 2013), https://data.consilium.europa.eu/doc/document/ST%20201357%202013%20INIT/EN/pdf (“Recognising that international law, including international conventions such as the Council of Europe Convention on Cybercrime (Budapest Convention) and relevant conventions on international humanitarian law and human rights, such as the International Covenant on Civil and Political Rights, the International Covenant on Economic, Social and Cultural Rights provide a legal framework applicable in cyberspace.”).
[T]he 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. In this sense jurisdiction is certainly territorial; it cannot be exercised by a State outside its territory except by virtue of a permissive rule derived from international custom or from a convention.97

Because sovereignty is a general rule, neutral as to the means of its violation, State practice and opinio juris do not have to establish that sovereignty applies in cyberspace. On the contrary, the default position is that sovereignty applies in cyberspace no less than in the physical world, with the burden of proof on the United Kingdom to show otherwise.98 That is a burden it cannot satisfy, given that other States uniformly insist sovereignty is a general rule of international law.

IV. WHAT DOES SOVEREIGNTY PROHIBIT IN CYBERSPACE?

The fundamental issue concerning the legality of low-intensity cyber operations conducted without the territorial State’s consent99 is thus not whether sovereignty applies to them but how. On this issue, States have adopted two very different positions.

---

97. S.S. Lotus (Fr. v. Turk.), Judgment, 1927 P.C.I.J. (ser. A) No. 10, at 18–19 (Sept. 7) (emphasis added); cf. Nicholas Tsagourias, Law, Borders, and the Territorialisation of Cyberspace, 15 INDONESIAN JOURNAL OF INTERNATIONAL LAW 523, 544 (2018) (describing sovereignty as “a ‘catch-all’ principle which can be dissected into more specific norms but remains the fall-back principle that captures any interference within a state’s exclusive internal and external authority which is not captured by other more specific rules such as those on non-intervention or non-use of force”).

98. See Akande et al., supra note 88 (noting that, for general rules of international law, “[i]t is the burden of those advocating for ICTs’ exclusion from their scope to present evidence that states, in their general practice accepted as law, have actively carved out ICTs”).

99. Because it is uncontroversial that a State can consent to a low-intensity cyber operation on its territory, this article addresses only those operations that are non-consensual. The expression “low-intensity cyber operation” thus refers to operations that take place without the territorial State’s consent. For sake of readability, the article will not constantly note that a low-intensity cyber operation is non-consensual.
A. Tallinn Manual 2.0

Although it does not have any formal legal status,100 the Tallinn Manual 2.0, issued in 2017, has generally set the terms of State debate over how sovereignty applies to low-intensity cyber operations. After noting that “[t]he precise legal character of remote cyber operations that manifest on a State’s territory is somewhat unsettled in international law,” the Manual summarizes the IGE’s findings as follows:

The International Group of Experts assessed their lawfulness on two different bases: (1) the degree of infringement upon the target State’s territorial integrity; and (2) whether there has been an interference with or usurpation of inherently governmental functions. The first is based on the premise that a State controls access to its sovereign territory, as described above, and the second on the sovereign right of a State to exercise within its territory, “to the exclusion of any other State, the functions of a State.”101

It is worth examining each basis in more detail.

1. Territorial Integrity

The IGE debated whether three different kinds of low-intensity cyber operations violate a State’s territorial integrity. The first is a cyber operation that causes physical damage, such as “malware that causes the malfunctioning of the cooling elements of equipment, thereby leading to overheating that results in components melting down.”102 The vast majority of the IGE agreed

---

100. See, e.g., Ney, supra note 82, at 8 (“Initiatives by non-governmental groups like those that led to the Tallinn Manual can be useful to consider, but they do not create new international law, which only states can make.”). Based on an empirical study, Efrony and Shany have concluded that “there appears to be limited support in state practice for certain key Rules of the Tallinn Manuals, and that it is difficult to ascertain whether states accept the Tallinn Rules and wish them to become authoritative articulations of international law governing cyberoperations.” Efrony & Shany, supra note 19, at 585. The findings of this article somewhat support that conclusion. As discussed below, States are quite evenly divided over the Tallinn Manual’s approach to sovereignty.

101. TALLINN MANUAL 2.0, supra note 11, at 20.

102. Id.
that such an operation violates sovereignty. The second is a cyber operation that causes cyber infrastructure in the territorial State to lose significant functionality, such as the 2012 Shamoon 1 virus, which rendered inoperable thousands of hard drives used by Saudi Aramco. The IGE agreed that sovereignty prohibits “a cyber operation necessitating repair or replacement of physical components of cyber infrastructure . . . because such consequences are akin to physical damage or injury.”

The third kind of cyber operation is one that does not cause either physical damage or equivalent loss of cyber infrastructure functionality. The IGE debated whether the following operations could be included in this category of non-harmful operations:

- causing cyber infrastructure or programs to operate differently;
- altering or deleting data stored in cyber infrastructure without causing physical or functional consequences . . . ;
- emplacing malware into a system;
- installing backdoors;
- and causing a temporary, but significant, loss of functionality, as in the case of a major DDoS [distributed denial of service] operation.

The IGE could not reach consensus on these kinds of operations, with all of the Experts justifying their positions by reference to the object and purpose of sovereignty—to “afford[] States the full control over access to and activities on their territory.”

As we will see, at least one State endorses a de minimis test for territorial integrity because they believe the IGE rejected the idea that non-harmful cyber operations are capable of violating sovereignty. But that is not what happened: because the Experts were divided, the IGE simply did not take a position on the legality of non-harmful cyber operations. Failing to agree that such operations violate sovereignty is not the same as concluding they do not.

103. Id.
104. Id. at 21.
105. Id.
106. For sake of readability, this article often refers to “harmful” and “non-harmful” cyber operations. Harmful cyber operations include both those that cause physical damage and those that cause loss of cyber infrastructure functionality equivalent to physical damage. Non-harmful refers to all other low-intensity cyber operations.
107. TALLINN MANUAL 2.0, supra note 11, at 21.
108. Id.
109. E-mail from Michael Schmitt to author (Feb. 26, 2021) (on file with author).
2. Inherently Government Functions

Although the IGE struggled to “definitively” define the concept of “inherently governmental functions,” the Experts uniformly agreed that a low-intensity cyber operation that “interferes with or usurps the inherently governmental functions of another State” violates sovereignty. They also agreed that, for cyber operations in this category, “[i]t matters not whether physical damage, injury, or loss of functionality has resulted or whether the operation qualifies in accordance with the various differing positions outlined above for operations that do not result in a loss of functionality.”

According to the IGE, interference and usurpation are separate concepts. A cyber operation interferes with an inherently governmental function when it disrupts “data or services” that are necessary for that function to operate normally. Examples include “changing or deleting data such that it interferes with the delivery of social services, the conduct of elections, the collection of taxes, the effective conduct of diplomacy, and the performance of key national defence activities.” By contrast, usurpation refers to a remote cyber operation that involves engaging in an inherently governmental function that is “exclusively reserved to another State on the latter’s territory.” The most important inherently governmental function cited by the IGE is law enforcement:

An example on point is the exercise of law enforcement functions within another State’s borders in the absence of either an allocation of authority under international law or consent (Rule 11). To illustrate, if one State conducts a law enforcement operation against a botnet in order to obtain evidence for criminal prosecution by taking over its command and control servers located in another State without that State’s consent, the former has violated the latter’s sovereignty because the operation usurps an inherently governmental function exclusively reserved to the territorial State under international law.

110. TALLINN MANUAL 2.0, supra note 11, at 21–22.
111. Id. at 22.
112. Id.
113. Id. at 23.
114. Id. at 22–23.
B. State Positions

To understand State positions on how sovereignty applies to low-intensity cyber operations, it is important to distinguish between territorial sovereignty and governmental sovereignty.

1. Territorial Sovereignty

Like the IGE, States are deeply divided over when a low-intensity cyber operation violates the territorial sovereignty of the targeted State. In general, adopting Harriet Moynihan’s terminology, we can distinguish between States that take a pure-sovereignist position and States that take a relative-sovereignist position—acknowledging that there are minor differences between States in each category.

i. Pure Sovereignty

The pure-sovereignist position is elegant in its simplicity: any low-intensity cyber operation that involves non-consensually penetrating a computer system located on another State’s territory violates the targeted State’s sovereignty. This position obviously goes well beyond the *Tallinn Manual*, prohibiting not only operations that cause physical damage or equivalent loss of cyber infrastructure functionality but also operations that involve nothing more than exfiltrating data or installing a backdoor into a computer system. Indeed, as the definition implies, most pure-sovereignist States view merely accessing a computer system located on another State’s territory as a violation of sovereignty.

Moynihan suggests that this “open-ended, maximally protective approach to violation of sovereignty in the cyber context appears to be at odds with the reality of states’ day to day interactions in cyberspace.” Her objection, however, is overstated. As discussed below, States have often used the language of territorial sovereignty to condemn cyber operations that fall short of causing physical damage or equivalent loss of cyber infrastructure functionality.

---

116. *Id.* at 20.
Moreover, at least three States have explicitly adopted the pure-sovereignist position: France, Iran, and Switzerland. France’s public statement about how international law applies in cyberspace says that “[a]ny cyberattack against French digital systems . . . constitutes a breach of sovereignty”\(^{117}\) and defines French digital systems to include all “information systems located on its territory.”\(^{118}\) Iran claims that “[a]ny utilization of cyberspace if and when involves unlawful intrusion to the (public or private) cyber structures which is under the control of another state, may be constituted as the violation of the sovereignty of the targeted state.”\(^{119}\) And Switzerland asserts that “state sovereignty protects information and communication technologies (ICT) infrastructure on a state’s territory against unauthorised intrusion or material damage,” including “computer networks systems and software supported by the ICT infrastructure, regardless of whether the infrastructure is private or public.”\(^{120}\)

A fourth State, Guatemala, has adopted a position that borders on pure sovereignty: “a State participating in a specific cyber operation violates a country’s sovereignty if, in the course of a cyber attack, it takes certain information from another State’s cyber realm, even when no harm that could affect equipment or the human rights of a person or persons is caused.”\(^{121}\) This position explicitly rejects the *Tallinn Manual’s* harm-based approach but requires more than merely accessing a computer system located on another State’s territory.

Six other States have implicitly endorsed a position similar to Guatemala’s. In 2013, WikiLeaks revealed that the U.S. National Security Agency

117. Statement of France, * supra* note 70, at 7; see Roguski, *Comparative Analysis*, * supra* note 4, at 5–6 (“In the French view, already an unauthorised penetration of ‘French systems’—and not the effect produced by this penetration in form of physical damage or interference with governmental functions—is sufficient to find a violation of sovereignty. France thus implicitly rejects the view . . . requiring more than *de minimis* effects upon the target State’s territorial integrity for a breach of sovereignty.”).

118. *Id*. at 6.

119. Statement of Iran, * supra* note 76, art. 2(4).


121. *Quoted in Hollis, supra* note 73, at 30. Guatemala’s position might be slightly narrower than France and Iran’s, given that its statement specifically mentions exfiltration. Nevertheless, in light of its explicit rejection of the *Tallinn Manual’s* approach, it seems more likely that Guatemala would view merely accessing a computer system on its territory as a violation of its sovereignty.
(NSA) had systematically intercepted the email and telephone communications of dozens of governments (friend and foe), international organizations, and NGOs.\(^{122}\) In response, Mercosur issued a statement on behalf of its five members—Argentina, Brazil, Paraguay, Uruguay, and Venezuela—“[s]trongly rejecting the interception of telecommunications and the acts of espionage carried out in our countries” on the ground that it “violates our sovereignty.”\(^{123}\) The Bahamas reacted similarly, insisting that international law guarantees in cyberspace “the primacy of sovereignty, maintenance of territorial integrity, [and] freedom from undue external intrusion and influence.”\(^{124}\) Given that the NSA’s cyber espionage did not cause any kind of harm to the penetrated computer systems, these statements strongly suggest that Argentina, the Bahamas, Brazil, Paraguay, Uruguay, and Venezuela subscribe to some version of the pure-sovereigntist position.

It is also worth noting that NATO appears to believe at least some low-intensity cyber operations that do not result in physical damage or equivalent loss of cyber infrastructure functionality are capable of violating sovereignty. NATO’s Allied Joint Command Doctrine for Cyberspace Operations says the following:

> COs [cyber operations] that generally would not constitute a use of force or armed attack might involve effects that create only temporary disruptions or denials of service, or those intended merely for disseminating or gathering information. . . . Depending on the context, such COs may nevertheless constitute a violation of international law as a breach of sovereignty or other internationally wrongful act.\(^{125}\)

Although this statement does not explicitly endorse the pure-sovereigntist position, it is closer to pure sovereignty than to the relative-sovereigntist position discussed below. The fuzziness of NATO’s position likely reflects

\(^{122}\) See, e.g., Buchan, supra note 17, at 184.


\(^{125}\) Statement of NATO, supra note 67, at 20 n.26.
the fact that its members are themselves divided over how territorial sovereignty functions in cyberspace.

ii. Relative Sovereignty

The relative-sovereignist position rejects the idea that the mere penetration of a computer system located on the territory of another State violates that State’s sovereignty. For States that adopt relative sovereignty, a cyber operation must cause at least some kind of harm to the targeted state to be internationally wrongful.

“Some kind of harm” is, of course, a vague expression. Unfortunately, it is difficult to make the relative-sovereignist test more concrete: although eight States have clearly endorsed relative sovereignty, they have not coalesced around a common understanding of what kind of harm separates a lawful low-intensity cyber operation from an unlawful one. The Czech Republic seems to set the bar the highest, limiting violations of sovereignty to cyber operations involving “damage to or disruption of cyber or other infrastructure” that has “a significant impact on national security, economy, public health or environment.”126 The Netherlands simply endorses Rule 4 of the Tallinn Manual,127 thereby requiring the cyber operation to cause physical damage or equivalent loss of functionality—a position echoed by Norway.128 And according to Finland, a cyber operation that causes “material harm” violates sovereignty.129

Four other States that endorse the relative-sovereignist position provide almost no indication of what kind of harm is required. Germany says only that “negligible physical effects and functional impairments below a certain impact threshold cannot—taken by themselves—be deemed to constitute a violation of territorial sovereignty,”130 while the United States simply insists that sovereignty cannot be violated when a cyber operation has “no effects

126. Statement of the Czech Republic, supra note 78, at 3.
127. Statement of the Netherlands, supra note 44, at 3.
129. Statement of Finland, supra note 45, at 2. Finland also suggests that a “relevant consideration” in determining a violation of sovereignty is whether a low-intensity cyber operation “modifies or deletes information.” Id. It is unclear, however, whether Finland believes that modification or deletion of information, standing alone, is sufficient for a sovereignty violation.
130. Statement of Germany, supra note 2, at 4.
or de minimis effects." Guyana is similarly unhelpful, asserting only that whether a low-intensity cyber operation violates sovereignty depends on “the degree of infringement” involved in the operation. And New Zealand is the least helpful of all, noting only that “there is a range of circumstances—in addition to pure espionage activity—in which an unauthorized cyber intrusion, including one causing effects on the territory of another State, would not be internationally wrongful.”

2. Governmental Sovereignty

In contrast to territorial sovereignty, States appear to generally agree with the Tallinn Manual’s position that low-intensity cyber operations that interfere with or usurp inherently governmental functions violate sovereignty. Pure-sovereigntist States obviously do because they believe that sovereignty prohibits all low-intensity cyber operations. As for relative-sovereigntist States, the few that have publicly commented on the Tallinn Manual’s approach to governmental sovereignty follow the IGE. Finland, for example, says that “an unauthorized intrusion by cyber means may be seen as a violation of the target State’s territorial sovereignty if it interferes with data or services that are necessary for the exercise of inherently governmental functions.” Similarly, Guyana insists that whether a low-intensity cyber operation violates sovereignty depends not only on territorial intrusion, but also on “the degree of infringement and whether there has been an interference

131. Statement of the United States, Official Compendium of Voluntary National Contributions, supra note 85, at 140.
132. Quoted in Hollis, supra note 73, at 30.
133. Statement of New Zealand, supra note 46, at 3.
134. See, e.g., Statement of Switzerland, supra note 77, at 3 (deeming “interference with or usurpation of an inherently governmental function” a violation of sovereignty).
135. Statement of Finland, supra note 45, at 2.
with government functions.” The Czech Republic, New Zealand, and the Netherlands have made similar statements.

Two relative-sovereignist States have also publicly agreed with the IGE’s conclusion that governmental sovereignty prohibits a State from engaging in extraterritorial law enforcement. Specifically, the Netherlands has said that “the act of exercising investigative powers in a cross-border context is traditionally deemed a violation of a country’s sovereignty unless the country in question has explicitly granted permission,” while New Zealand insists that the “standalone rule of territorial sovereignty . . . prohibits a state from carrying out official investigations or otherwise exercising jurisdiction on foreign territory.” Moreover, the IGE’s position on extraterritorial law enforcement reflects the Council of Europe’s Convention on Cybercrime (Budapest Convention), ratified by sixty-seven States, which prohibits “trans-border access to stored computer data” unless a State has consent or the data is publicly available.

As Ghappour notes, the drafters of the Budapest Convention specifically rejected a law enforcement exception precisely because of concerns about territorial sovereignty.

3. Pure Sovereignty vs. Relative Sovereignty

The practical difference between the pure-sovereignist and relative-sovereignist positions should not be overstated. Most importantly, both view extraterritorial law enforcement (including counterterrorism) as a violation of sovereignty, although they reach that conclusion through different paths.

136. Quoted in Hollis, supra note 73, annex at 30.
137. Statement of the Czech Republic, supra note 78, at 3 (arguing that a low-intensity cyber operation violates sovereignty if its interference with “data or services” has a “significantly disrupting” effect on “the exercise of inherently governmental functions”).
138. Statement of New Zealand, supra note 46, at 2 (“The principle of sovereignty prohibits the interference by one state in the inherently governmental functions of another.”).
139. Statement of the Netherlands, supra note 44, at 3 (claiming that sovereignty has been violated if “there has been an interference with or usurpation of inherently governmental functions of another state”).
140. Id. at 2. The Netherlands notes, though, that “[o]pinion is divided as to what qualifies as exercising investigative powers in a cross-border context.” Id.
141. Statement of New Zealand, supra note 46, at 2.
For a pure-sovereigntist State, low-intensity law enforcement operations violate sovereignty simply because they involve penetrating a computer system located on the territory of another State. For a relative-sovereigntist State, by contrast, low-intensity law enforcement operations violate sovereignty because they usurp one of the targeted State’s inherently governmental functions—a type of sovereignty violation that does not require causing any kind of harm to the penetrated computer system.

The pure-sovereigntist and relative-sovereigntist positions differ significantly, however, concerning the legality of cyber espionage. Pure sovereignty deems all cyber espionage unlawful, because it necessarily involves non-consensually penetrating a computer system on another State’s territory.144 By contrast, despite their differences, the States that have adopted relative sovereignty agree the mere penetration of a computer system is not enough. That means they all accept that cyber espionage—from installing backdoors to exfiltrating information—does not violate international law as long as it does not cause any harm to the targeted State’s cyber infrastructure. That is a fundamental difference from pure sovereignty, which necessarily deems cyber espionage just as unlawful as cyber law enforcement.

C. Legal Analysis

The pure-sovereigntist position has a much stronger foundation in general international law than the relative-sovereigntist position.

1. Extraterritorial Power and the Lotus Case

As we have seen, unlike relative sovereignty, pure sovereignty does not limit violations of sovereignty to low-intensity cyber operations that cause some kind of harm to the territorial State’s cyber infrastructure. Merely penetrating a computer system located on the territory of another State is a violation.

144. Interestingly, France’s statement on international law in cyberspace includes a footnote that says “[t]his document does not contain any specific analysis or treatment of cyberespionage, which is not illegal in international law, though it may infringe such law when linked with an internationally wrongful act.” Statement of France, supra note 70, at 4 n.2. Unless France believes that there is an exception in customary international law specifically permitting espionage—a possibility considered and rejected in the next Part—France’s pure-sovereigntist approach would deem all acts of cyber espionage on its territory internationally wrongful, because by definition cyber espionage involves non-consensually penetrating a French computer system.
The pure-sovereign position is thus based on directly applying the first Lotus principle to cyberspace. Recall what the PCIJ said:

Now 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. In this sense jurisdiction is certainly territorial; it cannot be exercised by a State outside its territory except by virtue of a permissive rule derived from international custom or from a convention.\textsuperscript{145}

The argument for the pure-sovereign position is straightforward: Lotus prohibits a State from exercising “any form” of power on the territory of another State in the absence of an international rule permitting it to do so; penetrating a computer system in another State is a form of exercising power on that State’s territory; no permissive rule of international law permits such penetration. All low-intensity cyber operations, therefore, violate the territorial State’s sovereignty, even those that do not cause any harm.

Although the PCIJ’s decision in the Lotus case is merely a subsidiary means for determining international law, the first Lotus principle is widely considered to accurately capture how custom understands territorial sovereignty.\textsuperscript{146} Indeed, even the Tallinn Manual takes the position that the first Lotus principle is customary: “The Experts agreed that a violation of sovereignty occurs whenever one State physically crosses into the territory or national airspace of another State without either its consent or another justification in international law.”\textsuperscript{147} The Manual specifically cites Lotus for that point.\textsuperscript{148}

The general scholarly consensus concerning the first Lotus principle is not surprising, because it is consistent with State practice. As Luke Chircop says:

\textsuperscript{145} S.S. Lotus (Fr. v. Turk.), Judgment, 1927 P.C.I.J. (ser. A) No. 10, at 18–19 (Sept. 7).

\textsuperscript{146} See, e.g., Simon Chesterman, The Spy Who Came in from the Cold War: Intelligence and International Law, 27 MICHIGAN JOURNAL OF INTERNATIONAL LAW 1071, 1081 (2006) (“The foundational rules of sovereignty . . . provide some guidance on what restrictions, if any, might be placed on different forms of intelligence gathering that do not rise to the level of an armed attack or violate other specific norms. The basic rule was articulated by the Permanent Court of International Justice in the 1927 Lotus case.”).

\textsuperscript{147} TALLINN MANUAL 2.0, supra note 11, at 19.

\textsuperscript{148} Id. at 67 n.82.
In the context of physical space, a state’s right to freedom from interference with territorial sovereignty is strictly protected. The physical territory of a state consists of its land, its territorial sea (if any) and its airspace. Accordingly, unwelcome state-sponsored incursions into each of these spaces has consistently been treated as a violation of territorial sovereignty, even where such incursions are of a low gravity.149

In terms of airspace, for example, the U.S. DoD has noted that aerial warfare led to the creation of “a highly restricted regime of air law in which any entry into a nation’s airspace without its permission [is] to be regarded as a serious violation of its sovereignty and territorial integrity.”150 That highly restricted regime is explicitly embraced by the Chicago Convention on International Civil Aviation, which “affirms that every state enjoys complete and exclusive sovereignty over the airspace above its territory”151 and categorically prohibits all State aircraft from entering another State’s airspace

149. Chircop, supra note 10, at 21; see also Przemysław Roguski, Violations of Territorial Sovereignty in Cyberspace, in GOVERNING CYBERSPACE: BEHAVIOR, POWER, AND DIPLOMACY 65, 77 (Dennis Broeders & Bibi van den Berg eds., 2020) (“[T]he exercise of state power is not measured by the effects of one state’s actions on the territory of another state, but rather by the nature of the action itself.”); BUCHAN, supra note 16, at 51 (“Any non-consensual incursion by one state into the territory of another state violates the rule of territorial sovereignty, regardless of whether that infraction produces damage.”); Craig Forcese, “Pragmatism and Principle”: Intelligence Agencies and International Law, 102 VIRGINIA LAW REVIEW 67, 80 (2016), https://www.virginialawreview.org/articles/pragmatism-and-principle-intelligence-agencies-and-international-law/ (“I am not aware of any authority demonstrating that the legality of enforcement jurisdiction depends on the scale of the physical presence.”); Quincy Wright, quoted in BUCHAN, supra note 16, at 181 (“In times of peace . . . espionage and, in fact, any penetration of the territory of a State by agents of another State in violation of the local law is also a violation of the rule of international law imposing a duty upon States to respect the territorial integrity and political independence of other States”); Stephane Beaulac, The Lotus Case in Context: Sovereignty, Westphalia, Vattel, and Positivism, in THE OXFORD HANDBOOK OF JURISDICTION IN INTERNATIONAL Law 41, 51 (Stephen Allen et al. eds., 2019) (“State power cannot be used to enforce legal rules outside its territory; the coercive force of a state—the police or the military—cannot be exercised on the territory of another state.”).


without its consent. 152 And, of course, States have routinely invoked their territorial sovereignty to condemn even the most minor and harmless incursions into their airspace as sovereignty violations, such as Estonia’s formal complaint to Russia when a Russian jet entered its airspace for less than sixty seconds. 153

States also view unauthorized entry into their territorial sea as a violation of sovereignty, even when that entry does not cause any harm. Schmitt and Vilhul cite a variety of examples of maritime disputes being conducted “in the vernacular” of territorial inviolability, such as the Iranian detentions of British and American ships mentioned earlier. 154 To be sure, that inviolability is limited by a variety of rights of passage and entry. But as Schmitt and Vilhul note, “[t]he regimes of innocent, transit, and archipelagic passage developed as customary and treaty-law exceptions to the territorial sea’s inviolability; they modify the baseline principle that maritime borders may not be pierced by other States.” The existence of such exceptions is specifically contemplated by the first *Lotus* principle.

State practice on land generally concerns abduction, which normally involves no harm. States have routinely protested abductions from their territory as inconsistent with their sovereignty. 155 We have already noted the most famous example, Israel’s kidnapping of Eichmann in Argentina, which was explicitly condemned on sovereignty grounds by the Security Council. A more recent example is the U.S. kidnapping of Abu Omar from the streets of Milan, which led Italy to insist that the United States had a legal duty to “fully respect Italian sovereignty.” 156

---

152. *Id.* art. 3(c).


155. *See, e.g., L.C. Green, The Eichmann Case, 23 THE MODERN LAW REVIEW 507, 509 (1960) (citing State practice concerning abductions for the proposition that “[a]n invasion by state agents, whether by force of arms or not, of the territory of another state constitutes a breach of the sovereignty of that state and involves the responsibility of the state of which the offenders are agents”).

Though not State practice, the ICJ has also affirmed that merely crossing the border on land violates a State’s territorial sovereignty. In the *Certain Activities* case, the Court held that Nicaragua had violated Costa Rica’s sovereignty by sending soldiers across its border even though no actual hostilities broke out and the Nicaraguan soldiers had no hostile intent. In fact, the Court did not even find it necessary to consider whether Nicaragua was occupying Costa Rican territory, because it had “already established that the presence of military personnel of Nicaragua in the disputed territory . . . violated Costa Rica’s territorial sovereignty.”

2. *Lotus* in Cyberspace

Two propositions, in short, have a strong basis in international law. The first is that sovereignty functions in cyberspace as a rule, not as a principle because it is a general rule of international law that applies to all forms of exercising power on another State’s territory. The second is that the general rule of sovereignty in the physical world prohibits any penetration of a State’s territory, even penetration that causes no harm.

Taken together, those propositions suggest that, in terms of low-intensity cyber operations, the pure-sovereignist position is correct: any remote penetration of a computer system, even penetration that does not cause any harm, violates the territorial sovereignty of the State in which the computer system is located. Simply put, there is no reason to believe that sovereignty functions any differently in cyberspace than in the physical world: “the same rules regarding violation of sovereignty apply whether the exercise of authority by the perpetrating State is carried out through a physical presence on the territory of the affected State or remotely from outside the affected territory.”


158. Id.

159. Moynihan, *supra* note 8, at 17; see also Chircop, *supra* note 10, at 20 (“[T]he strongest argument in favour of the strict inviolability approach is that an equivalent standard of territorial sovereignty has long been accepted by states in respect of physical space, and that the content of the principle should not differ across the physical and cyber domains.”); FRANCOIS DELARUE, *CYBER OPERATIONS AND INTERNATIONAL LAW* 217 (2020) (noting that there is no reason to treat cyberspace any differently than physical territory in terms of whether penetration violates sovereignty).
This conclusion is supported not only by the nature of general rules of international law discussed above but also by two additional and related considerations. The first is the ICJ’s insistence in the *Legality of the Threat or Use of Nuclear Weapons* case that general rules of international law are normally technologically neutral. When a State uses a low-intensity cyber operation to obtain evidence of a crime, delete terrorist recruiting videos, or steal corporate intellectual property, it is still engaging in law enforcement, counterterrorism, or espionage. Only the means of carrying out those traditional State functions are different. The idea that sovereignty functions differently in cyberspace than in the physical world is thus no more compelling than the idea that key rules of IHL function differently for nuclear weapons than for conventional ones.

The second consideration is that, however new and different it might seem, cyberspace is no less a territorial domain than air, sea, or land. As the *Tallinn Manual* points out, “[c]yber activities occur on territory and involve objects, or are conducted by persons or entities, over which States may exercise their sovereign prerogatives.”160 This means that a State’s sovereign right to protect data is no different than its sovereign right to protect brick-and-mortar objects.161 Why, then, would the general rule of sovereignty provide a State’s cyber infrastructure with less protection than its physical infrastructure?162

3. Are Low-Intensity Cyber Operations an “Exercise of Power”? To be sure, the first *Lotus* principle applies to remote low-intensity cyber operations only if they qualify as a State “exercis[ing] its power . . . in the territory of another state.” One scholar, Katharina Ziolkowski, has suggested

---

160. *TALLINN MANUAL 2.0*, *supra* note 11, at 12.
161. Chircop, *supra* note 10, at 17 (“The critical next step is to recognise that states also exercise territorial sovereignty over data emanating from their cyber infrastructure. The basis of a state’s claim to territorial sovereignty over data remains physical, in that it is limited to data that emanates from infrastructure located on its territory.”); cf. Buchan, *supra* note 17, at 177 (“[T]he accessing and copying of confidential information located in cyberspace, and which belongs to entities that fall under the sovereignty of a State (whether this is public authorities, private companies, individuals, etc), is regarded by States as a violation of their sovereignty.”).
162. See, e.g., Chircop, *supra* note 10, at 23 (pointing out that “it would be curious if the rule of territorial sovereignty provided a state’s sovereign cyber infrastructure with less protection from intrusion than a state’s sovereign physical territory”).
in the context of cyber espionage (discussed in more detail below) that “[i]t is doubtful whether an unauthorised ‘virtual trespass’ of or ‘virtual presence’ in an IT-system or computer network that runs on servers located in the sovereign area of another State can be equated with a physical presence of a spying State organ, agent etc. or a platform.”163 Her argument, however, is based on the idea that the “unauthorised copying of data and of necessary adjunctive activities, i.e., amendments of data to obtain access to the IT-systems and cover the traces of any espionage activity . . . do not cause any further, i.e. secondary, tertiary etc., physical effects in a foreign State’s sovereign area.”164 As we have seen, the mere penetration of a State’s airspace, territorial sea, or land violates the first Lotus principle in the absence of a conventional or customary exception allowing it; no physical effects of any kind are required. Mutatis mutandis, merely penetrating a computer system located on another State’s territory, should also qualify as an exercise of power.165

Such “mere penetration,” it is important to note, is distinguishable from a situation in which a State intercepts wireless signals emanating from another State without penetrating a computer system located on its territory. That kind of interception does not violate sovereignty because the interception is not considered extraterritorial. In Weber and Saravia v. Germany, for example, the European Court of Human Rights affirmed the legality of a program in which “[s]ignals emitted from foreign countries are monitored by interception sites situated on German soil.”166 The Court held that such “strategic monitoring measures” did not violate Uruguay’s territorial sovereignty because they involved “international wireless telecommunications,

164. Id. at 459.
165. See, e.g., Patricia L. Bellia, Chasing Bits Across Borders, 2001 UNIVERSITY OF CHICAGO LEGAL FORUM 35, 77 (rejecting the argument that “a remote search is less invasive than a physical search” because “[i]f the sovereignty interest at issue is the target state’s power to protect persons and property within its borders, it does not matter whether interference with that power comes from inside or outside of the target state”); Moynihan, supra note 8, at 19–20 (“There seems to be no reason in principle to distinguish physical violations (i.e. activity carried out by a state agent physically on the territory of the victim state) and remote violations (i.e. activity carried out from outside the affected state’s territory).”).
that is, telecommunications which are not effected via fixed telephone lines but, for example, via satellite or radio relay links.\textsuperscript{167} Similarly, in X (Re), the Federal Court of Canada approved a Canadian Secret Intelligence Service (CSIS) plan “to use listening posts within Canada to intercept communications emanating from foreign territory.”\textsuperscript{168} The Court acknowledged that it had relied on the concept of territorial sovereignty two years earlier to invalidate a CSIS program that permitted “covert electronic surveillance” of Canadians living abroad. But it found the listening-post plan to be materially different from the earlier program because it would involve not “a warrant that authorizes activities abroad but one which authorizes investigative activities to be conducted in Canada which will allow for communications to be listened to and information obtained from Canada.”\textsuperscript{169}

These kinds of cyber operations—which also include using spy satellites to intercept wireless signals\textsuperscript{170}—do not violate territorial sovereignty for two reasons: (1) the State agents intercepting the information are located outside of the targeted State; and (2) the interception does not require accessing cyber infrastructure located on the targeted State’s territory. A low-intensity cyber operation satisfies (1) but not (2): although the operation is conducted remotely, obtaining the information requires accessing computer systems located on the territory of the targeted State.\textsuperscript{171} Such low-intensity cyber operations thus involve precisely the “exercise [of] power . . . in the territory of another state” that the first \textit{Lotus} principle prohibits.\textsuperscript{172}

\begin{flushleft}
\textsuperscript{167} Id.
\textsuperscript{168} BUCHAN, supra note 16, at 58.
\textsuperscript{169} X (Re), 2009 FC 1058, [2010] 1 F.C.R. 460, ¶ 40 (Can.).
\textsuperscript{170} See, e.g., Chesterman, supra note 146, at 108.
\textsuperscript{171} See, e.g., Ziolkowski, supra note 163, at 429 (arguing that cyber-espionage does not include “electronic reconnaissance and surveillance methods . . . using, for example, satellites, long-range cameras and acoustic devices, as such methods do not include copying of data from IT-systems or computer networks”).
\textsuperscript{172} See, e.g., Sean Watts, \textit{Low-Intensity Cyber Operations and the Principle of Non-Intervention}, 14 BALTIĆ \textsc{Yearbook of International Law} 137, 145 (2017) (“[I]t could well be argued that the intrusion by US officials into data stored on servers located on German soil amounts to a violation of Germany’s territorial sovereignty because they are hereby, albeit remotely, exercising US governmental authority on German territory without German consent.”); Patrick C.R. Terry, “Don’t Do as I Do”—\textit{The US Response to Russian and Chinese Cyber Espionage and Public International Law}, 19 GERMAN LAW JOURNAL 613, 617 (2018) (noting that “the intrusion of Russian and/or Chinese government officials into data stored on servers located on US soil violated the US’s territorial sovereignty,” despite being conducted remotely, “because it is sufficient that the foreign government’s intrusive activities occurred on US
This analysis is supported by the Tallinn Manual itself. The Manual specifically distinguishes between remote cyber operations that simply intercept wireless signals and remote cyber operations that involve accessing computer systems located on the territory of another State. In the IGE’s view, the former cannot violate sovereignty “because the cyber operation does not manifest in cyber infrastructure on the target State’s territory.”  

173 By contrast, the latter at least potentially violate sovereignty because such operations do territorially manifest. 174 In other words, the IGE does not deny that low-intensity cyber operations are an “exercise [of] power . . . in the territory of another state.” Instead, it suggests—wrongly, as argued above—that the “precise legal character” of such operations “is somewhat unsettled in international law.” 175

The idea that the remote penetration of a computer system involves exercising power on the territory of the targeted State is also reflected in the Manual’s distinction between public and private data. According to the IGE, intercepting data is territorial, not extraterritorial, “so long as the data is meant to be accessible” from the State doing the intercepting. 176 That means there can be no violation of sovereignty if data stored abroad is either publicly available on the internet or is not meant to be publicly available but is nevertheless accessible from the intercepting State with the requisite passwords. 177 By contrast, intercepting data is extraterritorial—manifesting on the targeted State’s territory—if the data is both stored privately and is meant to be accessible only from the targeted State’s territory:

Such cases must be distinguished from those in which data is not meant to be made available to individuals in the State. An example would be data that is stored on a private computer abroad, even if connected to the Internet, that is not meant to be accessible. Thus, as an example, if a law enforcement agency hacks into a suspected criminal’s computer located in

173. TALLINN MANUAL 2.0, supra note 11, at 19–20.
174. Id. at 20.
175. Id.
176. Id. at 69–70.
177. Id.
another State, it is exercising enforcement jurisdiction in that State and the
day requires the latter State’s consent or a specific allocation of author-
ity under international law.\textsuperscript{178}

The Budapest Convention adopts a similar test for determining whether
intercepting data is territorial or extraterritorial. Article 32 of the Convention
provides that “[a] Party may, without the authorisation of another Party . . .
access publicly available (open source) stored computer data, regardless of
where the data is located geographically.” Accessing data that is not publicly
available, by contrast, is an extraterritorial exercise of power that requires
authorization by the territorial State.\textsuperscript{179}

4. Does a Permissive Rule Apply to Low-Intensity Cyber Operations?

Because remotely penetrating a computer system involves the “exercise [of]
power . . . in the territory of another state,” all low-intensity cyber operations
violate the first \textit{Lotus} principle unless there is either a conventional or cus-
tomy rule that permits such penetration. Moreover, as the \textit{Tallinn Manual}
notes, “[a]llocation of extraterritorial enforcement authority under treaty and
customary international law must be explicit, that is, it may not be implied
on the basis of other rules of general international law.”\textsuperscript{180}

There are numerous conventional rules that explicitly permit States, on
an exceptional basis, to violate another State’s territorial sovereignty. Two
obvious examples are Article 17 of the United Nations Convention on the
Law of the Sea, which provides that, “[s]ubject to this Convention, ships of
all States, whether coastal or land-locked, enjoy the right of innocent passage
through the territorial sea,”\textsuperscript{181} and Article 25 of the Convention on Interna-
tional Civil Aviation, which permits a State to provide assistance to a dis-
ressed civilian airplane in another State’s territory.\textsuperscript{182}

By contrast, no convention explicitly or even implicitly permits States to
engage in low-intensity cyber operations on the territory of another State as
long as they are not harmful. On the contrary, the Budapest Convention
suggests that States view the mere penetration of a computer system located

\textsuperscript{178} Id. at 70.
\textsuperscript{179} Convention on Cybercrime, supra note 142, art. 32(a).
\textsuperscript{180} \textit{Tallinn Manual} 2.0, supra note 11, at 67.
U.N.T.S. 397.
\textsuperscript{182} Convention on International Civil Aviation, supra note 151, art. 25.
on another State’s territory as a violation of their sovereignty. Article 2 thus requires each State party to criminalize, “when committed intentionally, the access to the whole or any part of a computer system without right.”

There is also no persuasive argument that customary international law imposes a de minimis test on low-intensity cyber operations that it does not impose on physical violations of territorial sovereignty. Even if we don’t count ratifications of the Budapest Convention as evidence to the contrary,183 the State practice discussed above indicates that, at best, States are nearly equally divided between the pure-sovereignist and relative-sovereignist positions. That is far from the “general practice” that the creation of a customary cyber exception to the first Lotus principle requires.

Because there is no conventional or customary exception to the first Lotus principle in cyberspace, the pure-sovereignist position is correct: all low-intensity cyber operations violate the sovereignty of the territorial State because sovereignty prohibits any exercise of power, no matter how minimal or harmless, on another State’s territory. Indeed, given that States almost universally accept that sovereignty applies in cyberspace as a rule, not a principle, that is not a difficult conclusion to reach.184

V. THE QUESTION OF ESPIONAGE

As noted earlier, despite some members of the IGE defending the pure-sovereignist position, the Tallinn Manual states that “[t]he precise legal character of remote cyber operations that manifest on a State’s territory is somewhat unsettled in international law.”185 The IGE’s reluctance to endorse pure sovereignty appears to be based on the supposed lawfulness of espionage under international law: given the nature of general rules, if sovereignty does


184. Watts & Richard, supra note 7, at 834; see also Schmitt & Vihul, Respect for Sovereignty, supra note 33, at 1670 (“Practice and opinio juris—and perhaps treaty law—will not determine whether territorial sovereignty is inviolable; it clearly is. Rather, practice and opinio juris will inform the contours of the rule as applied in the cyber context. Over time, it may even contribute to the emergence of lex specialis rules that provide for exceptions to the lex generalis rule protecting territorial integrity and inviolability. But for the present, such possibilities amount to nothing more than lex ferenda.”).

185. TALLINN MANUAL 2.0, supra note 11, at 20.
not prohibit espionage in the physical world, there is no reason to assume it prohibits espionage in cyberspace.

The espionage argument takes two very different forms: (1) espionage is affirmatively permitted by international law, and (2) international law does not regulate espionage, so it is neither affirmatively lawful nor affirmatively unlawful. Neither argument is persuasive.

A. Is Espionage Lawful?

A minority of scholars make the more assertive claim that State practice and *opinio juris* have created a customary exception to territorial sovereignty that permits States to engage in espionage, whether kinetic or cyber. According to Jeffrey Smith, for example, “because 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.”

Similarly, Gary Brown and Keira Poellet argue that “[y]ears of state practice accepting violations of territorial sovereignty for the purpose of espionage have apparently led to the establishment of an exception to traditional rules of sovereignty—a new norm seems to have been created.”

That argument, however, suffers from a glaring problem: although many States engage in espionage in both the physical world and cyberspace, they rarely—if ever—argue that international law affirmatively entitles them to do so. The creation of customary international law requires both State


188. See, e.g., BUCHAN, supra note 16, at 162 (noting that, although “on rare occasions states have publicly acknowledged their espionage activities and, in doing so, have sought to provide justifications for this conduct. . . . these states have steadfastly refused to justify their conduct on the basis that it is lawful under customary international law”); Pål Wrange, Intervention in National and Private Cyberspace and International Law, in INTERNATIONAL LAW AND CHANGING PERCEPTIONS OF SECURITY: LIBER AMICORUM SAID MAHMUDI 307, 321 (Jonas Ebbesson et al. eds., 2014) (“I know of no state that has publicly claimed that espionage in all its forms is legal. On the contrary, states generally deny being involved in illegal espionage, and admit only when there is full proof.”).
practice and *opinio juris*; State practice is not enough.189 The brute fact that espionage is commonplace is thus incapable of creating a customary exception to territorial sovereignty.190 

Moreover, in marked contrast to States’ silence concerning the legality of espionage, numerous States have denounced espionage as internationally unlawful—*opinio juris* that cuts precisely the other way. A particularly powerful example is Mercosur’s five-party statement “strongly rejecting the [NSA’s] interception of telecommunications and the acts of espionage carried out in our countries” on the ground that such “unacceptable behaviour . . . violates our sovereignty.”191 Mexico, 192 Indonesia, 193 and the Bahamas194 took similar positions on the NSA’s spying. An older example is the international reaction to the Soviet Union’s discovery in 1960 that the United States

189. See, e.g., North Sea Continental Shelf (F.R.G. v. Den., F.R.G. v. Neth.), Judgment, 1969 I.C.J. 3, ¶77 (Feb. 20) (“Not only must the acts concerned amount to a settled practice, but they must also be such, or be carried out in such a way, as to be evidence of a belief that this practice is rendered obligatory by the existence of a rule of law requiring it.”). Interestingly, Innaki Navarrete and Russell Buchan claim that the widespread use of espionage does not even satisfy the State practice element of custom, because “[s]tate practice must be public in character to inform the development of CIL.” Inaki Navarrette & Russell Buchan, *Out of the Legal Wilderness: Peacetime Espionage, International Law, and the Existence of Customary Exceptions*, 51 CORNELL INTERNATIONAL LAW JOURNAL 897, 919 (2019). 

190. See, e.g., Craig Forcese, *Spies Without Borders: International Law and Intelligence Collection*, 5 JOURNAL OF NATIONAL SECURITY LAW AND POLICY 179, 202 (2011) (“Even if it is commonplace, spying is a poor candidate for a customary international law exception to sovereignty—whatever state practice exists in the area is hardly accompanied by *opinio juris*.”); BUCHAN, *supra* note 16, at 156–57 (“[E]ven though it may be an open secret that countries spy on friends and foes alike’, non-acknowledgment of their participation in this activity precludes the formation of state practice of the requisite quality to influence the shape and content of customary law.”); Ziolkowski, *supra* note 163, at 442 (“In contrast to the assertions of some legal commentators, the consistent State practice of espionage activities and the lack of *opinio juris* on its illegality do not constitute the practice’s (positive) legality.”). Some States have domestic legislation that authorizes foreign espionage. See, e.g., TALLINN MANUAL 2.0, *supra* note 11, at 169 (citing Sweden, Netherlands, United Kingdom, Switzerland, and Austria). Such legislation does not contribute to a customary exception, however, unless it includes or is accompanied by a statement that international law permits espionage. States are obviously entitled to authorize actions that violate international law. 


193. *Id.* at 55. 

194. *Id.* at 54 (“The Bahamas wishes to underscore . . . that international law is the standard of conduct of States, [and protects] the primacy of sovereignty, [the] maintenance of territorial integrity, [and] freedom from undue external intrusion and influence.”).
had been using reconnaissance aircraft to spy on it from within its airspace. The U.S.’s espionage was condemned as a violation of sovereignty not only by the Soviet Union but also by Poland, Tunisia, and Ceylon (now Sri Lanka). A complete survey of such contrary opinio juris is beyond the scope of this article, but Ian Brown and Douwe Korff’s conclusion about espionage and customary international law seems well-justified:

It is quite clear from the strong protests against transnational surveillance, as expressed both by individual states in Europe, South America and elsewhere, and by major intergovernmental bodies and fora such as the UN General Assembly, the Council of Europe, the European Parliament and Commission, that opinio juris, if anything, is on the opposite side: that it is a principle of public international law, confirmed in international customary law, that transnational collection of data from a country without that country’s consent, for either law enforcement or national security purposes, is unlawful.

This conclusion, it is worth noting, is supported by the fact that most States criminalize espionage conducted on their territory, because such criminalization indicates that they do not view espionage as affirmatively permitted by international law. Catherine Lotrionte has argued that such domestic laws are irrelevant to the legality of cyber espionage because “[t]he criminalization of such methods . . . is distinct from intelligence collection per se being unlawful under international law.” But that is not correct: if customary international law affirmatively permitted espionage, a State would commit a wrongful act by prosecuting a foreign national for engaging in espionage on its territory. This is the second Lotus principle, which holds that, for actions that take place on its own territory, “all that can be required of a State is that it should not overstep the limits which international law places upon its jurisdiction; within these limits, its title to exercise jurisdiction rests

195. Id. at 164.
197. See, e.g., Catherine Lotrionte, Countering State-Sponsored Cyber Economic Espionage under International Law, 40 NORTH CAROLINA JOURNAL OF INTERNATIONAL LAW 443, 479 (2014).
198. Id. at 481.
199. The spy would also presumably be entitled to immunity ratione materiae in the domestic prosecution, as she was acting lawfully on behalf of her State.
in its sovereignty.”200 In other words, because international law is superior to domestic law, a State cannot prohibit what international law specifically permits. A useful analogy is the combatant’s privilege to kill in an international armed conflict. That privilege is specifically guaranteed by international humanitarian law,201 so it would be internationally wrongful for a State to bring murder charges against an enemy soldier who killed in the heat of battle.

B. Is Espionage Unregulated?

The weakness of the idea that espionage is affirmatively permitted by international law likely explains why most scholars, including the IGE,202 take the position that espionage is simply unregulated by international law—neither permitted nor prohibited. Edwin Djabatey’s argument is the most legally precise:

It is worth noting that cyber espionage itself, that is, the collection of information vital to the protection of the State, does not breach international law irrespective of whether it is conducted for economic purposes or for more traditional military/political purposes. International law is generally silent on the permissibility of States collecting intelligence on each other. This is due to widespread acceptance that all States engage in it to some degree. Generally, those matters that international law does not regulate are left to States’ domestic legal orders to regulate (the Lotus case).203

202. TALLINN MANUAL 2.0, supra note 11, at 169.
203. Edwin Djabatey, U.S. Offensive Cyber Operations against Economic Cyber Intrusions: An International Law Analysis – Part I, JUST SECURITY (July 11, 2019), https://www.justsecurity.org/64875/u-s-offensive-cyber-operations-against-economic-cyber-intrusions-an-international-law-analysis-part-i/; see also Gary Brown, Spying and Fighting in Cyberspace: Which is Which?, 8 JOURNAL OF NATIONAL SECURITY LAW AND POLICY 621, 622 (2016) (“Espionage has been considered unregulated under the international legal system—meaning cyber activities that constitute espionage are neither lawful nor unlawful under international law.”); Moynihan, supra note 8, at 45 (“[T]he majority position among commentators is that with the exception of certain rules, espionage is largely left unregulated by international law and as such is not prohibited by international law per se. Many commentators argue that this approach also applies in the cyber context.”); Chircop, supra note 10, at 14 (“[T]he weight of authority . . . currently favours the view that cyber espionage is not per se prohibited under international law.”).
This position has the advantage of making the widespread domestic criminalization of espionage irrelevant to whether international law prohibits committing espionage on the territory of another State. If the baseline position is that espionage is unregulated by international law, the fact that States choose to criminalize espionage domestically does not count—at least without more—as either State practice or *opinio juris* toward a customary rule prohibiting its extraterritorial commission.

Notably, the U.S. DoD has made precisely this argument:

Of course, most countries, including the United States, have domestic laws against espionage, but international law, in our view, does not prohibit espionage per se even when it involves some degree of physical or virtual intrusion into foreign territory. There is no anti-espionage treaty, and there are many concrete examples of States practicing it, indicating the absence of a customary international law norm against it.²⁰⁴

The DoD argument assumes that extraterritorial espionage is lawful as long as it is not specifically prohibited by a customary rule. But that idea is based (as the quote from Djabatey indicates) on the second *Lotus* principle, which applies only to legislative and adjudicative jurisdiction. The relevant paragraph from *Lotus* is worth quoting at length:

It does not . . . follow that international law prohibits a State from exercising jurisdiction in its own territory, in respect of any case which relates to acts which have taken place abroad, and in which it cannot rely on some permissive rule of international law. Such a view would only be tenable if international law contained a general prohibition to States to extend the application of their laws and the jurisdiction of their courts to persons, property and acts outside their territory, and if, as an exception to this general prohibition, it allowed States to do so in certain specific cases. But this is certainly not the case under international law as it stands at present. Far from laying down a general prohibition to the effect that States may not extend the application of their laws and the jurisdiction of their courts to persons, property and acts outside their territory, it leaves them in this respect a wide measure of discretion, which is only limited in certain cases by prohibitive rules; as regards other cases, every State remains free to adopt the principles which it regards as best and most suitable.²⁰⁵

As the quote makes clear, the second *Lotus* principle is that States are free to apply their laws to acts committed outside of their territory unless a rule of customary international law specifically prohibits them from doing so. That principle, however, does not extend to extraterritorial *enforced jurisdiction*—where a State exercises power on the territory of another State. That is the domain of the first *Lotus* principle, which (again) provides that “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. In this sense, jurisdiction is certainly territorial.”

It seems self-evident that, like remote cyber operations generally, remote cyber espionage represents “the exercise of power” on the territory of another State. After all, remote cyber espionage is simply a type of remote low-intensity cyber operation, one distinguished from other types—particularly law enforcement—solely by its purpose. In terms of territorial sovereignty, that is a distinction without a difference. As Pål Wrange notes, nothing in international law suggests that “measures undertaken for security and intelligence purposes should be treated differently from measures undertaken to punish and prevent crime.” We have already seen that States, scholars, and even the IEG agree that sovereignty categorically prohibits extraterritorial law enforcement in the absence of the territorial State’s consent. States are thus equally prohibited from committing espionage on the territory of another State “except by virtue of a permissive rule derived from international custom or from a convention”—and no such permissive rule exists.

**C. Remote vs. Close Access Cyber Espionage**

The *Tallinn Manual* rejects this analysis, of course, insisting that remote cyber espionage does not violate the targeted State’s territorial sovereignty unless it causes physical damage or the equivalent loss of cyber infrastructure functionality. Indeed, the *Manual* goes so far as to specifically distinguish between non-harmful remote cyber espionage and non-harmful “close-access” cyber espionage, in which the cyber operation is initiated by a State agent who is physically present on the territory of the targeted State. According to the *Manual*, only the latter violates the targeted State’s territorial sovereignty:

206. Id. at 18–19.
207. Wrange, supra note 188, at 320.
Neither could the Experts agree on the lawfulness of close access cyber espionage operations, such as the insertion of a USB flash drive into a computer located on one State’s territory by an individual acting under the direction or control (Rule 17) of another State. The majority viewed such activity as a violation of sovereignty, not because cyber espionage is involved, but rather by virtue of the fact that the individual is on another State’s territory while non-consensually engaging in the operation.\footnote{209. TALLINN MANUAL 2.0, supra note 11, at 171. At least one State, the Czech Republic, agrees. See Roguski, Importance of New Statements, supra note 72.}

This is a curious and indefensible distinction. It is obviously based on the idea that remote cyber espionage—unlike close-access cyber espionage—does not involve non-consensual presence on another State’s territory. But that idea makes little logical sense, given that the penetrated computer system is physically located on the territory of the targeted State in both situations.\footnote{210. Cf. Roguski, Importance of New Statements, supra note 72 (“It is not clear why a close-access cyber operation resulting in the installation of malware on a computer in the targeted State should be regarded as a violation of that State’s sovereignty, while a remote-access cyber operation producing exactly the same result should not.”); see also BUCHAN, supra note 16, at 54 (“[T]he Tallinn Manual 2.0 does not explain why the majority of the Experts considered close access cyber espionage to be unlawful as soon as the responsible state intrudes into the physical territory of the victim state (and regardless of whether that operation causes damage or harm), but remote access cyber espionage that trespasses upon another state’s cyber infrastructure is lawful (unless it gives rise to damage or harm.”).} Moreover, it is inconsistent with the IGE’s own belief, discussed earlier, that cyber operations “manifest on a State’s territory” when they involve accessing non-public data that is stored on a computer system located in another State.\footnote{211. TALLINN MANUAL 2.0, supra note 11, at 20.} Remote cyber espionage targets non-public data almost by definition.\footnote{212. See, e.g., id. at 168.}

There is, in short, no legally relevant difference between remote and close-access cyber espionage: either both violate sovereignty or neither does. Interestingly, at least a few members of the IGE acknowledged the need for symmetry between the two types of espionage, claiming that both are lawful because “extensive State practice of conducting espionage on the target State’s territory has created an exception to the generally accepted premise that non-consensual activities attributable to a State while physically present on another’s territory violate sovereignty.”\footnote{213. Id. at 19.} That position is coherent, unlike the position taken by the IGE majority. But it is legally meritless: as we
have seen, opinio juris in support of a customary exception for espionage, physical or cyber, is completely lacking.

D. Cyber Espionage and Inherently Governmental Functions

The Tallinn Manual appears to recognize that limiting violations of sovereignty to cyber operations that cause physical damage or equivalent loss of cyber infrastructure functionality would be too permissive, effectively giving States carte blanche to engage in cyber operations—law enforcement and espionage alike—that “merely” involve installing backdoors or monitoring malware, manipulating or exfiltrating data, or causing temporary loss of functionality. That possibility almost certainly explains why the IGE endorsed a second category of low-intensity cyber operations that violate sovereignty, those that interfere with or usurp an inherently governmental function. According to the Manual, such cyber operations are not subject to a de minimis test; any operation that interferes with or usurps an inherently governmental function is internationally wrongful.214

This second category of sovereignty violations, which reflects internal sovereignty’s governmentality aspect, makes it possible for the IGE to distinguish between law enforcement and espionage, even though both normally involve cyber-activities—particularly the exfiltration of data—that by design do not cause the kind of physical damage or loss of functionality that (according to the IGE) violates territorial sovereignty. Cyber operations that exfiltrate data for law enforcement purposes violate sovereignty because law enforcement is an inherently governmental function; cyber operations that exfiltrate the same data for purposes of espionage do not violate sovereignty because espionage is not an inherently governmental function. Here is what the Manual says about law enforcement:

With respect to usurpation, the International Group of Experts concurred that a State may not conduct inherently governmental functions exclusively reserved to another State on the latter’s territory. An example on point is the exercise of law enforcement functions within another State’s borders in the absence of either an allocation of authority under international law or consent (Rule 11). To illustrate, if one State conducts a law enforcement

214. Id. at 21 (“It matters not whether physical damage, injury, or loss of functionality has resulted or whether the operation qualifies in accordance with the various differing positions outlined above for operations that do not result in a loss of functionality.”).
operation against a botnet in order to obtain evidence for criminal pros-ecution by taking over its command and control servers located in another State without that State’s consent, the former has violated the latter’s sovereignity because the operation usurps an inherently governmental function exclusively reserved to the territorial State under international law.215

The Manual does not specifically argue that espionage does not usurp an inherently governmental function, but that assumption is implied in its differential treatment of espionage and law enforcement: if espionage did usurp an inherently governmental function, no de minimis test would apply, and any extraterritorial act of espionage would violate sovereignty.216

The distinction between law enforcement and espionage makes sense in terms of usurpation. As the quote above from the Manual indicates, international law reserves to States the exclusive right to engage in law enforcement on their territory. The same is not true of espionage: international law does not affirmatively permit States to engage in espionage at all, at least outside of armed conflict. Unlike law enforcement, therefore, espionage does not usurp an inherently governmental function.

The difficulty with the Tallinn Manual’s distinction between law enforcement and espionage is that “usurpation” is not the only basis for a violation of sovereignty. A State is also prohibited, according to the IGE, from “interfering” with an inherently governmental function. The focus with interference is not on the nature of the cyber operation (law enforcement or espionage) but on whether that cyber operation makes it more difficult for the territorial State to engage in governmentality.217

It seems clear that at least some kinds of cyber espionage should violate sovereignty because they interfere with an inherently governmental function. Consider, for example, a situation in which a State hacks into another State’s defense system and steals its nuclear launch codes. According to the Tallinn Manual, the hacking does not violate the targeted State’s territorial sovereignty because it did not cause physical damage or render the targeted State’s

215. Id. at 22–23.
216. Schmitt has confirmed this interpretation in an e-mail to the author. E-mail from Michael Schmitt to author, supra note 109.
cyber infrastructure inoperable. The hacking also does not usurp the targeted State’s governmental sovereignty because espionage is not an inherently governmental function. But surely the hacking interferes with the targeted State’s governmental sovereignty? After all, national security is the prototypic governmental function,218 and the theft of the launch codes makes it possible for the perpetrator State to disrupt, and perhaps even neutralize, the targeted State’s nuclear defense capability. A more significant interference is difficult to imagine.

This analysis is straightforward—yet the Tallinn Manual explicitly rejects it:

The majority of the Experts was of the view that exfiltration violates no international law prohibition irrespective of the attendant severity. They suggested that the legal issue is not severity, but instead whether the method employed is unlawful. A few Experts took the position that at a certain point the consequences suffered by the target State are so severe (e.g., the exfiltration of nuclear launch codes) that the operation is a violation of sovereignty (Rule 4). The majority countered by stating that this position is not reflective of lex lata.219

It is a strange view of sovereignty that prohibits a State’s law enforcement officials from hacking into a suspected criminal’s laptop when he is abroad220 but permits that same State’s intelligence service to hack into an enemy’s defense system and steal its nuclear launch codes.

To be sure, it is possible to defend a broader understanding of inherently governmental functions, one that would effectively prohibit any act of cyber espionage. A number of States believe that they have the exclusive right to regulate all cyber-activity that takes place on their territory, what is often

218. TALLINN MANUAL 2.0, supra note 11, at 22 (deeming “the performance of key national defence activities” an exclusively governmental function).

219. Id. at 171.

220. A violation of sovereignty on usurpation grounds. See id. at 70 (“[I]f a law enforcement agency hacks into a suspected criminal’s computer located in another State, it is exercising enforcement jurisdiction in that State and the activity requires the latter State’s consent or a specific allocation of authority under international law.”).
referred to as “cyber sovereignty.” China articulates cyber sovereignty—echoed in softer forms by States such as Finland, Germany, and the Netherlands—as follows:

National governments are entitled to administer cyberspace in accordance with law. They exercise jurisdiction over ICT infrastructure, resources and activities within their territories, and are entitled to protect their ICT systems and resources from threat, disruption, attack and destruction so as to safeguard citizens’ legitimate rights and interests in cyberspace. National governments are entitled to enact public policies, laws and regulations with no foreign interference.

If States have the exclusive right “to protect their ICT systems and resources from threat, disruption, attack and destruction,” it is difficult to understand how any act of cyber espionage does not interfere with a State’s governmental sovereignty. By definition, cyber espionage makes it more difficult for a State to ensure that only legally authorized cyberactivity takes place on its territory. It is not surprising, therefore, that at least one State—

221. Statement of Finland, supra note 45, at 1 (“While cyberspace as a whole cannot be subject to appropriation by any State, each State has jurisdiction over the cyber infrastructure and the persons engaged in cyber activities within its territory. Sovereignty confers each State the exclusive right to exercise the functions of a State within a certain territory.”).

222. Statement of Germany, supra note 2, at 3 (“Within its borders, a State has the exclusive right—within the framework of international law—to fully exercise its authority, which includes the protection of cyber activities, persons engaging therein as well as cyber infrastructures in the territory of a State against cyber and non-cyber-related interferences attributable to foreign States.”).

223. Statement of the Netherlands, supra note 44, at 2 (“States have exclusive authority over the physical, human and immaterial (logical or software-related) aspects of cyberspace within their territory. Within their territory they may, for example, set rules concerning the technical specifications of mobile networks, cybersecurity and resilience against cyberattacks, take measures to combat cybercrime, and enforce the law with a view to protecting the confidentiality of personal data.”).


225. Such cyber sovereignty obviously carries with it significant risk of human-rights abuse regarding privacy, freedom of expression, etc. The exercise of cyber sovereignty is, however, always limited by prohibitive rules of international law. See TALLINN MANUAL 2.0, supra note 11, at 14 (noting that although “a State may regulate the cyber activities of those
the Bahamas, in response to NSA surveillance—has denounced cyber espionage as inherently incompatible not only with territorial integrity but also with “freedom from undue external intrusion and influence.” In fact, Russell Buchan has suggested that the WikiLeaks revelations have “given rise to state practice which, albeit embryonic, indicates that espionage is being increasingly regarded as impermissible interference with the performance of governmental functions” and thus violates sovereignty.

Debates over the scope of governmental sovereignty matter, however, only because a number of States and the Tallinn Manual do not endorse the pure-sovereignist position, despite it having a much stronger foundation in general international law than its relative-sovereignist competitor. If any low-intensity cyber operation violates territorial sovereignty, including espionage, there is no need to create a special category of non-harmful operations that violate sovereignty because they interfere with or usurp an inherently governmental function.

VI. POLICY CONSIDERATIONS

The reluctance of States and the Tallinn Manual to adopt the pure-sovereignist position would be understandable if either of the other positions on sovereignty in cyberspace—sovereignty as a principle or relative sovereignty—was superior from a policy perspective. But that is not the case.

A. Sovereignty as a Principle

If sovereignty was a principle and not a rule in cyberspace, as the United Kingdom argues, international law would give States carte blanche to conduct cyber operations that do not rise to the level of a use of force or prohibited intervention. In other words, States could conduct any of the low-intensity

---

226. BUCHAN, supra note 16, at 54.
227. Id. at 55.
228. See, e.g., Corn & Taylor, supra note 60, at 210 (“Because the doctrine of sovereignty does not prevent all actions by one state that affect another state or even ‘encroachment on other sovereign jurisdictions’, a state involved in operations against ISIS, such as the United States, is not precluded from taking action against ISIS’s cyber facilities in other states, even on its territory, including both natural and legal persons. . . . State censorship of, or restrictions on, online communications and activities are subject to applicable international human rights law”).
cyber operations discussed in this article—whether for law enforcement, counterterrorism, or espionage—without fear of (lawful) retaliation by the targeted State. As discussed earlier, States are entitled to engage in countermeasures only in response to internationally wrongful acts.

To be sure, the unavailability of countermeasures would not leave a State targeted by a low-intensity cyber operation powerless to defend itself. The targeted State would be free to engage in a retaliatory low-intensity cyber operation of its own. That freedom, however, is not an adequate substitute for the legal right to engage in countermeasures. Not all States—indeed, relatively few—have the technological ability to respond to a low-intensity cyber operation with a low-intensity cyber operation of their own. For those that do not, the freedom to engage in counter-cyber operations would be illusory: they would simply have to tolerate low-intensity cyber operations that manifest on their territory, law enforcement, counterterrorism, and espionage alike—even when those operations caused physical damage or rendered cyber infrastructure inoperable. International law would only prohibit other States from targeting them with cyber operations that rose to the level of a prohibited intervention or use of force.

This is why countermeasures are so important for less powerful States: they do not have to be in kind. A State targeted by a low-intensity cyber operation that violates its sovereignty does not have to respond with its own cyber operation; it can engage in any proportionate response to that internationally wrongful act, such as by “denying the state launching [the cyber operation] overflight or landing rights provided for in a respective treaty.” The availability of countermeasures thus ensures that every State, no matter its technological capability, has both the right and the ability to defend itself against an unlawful cyber operation.

From a policy perspective, then, sovereignty as a principle is attractive only for powerful States that want the legal right to engage in offensive low-intensity cyber operations and have the technological capability to defend themselves against such operations with low-intensity cyber operations of

without the consent of the host state, unless doing so constitutes a prohibited intervention or use of force.”

229. See Schmitt, Defense of Sovereignty, supra note 82, at 5.

230. As noted earlier, data compiled by the Council on Foreign Relations indicates that only thirty-four States have engaged in low-intensity cyber-operations over the past sixteen years. See Cyber-Operations Tracker, supra note 9.

their own. For less technologically sophisticated States, or for States that are simply in favor of greater regulation of cyberspace by international law, that position makes little sense. It is thus not surprising that so few States have endorsed the sovereignty-as-a-principle position—or that some States, such as Finland, have specifically condemned it.

It is also worth noting that even technologically sophisticated States have reason to endorse sovereignty as a rule. The first reason is reputational: as Schmitt notes, “[s]tates that do not intend to conduct offensive cyber operations or see themselves as likely victims will understandably perceive the approach as threatening, particularly if espoused by states wielding substantial cyber capability.” The second reason is more pragmatic. Advocates of sovereignty as a principle often invoke the need for States like the United States to be able to engage in counterterrorism on the territory of hostile States without fear of lawful countermeasures. Leaving low-intensity cyber operations unregulated by international law, however, empowers all States with offensive capability—not just those who will ostensibly use their power wisely:

While fighting terrorist groups like ISIS is a laudable policy objective from both a domestic and international security perspective, the principle of sovereign equality means that such a justification will be equally available to all other states. Thus, the proposition that cyber operations on foreign soil are permissible if undertaken to counter terrorist activities . . . could open the door to other states’ cyber operations against U.S. cyber infrastructure, for understandings of what the term “terrorism” denotes differ dramatically. For example, China’s 2015 counterterrorism legislation provides an open-ended definition of terrorism that could extend to nonviolent dissident activities and certain exercises of speech. If the United States justifies unilateral actions in foreign cyber infrastructure on the basis of counterterrorism, it is reasonable to assume that other states will feel entitled to do the same, and may use expansive definitions in doing so.

232. Efrony & Shany, supra note 19, at 648–49 (pointing out that “[o]ptionality is particularly relevant for those states that have the greatest capacity to operate covertly in cyberspace and to protect their national security interests outside the framework of international law”).

233. See Statement of Finland, supra note 45, at 3 (condemning the position because “[a]greement that a hostile cyber operation below the threshold of prohibited intervention cannot amount to an internationally wrongful act would leave such operations un-regulated and deprive the target State of an important opportunity to claim its rights”).


235. Schmitt & Vihul, Sovereignty in Cyberspace, supra note 8, at 217.
Needless to say, a counterterrorism cyber-free-for-all is hardly conducive to international peace and security.

B. Sovereignty as a Rule

Every State, in short, has an interest in promoting the idea that sovereignty applies in cyberspace as a rule, not as a principle. The question is which position they should endorse: pure sovereignty or relative sovereignty. As explained earlier, because both categorically prohibit low-intensity cyber operations that involve extraterritorial law enforcement (including counterterrorism), the critical difference between them is the legality of cyber espionage: whereas the pure-sovereignist position deems all cyber espionage a violation of sovereignty, the relative-sovereignist position permits cyber espionage as long as it is not harmful.

Which position to endorse depends on whether a State wants the freedom to engage in cyber espionage. If a State does not want that freedom—whether out of principle or (more likely) because it lacks the technological ability—pure sovereignty is obviously the more desirable position: any act of cyber espionage will be an internationally wrongful act that entitles the State to respond with proportionate countermeasures. The pure-sovereignist position thus maximizes a State’s ability to defend itself against cyber espionage—and likely helps deter cyber espionage in general because would-be perpetrator States will have no “grey zone” concerning the legality of a particular operation to exploit.236

For the same reasons, a State that wants to engage in cyber espionage and has the requisite technological ability should prefer the relative-sovereignist position. That position would permit the State to engage in cyber espionage as long as it avoided causing physical damage or rendering cyber infrastructure inoperable. And although the State would lose the right to engage in countermeasures against non-harmful cyber espionage that targeted its computer systems, it would still have the freedom to respond to such cyber espionage with low-intensity cyber operations of its own.

236. See Michael N. Schmitt, “Grey Zones” in the International Law of Cyberspace, 42 YALE JOURNAL OF INTERNATIONAL LAW 1, 21 (2017) (“Certitude that a cyber operation can risk consequences at a set level can deter the taking of that operation, because the State concerned cannot act in the hope that the target State will hesitate to respond out of concern that its response might be viewed as unlawful.”).
The relative-sovereigntist position would thus seem particularly attractive for technologically sophisticated States that respect international law. Those States would presumably be uninterested in engaging in cyber espionage that causes physical damage to the territorial State or renders its cyber infrastructure inoperable. Their interest would lie in non-harmful forms of cyber espionage, such as the NSA surveillance revealed by WikiLeaks: monitoring communications, exfiltrating information, deleting or amending data. For them, relative sovereignty would appear to strike the perfect balance between offense and defense—neither too restrictive nor too permissive.\(^\text{237}\)

That said, even States with the ability to engage in cyber espionage have reason to prefer an international legal regime that categorically prohibits, and thus helps deter, such espionage even when it is not harmful. Simply put, many types of “harmless” cyber espionage—both public and private—pose a threat to even the most powerful and technologically sophisticated States.

This is most obvious in terms of espionage against corporations. It is uncontroversial that a State’s territorial sovereignty extends to both private and public cyber infrastructure,\(^\text{238}\) and there may well be acts of cyber espionage that satisfy the relative-sovereigntist position by causing significant harm to private cyber infrastructure.\(^\text{239}\) An example is the Shamoon 1 malware attack on Saudi Aramco mentioned earlier, widely attributed to Iran, which wiped out the memory of at least 30,000 computers. Not only was

\(^\text{237}\). See, e.g., Moynihan, supra note 8, at 23 (“An approach based on quantitative and/or qualitative effects in the target state, or some other form of de minimis threshold, is attractive from a practical and pragmatic point of view as it enables states to take action in relation to cyber intrusions that may not reach the threshold of intervention but that nevertheless cause harmful effects within the territory.”).

\(^\text{238}\). See, e.g., TALLINN MANUAL 2.0, supra note 11, at 13–14 (“With respect to a State’s internal sovereignty, it is irrelevant as a matter of international law whether the cyber infrastructure in question is public or private in character, or whether the cyber activities concerned are engaged in by the State’s organs or by private individuals or entities.”); Buchan, supra note 17, at 183 (“State practice reveals that States consider their sovereignty to extend to information in cyberspace which belongs to government institutions and to private entities and individuals over which they exercise jurisdiction.”).

\(^\text{239}\). Some private cyber-espionage might even violate the principle of non-intervention. Moynihan suggests as much for the distributed denial of service attacks, attributed to Iran, that targeted the entire U.S. financial sector between 2011 and 2013. See Moynihan, supra note 8, at 39.
Saudi Aramco’s entire computer network inoperable for ten days, it needed months to replace all of the affected systems.\(^{240}\)

Most private cyber espionage, however, will not cause physical damage or equivalent loss of cyber infrastructure functionality. As Djabatey points out, “the creation of a backdoor to access commercial or technological information is unlikely to be of a scale equivalent to the emplacement of malware capable of significantly impairing or damaging critical infrastructure.”\(^{241}\) Consider the examples mentioned in the introduction to this article: China’s theft of intellectual property from Lockheed-Martin in 2009 and Google in 2010; Iran’s hacking of universities in the United States, United Kingdom, Australia, and other States between 2016 and 2019.\(^{242}\) Or consider the Flame virus, believed to be the work of the United States and Israel, which targeted Iranian oil companies and had the ability to “activate computer microphones and cameras, log keyboard strokes, take screenshots, extract geolocation from images, and send and receive commands and data through Bluetooth wireless technology.”\(^{243}\) The pure-sovereignist position would deem all of these acts of private cyber espionage internationally wrongful simply because they involved penetrating computer systems located on another State’s territory. But they would be entirely lawful under the relative-sovereignist position because they did not harm the computer systems from which the information was exfiltrated.

Private cyber espionage is extraordinarily costly. The IP Commission Report, for example, states that the theft of intellectual property from American companies alone amounts to “hundreds of billions of dollars per year.”\(^{244}\) It seems safe to assume that, as a general rule, law-abiding States are far less likely to engage in private cyber espionage than lawless ones. Law-abiding States thus have little incentive to accept a conception of sovereignty that does not deem private cyber espionage internationally wrongful and thereby prohibits them from taking countermeasures against the responsible State. Yet, that is precisely what the relative-sovereignist position does.

\(^{240}\) Efrony & Shany, supra note 19, at 621. Schmitt argues persuasively that “the 2012 cyber operations against Saudi Aramco necessitated the replacement of affected computers and therefore, if conducted by another State as is suspected, amounted to a violation of sovereignty even though the systems suffered no physical damage.” Schmitt, “Virtual Disenfranchisement, supra note 217, at 44.

\(^{241}\) Djabatey, supra note 203, at 5.

\(^{242}\) See, e.g., Moynihan, supra note 8, at 3.

\(^{243}\) Buchan, supra note 17, at 169.

\(^{244}\) Quoted in Lotrionte, supra note 197, at 451.
The policy calculus is more complicated for public cyber espionage, because the relative-sovereigntist position prohibits low-intensity cyber operations that interfere with or usurp inherently governmental functions regardless of whether they cause harm. Properly understood, that aspect of internal sovereignty should prohibit much, if not all, public cyber espionage. Insofar as States follow the Tallinn Manual’s curious approach to “interference,” however, the relative-sovereigntist position—unlike its pure-sovereigntist competitor—will tolerate at least some public-cyber espionage. Consider, for example, the United States’ “Cyber Pearl Harbor,” in which China allegedly hacked the Office of Personnel Management and stole the personal data of millions of past and present government employees. It is difficult to see how that act of cyber espionage violated relative sovereignty, given that it did not harm the accessed computer systems. Dan Efrony and Yuval Shany believe the theft likely “had short-term adverse consequences for counterintelligence activities and compromised the safety of American intelligence agents operating abroad.” But even so, if stealing nuclear launch codes doesn’t interfere with an inherently governmental function, surely stealing personnel information from a government computer system doesn’t either.

Other notorious acts of public cyber espionage also avoid running afoul of the relative-sovereigntist position. For example, Russia’s Solar Winds operation planted backdoors in the computer systems of a variety of U.S. government agencies (as well as in corporate computer systems) that “allowed them to come and go, steal data and . . . alter data or conduct destructive attacks.” Then-president-elect Biden described Solar Winds as a “cyber assault” and vowed “not to stand idly by”—yet Schmitt concludes, applying the Tallinn Manual’s rules, that the operation did not violate U.S. sovereignty.

Proponents of the relative-sovereigntist position—States and scholars alike—never explain why any State would want to tolerate these kinds of public cyber espionage. The U.S. reluctance to endorse pure sovereignty

245. Efrony & Shany, supra note 19, at 601.
might be somewhat understandable, because it does not have to “stand idly by” in the face of cyber espionage like Solar Winds if it cannot engage in countermeasures: given its technological sophistication, the United States will almost always be able to retaliate with a far more effective low-intensity cyber operation of its own. Once critical information is stolen through espionage, however, counter-espionage cannot unsteal it. All a State like the United States can do is punish the responsible State, hoping to deter it from engaging in similar acts in the future.

That potential response might be sufficient to justify relative sovereignty if the threat of retaliation would be more likely to deter public cyber espionage than the threat of countermeasures. But that is almost certainly not the case. A cyber operation launched in response to lawful public cyber espionage would have to remain within the limits imposed by international law. That means it could not involve a use of force against the targeted State, could not intervene in the targeted State’s internal affairs, could not damage or render inoperable the targeted State’s cyber infrastructure, and could not usurp or interfere with the targeted State’s inherently governmental functions. The deterrent value created by the threat of such retaliation would thus likely be limited—particularly in contrast to the threat of countermeasures, which could involve any proportionate response to the public cyber espionage, including responses in the physical world.

Moreover, few States have the U.S.’s cyber capabilities. For States that cannot credibly threaten cyber retaliation, the relative-sovereigntist position removes the one deterrent and the one potentially effective response they have against cyber espionage. They simply have to accept non-harmful cyber espionage, public and private. Indeed, they must accept it even when non-harmful cyber espionage has the potential to become extremely damaging later on—such as Operation Nitro Zeus, which involved “the US penetrating deeply into Iran’s infrastructure before the 2015 nuclear accord [and] placing digital ‘implants’ in systems that would enable it to bring down power grids, command-and-control systems and other infrastructure in case a conflict broke out.” According to the relative-sovereigntist position, Iran had no right to engage in countermeasures unless and until the United States decided to activate the digital implants and actually caused physical damage or equivalent loss of cyber infrastructure functionality. That is a problematic

limitation—akin to prohibiting the police from arresting a suspect who is pointing a gun at someone until he pulls the trigger.

To be sure, some scholars have argued that tolerating public espionage promotes international peace and security. Christopher Baker, for example, adopts a “functionalist” defense of espionage, claiming that it enables States “to better appreciate their partners’ negotiating positions,” thereby encouraging “strategic dialogue,” and functions as “a tool that enables ‘super-validation’ of international compliance with security agreements.” He thus concludes that espionage’s supposed permissibility means that “a heightened level of international cooperation is achieved.”

Baker’s argument is not convincing. It is difficult to understand how international peace and security are promoted by China stealing plans for the F-35 fighter from Lockheed-Martin, Russia planting backdoors in the computer systems of critical U.S. government agencies, or the United States systematically intercepting the private communications of its allies, including their heads of State. Indeed, the Brazilian president’s response to the NSA surveillance in front of the General Assembly—made after she canceled an important visit to Washington—provides the most powerful rebuttal to Baker: “Friendly governments and societies that seek to consolidate a truly strategic partnership, such as is our case, cannot possibly allow recurring and illegal actions to go on as if they were normal, ordinary practice. Such actions are totally unacceptable.” Insofar as States care about international peace and security, therefore, they should oppose the legality of all public cyber espionage—which means endorsing the pure-sovereigntist position.

C. The Problem of Ambiguity

In short, all but the most lawless States have no incentive to engage in, much less tolerate, private or public cyber espionage. Moreover, even if law-abiding States are inclined to maintain some legal freedom to engage in offensive
In Defense of Pure Sovereignty in Cyberspace

The practical utility of the relative-sovereigntist position is undermined by three important ambiguities.

The first ambiguity is the most obvious: no one—not States, not scholars—is quite sure where the red line is or should be drawn between low-intensity cyber operations that violate a State’s territorial sovereignty and low-intensity cyber operations that do not. Proponents of relative sovereignty agree at the margins: it is lawful for a cyber operation to merely penetrate a computer system or exfiltrate information; it is unlawful for a cyber operation to cause physical damage or equivalent loss of cyber infrastructure functionality. Between the margins, however, lies a significant “grey zone” of uncertainty.256 Some States, like New Zealand, endorse relative sovereignty without even attempting to establish a red line. Others, like the Netherlands, follow the Tallinn Manual. And still others adopt their own idiosyncratic tests, from permitting cyber operations that have no more than “negligible physical effects” (Germany) to prohibiting those that cause “material harm” (Finland).

The German and Finnish tests are ambiguous, and the Dutch position is even less helpful. As discussed earlier, the IGE did not rule out the possibility of cyber operations violating territorial sovereignty despite not causing physical damage or equivalent loss of cyber infrastructure functionality. Instead, according to Schmitt, the director of the project, the Experts offered a “confusing mélange of views” on the appropriate test, making it “impossible to draw definitive red lines.”257 Moreover, all of the Experts justified their views by reference to the object and purpose of sovereignty,258 making it clear that any attempt to harmonize the various versions of the relative-sovereigntist position would be unlikely to succeed.

The second ambiguity concerns the other aspect of the relative-sovereigntist position: governmentality. At first glance, that aspect appears easier to apply because States have generally endorsed the Tallinn Manual’s position that no de minimis test applies to low-intensity cyber operations that interfere with or usurp inherently governmental functions. The problem is that, as the Manual openly acknowledges, the IGE could not “definitively” identify which functions should be considered inherently governmental.259 Instead,

256. The helpful term is Schmitt’s. See generally Schmitt, “Virtual” Disenfranchisement, supra note 217.
257. Id. at 45.
258. Id.
259. TALLINN MANUAL 2.0, supra note 11, at 22.
the Experts simply offered a few indicative examples of such functions, leaving it to States to further develop governmentality through their practice and opinio juris.

Relative sovereignty’s third ambiguity concerns the distinction between law enforcement and non-harmful espionage. As we have seen, the relative-sovereigntist position draws a hard line between the two: law enforcement always violates the territorial State’s sovereignty because it usurps an inherently governmental function; non-harmful espionage never does because espionage is unregulated by international law. As Jennifer Daskal notes, however, because law enforcement and espionage are distinguished more by purpose than by method, it can be extremely difficult in practice to categorize a specific low-intensity cyber operation:

[S]uch a purpose-based test will be almost impossible to implement. It assumes a clear-cut division of intelligence and law enforcement operations that can easily be discerned, where in practice the lines between intelligence gathering and law enforcement are often blurred. Moreover, even when there are relatively clear-cut divisions between law enforcement and intelligence operations, information obtained for one purpose may ultimately be shared and used for another. In such situations, how does one assess purpose? Based on the entity that did the information gathering—an easily manipulated factor? Based on how it is ultimately used—a consideration that raises all kinds of practical complexities, given the inevitable and perhaps lengthy time lag between collection and use?260

The Tallinn Manual openly acknowledges that “it can be challenging for a target State to distinguish cyber espionage activities from other cyber operations.”261 But instead of questioning the validity of the distinction, the IGE simply punted the issue, insisting—without explanation—that “this dilemma” can be resolved “by the various requirements regarding certainty that apply with respect to State responses to cyber operations.”262

If the relative-sovereigntist position wins out, the grey zones created by these three ambiguities will make it highly likely, if not unavoidable, that States will clash over both the legality of specific low-intensity cyber operations and the legality of countermeasures taken in response to them. As

261. TALLINN MANUAL 2.0, supra note 11, at 172.
262. Id. at 173.
Schmitt points out, “[r]esolution of this quandary through State practice and opinio juris is likely to take time; until then, hostile non-injurious or non-destructive cyber operations conducted into other States’ territory will benefit from the uncertainties surrounding the legal concept of a sovereignty violation.” And Schmitt is likely being overly optimistic: if the forty scholars in the IGE could not agree on fundamental cyber sovereignty concepts such as “de minimis” and “inherently governmental function,” it beggars belief to think that 193 States will be able to do so.

Even worse, the relative-sovereigntist position’s grey zones will almost certainly be exploited more often by technologically sophisticated States than by States that are less technologically capable. Most States simply lack the ability to exploit those grey zones through offensive cyber operations, as indicated by the fact that only thirty-four States have conducted such operations since 2005, with the vast majority—77 percent—being the work of just four States: China, Russia, Iran, and North Korea. But even States that do have offensive capabilities will be asymmetrically affected by relative sovereignty’s ambiguities, because most will be deterred by the threat of a targeted State applying a different understanding of de minimis or inherently governmental function and engaging in countermeasures. Powerful States might be able to weather countermeasures “wrongly” imposed. For the less powerful, such countermeasures could prove calamitous.

It is not surprising, then, that Efrony and Shany have found that “several States that are heavily engaged in cyberoperations appear at this point in time to have a limited interest in promoting legal certainty regarding the regulation of cyberspace”—particularly Russia, China, and the United States. Simply put, ambiguity favors the strong. All other States have a compelling interest

265. See Moynihan, supra note 8, at 20 (“International law must be applied objectively, rather than sovereignty simply meaning whatever a state says it is, but the lack of any specific criteria for violations increases the risk of states interpreting sovereignty subjectively.”).
266. Efrony & Shany, supra note 19, at 585.
in endorsing a conception of sovereignty that is clearer and more administra-
ble—namely, the pure-sovereigntist position. As Schmitt says, “legal clarity breeds international stability. The brighter the red-lines of interna-
tional law as applied to cyber activities, the less opportunity States will have
to exploit grey zones in ways that create instability.”

VII. CONCLUSION

Chircop has described the legal status of low-intensity cyber operations—
those that do not violate either the prohibition of the use of force or the
principle of non-intervention—as the “foremost” controversy concerning
how international law applies in cyberspace. That description seems war-
ranted, given how deeply divided States are over the question of when such
operations violate sovereignty and permit the targeted State to engage in
countermeasures.

This article has considered the three positions States have taken on that
issue. It has rejected out of hand the idea, consistently defended only by the
United Kingdom, that low-intensity cyber operations never violate sover-
eignty because sovereignty functions in cyberspace as a principle, not as a
rule. That idea is simply irreconcilable with the nature of international law
and with overwhelming State practice and opinio juris to the contrary.

The real choice is between the pure-sovereigntist position and the rela-
tive-sovereigntist position, both of which view sovereignty as a rule that ap-
plies in cyberspace. According to the former, all low-intensity cyber opera-
tions violate sovereignty because sovereignty prohibits any non-consensual
penetration of a computer system located on the territory of another State.
According to the latter, only some low-intensity cyber operations violate the
sovereignty of the targeted State—those that either (1) cause physical dam-
age or equivalent loss of cyber infrastructure functionality, or (2) interfere
with or usurp inherently governmental functions. In practice, the difference

267. Cf. Moynihan, supra note 8, at 4–5 “(States that are the victim of cyberattacks by
other states need to be able to identify which rules of international law have been breached
in order to know what action they are permitted to take in response, including whether they
are entitled to take countermeasures.”).

268. See Roguski, Violations of Territorial Sovereignty, supra note 149, at 80 (noting that, in
contrast to relative sovereignty, pure sovereignty provides “a familiar, less ambiguous and
more viable tool for assessing violations of sovereignty in cyberspace”).


between the two positions concerns cyber espionage, which pure sovereignty categorically prohibits and relative sovereignty generally permits.

Very few scholars have explicitly defended the pure-sovereignty position, most likely because of the influence of the *Tallinn Manual*, which leans toward relative sovereignty. Similarly, while ten States can safely be categorized as endorsing some version of pure sovereignty, only three have explicitly adopted that position—France, Iran, and Switzerland—and none have defended it at any length.

This article has endeavored to fill that lacuna, arguing that the pure-sovereignty position is superior to its relative-sovereignty competitor both as a matter of law and as a matter of policy. In terms of law, it has shown that pure sovereignty represents the natural application of the first *Lotus* principle in the cyber realm, while relative sovereignty represents a significant deviation from that principle—one unsupported either by convention or by custom. In terms of policy, it has shown that no State, not even the most powerful, has a compelling reason to reserve the right to engage in non-harmful public or private cyber espionage. Permitting cyber espionage is not only likely to cause them economic harm, it is an invitation to international instability.

The choice between the pure-sovereignty position and the relative-sovereignty position, therefore, is not much of a choice at all. All States, the powerful no less than the weak, have reason to endorse an international law of cyberspace based on pure sovereignty.