A HOOVER INSTITUTION ESSAY

"Defend Forward" and Sovereignty

JACK GOLDSMITH AND ALEX LOOMIS

Aegis Series Paper No. 2102

Damaging state-sponsored cross-border cyber operations beyond mere espionage have long been on the rise and appear to many to be on the verge of spinning out of control. While there has been much talk about how international law might regulate this dangerous behavior, no concrete rules have emerged. The governments of the world tried to hammer out a legal consensus on such rules in a United Nations process that lasted two decades but ended in failure in 2017.[1] A related process that began in 2018 ended in March 2021, once again without any agreement by governments on "how international law applies to State use of" information and communications technologies across borders.[2]

Against the background of these failures, and in the face of growing and seemingly more dangerous cross-border cyber operations, it is understandable that norm entrepreneurs would step in to try to do better. This in a nutshell is the aim of the *Tallinn Manual*, which argues that customary international law imposes a variety of binding rules on state behavior related to cyber operations. The first version, *Tallinn Manual 1.0*, published in 2013, proposed to describe international law on cyber operations involving the use of force and in armed conflict more generally.[3] *Tallinn Manual 2.0*, published in 2017, builds on and supersedes the original.[4] It covers peacetime cyber operations as well as ones related to armed conflict, and it revises some of its earlier rules.

Among the most discussed provisions of the *Tallinn Manual 2.0* is Rule 4 on "Violation of sovereignty." Rule 4 provides: "A State must not conduct cyber operations that violate the sovereignty of another State."[5] Considered alone, Rule 4 is banal and unobjectionable, since there are many established sovereignty-based international-law rules that cyber operations might violate. For example, the UN Charter's prohibition on certain uses of force and the customary international-law rule of nonintervention constrains cyber operations by one state in another. The hard question is whether international law related to sovereignty requires anything more. Here the commentary to Rule 4 is quite ambitious. It argues that a stand-alone customary international-law concept of state sovereignty operates to regulate and render illegal certain cyber operations that would not otherwise be illegal under any of the specific and acknowledged sovereignty-based rules of international law.

The rules articulated in the Rule 4 commentary, if valid, have important implications for nonconsensual cyber operations in many contexts. As the *Tallinn Manual 2.0* editors note, "[T]he vast majority of hostile cyber operations attributable to states implicate only the prohibition of violation of sovereignty."[6] Thus, "[T]he rule represents the most significant

red line between lawful and internationally wrongful conduct"[7]—assuming, that is, it truly represents customary international law.

In this paper we argue that the discrete rules articulated in the Rule 4 commentary do not reflect customary international law. The Rule 4 commentary cites very little legal authority in support of its bold conclusions and lacks any practical connection to the complex interplay of extensive state practice and *opinio juris* that constitutes customary international law.

We consider the validity of the Rule 4 commentary primarily in the context of the United States' "defend forward" (DF) strategy for disrupting cyber threats. The United States of course is not the only nation to engage in cross-border cyber operations that might implicate Rule 4. But the DF concept is the most prominent public example of a nation announcing its intention to conduct cyber operations that might violate the rules articulated in the Rule 4 commentary. DF is thus proper to study in this context.

The first part of this paper explains DF and sets up the question it poses for Rule 4's ostensible customary international-law restriction based on sovereignty. The second section summarizes and critiques the discrete rules in the Rule 4 commentary on their own terms. The third part provides broader reasons to doubt that these rules have a plausible basis in customary international law. The last section engages the policy aims of Rule 4 and speculates on how international-law rules in this context may develop in the future.

Defend Forward

DF aims "to disrupt or halt malicious cyber activity *at its source*, including activity that falls below the level of armed conflict."[8] It is a defensive strategy. But it contains "offensive components at the tactical and operational levels," since "to achieve defensive strategic objectives in cyberspace, forces and capabilities must be forward-positioned, both geographically and virtually."[9] As National Security Agency director Paul Nakasone explained, the United States seeks "to achieve and maintain the initiative in cyberspace over an adversary by continuously contesting them *where they operate*, particularly below the level of armed conflict."[10] Nakasone added that DF is about "confronting our adversaries *from where they launch cyber attacks*."[11]

DF thus appears to include US government cyber operations conducted in the physical territories of other nations to halt or disrupt planned malicious cyber activity. The contemplated actions go beyond intelligence collection in other countries and may involve elements of what the Defense Department defines as "cyberspace attack": actions "that create noticeable denial effects (i.e., degradation, disruption, or destruction)."[12]

The public does not know precisely what techniques US Cyber Command deploys in meeting cyber threats at their source in other countries. We have only one acknowledged example of DF: the action to prevent the Russian Internet Research Agency (IRA) from interfering with the 2018 congressional elections. Among other things, according to unnamed US officials, US Cyber Command sent Russian trolls and hackers messages using emails, pop-ups, texts, and direct messages, and blocked internet access to the IRA.[13] Other DF techniques might include the introduction of code that temporarily halts the operation of computers, that deletes or encrypts data, or that enables further surveillance and tracking. Obviously, there are many variations on these themes, and many other imaginable scenarios. And all of these activities might take place either in the nation sought to be deterred or in a neutral third country.

But regardless of specifics, DF seems to contemplate cyber operations against cyber infrastructure in the physical territories of other nations to halt or disrupt planned malicious cyber activity.

DF marks a turn from a decade of seemingly passive US government responses to increasingly damaging malicious cyber activity inside the United States. This activity was conducted primarily (but not exclusively) by Russia, China, Iran, North Korea, and nonstate actors, and ranged from massive intellectual property theft to the Russian interference in the 2016 elections to various cyberattacks on government and private networks.

Change was needed because, according to Nakasone, "inaction on our part cedes advantage to capable adversaries willing to flout international law and impose their own norms of cyber conduct."[14] DF aims to deter or preempt "malicious adversary behavior below the level of armed attack" by imposing "credible and sufficient costs against malicious adversary behavior."[15] Another aim is to develop "norms of responsible State behavior" in cyberspace.[16] In this regard, the United States maintains that DF is consistent with international law.[17]

By so prominently announcing a policy of engaging in cross-border cyber operations to disrupt or deter malicious cyber activity, the United States is doing the same thing that the editors of the *Tallinn Manual 2.0* are doing. Both stake out a position in an effort to clarify and influence the content of international law in an area where state practice is often secret and the proper application of ancient principles of sovereignty to new technologies is opaque. But there is one big difference as far as international law is concerned: the United States is a state actor, a subject of international law, and a contributor to the content of customary international law.

Tallinn Manual 2.0 and Sovereignty

This section examines and critiques on its own terms the commentary to Rule 4 of the *Tallinn Manual 2.0*.

The Tallinn Manual

The *Tallinn Manual 2.0* consists of rules followed by commentary. The rules all purport to "reflect customary international law" and thus to be "binding on all States, subject to" any persistent objector exceptions.[18]

The rules were formulated by a group of "distinguished international law practitioners and scholars, the so-called 'International Group of Experts.'"[19] The *Tallinn Manual 2.0* "is not an official document," the editors emphasize, "but rather the product of two separate endeavors undertaken by groups of independent experts acting solely in their personal capacity."[20] It does, however, purport to reflect international law "as it existed at the point of the Manual's adoption" in 2016.[21] It disclaims any intention to be a "progressive development of the law," insists it is "policy and politics-neutral," and asserts that it "is intended as an objective restatement of the *lex lata*."[22]

The commentary accompanying each rule in the *Tallinn Manual 2.0* aims "to identify the rule's legal basis, explain its normative content, address practical implications in the cyber context, and set forth differing positions as to scope or interpretation."[23] Sometimes the commentary reflects the experts' unanimous views, while at other times the experts disagree and the commentary explains the majority and minority views.

Despite claiming to discern and describe customary international law, the *Tallinn Manual 2.0* says practically nothing about how the publicly known cross-border state-sponsored cyber activity, and significant public discussion by states about this activity, inform its rules and commentary. The *Tallinn Manual 2.0* notes that "State cyber practice is mostly classified and publicly available expressions of *opinio juris* are sparse."[24] But it never explains why known state practice and the "sparse" *opinio juris* should not be relevant to the content of customary international law.

Rule 4

Chapter 1 of the *Tallinn Manual 2.0* is entitled "Sovereignty." It contains five rules, of which Rule 4—"Violation of sovereignty"—is the most pertinent to this paper.[25] Rule 4 states: "A State must not conduct cyber operations that violate the sovereignty of another State."[26] By itself, this statement is unremarkable, since it says nothing about which cyber operations violate sovereignty. And indeed, as the manual goes on to analyze in later rules, there are many specific sovereignty-based restrictions that might apply to cross-border cyber operations, including the prohibition on the use of force, the prohibition on coercive intervention, sovereign immunity, neutrality, the limits on enforcement and prescriptive jurisdiction, diplomatic law, the law of the sea, air law, space law, and international telecommunications law.[27]

It is in the commentary to Rule 4 where the novel claims appear. The commentary is filled with interesting insights and analysis. It purports to derive from the general principle of

sovereignty a number of discrete prohibitions that govern state behavior independent of and in addition to the established specific doctrines. It is the legal status of these discrete rules, and not the practically empty formulation in Rule 4, that is important. Our analysis focuses on the discrete prohibitions in the commentary that are supported by either all of the experts or a majority of them. These discrete rules rest on legal authority at a very high level of generality, misinterpret or overinterpret some legal authorities, or (most often) constitute *ipse dixits*, lacking any basis at all.

Consider comment 6 to Rule 4. It provides that "it is a violation of territorial sovereignty for an organ of a State . . . to conduct cyber operations while physically present on another State's territory."[28] The *Tallinn Manual 2.0* provides no authority for this proposition but appears to derive it from two more general principles of international law: a state's sovereignty over its territorial integrity, and the international-law rules pertaining to "enforcement jurisdiction."[29]

The experts assert without legal citation 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."[30] But this proposition is overbroad to the point of being erroneous. Sometimes a state (or its agents) crossing into foreign territory violates international law (when, for example, a state's fighter aircraft or reconnaissance drone trespasses foreign airspace), and other times it does not (such as when a state's spy crosses a border with stealth but engages in no internationally unlawful activity, or when a state sends propaganda digitally into another state). The naked principle of "sovereignty" cannot tell us why some border crossings are unlawful and some not. As we explain in the next section, one needs to look at state practice and *opinio juris* in discrete contexts to figure that out. This the manual does not do.

The Rule 4 commentary's reliance on enforcement jurisdiction commits a different type of error. Comment 6 to Rule 4 states correctly that "the non-consensual exercise of enforcement jurisdiction in another State's territory . . . is a violation of that State's sovereignty."[31] It then concludes that, "*therefore*," international law prohibits one nation from "[conducting] cyber operations while physically present on another State's territory."[32] This reliance on enforcement jurisdiction is a category mistake. Enforcement jurisdiction is a specific sovereignty-based prohibition on a specific type of activity with a specific purpose: "to induce or compel compliance or punish noncompliance with its laws or regulations."[33] As James Crawford explains, the "governing principle of enforcement jurisdiction is that a state cannot take measures on the territory of another state *by way of enforcement of its laws* without the consent of the latter."[34] The rule prohibits law enforcement–related actions such as arrest, summons, police actions, and production orders on the territory of another state.[35] Rule 11 of the manual covers this specific prohibition. A cross-border cyber operation that is not in aid of law enforcement does not implicate this particular sovereignty-based rule any more than does a black-bag job in furtherance of espionage or the firing of a cruise missile in anticipatory self-defense.

The Rule 4 commentary next asserts, in comment 7, that a majority of its experts concluded that the sovereignty rule prohibits one state's cyber espionage conducted while physically present in another state "without its consent or other legal justification."[36] They did not, however, believe that espionage conducted by remote cyber operations violated international law.[37] The *Tallinn Manual 2.0* provides no legal authority at all for this supposed prohibition (or distinction) other than the opinions of most of its experts. And yet it acknowledges a "widespread State practice of engaging in non-consensual espionage while present on another State's territory."[38] (We consider the relevance of state practice in the next part.)

The Rule 4 commentary next moves to the issue of "remote cyber operations that manifest on a State's territory," which is an issue likely implicated by the bulk of what goes on under DF.[39] Comment 10 states that the issue is "somewhat unsettled in international law" and then offers a two-part framework for assessing lawfulness: "(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."[40]

Applying the "degree of infringement" criterion, most experts agreed that a remote cyber operation causing "physical damage" violates Rule 4, while some thought that physical damage was one factor to be considered.[41] No legal authority or analysis is provided for either the degree-of-infringement criterion or these specific conclusions. Comment 10 does state that the "degree of infringement" criterion "is based on the premise that a State controls access to its sovereign territory."[42] This explanation suffers from the overgenerality problem noted above. It is thus little surprise that the experts disagreed on its application to "physical damage," and that the manual does not explain the nature of or reasons for the disagreement.

The experts further agreed that "the remote causation of loss of functionality of cyber infrastructure located in another State sometimes constitutes a violation of sovereignty, although no consensus could be achieved as to the precise threshold at which this is so due to the lack of expressions of *opinio juris* in this regard."[43] We will consider the relevance of *opinio juris* in the next part. For now, we simply note again that the commentary to Rule 4 provides no authority for its normative claims. Finally, comment 14 states that "no consensus could be achieved as to whether" a cyber operation falling below the physical-damage and loss-of-functionality thresholds (such as "a major DDoS [distributed denial of service] operation" or "emplacing malware into a system") would violate Rule 4.[44] The manual again fails to explain any legal or practical basis, if any, for the disagreement.

As for the second criterion, the experts in comment 15 state that Rule 4 prohibits "one State's cyber operation [that] interferes with or usurps the inherently governmental functions of another State."[45] They could not agree on a definition of "inherently

governmental functions," but they concluded that "a cyber operation that interferes with data or services that are necessary for the exercise of inherently governmental functions is prohibited as a violation of sovereignty."[46] Most experts believed these activities would violate Rule 4 irrespective of the cyber operation's direct effects in the affected state. Comments 17 through 21 apply this test to various hypotheticals, such as inhibiting communications between a state's leadership (illegal) and inhibiting a state's communication to the public (legal).[47]

The experts' only legal basis for these fine-grained rules comes from "the sovereign right of a State to exercise within its territory, 'to the exclusion of any other State, the functions of a State.'"[48] The internal quotation is from the 1928 *Island of Palmas* arbitration award. That award involved a dispute between the United States and the Netherlands over the Island of Palmas, a tiny piece of land in the Pacific Ocean fifty or so miles southeast of the island of Mindanao, Philippines. The case was resolved on the basis of international-law concepts of discovery, possession, competing state activity, and other propositions about title to land under international law.[49] Along the way the arbitrator made "some general remarks on *sovereignty in its relation to territory*," one of which was the following: "Sovereignty in the relations between States signifies independence," which "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."[50] This dictum from a century-old, colonial maritime territory dispute is the only legal authority even in the neighborhood of Rule 4's claim that "a cyber operation that interferes with data or services that are necessary for the exercise of inherently governmental functions is prohibited as a violation of sovereignty."[51] Yet again, state practice and *opinio juris* go unmentioned.[52]

In sum, the Rule 4 commentary maintains that the customary international-law principle of sovereignty forbids a variety of cyber operations by one state in another. It makes these claims often without citing any legal authority, sometimes on the basis of inapt or very general legal authority, and always without ever seriously examining state practice or *opinio juris*.

Tallinn Manual 2.0 and the Identification of Customary International Law

As noted above, Rule 4 and the subrules in its commentary purport to be "an objective restatement of the *lex lata*," or "the law as it currently exists."[53] The *Tallinn Manual 2.0* experts, we are told, "assiduously avoided including statements reflecting *lex ferenda*," or the law as it should be.[54] These are surprising statements with respect to the Rule 4 commentary, which purports to identify fine-grained rules of customary international law yet cites very little legal authority and mentions state practice even less. The commentary to Rule 4 adopts an unorthodox method for identifying customary international law—so unorthodox, we argue in this section, that it is entirely implausible that it reflects *lex lata*.

Why State Practice and Opinio Juris *Matter*

Customary international law, says the Restatement (Third) of Foreign Relations Law, "results from a general and consistent *practice* of states followed by them from a sense of legal obligation."[55] The International Law Commission recently stated: "To determine the existence and content of a rule of particular customary international law, it is necessary to ascertain whether there is a general practice among the States concerned that is accepted by them as law (*opinio juris*) among themselves."[56] As these and every other canonical definition of customary international law make plain, the identification of customary international law that binds states turns on the right kind of state practice and the presence of *opinio juris*, the sense of legal obligation that attaches to practice.[57]

Governments in their statements about and analyses of customary international law take these traditional two-element criteria very seriously.[58] International and domestic courts are in practice less rigorous. They sometimes elevate the *opinio juris* requirement over state practice and discern *opinio juris* in multilateral treaties, domestic and international case law, and authoritative nonbinding instruments (such as UN General Assembly resolutions).[59] They sometimes rely in part on secondary sources, including the work of scholars, even though the opinion of experts without probative supporting legal materials obviously cannot count.[60] And they sometimes use what some have described as a deductive method for identifying customary international law, but tend to do so only after considering state practice and *opinio juris*.[61]

A serious analysis of customary international law must at least be attentive to extant state practice and expressions of *opinio juris*, and it is very rare for a rule to develop and become binding without any consideration of either ingredient. The commentary in Rule 4, however, is almost entirely oblivious to state practice and *opinio juris* and proceeds instead to derive discrete fine-grained rules of ostensible *lex lata* based on the mostly unexplained votes of its experts. Its only justification for ignoring state practice and *opinio juris* is that the former is "mostly classified" and the latter is sparse. But even in the stealthy world of adverse cyber operations, there is plenty of both if one looks, and they cut against the Rule 4 commentary.

Before turning to this real world of cyber operations and state commentary about them, a brief word is in order on the debate in the scholarly literature about whether "sovereignty is . . . a primary rule of international law susceptible to violation," and not just a "principle" from which other rules of international law "derive."[62] The rule-versus-principle debate is mainly about the question of whether Rule 4 as formulated is a stand-alone rule of customary international law, rather than a generalization about specific, recognized rules such as limitations on enforcement jurisdiction or the prohibition on intervention. This academic debate has obscured the settled legal test for determining which state cyber operations below recognized thresholds violate customary international law. That test turns

entirely on how nations behave and what they say and believe about the legality of such behavior.[63] It is to that task that we now turn.

The Real World

States have not been oblivious to the problems raised by cross-border cyber operations. The news for over a decade has been filled with weekly reminders that states are intensively engaged on both the sending and receiving ends of damaging or disruptive cross-border cyber operations. And of course the news reflects only the activities that have been made public. We can safely assume that there are many more state-sponsored cross-border cyber operations that cause damage or disruption below the use-of-force level but that are not in the news. Any assessment of the customary law claims in the Rule 4 commentary must examine what states have done and said.

Begin with state practice. To make the analysis concrete and manageable, we will consider two of the manual's proposed rules on "remote cyber operations that manifest on a State's territory" that likely implicate DF.[64] The Rule 4 commentary claims that such operations violate the customary international law of sovereignty (1) if they cause physical damage or "loss of functionality of cyber infrastructure"; or (2) if they "[interfere] with or [usurp] the inherently governmental functions of another State," regardless of whether the interference results in "physical damage, injury, or loss of functionality."[65] There have been many examples in the news in the last fifteen years that plausibly fit these categories, some of which we list in the appendix.[66]

By our (no doubt incomplete) count, between 2007 and 2020, at least sixteen cyberattacks caused a loss of functionality, and twelve cyberattacks interfered with or usurped inherent government functions.[67] (Some cyber operations did both.) As Sean Watts and Theodore Richard put it in 2018, "State cyber practice is brimming with examples of what the *Manual* would consider violations of sovereignty."[68]

Moreover, in none of these examples, not a single one, have we found evidence that the victim state complained about a violation of a customary international-law rule of sovereignty. The closest case is Russia's 2019 cyber operation against Georgia that took offline or defaced Georgia's government sites and damaged its government servers, thus violating Rule 4's prohibition against interfering with inherent government functions.[69] More than twenty countries formally attributed the attack to Russia and condemned it in the strongest terms.[70] None labeled it a violation of international law. Georgia accused Russia only of going "against international norms and principles" and "[violating its] sovereignty," but did not contend that Russia had violated international law.[71]

States often publicly denounce cyber operations as violations of sovereignty generally. Yet they don't make claims that cyber operations violate an international law of sovereignty,

much less ones that align with the Rule 4 commentary. Many cyber operations have caused harm or disruption; many have been attributed to specific aggressors, either officially or by credible news outlets and experts; many were strongly condemned—though not as violations of international law; and some even prompted retaliation.[72] States' failure to condemn these cyberattacks under international law contrasts sharply with the long history of states labeling extraterritorial law enforcement and certain noncyber breaches of territorial integrity as violations of international law.[73] All of this strongly suggests that Rule 4 does not reflect international practice or *opinio juris*.

States' failure to link their condemnations of cross-border cyber operations to anything like an international-law rule of sovereignty is all the more striking because states have been formally discussing these principles *for almost two decades*. In 2003, the United Nations established a state-based "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security" (GGE) to develop rules and norms governing the harmful uses of information technologies in international relations.[74] After about the first decade of work, the third GGE concluded that "international law" applies to information and communication technologies (ICT) and that "State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities."[75] It said nothing about whether "sovereignty" prescribes anything beyond the acknowledged sovereignty-based prohibitions (such as the principle of noninterference), much less what that something more might be. And neither the 2013 report nor its successor 2015 report reached any conclusion on how this or other norms constrain state behavior.[76]

The fifth GGE working group was commissioned to fill this gap in 2015.[77] It failed. The GGE met around the same time that the *Tallinn* experts were formulating their rules and was supposed to issue its report shortly after the manual published its views on extant international law. But in contrast to the confident assertions of the *Tallinn Manual 2.0* experts, the state-led GGE process collapsed one year after publication of *Tallinn Manual 2.0* because it "failed to agree on a draft for a consensus report."[78] It ostensibly broke down over differences about whether and how *jus ad bellum* applies to the legality of cross-border cyber operations, and over the contention by some states that it was "premature" to decide "*how* international legal rules and principles apply" in cyberspace.[79] Given this lack of consensus on the applicability of well-accepted sovereignty-based international law, such as the prohibition of the use of force in the UN Charter, and the stated uncertainty by states about how any international law applies in cyberspace, it is inconceivable that, as the *Tallinn Manual 2.0* claimed, there was at the same time a settled customary international-law rule that prohibits various types of cross-border cyber operations far below the use-of-force threshold.[80]

Events since the manual was published call the validity of the Rule 4 commentary into greater question. In 2018, the United Nations created a new GGE and an adjacent Open-Ended Working Group (OEWG) that is open to all states.[81] As of December 2019,

the latest GGE had made no progress "on *how* [international law] applies [to cyber operations]."[82] The final OEWG report, issued in March 2021, reveals the current diminished state of consensus among nations.[83] It is a modest and defensive document that seeks to preserve the 2015 GGE report's thin consensus. Its main international-law concern was preserving the minimalist notion that "international law, and in particular the Charter of the United Nations, is applicable and essential to maintaining peace and stability" in the digital environment.[84] Governments could agree on nothing regarding international law below the use-of-force threshold beyond that minimalist statement about the charter, and indeed acknowledged that "further common understandings need to be developed on how international law applies to State use of" the digital realm.[85] In short, this report, issued six years after *Tallinn Manual 2.0*, shows that the nations of the world have reached no consensus on anything approaching the Rule 4 commentary.[86]

To be sure, individual nations have in various contexts issued statements expressing more concrete views about how international law applies to the digital realm. Some of these statements were issued on an ad hoc basis. More than fifty statements came in the context of the OEWG process.[87] All of these statements came after the *Tallinn Manual 2.0*'s claims about sovereignty had been public and widely discussed. The vast majority did not come close to endorsing anything like Rule 4 and its commentary.

A few states have appeared to embrace something like Rule 4 and its commentary—some in the OEWG process, and some not. The Czech Republic and Finland have embraced Rule 4.[88] The Netherlands has "in general . . . endorse[d]" Rule 4, but acknowledged that the "precise interpretation" of the commentary principles "is a matter of debate,"[89] and later explained that there is a "clear gap" in how international law "applies in cyberspace," including on matters related to the international law of sovereignty.[90] Citing Rule 4 and its commentary, Germany takes the view that any cyber operations that "lead to physical effects and harm" or "functional impairments" in another state violate an international-law rule of sovereignty.[91] But, apart from stating that "interference in the conduct of elections of a State may under certain circumstances constitute a breach of sovereignty" (which may be entirely coextensive with the prohibition on coercive intervention),[92] it does not embrace the "inherently governmental functions" prong of the Rule 4 commentary.[93] Two states—Iran and Guatemala—have gone further than Rule 4 and its commentary by claiming that all cross-border cyber operations violate an international-law rule of sovereignty.[94] France takes the view that all unauthorized cross-border cyber operations "[constitute] a violation of sovereignty" but does not assert that such violations are contrary to international law, and has elsewhere described sovereignty as a "principle," not a rule of international law.[95]

These statements are probative of these nations' views about the content of customary international law, but so too are their practices, which often do not match the statements. For example, Germany's interior minister and the head of Germany's cyber agency have both defended the use of "active cyberdefense" cyber operations to "delete data" in hostile

networks and "shut down enemy servers."[96] France's intelligence agencies have used cyber operations to spy on foreign countries and to disable botnets in foreign countries without their permission, which is inconsistent with its seemingly absolutist position.[97] And Iran has conducted several cyber operations that disregard Rule 4.[98]

Far more states have demurred on Rule 4 and its commentary. At least five states (New Zealand, Israel, Austria, Guyana, and Bolivia) have claimed that sovereignty is in some respects a rule of international law that applies in cyberspace. But none of these states claim that the content of international law reflects Rule 4 and its commentary, or even offer an example of a cyber operation below the use-of-force or nonintervention threshold that has violated or would violate an ostensible international-law rule of sovereignty.[99] The United Kingdom has rejected Rule 4 outright.[100]

The United States has not rejected Rule 4 outright but has not embraced it either, and has never endorsed any part of the commentary. It claims that its defend forward operations, which at a general level seem hard to square with the Rule 4 commentary, are consistent with international law.[101] And it has further stated that "it does not appear that there exists a rule that all infringements on sovereignty in cyberspace necessarily involve violations of international law," and that "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 [below the use-of-force and prohibited-intervention thresholds] in another State's territory."[102]

And finally, many states (including Iran, despite its absolutist position) have made public statements—consistent with decades of GGE and OEWG gridlock—that note a lack of consensus as to "how provisions of international law apply" in cyberspace.[103]

The bottom line is this: during the three years after the failure of the GGE process, and the four years after publication of the *Tallinn Manual 2.0*, damaging cross-border cyber operations seem to have grown and grown, and during this period states have conducted intensive formal and informal discussions, in domestic and international fora, about the international law governing cyber operations. Yet only two states (the Czech Republic and Finland) have clearly embraced Rule 4 and its commentary; one (the Netherlands) seems to have done so (though its statements are ambiguous); one (Germany) has endorsed Rule 4 and half its commentary (but may disregard it in practice); perhaps three others (if one includes France, an ambiguous case) have gone further in their statements (if not their practice); two states appear to have rejected it; and the vast majority of states have been either silent or noncommittal. All of this has taken place against the background of continuous debate and discussion by the nations of the world in the OEWG process about how international law might apply to cyberspace. The final OEWG report's call for yet more future discussion about how international law applies to cyberspace—and the inability to reach any further concrete conclusion—confirms the utter lack of consensus here.

The *Tallinn Manual 2.0*'s defenders have not sufficiently credited these developments. Some commentators claim that states may secretly agree with Rule 4 but are afraid to say so, and that they ignore it in practice because aggressor states think "the benefits of nonconsensual intrusions outweigh the costs," while victim states fear accusations of hypocrisy.[104] We do not see how states' private, unexpressed beliefs might be credited in discerning a rule of customary international law. But in any event, this explanation is belied by the decades of discussion and negotiation by the nations of the world in the GGE and OEWG processes, and by the scores of affirmative statements by states acknowledging a lack of consensus about how international law applies in cyberspace.[105] The *Tallinn Manual 2.0* advocates maintain that state actors "bear the burden of justifying the non-applicability of the existing sovereignty rule to cyber operations."[106] We doubt any such burden exists: as explained above, the Rule 4 commentary does not come close to establishing that its purported rules flow from well-established international-law principles. In any case, states' collective refusal to embrace anything like Rule 4 and its commentary—after decades of discussion and debate, and amidst growing state practice of cross-border cyber operations—more than meets any such burden.[107]

The simple fact is that Rule 4's commentary does not align with how states practice or talk about international law. That is dispositive because international law is constituted by what states do, say, and agree to. Private individuals' judgments about how abstract legal principles apply to new domains, which side has the burden of proof, and states' implicit motivations for ignoring their analysis are beside the point. There is, to be sure, an important role for private norm entrepreneurship when developing new rules of international law. But we should recognize that the Rule 4 commentary fits squarely in that category.

In sum, the legal status of the rules articulated in Rule 4 is not a hard question: they are (at most) *lex ferenda*, not *lex lata*. States have intensively engaged in cyber operations below the use-of-force line for a long time, and have failed after decades of efforts to reach consensus about whether and how better-established, sovereignty-based rules of international law, such as use of force, apply in cyberspace. Many of these admittedly unresolved and still-hard questions would be irrelevant if the much lower threshold for illegality posited by the Rule 4 commentary were valid. It clearly is not.

The Bigger Picture

The argument thus far has been internal to the logic of international law—that the Rule 4 commentary employs an improper international-law standard, and does not in fact reflect customary international law. This argument entails no view on what the content of international law in this context should be in an ideal world. That is a very hard question that requires consideration of, among other things, the broader strategic context in which the debate over the Rule 4 commentary has been taking place. Which brings us back to DF.

The United States has prominently engaged in cyberspace operations, from using cyberattacks in armed conflict and in self-defense to various sorts of operations below the use-of-force threshold, and pervasive global cyber exploitation and espionage. It has also prominently been on the losing end of many notorious cyber operations. President Barack Obama bragged in the fall of 2016 that the United States has greater offensive and defensive cyber capabilities than any other nation.[108] He said this right in the middle of Russia's consequential intervention in the US election, after years of cyber disruptions in the US domestic sphere below the use-of-force threshold that exposed the United States' weak cyber defenses. DF is a direct response to this history.

The Russian operation violated the Rule 4 commentary, but no US government official claimed that it violated international law—because in the US view it didn't. It is entirely understandable, even if we don't like it, that Russia would use its cyber capabilities against the United States to serve its interests. The United States engages in analogous operations, including against Russia. The Russian operation may have been deeply damaging to the United States and, from the perspective of global stability, a bad act. But the same can probably be said of some US cyber operations abroad.

In an ideal world, nations should want rules that constrain cyber operations in ways that promote global harmony. But, of course, this is much easier said than done, because every rule has distributional consequences due to vast differences in national capacities and interests. Generalizing quite a lot: the United States is likely dominant in using cyber in military conflict situations and in cyber exploitation on the whole (and Israel is very good at cyber for military operations as well). Russia seems to dominate in the gray zone. China is by far the world's leader in commercial cyber theft and is also adept, as is Russia, at large-scale cyber exploitations of government networks. Many weaker countries are on the losing end of these sticks, though some—notably, Iran and North Korea—are using cyber operations to their asymmetrical advantage.[109]

Against this background, the primary strategic logic behind the *Tallinn Manual 2.0* is that a firm, customary international-law rule of sovereignty that bans defend forward–type operations would permit nations to condemn those operations as unlawful, "ostracize the state that launched them," and presumably deter such harmful cross-border digital operations.[110] But matters are much more complex than this. As Gary Corn observes, using countermeasures—that is, actions otherwise illegal under international law—in response to cyber operations that violate Rule 4 and its commentary might heighten escalation.[111] Moreover, states (especially powerful ones) benefit too much from deploying cyber operations opportunistically to yield to criticism about violating novel, top-down legal rules that are divorced from the reality of their interests.

Relatedly, any powerful nation that obeyed Rule 4 tomorrow would be put at an enormous disadvantage vis-à-vis its adversaries. These are but some of the reasons to think that ostracization would not work in this context, even if Rule 4 somehow reflected customary international law, especially against the powerful nations that act contrary to Rule 4 the most in practice. As President Obama said in response to the Russian electoral hack in 2016, "The idea that somehow public shaming is going to be effective I think doesn't read the thought process in Russia very well."[112]

The DF strategy takes a very different approach to influencing mischievous cyber behavior below the use-of-force threshold. Rather than seeking to shame nations into refraining from certain cyber operations, it aims to alter their capacities and material incentives to engage in such operations. This approach poses at least two dangers. First, it might provoke bilateral escalation that will leave the digitally dependent United States worse off on balance. And second, it might spark a global escalation in the use of such techniques, to the detriment of all or at least most nations. (This is an especial danger since DF probably involves below-the-threshold cyber operations in another country that mirror in some respects the below-the-threshold cyber operations it seeks to check.)

Presumably the United States considered these risks and decided that, given its capabilities, weaknesses, and recent run of damaging cyber losses, DF made sense on balance. Yet it remains far from clear that the DF strategy will work. Perhaps it is best seen as a first step in altering adversary incentives on a path toward mutually beneficial confidence-building measures or soft or hard cooperative agreements.[113]

Conclusion

Whether DF, diplomatic approaches, or any similar state-driven approach will successfully forge a better global cyber order remains very much an open question. It is also unclear which strategy—carrot, stick, or some combination of the two—has the best chance of success. Top-down entrepreneurial sovereignty theories such as Rule 4 and its commentary might well influence customary international law, depending on what states subsequently do and say.[114] But as developments since it was published in 2017 underscore, it does not reflect customary international law today.

APPENDIX

This is a selective list of many of the publicly known state-sponsored cross-border cyber operations below the use-of-force level that implicate two of the rules articulated in the commentary to Rule 4. Category 1 concerns such operations that cause "loss of functionality of cyber infrastructure."[115] Category 2 concerns operations that "[interfere] with or [usurp] the inherently governmental functions of another State," regardless of whether the interference results in "physical damage, injury, or loss of functionality."[116]

Year	*Category 1*	*Category 2*
2020	Israeli cyberattack resulted in explosion at Natanz nuclear facility.[117]	Israeli cyberattack disabled Iranian port computers, in response to April 2020 Iranian cyberattack on Israeli water-distribution networks.[118] In July 2020, Iranian cyberattacks shut down Israeli water-distribution networks.[119] Iranian actors hacked voter rolls to obtain voter information and sent voter-intimidation emails to US voters during presidential election.[120] Three-year-long campaign by Russian hackers to compromise news sites in Eastern Europe attributing false quotations to government officials was disclosed.[121]
2019	US government "wiped" computers and shut down communications networks of Iranian government officials used to plot attacks on oil tankers.[122]	Russian cyberattacks in Georgia in October 2019 disabled and defaced state websites.[123]
2018	Russian hackers wiped computers that were part of the 2018 South Korea Olympics.[124] US Cyber Command removed Russia's Internet Research Agency's online capabilities during midterm elections.[125]	
2017	North Korean WannaCry attack encrypted data on every computer it reached, leaving hundreds of thousands of computers unusable around the world.[126] Russia's NotPetya attack rendered millions of computers around the world unusable, causing more than $10 billion in damages and devastating giants like Maersk, FedEx, and Merck.[128] "Shamoon 4" attack by Iran wiped computers belonging to Saudi government offices as well as Saudi and American companies.[130]	WannaCry also crippled the United Kingdom's National Health Service, interrupting the delivery of medical services.[127] NotPetya effectively wiped 10 percent of Ukrainian computers, forcing health care providers and government ministries to shut down or disconnect from the internet.[129] United Arab Emirates hacked Qatari government and media sites to attribute false quotations to the Qatari emir.[131]
2016	Russia used cyberattacks to cause power outages in Ukraine, affecting millions of people.[132] "Shamoon 3" attack by Iran against Saudi Arabia erased data in Saudi government computers.[134]	Russia interfered in the 2016 election by generating social media content without disclosing its source, and hacking and leaking the Democratic National Committee and chairman of the Clinton campaign John Podesta's emails. Many have argued that this changed the result in what was an extremely close election.[133]
2015	Russia used cyberattacks to cause power outages in Ukraine, affecting hundreds of thousands of people.[135]	Russian cyberattack on Germany forced the Bundestag to shut down its internal parliamentary network and reinstall software on many of its computers.[136]
2014	Attack by North Korea against the United States wiped 70 percent of Sony's computing power.[137] Attack by Iran against the United States permanently wiped data on thousands of Sands Casinos computers and servers.[138]	

Continued

2012	"Wiper" attack by United States against Iran erased data on computers connected to Iran's oil industry.[139] "Shamoon 2" attack by Iran against Qatar forced the oil company RasGas to shut down its internal network.[141] "Shamoon" attack by Iran against Saudi Arabia wiped tens of thousands of hard drives belonging to Saudi Aramco.[142]	"Wiper" attack shut down six of Iran's oil terminals, which were responsible for most of its exports.[140]
2010	United States and Israel attacked Iran with the Stuxnet virus, physically disabling centrifuges.[143]	
2007		Russian DDoS (distributed denial of service) attack on Estonia disrupted government networks and banks.[144]

ACKNOWLEDGMENTS

The authors wish to thank Elena Chachko, Bobby Chesney, Gary Corn, Eric Jensen, Sean Watts, and participants in a Hoover Institution workshop for outstanding comments; and Casey Corcoran, Matthew Gluck, Katarina Krasulova, and Jacques Singer-Emery for outstanding research assistance. The opinions expressed are those of the authors and do not necessarily reflect the views of Quinn Emanuel or its clients.

NOTES

1 *See* Anders Henriksen, *The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace*, 5 J. Cybersecurity 1, 1 (2019).

2 Open-Ended Working Grp. on Devs. in the Field of Info. and Telecomms. in the Context of Int'l Sec., Final Substantive Report, U.N. Doc. A/AC.290/2021/CRP.2, at ¶ 34 (2021) [hereinafter OEWG Final Substantive Report].

3 *See* Tallinn Manual on the International Law Applicable to Cyber Warfare 3–4 (Michael N. Schmitt ed., 2013) [hereinafter Tallinn Manual 1.0]. ("This project was launched in the hope of bringing some degree of clarity to the complex legal issues surrounding cyber operations, with particular attention paid to those involving the *jus ad bellum* and the *jus in bello*.")

4 *See generally* Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Michael N. Schmitt & Liis Vihul eds., 2017) [hereinafter Tallinn Manual 2.0].

5 *Id.* at 17.

6 Michael N. Schmitt & Liis Vihul, *Sovereignty in Cyberspace:* Lex Lata Vel Non, 111 AJIL Unbound 213, 214 (2017).

7 *Id.* at 213.

8 U.S. Dep't of Defense, Summary: Department of Defense Cyber Strategy 2018, at 1 (2018) (emphasis added).

9 Cyberspace Solarium Comm'n, Report 33 (2020).

10 Michael Sulmeyer, *Military Set for Cyber Attacks on Foreign Infrastructure*, Harvard Kennedy School Belfer Center (Apr. 11, 2018) (emphasis added). Nakasone made this statement in explaining "persistent engagement," which the Solarium Project states is the "concept by which U.S. Cyber Command implements defend forward." Cyberspace Solarium Comm'n, *supra* note 9, at 137.

11 *Hearing on U.S. Special Operations Command and U.S. Cyber Command in Review of the Defense Authorization Request for FY 2020 before the S. Comm. on Armed Servs*., 116th Cong. 23 (2019) [hereinafter Nakasone Testimony] (emphasis added) (statement of Gen. Paul M. Nakasone, Commander, U.S. Cyber Command).

12 Joint Chiefs of Staff, U.S. Dep'ts of the Army, the Navy, the Air Force, and the Marine Corps, Joint Pub. 3-12, Doctrine for Cyberspace Operations Logistic Support of Joint Operations II-7 (2013).

13 Ellen Nakashima, *U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms*, Wash. Post (Feb. 27, 2019, 5:22 AM).

14 Nakasone Testimony, *supra* note 11, at 3.

15 *Evolving the U.S. Cybersecurity Strategy and Posture: Reviewing the Cyberspace Solarium Commission Report before the S. Comm. on Homeland Sec. and Governmental Affs*., 116th Cong. 11 (2020) (statement of Sen. Angus King, Rep. Mike Gallagher, Suzanne Spaulding, and Tom Fanning, Comm'rs of the Cyberspace Solarium Comm'n).

16 U.S. Dep't of Defense, *supra* note 8, at 5.

17 Cyberspace Solarium Comm'n, *supra* note 9, at 2.

18 Tallinn Manual 2.0, *supra* note 4, at 4.

19 *Id.* at 1.

20 *Id.* at 2.

21 *Id.* at 2–3.

22 *Id.* at 3.

23 *Id.*

24 *Id.*

25 *Id.* at v, 17. Rules 1–3 articulate general principles of international law related to sovereignty but say nothing concrete about how they regulate operations in cyberspace. Rule 5 is about sovereign immunity.

26 *Id.* at 17.

27 *See id.* at 27–29, 51–78, 212–83, 294–98, 312–25, 329–39, 555–62.

28 *Id.* at 19, ¶ 6.

29 *Id.*

30 *Id.*

31 *Id.*

32 *See id.* (emphasis added). *Tallinn* offers as an example one state using a flash drive to introduce malware into cyber infrastructure in another state as a violation of the rule.

33 Restatement (Third) of Foreign Relations Law § 431 (*Am. L. Inst.* 1987). *Tallinn* confirms this scope for enforcement jurisdiction when it cites the Eichmann Security Council resolution. *See* Tallinn Manual 2.0, *supra* note 4, at 19 n.22.

34 James Crawford, Brownlie's Principles of Public International Law 462 (9th ed. 2019) (emphasis added).

35 *Id.* at 462.

36 Tallinn Manual 2.0, *supra* note 4, at 19, ¶ 7.

37 *Id.* at 169, ¶ 5.

38 *Id.* at 19, ¶ 7.

39 *Id.* at 20, ¶ 10.

40 *Id.*

41 *Id.* at 20, ¶ 11.

42 *Id.* at 20, ¶ 10.

43 *Id.* at 20–21, ¶ 13.

44 *Id.* at 21, ¶ 14.

45 *Id.* at 21, ¶ 15.

46 *Id.* at 22, ¶ 16. The examples of what the experts have in mind 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." *Id.*

47 *Id.* at 22–23, ¶¶ 17–21.

48 *Id.* at 20, ¶¶ 10 & n.24 (quoting Island of Palmas (Neth. v. U.S.), 2 R.I.A.A. 829, 838 (1928)).

49 *See* Island of Palmas (Neth. v. U.S.), 2 R.I.A.A. 829, 867–69.

50 *Id.* at 838 (emphasis in original).

51 Tallinn Manual 2.0, *supra* note 4, at 22, ¶ 16. A footnote suggests that when "assessing the inherently governmental nature of cyber activities . . . the notion of *acta jure imperii*, used in the context of State immunity, could prove helpful," but it does not explain why the two concepts connect. *Id.* at 22, ¶ 17 n.26. Otherwise, it seems to vaguely connect usurpation of government functions with the prohibition on extraterritorial exercise of jurisdiction, as discussed above. *See id.* at 22–23, ¶ 18.

52 The rest of Rule 4's commentary addresses other interstitial applications of Rule 4. Comment 23, for example, states that "a State's cyber operations may constitute a violation of another State's sovereignty . . . irrespective of [where] the operations are launched from," and comments 24 and 25 make clear that a state's intent to violate (or not to violate) sovereignty is irrelevant. *See id.* at 24, ¶¶ 23–25. Cyber operations targeting one country would "generally not violate the sovereignty" of a state that suffers incidental spillover effects, nor would cyber operations that just "result in severe economic loss," propaganda, crimes committed by private actors, or operations taken with the target state's consent. *See id.* at 24–27, ¶¶ 26, 28–32.

53 *Id.* at 2–3.

54 *Id.* at 3.

55 Restatement (Third) of Foreign Relations Law § 102(2) (*Am. L. Inst.* 1987) (emphasis added).

56 Int'l Law Comm'n, Draft Conclusions on Identification of Customary International Law, with Commentaries, U.N. Doc. A/73/10, at 154 (2018).

57 *See* Statute of the International Court of Justice, art. 38(1), June 26, 1945, 59 Stat. 1055, 3 Bevans 1179 (explaining that the Court shall apply "international custom, as evidence of a general practice accepted as law"); Shabtai Rosenne, Practice and Methods of International Law 55 (1984) (stating that customary international law "consists of rules of law derived from the consistent conduct of States acting out of the belief that the law

required them to act that way"); Int'l L. Ass'n London Conference, *Statement of Principles Applicable to the Formation of General Customary International Law*, at 8 (2000).

58 Int'l Law Comm'n, *supra* note 56, at 126; Noora Arajärvi, *The Requisite Rigour in the Identification of Customary International Law: A Look at the Reports of the Special Rapporteur of the International Law Commission*, 19 Int'l Comm. L. Rev. 9, 11–12 (2017).

59 *See, e.g.*, Ryan M. Scoville, *Finding Customary International Law*, 101 Iowa L. Rev. 1893, 1917 (2016); Cedric M. J. Ryngaert & Duco W. Hora Siccama, *Ascertaining Customary International Law: An Inquiry into the Methods Used by Domestic Courts*, 65 Neth. Int'l L. Rev. 1, 2 (2018); Alberto Alvarez-Jimenez, *Methods for the Identification of Customary International Law in the International Court of Justice's Jurisprudence: 2000–2009*, 60 Int'l & Compar. L. Q. 681, 687 (2011); Curtis A. Bradley & Jack L. Goldsmith, *Customary International Law as Federal Common Law: A Critique of the Modern Position*, 110 Harv. L. Rev. 815, 839–42 (1997).

60 As the International Law Commission (ILC) recently explained: the writings of scholars "are not themselves a source of international law," but their teachings may be valuable "in collecting and assessing State practice; in identifying divergences in State practice and the possible absence or development of rules; and in evaluating the law." Int'l Law Comm'n, *supra* note 56, at 151. The ILC noted caution when drawing on these writings, since the writings are of uneven quality, sometimes reflect national or personal viewpoints, and sometimes "seek not merely to record the state of the law as it is (lex lata) but to advocate its development (lex ferenda)." *Id.* It then quoted favorably from *The Paquete Habana*, which noted that the writings of jurists "are resorted to by judicial tribunals, not for the speculations of their authors concerning what the law ought to be, but for trustworthy evidence of what the law really is." 175 U.S. 677, 700 (1900).

61 Stefan Talmon, *Determining Customary International Law: The ICJ's Methodology between Induction, Deduction and Assertion*, 26 Eur. J. Int'l L. 417, 418 (2015); William Thomas Worster, *The Inductive and Deductive Methods in Customary International Law Analysis: Traditional and Modern Approaches*, 45 Geo. J. Int'l L. 445 (2014).

62 Michael Schmitt, *In Defense of Sovereignty in Cyberspace*, Just security (May 8, 2018); *see also, e.g.*, Schmitt & Vihul, *supra* note 6, at 214. *But see* Gary P. Corn & Robert Taylor, *Sovereignty in the Age of Cyber*, 111 AJIL Unbound 207, 211 (2017) (arguing that sovereignty is a principle only).

63 *Cf.* Eric Talbot Jensen, *The Tallinn Manual 2.0: Highlights and Insights*, 48 Geo. J. Int'l L. 735, 741–42 (2017) ("[S]overeignty is a principle that depends on the domain and the practical imperatives of states and is subject to adjustment in interstate application.").

64 Tallinn Manual 2.0, *supra* note 4, at 20, ¶ 10.

65 *Id.* at 20–22, ¶¶ 13–15.

66 We focus here on examples that fall below the use-of-force threshold and take no position on whether they implicate any other established rule of international law below the use-of-force level, such as prohibited coercive intervention. These examples are based on one nation accusing another nation of the cyber operation, or credible sources in credible publications confirming them. We borrow, in part, from the list compiled by Dan Efrony & Yuval Shany, *A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice*, 112 Am. J. Int'l L. 583, 655–57 (2018), though we disagree with some of their conclusions.

67 *See infra* Appendix.

68 *See* Sean Watts & Theodore Richard, *Baseline Territorial Sovereignty and Cyberspace*, 22 Lewis & Clark L. Rev. 771, 869 (2018).

69 *Georgia Hit by Massive Cyber-Attack*, BBC News (Oct. 28, 2019).

70 Przemyslaw Roguski, *Russian Cyber Attacks against Georgia, Public Attributions and Sovereignty in Cyberspace*, Just Security (Mar. 6, 2020).

71 *Georgia Blames Russia for Cyberattack, US, UK Agree*, Associated Press (Feb. 20, 2020).

72 For example, the United States attributed 2016 election interference to Russia, condemned it for undermining "international norms," imposed sanctions, and even indicted (under domestic law) Russians responsible for the operation; but it never labeled the operation a violation of international law. Press release, Office of the Press Sec'y, Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment (Dec. 29, 2016).

73 A paper by the lead editors of the *Tallinn Manual 2.0* offers many revealing examples. *See* Michael N. Schmitt & Liis Vihul, *Respect for Sovereignty in Cyberspace*, 95 Tex. L. Rev. 1639, 1656–63 (2017) (giving the examples of Pakistan complaining about US drone strikes, Iran complaining about US breaches of its territorial waters, Canada complaining about radioactive debris on its territory from a Russian satellite, and Argentina complaining about Israel's abduction of Adolf Eichmann—all by reference to international-law rules related to sovereignty).

74 For a thorough summary of the history of the GGE, *see generally* Henriksen, *supra* note 1.

75 Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2013), transmitted by Letter dated 7 June 2013 from the Chair of the Group Established Pursuant to G.A. Res. 66/24 (2012) Addressed to General Assembly, ¶ 20, U.N. Doc. A/68/98 (June 24, 2013) [hereinafter 2013 GGE Report]. Apart from an admission in the Secretary-General's foreword that states had "only begun to develop the norms, laws and modes of cooperation needed for this new information environment," the 2010 GGE report ignored international law and sovereignty entirely. Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2010), transmitted by Letter dated 16 July 2010 from the Chairman of the Group Established Pursuant to G.A. Res. 60/45 (2006) Addressed to General Assembly, at 4, U.N. Doc. A/65/201 (July 31, 2010). The first GGE working group, by contrast, reached "no consensus" on any issue. U.N. Secretary-General, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, ¶ 5, U.N. Doc. A/60/202 (Aug. 5, 2005).

76 *See* 2013 GGE Report, *supra* note 75, at ¶ 16; *see also id.* at 25 ("Member states should consider how best to cooperate in implementing the above norms and principles of responsible behavior."). The 2015 GGE noted that 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" but again offered no specifics. Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2015), transmitted by Letter dated 26 June 2015 from the Chair of the Group Established Pursuant to G.A. Res. 68/243 (2014) Addressed to General Assembly, ¶ 28, U.N. Doc. A/70/174 (July 22, 2015) [hereinafter 2015 GGE Report].

77 G.A. Res. 70/237, ¶ 5 (Dec. 30, 2015) ("*Requests* the Secretary-General, with the assistance of a group of governmental experts . . . to continue to study . . . how international law applies to the use of information and communications technologies by States.") (emphasis in original).

78 Henriksen, *supra* note 1, at 3.

79 Michele G. Markoff, Deputy Coordinator for Cyber Issues, Off. of the Coordinator for Cyber Issues, U.S. Dep't of State, Remarks at the U.N. GGE: Explanation of Position at the Conclusion of the 2016–2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security (June 23, 2017) (emphasis in original).

80 *Cf.* Oona Hathaway & Alasdair Phillips-Robins, *COVID-19 and International Law Series: Vaccine Theft, Disinformation, the Law Governing Cyber Operations*, Just Security (Dec. 4, 2020) ("[T]he very fact of wide disagreement among States about a potential rule of cyber sovereignty itself forecloses the existence of such a norm—at least at present.").

81 Samuele De Tomas Colatin, *A Surprising Turn of Events: UN Creates Two Working Groups on Cyberspace*, NATO Coop. Cyber Def. Ctr. Excellence (last visited Apr. 12, 2021), https://ccdcoe.org/incyder-articles/a-surprising-turn-of-events-un-creates-two-working-groups-on-cyberspace.

82 Chair's Summary: Informal Consultative Meeting of the Group of Governmental Experts (GGE) on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (Dec. 5–6, 2019) (emphasis in original). So far, none of the few public GGE submissions or meeting summaries mention international-law rules governing cyber operations below the use-of-force threshold. *See Group of Governmental Experts*, U.N., https://www.un.org/disarmament/group-of-governmental-experts/ (publishing countries' statements).

83 OEWG Final Substantive Report, *supra* note 2, at ¶ 7.

84 *Id.* at ¶ 34.

85 *Id.*

86 *Inside Cyber Diplomacy: Discussing the UN OEWG with Mother of Norms*, CSIS (Mar. 2021) (interviewing US State Department official Michele Markoff, who concludes that the 2021 OEWG Report "doesn't break new ground" and "doesn't add new norms").

87 For countries' submissions, see *Open-Ended Working Group*, U.N., https://www.un.org/disarmament/open-ended-working-group/. While the states were formally asked to comment on the draft proposals, many states' submissions touched on their views on international law related to cyber operations.

88 *See* Special Envoy of Czech Republic for Cyberspace, Director of Cybersecurity Department, Statement dated Feb. 11, 2020, from the Special Envoy of Czech Republic for Cyberspace, Director of Cybersecurity Department at the 2nd Substantive Session of the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security of the First Committee of the General Assembly of the United Nations (Feb. 11, 2020); International Law and Cyberspace: Finland's National Positions (Oct. 15, 2020).

89 Appendix: International Law in Cyberspace (2019), transmitted by Letter dated 5 July 2019 from the Minister of Foreign Affairs to the President of the House of Representatives on the International Legal Order in Cyberspace (Sept. 26, 2019) (Neth.).

90 The Kingdom of the Netherlands' Response to the Pre-Draft Report of the OEWG, at ¶ 17 (April 2020).

91 German Federal Foreign Office, German Federal Ministry of Defence & German Federal Ministry of the Interior, Building and Community, On the Application of International Law in Cyberspace: Position Paper 4 (Mar. 2021).

92 *Cf.* Brian J. Egan, Legal Adviser, U.S. Dep't of State, Remarks on International Law and Stability in Cyberspace, Berkeley Law (Nov. 10, 2016) (noting that "a cyber operation by a State that interferes with another country's ability to hold an election or that manipulates another country's election results would be a clear violation of the rule of non-intervention").

93 *Id.* at 3. *But see* Michael Schmitt, *Germany's Positions on International Law in Cyberspace Part I*, Just Security (Mar. 9, 2021) (arguing that Germany embraces both bases for violation).

94 Ministry of the Armed Forces of France, International Law Applied to Operations in Cyberspace 7, 18 (2019); *General Staff of Iranian Armed Forces Warns of Tough Reaction to Any Cyber Threat*, NournNews (Aug. 18, 2020, 5:59 AM); Letter from Gabriel Juárez Lucas, Fourth Vice Minister, Interior Ministry, Government of the Republic of Guatemala, to the honorable Department of International Law, General Secretariat of the Organization of American States, Washington, D.C. (July 9, 2019).

95 French Ministry of Defense, International Law Applied to Operations in Cyberspace 7, 18 (2019); France's response to Resolution 73/27 "Developments in the field of information and telecommunications in the context of international security" and Resolution 73/266 "Advancing responsible State behaviour in cyberspace in the context of international security" 8; *see also* Gary Corn, *Punching on the Edges of the Grey Zone: Iranian Cyber Threats and State Cyber Responses*, Just Security (Feb. 11, 2020).

96 Naomi Conrad & Nina Werkhäuser, *Germany Debates Stepping Up Active Cyberoperations*, Deutsche Welle (June 26, 2019); Maria Sheahan, *German Cyber Agency Calls for Authority to Hack Back: Spiegel*, Reuters (Nov. 22, 2017, 7:17 AM).

97 *See* Jack Kenny, *France, Cyber Operations and Sovereignty: The "Purist" Approach to Sovereignty and Contradictory State Practice*, Lawfare (Mar. 12, 2021, 8:01 AM); Pierluigi Paganini, Animal Farm APT and the Shadow of French Intelligence, Infosec Resources (July 8, 2015).

98 *See infra* Appendix.

99 *See* New Zealand Ministry of Foreign Affairs & Trade, The Application of International Law to State Activity in Cyberspace ¶¶ 11–15 (Dec. 2020); Roy Schondorf, Israeli Deputy Attorney General (International Law), Keynote Address at the U.S. Naval War College conference on Disruptive Technologies and International Law: Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations (Dec. 8, 2020); Comments by Austria on the Pre-Draft Report of the OEWG–ICT (Mar. 3, 2020); Permanent Mission of the Republic of Guyana to the Organization of American States, Note No: 105/2019 (July 30, 2019) ("Whether a violation occurs depends on the degree of infringement and whether there has been an interference with Government functions."); Office of the Commander-in-Chief of the State Inspector General of the Armed Forces of Bolivia, OAS Inter-American Juridical Committee Questionnaire (July 17, 2019).

Some have argued that NATO's *Allied Joint Doctrine for Cyberspace Operations* recognized sovereignty as a rule of international law, but they are wrong. NATO's publication merely noted that cyber operations below the threshold of use of force or armed attack may "constitute a violation of international law as a breach of sovereignty or other internationally wrongful act." N. Atl. Treaty Org., Allied Joint Publication-3.20: Allied Joint Doctrine for Cyberspace Operations, at 20 n.26 (2020). That statement does not affirmatively embrace anything approaching the Rule 4 commentary and might refer simply to cyber operations that violate one of the many sovereignty-based rules, such as the prohibition against intervention. At a minimum, the NATO report does not comment on the scope of any such sovereignty-based rules below the use-of-force threshold.

100 Jeremy Wright QC MP, U.K. Att'y Gen., Address at Chatham House Royal Institute for International Affairs: Cyber and International Law in the 21st Century (May 23, 2018).

101 *See* Cyberspace Solarium Comm'n, *supra* note 9, at 2, 24, 29.

102 Paul C. Ney Jr., U.S. Dep't of Def. Gen. Couns., DOD General Counsel Remarks at U.S. Cyber Command Legal Conference (Mar. 2, 2020). Previously, the United States had stated that a "cyber operation [could violate] the sovereignty of another State." Tallinn Manual 2.0, *supra* note 4, at 17. But it has not elaborated or specified whether it was referring to a stand-alone international-law rule or what that rule was. Harold Koh, Legal Adviser, U.S. Dep't of State, Remarks at the U.S. Cyber Command Inter-Agency Legal Conference: International Law in Cyberspace (Sept. 18, 2012) (transcript available at Chris Borgen, *Harold Koh on International Law in Cyberspace*, Opinio Juris [Sept. 19, 2012]); Egan, *supra* note 92. On April 15, 2021, President Joseph R. Biden by executive order imposed sanctions on various Russian entities for a variety of real-space and cyberspace activities. Exec. Order No. 14,024, 86 Fed. Reg. 20,249 (Apr. 19, 2021). The order stated that the "specified harmful foreign activities of the Government of the Russian Federation" that formed the basis for the sanctions included interference in US and foreign elections, "malicious cyber-enabled activities against the United States" and allies, transnational corruption to influence foreign governments, extraterritorial activities targeting dissidents or journalists, *and* violation of "well-established principles of international law, including respect for the territorial integrity of states." The listing of malicious cyber activities separate from the well-established violations of international law related to territorial integrity, among other things, indicates that the statement does not mark an implicit change of the US position on the topic of this paper. Moreover, the White House fact sheet on the sanctions make plain that many of the new sanctions related to Russia's "occupation . . . [of] Crimea." White House, Fact Sheet: Imposing Costs for Harmful Foreign Activities by the Russian Government (Apr. 15, 2021).

103 Estonia's Comments to the OEWG Pre-Draft Report, at 9 (Apr. 16, 2020); *see, e.g.*, Intervention by Delegation of the Islamic Republic of Iran on International Law (Oct. 1, 2020); *see also* Statement by the Representative of the Russian Federation at the Online Discussion of the Second "Pre-Draft" of the Final Report of the UN Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (June 15, 2020); Permanent Mission of Denmark to the United Nations, Denmark's Response

to the Initial "Pre-Draft" Report of the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, Ref. no. 2019-36843 (Apr. 16, 2020).

104 Watts & Richard, *supra* note 68, at 837–38.

105 *See supra* note 103 and accompanying text.

106 Michael Schmitt, *The Defense Department's Measured Take on International Law in Cyberspace*, Just Security (March 11, 2020); *see also* Schmitt & Vihul, *supra* note 73, at 1670.

107 *See supra* note 103 and accompanying text.

108 Joe Uchill, *Obama: US Government Has Largest Capacity to Hack*, The Hill (Sept. 6, 2016, 9:55 AM).

109 *See generally* David Sanger, The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age (2018).

110 Schmitt, *supra* note 62. Another justification, also presumably related to deterrence, is that violation of a low-level sovereignty rule would permit a broader array of countermeasures. *Id.*

111 Corn, *supra* note 95.

112 President Barack Obama, Press Conference by the President (Dec. 16, 2016).

113 *See, e.g.*, Jack Goldsmith, On the Russian Proposal for Mutual Noninterference in Domestic Politics, Lawfare (Dec. 11, 2017, 9:30 AM); Jack Goldsmith, *Contrarian Thoughts on Russia and the Presidential Election*, Lawfare (Jan. 10, 2017, 11:30 AM); *see also, e.g.*, Ben Buchanan, The Cybersecurity Dilemma: Hacking, Trust, and Fear between Nations 157–86 (2017).

114 *Cf.* Henriksen, *supra* note 1, at 2 ("[D]espite what many international lawyers seem to believe, the discussion about how ICT should be regulated is as much about strategy, politics and ideological differences (if not more so) than it is about law. And at present, states' interests and normative preferences are simply too diverse for consensus on anything but the most basic of such issues to arise.").

115 Tallinn Manual 2.0, *supra* note 4, at 20, ¶ 13.

116 *Id.* at 21–22, ¶ 15.

117 Kate O'Flaherty, *Stuxnet 2? Iran Hints Nuclear Site Explosion Could Be a Cyberattack*, Forbes (July 4, 2020, 7:03 AM). While Iran acknowledged there was some ambiguity whether the explosion was caused by a cyber operation, it did not suggest that any such cyber operation would be unlawful under international law.

118 Joby Warrick & Ellen Nakashima, *Officials: Israel Linked to a Disruptive Cyberattack on Iranian Port Facility*, Wash. Post (May 18, 2020, 2:48 PM).

119 Toi Staff, *Cyber Attacks Again Hit Israel's Water System, Shutting Agricultural Pumps*, Times Isr. (July 17, 2020, 1:18 AM).

120 Cybersecurity & Infrastructure Sec. Agency, *Alert (AA20-304A): Iranian Advanced Persistent Threat Actor Identified Obtaining Voter Registration Data* (Oct. 30, 2020).

121 Mandiant, "Ghostwriter" Influence Campaign: Unknown Actors Leverage Website Compromises and Fabricated Content to Push Narratives Aligned with Russian Security Interests 3 (2020).

122 Julian E. Barnes, *U.S. Cyberattack Hurt Iran's Ability to Target Oil Tankers, Officials Say*, N.Y. Times (Aug. 28, 2019).

123 Ryan Browne, *US and UK Accuse Russia of Major Cyber Attack on Georgia*, CNN (Feb. 20, 2020, 1:19 PM).

124 Andy Greenberg, *The Untold Story of the 2018 Olympics Cyberattack, the Most Deceptive Hack in History*, Wired (Oct. 17, 2019, 6:00 AM).

125 Garrett M. Graff, *The Man Who Speaks Softly—and Commands a Big Cyber Army*, Wired (Oct. 13, 2020, 6:00 AM).

126 *See* Ben Buchanan, The Hacker and the State 280–81 (2020).

127 Ellen Nakashima & Philip Rucker, *U.S. Declares North Korea Carried Out Massive WannaCry Cyberattack*, Wash. Post (Dec. 19, 2017); *see generally* United Kingdom National Audit Office, Department of Health, Investigation: WannaCry Cyber attack and the NHS (2018).

128 *See id.* at 289–90, 295–96, 299; Kimberly Crawley, *NotPetya Development May Have Started before EternalBlue*, Infosecurity Mag. (June 30, 2017).

129 *See* Buchanan, *supra* note 126, at 300–01.

130 Nicole Perlroth & Clifford Krauss, *A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try*, N.Y. Times (Mar. 15, 2018).

131 Karen DeYoung & Ellen Nakashima, *UAE Orchestrated Hacking of Qatari Government Sites, Sparking Regional Upheaval, According to U.S. Intelligence Officials*, Wash. Post (July 16, 2017).

132 *See* Buchanan, *supra* note 126, at 188.

133 Sanger, *supra* note 109, at 201, 205, 212, 232; Nicole Perlroth, This Is How They Tell Me the World Ends: The Cyberweapons Arms Race 318–19 (2021) (speculating that this might have swayed the election); Michael N. Schmitt, *"Virtual" Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law*, 19 Chi. J. Int'l L. 30, 46–47 (2018) (arguing that the operation violated Rule 4, at least in part).

134 Michael Riley, Glen Carey & John Fraher, *Destructive Hacks Strike Saudi Arabia, Posing Challenge to Trump*, Bloomberg (Dec. 1, 2016, 3:21 AM).

135 *See* Buchanan, *supra* note 126, at 188.

136 *Russia "Was Behind German Parliament Hack"*, BBC News (May 13, 2016); *Bundestag Counting Cost of Cyberattack*, Deutsche Welle (Nov. 6, 2015); *see also* Efrony & Shany, *supra* note 66, at 617–19, 640 (outlining the operation and noting that Germany responded by beefing up its cyber capabilities).

137 John P. Carlin, Dawn of the Code War: America's Battle against Russia, China, and the Rising Global Cyber Threat 310 (2019) ("The company's computers had, it turned out, been nuked—not just frozen, but wiped clean, turned into expensive bricks sitting across 3,000 desks."); Sanger, *supra* note 109, at 141.

138 Benjamin Elgin & Michael Riley, *Nuke Remark Stirred Hack on Sands Casinos That Foreshadowed Sony*, Bloomberg (Dec. 11, 2014, 9:01 PM). The *Tallinn Manual 2.0* says that a cyberattack that wipes computers like this would violate Rule 4 because it causes computers to lose "functionality." Tallinn Manual 2.0, *supra* note 4, at 20, ¶ 13.

139 Buchanan, *supra* note 126, at 143.

140 *Id.*

141 Nicole Perlroth, *In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back*, N.Y. Times (Oct. 23, 2012).

142 Sanger, *supra* note 109, at 52; *see also* Efrony & Shany, *supra* note 66, at 624 (noting that Saudi Arabia never condemned it).

143 *See generally* Kim Zetter, Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon (2015).

144 Lucas Kello, *The Meaning of the Cyber Revolution: Perils to Theory and Statecraft*, 38 Int'l Sec. 7, 24 (2013).

27 26 25 24 23 22 21 7 6 5 4 3 2 1

The preferred citation for this publication is Jack Goldsmith and Alex Loomis, *"Defend Forward" and Sovereignty*, Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 2102 (April 29, 2021), available at https://www.lawfareblog.com/defend-forward-and-sovereignty.

About the Authors

JACK GOLDSMITH

Jack Goldsmith is the Learned Hand Professor at Harvard Law School, cofounder of *Lawfare*, and a senior fellow at the Hoover Institution. Before coming to Harvard, Professor Goldsmith served as assistant attorney general, Office of Legal Counsel, from 2003 to 2004, and as special counsel to the Department of Defense from 2002 to 2003.

ALEX LOOMIS

Alex Loomis is an associate at Quinn Emanuel Urquhart & Sullivan, LLP (affiliation provided for identification purposes only). Before joining Quinn Emanuel, Alex worked as a clerk to the Honorable Judge Debra Ann Livingston on the US Court of Appeals for the Second Circuit. Loomis graduated magna cum laude from Harvard Law School in 2017.

The Jean Perkins Foundation Working Group on National Security, Technology, and Law

The Jean Perkins Foundation Working Group on National Security, Technology, and Law brings together national and international specialists with broad interdisciplinary expertise to analyze how technology affects national security and national security law and how governments can use that technology to defend themselves, consistent with constitutional values and the rule of law.

The group focuses on a broad range of interests, from surveillance to counterterrorism to the dramatic impact that rapid technological change—digitalization, computerization, miniaturization, and automaticity—are having on national security and national security law. Topics include cybersecurity, the rise of drones and autonomous weapons systems, and the need for—and dangers of—state surveillance. The group's output will also be published on the *Lawfare* blog, which covers the merits of the underlying legal and policy debates of actions taken or contemplated to protect the nation and the nation's laws and legal institutions.

Jack Goldsmith is the chair of the National Security, Technology, and Law Working Group.

For more information about this Hoover Institution Working Group, visit us online at http://www.hoover.org/research-teams /national-security-technology-law-working-group.

Hoover Institution, Stanford University
434 Galvez Mall
Stanford, CA 94305-6003
650-723-1754

Hoover Institution in Washington
The Johnson Center
1399 New York Avenue NW, Suite 500
Washington, DC 20005
202-760-3200

HOOVER INSTITUTION