TEMPLE LAW REVIEW

VOL. 97 NO. 1 **FALL 2024**

ESSAY

THE 2024 ARLIN M. AND NEYSA ADAMS LECTURE

INTERNATIONAL LAW AND CYBERSPACE: BUILDING CONSENSUS

Richard C. Visek[*]

Thank you, Dean Rachel Rebouché and Professor Duncan Hollis. It is a pleasure to be here this afternoon for the 2024 Arlin M. and Neysa Adams Lecture. I always enjoy getting a chance to meet with students, and I am grateful to the Adams family and Temple University Law School for inviting me here to speak. I also want to thank my colleague, Marguerite Walter, who was instrumental in putting these remarks together.

Today, I would like to talk about how States over the past decade or so have discussed the ways in which international law applies in cyberspace. I am going to focus on how international law applies to cyber activities of States that affect, directly or indirectly, the interests of other States.

Since the United States first began thinking about international law and cyberspace in the 1990s, it has been clear to us that international law applies to what States do in cyberspace, just as it does to what they do in other domains.[1] When I say international law, I mean all of it—treaties, of course, but also customary international

[*] Richard C. Visek is the Principal Deputy Legal Adviser in the Office of the Legal Adviser at the U.S. Department of State. When he gave these remarks, he was serving as the Acting Legal Adviser. This Essay was presented orally on April 24, 2024, at the Temple University James E. Beasley School of Law Arlin M. and Neysa Adams Lecture. This Essay includes footnotes and additional content that, due to time constraints, were not included in the remarks as delivered orally.

1. *See, e.g.*, U.S. DEP'T OF DEF., OFF. OF GEN. COUNS., AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS (2nd ed., 1999), *reprinted in* 76 INT'L L. STUD. 459 (2002) (exploring how existing international law, particularly the law of war, would apply to "information operations," while noting that some additional interpretation is likely necessary).

law, which develops over time through State practice and *opinio juris*. Customary international law encompasses many of the fundamental rules that underpin our understanding of what States may or may not lawfully do.

The question is how to interpret and apply the law to the ways new technology is used. But some other States, notably Russia, questioned whether any law applied to activities in cyberspace, suggesting there needed to be an entirely new legal regime.[2] Twenty-five years later, Russia is still making versions of this argument. But the broader landscape has changed enormously. States are actively discussing at the United Nations (UN) and elsewhere how international law applies in cyberspace and, particularly since 2016, many have issued public statements on how they interpret its application to cyber activities.

Partly in response to Russia's proposal for a resolution describing cyber capabilities as a new "information weapon" and calling for a new legal regime to govern cyberspace,[3] the UN First Committee took up the issue of international peace and security in cyberspace in the late 1990s, which led to a series of expert working groups, called Groups of Governmental Experts (GGEs), to discuss potential threats to international peace and security in cyberspace.

International law has been part of this discussion from the outset, and in 2013, the GGE issued its first report, affirming that international law applies in cyberspace.[4] This report was endorsed by consensus in the UN General Assembly that year, confirming universal acceptance that existing international law applies to what States do in cyberspace.

Perhaps the key achievement of the GGEs is the 2015 GGE report, which was also endorsed by the UN General Assembly and which set up a structure that combines normative expectations, confidence-building measures, international cooperation, capacity building, and a commitment to developing common understandings of how international law applies in cyberspace. This is what has come to be known as the framework for responsible State behavior in cyberspace.[5] I'll discuss the framework, and specifically certain norms, a bit more later on, but would like to focus first on the legal piece of it.

The 2015 GGE report was the first consensus document created by States that discussed how international law applied in cyberspace. But even more importantly, it called on States to develop "common understandings on how international law applies

---

2. *See* Harold Hongju Koh, *International Law in Cyberspace*, HARV. INT'L L.J. ONLINE, Dec. 2012, at 1, 3, 11, https://journals.law.harvard.edu/ilj/wp-content/uploads/sites/84/2012/12/Koh-Speech-to-Publish1.pdf [https://perma.cc/9Z7R-KC45] ("At least one country has questioned whether existing bodies of international law apply to the cutting edge issues presented by the internet. Some have also said that existing international law is not up to the task, and that we need entirely new treaties to impose a unique set of rules on cyberspace.").

3. *See* Permanent Rep. of the Russian Federation, Letter dated Sept. 23, 1998, from the Permanent Rep. of the Russian Federation to the United Nations addressed to the Secretary-General, U.N. DOC. A/C.1/53/3 (Sept. 30, 1998).

4. *See* Rep. of the Grp. of Governmental Experts on Devs. in the Field of Info. and Telecomms. in the Context of Int'l Sec., U.N. DOC. A/68/98 (June 24, 2013).

5. *See* Rep. of the Grp. of Governmental Experts on Devs. in the Field of Info. and Telecomms. in the Context of Int'l Sec., U.N. DOC. A/70/174 (July 22, 2015) [hereinafter 2015 GGE report].

to State use of [cyber capabilities]," which it said were "important for promoting an open, secure, stable, accessible and peaceful [cyber] environment."[6]

In 2016, Brian Egan, the State Department Legal Adviser at the time, gave a speech setting forth detailed U.S. views on how international law applies in cyberspace.[7] He built upon a 2012 speech by his predecessor, Harold Koh.[8] But, Egan said, "remote cyber operations" involving devices on another State's territory were not a "per se violation of international law," particularly where such activities had no effects or de minimis effects.[9] In certain circumstances, though, a cyber operation could violate international law even if it fell below the threshold of a use of force.[10]

Noting that "[p]recisely when a non-consensual cyber operation violates the sovereignty of another State is a question lawyers within the U.S. government continue to study carefully,"[11] Egan was clear, however, that "[a]ny regulation by a State of matters within its territory, including use of and access to the Internet, must comply with that State's applicable obligations under international human rights law."[12] In other words, sovereignty could not be "a justification for excessive regulation of online content, including censorship and access restrictions."[13] Ultimately, the question of when cyber operations violate another State's sovereignty would be resolved through State practice and *opinio juris*, that is, whether States accept the practice as reflecting a legal obligation.[14]

Perhaps heeding these words and the 2015 GGE call that States develop common understandings on international law, other States soon began to offer their own public statements on how international law applies.[15] The last GGE, which convened from

---

6. *Id.* ¶ 29.

7. Brian J. Egan, *International Law and Stability in Cyberspace*, 35 BERKELEY J. INT'L L. 169 (2017).

8. Koh, *supra* note 2; Egan, *supra* note 7, at 173.

9. Egan, *supra* note 7, at 174 (emphasis omitted).

10. *Id.*

11. *Id.*

12. *Id.* at 175.

13. *Id.*

14. *Id.* at 174.

15. *See, e.g.*, COMMONWEALTH OF AUSTL., DEP'T OF FOREIGN AFFS. AND TRADE, AUSTRALIA'S INTERNATIONAL CYBER ENGAGEMENT STRATEGY 90, annex A (2017), https://web.archive.org/web/20190421024033/https://dfat.gov.au/international-relations/themes/cyber-affairs/aices/chapters/annexes.html#Annex-A; Jeremy Wright, U.K. Att'y Gen., Cyber and International Law in the 21st Century (May 23, 2018), https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century [https://perma.cc/74ZV-2RST]; Kersti Kljulaid, President of Est., *President Kaljulaid at CyCon 2019: Cyber Attacks Should Not be Easy Weapon*, ERR (May 29, 2019), https://news.err.ee/946827/president-kaljulaid-at-cycon-2019-cyber-attacks-should-not-be-easy-weapon [https://perma.cc/TD8A-UDG7]; Letter from the Dutch Minister of Foreign Aff. to the President of the House of Representatives on the Int'l Legal Order in Cyberspace (July 5, 2019), https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace [https://perma.cc/9QE2-TJ9X]; FR. MINISTRY OF THE ARMED FORCES, INTERNATIONAL LAW APPLIED TO OPERATIONS IN CYBERSPACE (2019), https://www.defense.gouv.fr/sites/default/files/ema/Droit%20international%20appliqu%C3%A9%20aux%20op%C3%A9rations%20dans%20le%20cyberespace.pdf [https://perma.cc/2F9K-UNXV].

2019 to 2021, invited States to submit position statements on international law to be included as a compendium to the 2021 GGE report, which fifteen States did.[16]

All told, in the past decade, over thirty States and one regional organization have provided public statements on how international law applies in cyberspace. Many of them have done so through written public statements; others have done so in spoken remarks. Most recently, the fifty-five Member States of the African Union came together to adopt a Common African Position on how international law applies in cyberspace, accompanied by a communiqué encouraging each State to consider issuing its own national statement.[17]

Meanwhile, the GGEs have been succeeded by two successive UN Open-Ended Working Groups (OEWGs) on the security and use of information and communications technologies.[18] International law has been an increasing focus for States in the OEWG, and many of them have called for further, in-depth discussions of this topic. I have no doubt that these discussions will continue to deepen as additional States share their views over the next few years.

Given how much the landscape has changed since Brian Egan spoke on this issue, I would like to offer a few reflections on areas of emerging consensus that can be gleaned from developments over the past eight years. I do not intend today to introduce new U.S. views on international law, but rather to take a step back and observe progress made in developing common understandings of how international law applies in cyberspace, reiterating the U.S. perspective where appropriate.

SOVEREIGNTY APPLIES IN CYBERSPACE

By and large, States that have issued statements so far have recognized that the principle of sovereignty applies in cyberspace,[19] and they generally look to the effects

16. *See* Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States Submitted by Participating Governmental Experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security Established Pursuant to General Assembly Resolution 73/266, U.N. DOC. A/76/136 (July 13, 2021) [hereinafter Compendium].

17. African Union Peace and Sec. Council, Common African Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace (Jan. 29, 2024) [hereinafter AU CAP], https://papsrepository.africa-union.org/bitstream/handle/123456789/2022/1196%20AU%20Common%20Position%20Adopted%20Version%20-%20EN.pdf?sequence=11 [https://perma.cc/8VYN-MVU4]; African Union Peace and Sec. Council, Communiqué PSC/PR/COMM.1196 (Jan. 29, 2024), https://papsrepository.africa-union.org/bitstream/handle/123456789/2022/1196.comm_en.pdf?sequence=1&isAllowed=y [https://perma.cc/FKP7-VBU3]. The European Union is also apparently working on a common position. *See* Anna-Maria Osula, Agnes Kasper & Aleksi Kajander, *EU Common Position on International Law and Cyberspace*, 16 MASARYK UNIV. J.L. & TECH. 89 (2022). The Inter-American Juridical Committee of the Organization of American States has issued several reports on international law and adopted a resolution recognizing that international law applies to cyberspace. *See* Organization of American States [OAS] G.A. Res. 2959, OAS Doc. AG/RES.2959 (L-O/20) (Oct. 21, 2020).

18. *See* G.A. Res. 73/27, Developments in the Field of Information and Telecommunications in the Context of International Security, A/RES/73/27 (Dec. 5, 2018); G.A. Res. 75/240, Developments in the Field of Information and Telecommunications in the Context of International Security, A/RES/75/240 (Dec. 31, 2020).

19. This includes Russia and others that argue for the necessity of new legally binding rules to address cyberspace. Russia's national position statement submitted to the GGE in 2021 says that "Russia assumes that,

of cyber activities when assessing their lawfulness.[20] Many of them believe that, under certain circumstances, cyber operations can violate what they consider to be an international law rule of territorial sovereignty when their effects rise to a sufficient level of seriousness, including some degree of harm or interference in governmental functions.[21] The United Kingdom is the only State that has said it does not see a standalone rule of sovereignty in cyberspace, but it does recognize sovereignty as a general principle that is reflected in the rule of nonintervention and elsewhere, which I will turn to in a bit.[22] For our part, the United States continues to study the question of precisely when cyber activities would violate a State's sovereignty.

---

for the present, the international community has reached consensus on the applicability of the universally accepted principles and norms of international law," which it says include the "sovereign equality of States." Contribution of Russian Federation, *in* Compendium, *supra* note 16, at 79. China's statement on sovereignty submitted to the second OEWG outlines a somewhat different view, sometimes described as "cyber sovereignty" or "Internet sovereignty," which emphasizes State control over information and cyber infrastructure, both internally and extraterritorially. *See* CHINA'S VIEWS ON THE APPLICATION OF THE PRINCIPLE OF SOVEREIGNTY IN CYBERSPACE (2021) [hereinafter CHINA], https://documents.unoda.org/wp-content/uploads/2021/12/Chinese-Position-Paper-on-the-Application-of-the-Principle-of-Sovereignty-ENG.pdf [https://perma.cc/395H-6HH5].

20. *See, e.g.*, Contribution of Germany, *in* Compendium, *supra* note 16, at 33 [hereinafter Germany] (cyber operations causing "**physical effects and harm in the territory of another State** constitute a violation of that State's territorial sovereignty," while "**negligible** physical effects and functional impairments below a certain impact threshold cannot – taken by themselves – be deemed to constitute a violation of territorial sovereignty"); Contribution of Japan, *in* Compendium, *supra* note 16, at 47 [hereinafter Japan] ("An act of causing physical damage or loss of functionality by means of cyber operations against critical infrastructure, including medical institutions . . . may constitute a violation of sovereignty."); *The Application of International Law to State Activity in Cyberspace*, N.Z. MINISTRY OF FOREIGN AFFS. AND TRADE (Dec. 1, 2020) [hereinafter NEW ZEALAND], https://www.mfat.govt.nz/en/media-and-resources/the-application-of-international-law-to-state-activity-in-cyberspace [https://perma.cc/YGC2-KHQV] ("[T]erritorial sovereignty prohibits states from using cyber means to cause significant harmful effects manifesting on the territory of another state," though territorial sovereignty does not prohibit "every unauthorised intrusion into a foreign ICT system or . . . all cyber activity which has effects on the territory of another state.").

21. *See, e.g.*, Contribution of the Netherlands, *in* Compendium, *supra* note 16, at 57 [hereinafter Netherlands] (citing Tallinn Manual 2.0 and stating that sovereignty may be violated where there is a territorial infringement and "interference with or usurpation of inherently governmental functions of another state"); Contribution of Norway, *in* Compendium, *supra* note 16, at 68 [hereinafter Norway]; Contribution of Switzerland, *in* Compendium, *supra* note 16, at 87 [hereinafter Switzerland]; ARMED FORCES CYBERSPACE CTR., *National Position of Iran (2020)*, CYBERLAW TOOLKIT (Aug. 2020) [hereinafter IRAN], https://cyberlaw.ccdcoe.org/wiki/National_position_of_Iran_(2020) [https://perma.cc/6UG4-QKNU] ("Any intentional use of cyber-force with tangible or non-tangible implications which is or can be a threat to the national security or may, due to political, economic, social, and cultural destabilization, result in destabilization of national security constitutes a violation of the sovereignty of the state."); POL. MINISTRY OF FOREIGN AFFS., THE REPUBLIC OF POLAND'S POSITION ON THE APPLICATION OF INTERNATIONAL LAW IN CYBERSPACE 3 (2022) [hereinafter POLAND], https://www.gov.pl/web/diplomacy/the-republic-of-polands-position-on-the-application-of-international-law-in-cyberspace [https://perma.cc/N3CU-HZBZ] (interfering with function of State organs could violate sovereignty).

22. *See* Suella Braverman, U.K. Att'y Gen., International Law in Future Frontiers (May 19, 2022), https://www.gov.uk/government/speeches/international-law-in-future-frontiers [https://perma.cc/B2WU-AWB8] ("The general concept of sovereignty by itself does not provide a sufficient or clear basis for extrapolating a specific rule of sovereignty or additional prohibition for cyber conduct going beyond that of non-intervention.").

A number of States acknowledge the difficulty of applying a rule of territorial sovereignty when it comes to cyber activities,[23] and many emphasize that violations of territorial sovereignty must be assessed on a case-by-case basis.[24] Some of them explicitly state that further State practice is necessary in order for a specific rule to become clear.[25]

Nevertheless, there appears to be general agreement in these statements that cyber activities would not violate a rule of territorial sovereignty unless their effects in a State's territory reached a certain threshold of harm, either in nature or scope. For example, Canada has said that it would assess a violation based on several key factors, including the "scope, scale, impact or severity of disruption caused, including the disruption of economic and societal activities, essential services, inherently governmental functions, public order or public safety."[26] Other States have outlined similar factors they would take into consideration.[27]

Overall, the statements suggest that, for many States, nonconsensual cyber operations with effects on another State's territory generally are not per se violations of territorial sovereignty and will only be seen as violating international law when cyber

---

23. *See, e.g.*, Switzerland, *supra* note 21, at 87 ("Switzerland recognises that defining what constitutes a violation of the principle of sovereignty in cyberspace is particularly challenging and has yet to be clarified conclusively."); Netherlands, *supra* note 21, at 56 (noting that sovereignty "has traditionally been aimed at protecting a state's authority over *property and persons within its own national borders*," but that "[i]n cyberspace, the concepts of territoriality and physical tangibility are often less clear").

24. *See, e.g.*, FIN. MINISTRY FOR FOREIGN AFFS., INTERNATIONAL LAW AND CYBERSPACE: FINLAND'S NATIONAL POSITIONS (2020) [hereinafter FINLAND], https://um.fi/documents/35732/0/KyberkannatPDF_EN.pdf/ [https://perma.cc/URR3-ENR2]; NEW ZEALAND, *supra* note 20, ¶¶ 12, 15; Norway, *supra* note 21, at 68; IT. MINISTRY OF FOREIGN AFFS., ITALIAN POSITION PAPER ON 'INTERNATIONAL LAW AND CYBERSPACE' 4 (2021) [hereinafter ITALY], https://www.esteri.it/wp-content/uploads/2021/11/Italian-Position-Paper-on-International-Law-and-Cyberspace.pdf [https://perma.cc/SJ7U-6UVF]; MINISTRY OF FOREIGN AFFS. OF THE CZECH REPUBLIC, POSITION PAPER ON THE APPLICATION OF INTERNATIONAL LAW IN CYBERSPACE (2024) [hereinafter CZECH REPUBLIC], https://mzv.gov.cz/file/5376858/_20240226___CZ_Position_paper_on_the_application_of_IL_cyberspace.pdf [https://perma.cc/CT8B-78YV] ("The Czech Republic will assess whether a violation of sovereignty has occurred on a case-by-case basis, since further State practice and *opinio juris* is needed to clarify the scope of customary law in this area . . . .").

25. *See, e.g.*, Netherlands, *supra* note 21, at 56 ("[States] may not conduct cyber operations that violate the sovereignty of another [State]. It should be noted in this regard that the precise boundaries of what is and is not permissible have yet to fully crystallise."); NEW ZEALAND, *supra* note 20, ¶ 12 ("New Zealand considers that the standalone rule of territorial sovereignty also applies in the cyber context but acknowledges that further state practice is required for the precise boundaries of its application to crystallise."); Switzerland, *supra* note 21, at 87.

26. *International Law Applicable in Cyberspace*, GOV'T OF CAN. ¶ 14 (Mar. 4, 2022) [hereinafter CANADA], https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng [https://perma.cc/RJ3A-WF5A].

27. *See, e.g.*, COSTA RICA MINISTRY OF FOREIGN AFFS. & WORSHIP, COSTA RICA'S POSITION ON THE APPLICATION OF INTERNATIONAL LAW IN CYBERSPACE ¶ 20 (2023) [hereinafter COSTA RICA] (listing possible breaches as physical damage or loss of functionality of cyber infrastructure, including operations that cause the need to repair or replace physical components, compromises physical equipment reliant on targeted cyber infrastructure, or causing an operating system or database to cease functioning as intended); Norway, *supra* note 21, at 68 ("The precise threshold of what constitute [sic] a cyber operation in violation of sovereignty is not settled in international law, and will depend on a case-by-case assessment.").

effects in another State's territory are sufficiently serious to undermine an identifiable State interest.[28]

A few States have suggested a stricter rule that would view even minimally harmful cyber operations as potential violations of international law. France is often cited as an example of this,[29] though there are some others, including most recently the African Union. The Common African Position states that "any unauthorised access by a State into the ICT [information and communication technology] infrastructure located on the territory of a foreign State is unlawful."[30]

The common element is that States generally agree that harmful cyber effects can violate a State's sovereignty. Some States might place the bar higher or lower, or might view the violation through a different rule of international law deriving from sovereignty, but, as the UK has pointed out, "differing viewpoints" on the specific details of any given international law rule "should not prevent States from assessing whether particular situations amount to internationally wrongful acts and arriving at common conclusions on such matters."[31]

In this context, it should also be stressed that, like the United States, many States recognize that international human rights law constrains what States may do concerning cyber activities, regardless of their views on sovereignty. Romania's statement is an example. It emphasizes that international human rights law places limits on States:

> International law does not recognise a right to States to derogate from their international human rights obligations as a defensive-type measure—for instance to restrict access to internet in all circumstance[s] as a responsive measure to counter some types of conduct in cyberspace . . . . [W]hatever regulation a State adopts (by virtue of its sovereign right) it must conform with its international obligations in the field of human rights.[32]

---

28. See *infra* notes 94–97 and accompanying text for a discussion of possible responses to lawful but unfriendly acts.

29. *See* FR. MINISTRY OF THE ARMED FORCES, *supra* note 15, at 7. A more recent statement in a French military manual suggests perhaps a more nuanced view. *See* CAMILLE FAURE, MINISTÈRE DES ARMÉES, MANUEL DE DROIT DES OPÉRATIONS MILITAIRES 302 (2022), https://www.defense.gouv.fr/sga/au-service-armees/droit-defense/droit-conflits-armes [https://perma.cc/YCL3-7V4D].

30. AU CAP, *supra* note 17, ¶ 16. This rule would not seem to reach the mere sending of packets of information sent in the ordinary course of business on the Internet, since that kind of activity would presumably be permitted by a State's applicable domestic law. But it is noteworthy that in rejecting the suggestion that there might be a de minimis threshold for a breach of sovereignty, the Common African Position states that "the obligation to respect the territorial sovereignty of States, as it applies in cyberspace, does not include a de minimis threshold of harmful effects below which an unauthorized access by a State into the ICT infrastructure located on the territory of a foreign State would not be unlawful." *Id.* (emphasis omitted). In essence, the AU appears to be saying that in its view, the threshold for a breach of territorial sovereignty is any harm to the implicated information infrastructure. *See id.*

31. Contribution of the United Kingdom, *in* Compendium, *supra* note 16, at 117 [hereinafter U.K.].

32. Contribution of Romania, *in* Compendium, *supra* note 16, at 78 [hereinafter Romania]. Italy similarly argues that "[r]espect for human rights obligations must be upheld at all times, including when preventing, mitigating or responding to cyber incidents." ITALY, *supra* note 24; *see also* Netherlands, *supra* note 21, at 60; U.K., *supra* note 31, at 117; COSTA RICA, *supra* note 27, ¶31; POLAND, *supra* note 21, at 6; SWED. MINISTRY OF FOREIGN AFFS., POSITION PAPER ON THE APPLICATION OF INTERNATIONAL LAW IN CYBERSPACE 7 (2022) [hereinafter SWEDEN], https://www.government.se/contentassets

Many of these States identify rights that may be particularly at issue when it comes to cyberspace, including freedoms of opinion and expression, peaceful assembly and association, as well as the right to be free from arbitrary or unlawful interference with privacy.[33] While not all States address human rights in their statements, only the People's Republic of China's statement suggests actual resistance to the idea that international human rights law constrains a State's internal (or even external) cyber-related activities.[34]

To further develop common understandings about the contours of the concept of sovereignty in the context of cyberspace, there are a number of questions that States may want to consider, and that may also be fruitful ground for legal scholars.

- What constitutes a harmful effect? Could a cyber activity that impairs the functioning of software or access to data, but has no physical effects, be unlawful? For example, if a cyber operation encrypts data but has no other effects, how would that factor into a State's analysis of potential breach?
- Does the nature of the infrastructure affected influence the assessment of unlawfulness? For example, if the affected infrastructure has been designated as "critical infrastructure" by the target State, does that affect the legal analysis?
- How does "cloud" storage affect States' views of the legal framework? Or, to put it another way, how is a State's sovereignty implicated, if at all, if another State's cyber activities affect its data stored on a cloud server located in a third State's territory?

CYBER OPERATIONS CAN CONSTITUTE A PROHIBITED INTERVENTION

Statements to date show a firm consensus on cyber activities that interfere coercively in what the International Court of Justice (ICJ) has described as "matters in which each State is permitted, by the principle of State sovereignty, to decide freely."[35] In its merits judgment in the *Nicaragua v. United States* case, the ICJ singled out "the choice of a political, economic, social and cultural system, and the formulation of foreign policy" as among those things that international law provides that States must be able to decide freely.[36] The United States and many others have cited the ICJ's

/3c2cb6febd0e4ab0bd542f653283b140/swedens-position-paper-on-the-application-of-international-law-in-cyberspace.pdf [https://perma.cc/5WX9-FGNY].

33. *See, e.g.*, Contribution of Australia, *in* Compendium, *supra* note 16, at 7 [hereinafter Australia]; Contribution of Estonia, *in* Compendium, *supra* note 16, at 27 [hereinafter Estonia]; Romania, *supra* note 32, at 78; Contribution of Singapore, *in* Compendium, *supra* note 16, at 85 [hereinafter Singapore]; CANADA, *supra* note 26, ¶ 40; COSTA RICA, *supra* note 27, ¶¶ 33–34; POLAND, *supra* note 21, at 7; SWEDEN, *supra* note 32, at 7–8.

34. *See* CHINA, *supra* note 19, at 2. China also asserts a right to exercise "necessary and reasonable personal, territorial and protective jurisdiction" over cyber activities outside its territory when such activities "have genuine and substantial connection" to it, "as well as over relevant [cyber]-related facilities, entities, data and information." *Id.* It considers that it may seek assistance from other States in exercising this jurisdiction, but only "in the spirit of self-restraint, comity and reciprocity," and, apparently, not because of any legal constraint. *Id.*

35. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep. 97–98, ¶ 205 (June 27).

36. *Id.*

articulation of this rule in affirming their belief that a State's cyber activities can constitute a prohibited intervention.[37]

One notable feature of many of these statements is a focus on interference with democratic processes as a potential breach.[38] For example, Poland mentions cyber activities that prevent a parliament convening virtually from being able to vote online to adopt a law, or that change the outcome of such a vote.[39] And, most States seem to agree that interference in a country's ability to hold an election or alteration of election results could constitute a prohibited intervention.[40] Brazil noted in its statement that to constitute prohibited intervention, "the malicious use of ICTs against another State must involve an element of coercion," adding that "[c]onsidering that elections are at the core of a State's internal affairs, should the malicious use of ICTs against a State involve some level of coercion, then it must be prohibited by the principle of non-intervention."[41] Singapore cited "interference in [its] electoral processes through cyber means" as a potential breach,[42] while Canada offered specific examples, such as a cyber activity that disables a State's election commission just before an election, "preventing a significant number of citizens from voting, and ultimately influencing the election outcome."[43]

Some statements have identified other types of cyber activities that States believe could breach this rule. Poland includes cyber activity that prevents the filing of tax returns[44] and Canada gives the example of a cyber activity that disrupts the functioning of a major gas pipeline, compelling the affected State to change its position during negotiation of an international energy agreement.[45] For Ireland, cyber operations that seriously compromise healthcare systems may violate international law,[46] something the United States also suggested in its 2021 GGE statement.[47]

---

37. Contribution of the United States, *in* Compendium, *supra* note 16, at 139–40 [hereinafter U.S.].

38. For example, the United States has said 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." *Id.* at 140.

39. POLAND, *supra* note 21, at 4.

40. *See, e.g.*, Australia, *supra* note 33, at 5; Estonia, *supra* note 33, at 25; Germany, *supra* note 20, at 32, 34–35; Norway, *supra* note 21, at 69; U.K., *supra* note 31, at 116; Jeppe Mejer Kjelgaard & Ulf Melgaard, *Denmark's Position Paper on the Application of International Law in Cyberspace*, 92 NORDIC J. INT'L L. 446, 450 (2023) ("An example of unlawful intervention in the cyber domain could be where a State coercively interferes in the internal political process of another. In the cyber context this could potentially occur by using cyber technology to alter electronic ballots and thereby affecting the results of a political election."); CZECH REPUBLIC, *supra* note 24, ¶ 12; CANADA, *supra* note 26, ¶ 24; POLAND, *supra* note 21, at 4; COSTA RICA, *supra* note 27, at 8; NEW ZEALAND, *supra* note 20, ¶ 10; FINLAND, *supra* note 24, at 3; Singapore, *supra* note 33, at 83; Roy Schöndorf, Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations, 97 INT'L L. STUD. 395, 403 (2021).

41. Contribution of Brazil, *in* Compendium, *supra* note 16, at 19 [hereinafter Brazil].

42. Singapore, *supra* note 33, at 83.

43. CANADA, *supra* note 26, ¶ 24.

44. POLAND, *supra* note 21, at 4.

45. CANADA, *supra* note 26, ¶ 24.

46. IR. DEP'T OF FOREIGN AFFS., POSITION PAPER ON THE APPLICATION OF INTERNATIONAL LAW IN CYBERSPACE ¶ 9 (2023) [hereinafter IRELAND], https://www.dfa.ie/media/dfa/ourrolepolicies/internationallaw/Ireland---National-Position-Paper.pdf [https://perma.cc/Y636-9DBC] ("In order for the principle to be engaged, an intervention in the cyber context must be of sufficient seriousness, comparable in scale and effects

Of course, a key element of a prohibited intervention is coercion,[48] something that States grapple with in their statements. Singapore mentions "cyber-attacks against [its] infrastructure in an attempt to coerce [its] government to take or forbear a certain course of action on a matter ordinarily within its sovereign prerogative" as one example.[49] The Netherlands suggests that "[t]he precise definition of coercion . . . has not yet fully crystallised in international law," but adds that "[i]n essence it means compelling a state to take a course of action (whether an act or an omission) that it would not otherwise voluntarily pursue."[50] Germany's statement cautions, however, that "the element of coercion must not be assumed prematurely," adding that

> [e]ven harsher forms of communication such as pointed commentary and sharp criticism as well as (persistent) attempts to obtain, through discussion, a certain reaction or the performance of a certain measure from another State do not as such qualify as coercion. Moreover, the acting State must intend to intervene in the internal affairs of the target State—otherwise the scope of the non-intervention principle would be unduly broad.[51]

In a 2022 speech, the United Kingdom's Attorney General, Suella Braverman, acknowledged that coercion could mean "forcing a State to act differently from how it otherwise would—that is, compelling it into a specific act or omission."[52] But she argued that coercion could be broader than this, reaching any intervention that "depriv[es] a State of its freedom of control over matters which it is permitted to decide freely by the principle of State sovereignty."[53] While the boundaries of coercion had not yet crystallized in international law, she argued that "we should be ready to consider whether disruptive cyber behaviours are coercive even where it might not be possible to point to a specific course of conduct" a State has been compelled to take or refrain from taking.[54]

---

to coercive action in a non-cyber context. For instance, malicious cyber-operations seriously compromising healthcare systems or national elections are capable of amounting to unlawful interventions.").

47. *See* U.S., *supra* note 37, at 140 ("[A] cyber operation that attempts to interfere coercively with a State's ability to protect the health of its population--for example, through vaccine research or running cyber-controlled ventilators within its territories during a pandemic--could be considered a violation of the rule of non-intervention.").

48. *See, e.g.*, Braverman, *supra* note 22.

49. Singapore, *supra* note 33, at 83.

50. Netherlands, *supra* note 21, at 57.

51. Germany, *supra* note 20, at 34.

52. Braverman, *supra* note 22.

53. *Id.* Note that both Australia and New Zealand have described coercion as a deprivation of control, a description that likely has its source in Oppenheim's International Law. *See* Australia, *supra* note 33, at 5; NEW ZEALAND, *supra* note 20, ¶ 9(b); *cf.* 1 OPPENHEIM'S INTERNATIONAL LAW 432 (Sir Robert Jennings & Sir Arthur Watts eds., 9th ed. 1992) ("It must be emphasised that to constitute intervention the interference must be forcible or dictatorial, or otherwise coercive, in effect depriving the state intervened against of control over the matter in question.").

54. *Id.* Some commentators have argued that the UK's invitation to explore what may be a more expansive understanding of coercion reflects an effort to bridge the gap between its views and those of States that recognize a rule of territorial sovereignty in cyberspace. *See, e.g.*, Michael Schmitt, *The United Kingdom on International Law in Cyberspace*, EJIL: TALK! (May 24, 2022), https://www.ejiltalk.org/the-united-kingdom-on-international-law-in-cyberspace/ [https://perma.cc/9HTH-4VF2] (arguing it had been anticipated that UK would "soften the coercion requirement to counterbalance its rejection of the sovereignty rule," but expressing doubt that 2022 speech actually did so).

Last year, Department of Defense (DoD) General Counsel Caroline Krass, building on the work of her predecessor, Paul Ney,[55] gave a speech in which she reflected on nonintervention and the requirement of coercion. Among other things, she asked what degree of severity was required in order for an act to be coercive, and what weight should be given to intent.[56] She also asked whether coercion must succeed in order for there to be a prohibited intervention.[57]

These are all useful questions for States to be asking, and States are clearly thinking about them. For instance, on the issue of whether coercion must succeed, some States have argued that cyber activity that is intended to be coercive does not need to succeed in order to be wrongful. For example, the AU Common African Position says that, while the definition of coercion "requires further study and deliberation between States," it is not necessary for an act intended to be coercive to succeed; "[a]n unsuccessful attempt of intervention is unlawful under international law."[58] Costa Rica similarly has said that "it suffices that a State intends to coerce another State, employs coercive methods, or eventually causes coercive effects in another State."[59]

A couple of States suggest that cyber-enabled propaganda or disinformation could play a role in prohibited intervention,[60] but for these States, it seems there would need to be concrete consequences caused by that information that affected the ability of the State to act freely. For example, New Zealand identifies "a prolonged and coordinated cyber disinformation operation that significantly undermines a state's public health efforts during a pandemic" as a possible wrongful act.[61] For Germany, an information campaign that significantly erodes public trust in the political process, including by dissuading significant groups of people from voting, could also qualify as wrongful under this rule.[62] At the same time, the Czech Republic rejects the notion that propaganda or other forms of influence, on their own, would generally constitute a prohibited intervention.[63] We would share this caution because of the risk that

55. Paul C. Ney, Jr., Gen. Couns., U.S. Dep't of Def., Some Considerations for Conducting Legal Reviews of U.S. Military Cyber Operations (Mar. 2, 2020), https://www.defense.gov/News/Speeches/speech/article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/ [https://perma.cc/TEY6-U5US].

56. Caroline Krass, Gen. Couns., U.S. Dep't of Def., DoD General Counsel Remarks at U.S. Cyber Command Legal Conference (Apr. 18, 2023), https://www.defense.gov/News/Speeches/Speech/Article/3369461/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/ [https://perma.cc/GFY2-5UNA].

57. *Id.*

58. AU CAP, *supra* note 17, ¶ 32.

59. COSTA RICA, *supra* note 27, ¶ 24.

60. *See, e.g.*, *id.* ¶¶ 24–25; Germany, *supra* note 40, at 34–35; NEW ZEALAND, *supra* note 20, ¶ 10.

61. NEW ZEALAND, *supra* note 20, ¶ 10.

62. Germany, *supra* note 20, at 35; *cf.* IRAN, *supra* note 21 ("Cyber activities paralyzing websites in a state to provoke internal tensions and conflicts or sending mass messages in a widespread manner to the voters to affect the result of the elections in other states is also considered as the forbidden intervention.").

63. CZECH REPUBLIC, *supra* note 24, ¶ 13 ("Prohibition of intervention does not cover cyber activities broadly described as 'propaganda', provided that they do not violate another specific rule of international law, such as direct and public incitement to commit genocide. Mere influencing, criticism or persuasion do not meet the requirements to be qualified as prohibited intervention either." (footnote omitted)).

repressive regimes may seek a justification to suppress the right to freedom of expression in the name of combating disinformation.[64]

A few questions emerge from these statements, including:

- The ICJ's articulation of prohibited intervention does not expressly include a territorial element. Does a "deprivation of control" theory of coercion for cyber activities implicitly depend on the existence of effects within a State's territory?
    - If so, how would nonintervention be different from the rule of territorial sovereignty articulated by many States?
    - If not, is there another limiting principle that would distinguish prohibited intervention from lawful forms of pressure?
- How does intent fit into the analysis of prohibited intervention? Assuming it is relevant, how can intent be established with respect to cyber activities?
- Is there a customary international law basis for finding a prohibited intervention where the attempt to interfere failed to achieve the intended results?

CYBER OPERATIONS CAN BE A USE OF FORCE AND CAN BE USED IN SELF-DEFENSE

National statements so far demonstrate a strong consensus among States that customary international law rules on the use of force, including relevant provisions of the UN Charter,[65] apply to cyber activities, and that a cyber activity may constitute a use of force or an armed attack under certain circumstances. Here again, States are consistent in looking to the effects of the cyber activities and taking each situation on a case-by-case basis.

In particular, there appears to be broad consensus that a cyber activity may qualify as a use of force if it causes damage similar to that of a kinetic, or physical, attack.[66] For example, Costa Rica states that "a cyber operation may amount to a prohibited use of force if it can cause harm or destruction analogous to a conventional weapon."[67] In its view, "this assessment can only be carried out on a case-by-case basis," though it would likely view cyber operations "causing physical harm to individuals or significant destruction of property, as well as those permanently disabling operating systems controlling critical infrastructure, such as an electrical grid or a water and sanitation

64. *See* Egan, *supra* note 7, at 175 (recalling that prohibited intervention "is generally viewed as a relatively narrow rule of customary international law"); Schöndorf, *supra* note 40, at 403 ("Traditionally, this concept has been understood as having a high threshold.").

65. *See* U.N. Charter arts. 2(4), 51.

66. The United States has said that, "although this is necessarily a case-by-case, fact-specific inquiry, cyber activities that proximately result in death, injury, or significant destruction, or represent an imminent threat thereof, would likely be viewed as a use of force [or] armed attack." U.S., *supra* note 37, at 137.

67. COSTA RICA, *supra* note 27, ¶ 36, at 10.

station,"[68] as examples of a use of force.[69] Many other States have expressed very similar views.[70]

States are also consistent that the legal assessment must be based on the facts and circumstances of each situation.[71] For example, Denmark has said that determining whether a cyber activity is a use of force "requires an individual assessment of the specific circumstances in each case to determine whether the scale and effects of a cyber operation correspond to what would qualify as use of force had they resulted from conventional weapons."[72] Most others take a similar position.[73]

Many States that have published views also agree that the inherent right of self-defense may be triggered by, and exercised through, cyber means. In this regard, it is important to recall that many States—although notably not the United States[74]—distinguish between a use of force, which in their view may not give rise to the right to use force in self-defense, and an armed attack, which would. Japan, for example, has said that "[w]hen a cyber operation constitutes an armed attack under Article 51 of the UN Charter, States may exercise the inherent right of individual or collective self-defense recognized under Article 51 of the UN Charter."[75] Switzerland notes that

> [t]here are no binding quantitative or qualitative guidelines as to when the threshold of an armed attack . . . has been reached. Current discussions on how to define an armed attack in cyberspace are focusing on attacks on critical infrastructure (e.g. nuclear power plants, power grids) which reach the required threshold in terms of scale and effect i.e. serious injury to persons and/or extensive damage to objects.[76]

---

68. *Id.* ¶ 36, at 10–11 (citation omitted).

69. *Id.* ¶ 36.

70. *See, e.g.*, Australia, *supra* note 33, at 5–6; Estonia, *supra* note 33, at 26, 30; Germany, *supra* note 20, at 35–36, 43; U.K., *supra* note 31, at 116; ITALY, *supra* note 24, at 8; NEW ZEALAND, *supra* note 20, ¶¶ 7–8; CANADA, *supra* note 26, ¶¶ 45, 49; COSTA RICA, *supra* note 27, ¶¶ 35–37; Schöndorf, *supra* note 40, at 398–99; SWEDEN, *supra* note 32, at 7; POLAND, *supra* note 21, at 5; CZECH REPUBLIC, *supra* note 24, ¶¶ 26–29.

71. *See, e.g.*, CANADA, *supra* note 26, ¶ 45; NEW ZEALAND, *supra* note 20, ¶ 8; COSTA RICA, *supra* note 27, ¶ 37; SWEDEN, *supra* note 32, at 3; ITALY *supra* note 24, at 9.

72. Kjelgaard & Melgaard, *supra* note 40, at 450–51.

73. *See, e.g.*, U.S., *supra* note 37, at 137 ("In determining whether a cyber activity constitutes a use of force prohibited by Article 2(4) of the UN Charter and customary international law or an armed attack sufficient to trigger a State's inherent right of self-defense, States should consider the nature and extent of injury or death to persons and the destruction of, or damage to, property. Although this is necessarily a case-by-case, fact-specific inquiry, cyber activities that proximately result in death, injury, or significant destruction, or represent an imminent threat thereof, would likely be viewed as a use of force / armed attack."); Singapore, *supra* note 33, at 84.

74. *See* U.S. DEP'T OF DEF., OFF. OF GEN. COUNS., DEPARTMENT OF DEFENSE LAW OF WAR MANUAL § 1.11.5.2, at 47–48, § 16.3.3.1, at 1030 (June 2015) (updated July 2023) (stating "the United States has long taken the position that the inherent right of self-defense potentially applies against any illegal use of force," including with respect to cyber activities, and noting views of others regarding distinction between use of force and armed attack). *See also* NEW ZEALAND, *supra* note 20, ¶ 8 ("Cyber activity that amounts to a use of force will also constitute an armed attack for the purposes of Article 51 of the UN Charter if it results in effects of a scale and nature equivalent to those caused by a kinetic armed attack.").

75. Japan, *supra* note 20, at 49.

76. Switzerland, *supra* note 21, at 88.

Many others likewise focus on effects such as injuries, deaths, or physical damage to objects as the key factors in assessing whether a cyber activity may qualify as an armed attack.[77] Estonia, like the United States and others, has affirmed its view that, when facing "an armed attack by cyber means, the injured state is not necessarily limited to taking measures by cyber means—all means remain reserved to states in order to respond to an armed attack in a manner that is proportionate and in accordance with other provisions of international law."[78]

A handful of States have suggested the possibility that a cyber activity that does not directly cause physical damage, injury, or death could qualify as a use of force if it caused severe nonphysical damage. Singapore suggests that "malicious cyber activity may amount to an armed attack even if it does not necessarily cause death, injury, physical damage or destruction, taking into account the scale and effects."[79] It provides the example of "a targeted cyber operation causing sustained and long-term outage of Singapore's critical infrastructure" as one situation that may rise to the level of an armed attack.[80] Norway likewise proposes that a cyber activity that causes "severe disruption to the functioning of the State such as the use of crypto viruses or other forms of digital sabotage against governmental or private power grid or telecommunications infrastructure, or cyber operations leading to the destruction of stockpiles of Covid-19 vaccines" could constitute uses of force.[81] Other States consider it possible that severe economic damage could cross the threshold into armed attack. Finland notes that "[a] question has . . . been raised" as to "whether a cyberattack producing significant economic effects such as the collapse of a State's financial system or parts of its economy should be equated to an armed attack."[82] It does not take a position, but observes that "[t]his question merits further consideration."[83] A few States, perhaps wanting to sound a note of caution, have explicitly recalled that, even

77. *See, e.g.*, U.S., *supra* note 37, at 137; Japan, *supra* note 20, at 49; Singapore, *supra* note 33, at 84; Estonia, *supra* note 33, at 30; Germany, *supra* note 20, at 43; Netherlands, *supra* note 21, at 64; Norway, *supra* note 21, at 73–74; Switzerland, *supra* note 21, at 88; U.K., *supra* note 31, at 116; Australia, *supra* note 33, at 5–6; CANADA, *supra* note 26, ¶¶ 46–47; CZECH REPUBLIC, *supra* note 24, ¶ 30; NEW ZEALAND, *supra* note 20, ¶ 8; IRAN, *supra* note 21 (stating armed forces' view that "their right to self-defense shall be reserved if the gravity of the cyber operation against the vital infrastructure of the state is reached in the threshold of the conventionally armed attack").

78. Estonia, *supra* note 33, at 30.

79. Singapore, *supra* note 33, at 84.

80. *Id.*

81. Norway, *supra* note 21, at 70.

82. FINLAND, *supra* note 24, at 6. *See also* Netherlands, *supra* note 21, at 58, 64 (stating that "at this time it cannot be ruled out that a cyber operation with a very serious financial or economic impact may qualify as the use of force," but conceding lack of "international consensus on qualifying a cyberattack as an armed attack if it does not cause fatalities, physical damage or destruction yet nevertheless has very serious non-material consequences").

83. *Id.* at 6. Finland also describes as "[a] widely discussed question" the issue of "to what extent the definition of a cyberattack comparable to an armed attack should take account of the indirect and long-term impacts of the attack," which it says "would require that the impacts can be assessed with sufficient precision." *Id.*

when a malicious cyber activity does not rise to the level of a use of force, it may be a prohibited intervention or a violation of territorial sovereignty.[84]

JUS IN BELLO

The published statements also generally affirm the application of the *jus in bello*, also known as the law of armed conflict or international humanitarian law (IHL), to cyberspace. IHL regulates the conduct of hostilities to minimize their effects on civilians and avoid unnecessary suffering, which it does in part through specific protections for civilians and civilian objects.[85] It also contains four widely recognized principles—the principles of humanity, necessity, proportionality, and distinction—which the GGE reports[86] and many individual position statements have recognized apply to cyber activities in armed conflict.[87]

Some statements offer more specifics than others on how IHL applies in the cyber context. For example, the Czech Republic states that "[p]arties to armed conflict must carefully design and use cyber tools to distinguish between the civilian population and combatants and between civilian objects and military objectives when conducting cyber operations."[88] But in general, more specific articulations of how IHL rules and principles apply in the cyber context would be useful for States to consider making in future statements.

Notably, many of the public statements seek to refute the argument still being made today by a small number of States, including the People's Republic of China, that even acknowledging the application of IHL to cyberspace somehow promotes the so-called militarization of cyberspace or condones armed conflict.[89] For instance, a working paper on how IHL applies in cyberspace, submitted to the OEWG by a group of States in March 2024, confirms that IHL applies to cyber activities in armed conflict and then goes on to say that "IHL addresses the realities of armed conflicts without considering the reasons for or the legality of the recourse to the use of force," adding that "[a]pplying IHL does not encourage or legitimise in any way the possible recourse to the use of force between States, in any situation or context, including in

84. *See, e.g.*, Netherlands, *supra* note 21, at 58 (noting that a cyber activity that does not rise to level of use of force may qualify as prohibited intervention or violation of sovereignty); POLAND *supra* note 21, at 5.

85. U.S., *supra* note 37, at 5.

86. *See* 2015 GGE Report, *supra* note 5, ¶ 28(d); Rep. of the Grp. of Governmental Experts on Advancing Responsible State Behav. in Cyberspace in the Context of Int'l Sec. ¶ 71(f), U.N. DOC. A/76/135 (July 14, 2021) [hereinafter 2021 GGE Report].

87. *See, e.g.*, U.S., *supra* note 37, at 137–39; Australia, *supra* note 33, at 6; Brazil, *supra* note 41, at 22; Estonia, *supra* note 33, at 24, 27; Japan, *supra* note 20, at 49–50; Norway, *supra* note 21, at 74; Singapore, *supra* note 33, at 85; U.K., *supra* note 31, at 119; IRELAND, *supra* note 46, ¶ 29; NEW ZEALAND, *supra* note 20, at ¶ 25; POLAND, *supra* note 21, at CZECH REPUBLIC, *supra* note 24, at 11; PERMANENT MISSION OF PAK. TO THE U.N., PAKISTAN'S POSITION ON THE APPLICATION OF INTERNATIONAL LAW IN CYBERSPACE ¶¶ 11–12 (Mar. 3, 2023), https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/UNODA.pdf [https://perma.cc/DS7D-ARLP].

88. CZECH REPUBLIC, *supra* note 24, ¶ 41.

89. *See, e.g.*, Brazil, *supra* note 41, at 22; Estonia, *supra* note 33, at 27; U.K., *supra* note 31, at 119; CZECH REPUBLIC, *supra* note 24, ¶ 47; COSTA RICA, *supra* note 27, ¶ 39; IRELAND, *supra* note 46, ¶ 32; CANADA, *supra* note 26, ¶ 51.

cyberspace."[90] The statement emphasizes the humanitarian goals of IHL before turning to the substantive discussion.

The fact that so many States feel the need to address the political argument against discussing how IHL applies in cyberspace demonstrates the difficulty sometimes of separating international law from foreign policy considerations. Yet a better shared understanding of how IHL applies to the use of cyber capabilities in armed conflict is all the more important given that such capabilities are being used in armed conflict right now, including in Ukraine, a point some States have repeatedly made in meetings of the OEWG since February 2022, when Russia launched its further invasion of Ukraine.[91]

OEWG discussions on IHL have also benefited from the participation of stakeholders such as the International Committee of the Red Cross (ICRC). The ICRC has been doing considerable work recently to try to advance discussion of how IHL applies in cyberspace. In the past several years, it has published a number of papers and made multiple public statements reflecting its views on how IHL applies in armed conflict.[92] Just a few months ago, concerned by the phenomenon of civilian hackers claiming to carry out cyber activities in support of parties to the Russia-Ukraine war, it published eight rules for civilian hackers to follow during times of armed conflict, along with four obligations on States to constrain their behavior, meant to reflect existing rules of IHL.[93]

The ICRC's views, of course, do not necessarily reflect those of every State in whole or in part. We look forward to continuing to discuss IHL with other States and with experts, such as those at the ICRC and in the OEWG.

---

90. Brazil, Canada, Chile, Colombia, the Czech Republic, Estonia, Germany, the Netherlands, Mexico, the Republic of Korea, Senegal, Sweden & Switzerland, Application of International Humanitarian Law to the Use of Information and Communication Technologies in Situations of Armed Conflicts 1 (Mar. 1, 2024) (working paper), https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/OEWG_Working_Paper_IHL_ICT_Operations.pdf [https://perma.cc/9DV6-X524].

91. In fact, Russia's further invasion on February 24, 2022, was accompanied by cyberattacks on commercial satellite networks serving Ukraine in an effort to disrupt Ukrainian command and control during the invasion. The United States and sixteen other States publicly attributed this cyberattack to Russia. *See, e.g.*, Press Release, Antony J. Blinken, Sec'y, U.S. Dep't of State, Attribution of Russia's Malicious Cyber Activity Against Ukraine (May 10, 2022), https://www.state.gov/attribution-of-russias-malicious-cyber-activity-against-ukraine/ [https://perma.cc/YG5U-FURH]; *Russia Behind Cyber Attack with Europe-Wide Impact an Hour Before Ukraine Invasion*, NAT'L CYBER SEC. CTR. (May 10, 2022), https://www.ncsc.gov.uk/news/russia-behind-cyber-attack-with-europe-wide-impact-hour-before-ukraine-invasion [https://perma.cc/5FTH-UNW5]; *Case Study: Viasat*, CYBERPEACE INST. (June 2022), https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat [https://perma.cc/LD82-TRKR].

92. *See Cyber and Information Operations*, INT'L COMM. OF THE RED CROSS, https://www.icrc.org/en/war-and-law/conduct-hostilities/cyber-warfare [https://perma.cc/H42Y-J673] (last visited Sept. 28, 2024).

93. Tilman Rodenhäuser & Mauro Vignati, *8 Rules for "Civilian Hackers" During War, and 4 Obligations for States To Restrain Them*, INT'L COMM. OF THE RED CROSS (Oct. 4, 2023), https://blogs.icrc.org/law-and-policy/2023/10/04/8-rules-civilian-hackers-war-4-obligations-states-restrain-them/ [https://perma.cc/XA9B-SL7V]. Both Russian and Ukrainian hacktivists apparently took note. *See* Joe Tidy, *Ukraine Cyber-Conflict: Hacking Gangs Vow To De-escalate*, BBC (Oct. 6, 2023), https://www.bbc.com/news/technology-67029296 [https://perma.cc/7M2X-SRSE].

A few questions States and other experts might want to consider when it comes to whether cyber activities give rise to the right to use force (i.e., when the *jus ad bellum*, or international law rules on when it is lawful for a State to resort to the use of force, is engaged by a cyber activity) and the *jus in bello* include:

- What degree of causal connection must occur between a cyber activity and physical damage, deaths, or injuries in order for a State to determine that the cyber activity was a use of force or armed attack?
- Can non-cyber conduct that does not result in physical damage, injury, or death constitute a use of force or armed attack giving rise to the right to use force in self-defense? If so, are there examples of this in previous State practice and *opinio juris*?
- How can States distinguish among the rules of territorial sovereignty, prohibited intervention, and use of force or armed attack when assessing the effects of cyber operations?

STATE RESPONSIBILITY, ATTRIBUTION, AND REMEDIES

National statements demonstrate a firm consensus on the application of the customary international law rules of State responsibility, including rules on attribution and available remedies, to cyber activities.[94] They also affirm that injured States may avail themselves of traditional customary international law remedies including countermeasures.[95] And here I should note that, even if an unfriendly act in cyberspace is lawful, a State can always respond with its own unfriendly but lawful act, which is what is known as a "retorsion." A retorsion could take the form of a cyber activity, but it would not have to do so, even if the original conduct was a cyber activity. Examples of such responses might include the imposition of sanctions or a declaration that a diplomat is persona non grata.[96] Most States that have made statements confirm the availability of retorsions as a possible response to malicious cyber activities carried out by other States.[97]

As with IHL, however, the application of the law of State responsibility in cyberspace is challenged by some States. They argue that determining who is behind a cyber activity is too difficult as a technical matter, and that publicly attributing malicious cyber activities is therefore unacceptable unless and until there is a new treaty to regulate this issue.[98] You may not be surprised to hear that some of the States

94. As the United States explained in its 2021 GGE statement, "[c]yber activities may . . . constitute internationally wrongful acts under the law of State responsibility if they are inconsistent with an international obligation of the State and are attributable to it." U.S., *supra* note 37, at 141.

95. *See, e.g.*, Australia, *supra* note 33, at 7–8; Singapore, *supra* note 33, at 84. Brazil largely agrees with other States but expresses some doubt about the customary international law status of countermeasures generally. *See* Brazil, *supra* note 41, at 21.

96. *See* U.S., *supra* note 37, at 142; Egan, *supra* note 7, at 117.

97. *See generally* Compendium, *supra* note 16.

98. *See, e.g.*, PERMANENT MISSION OF THE RUSSIAN FED'N TO THE U.N., STATEMENT BY THE REPRESENTATIVE OF THE RUSSIAN FEDERATION AT THE FOURTH SESSION OF THE UN OPEN-ENDED WORKING GROUP ON SECURITY OF AND IN THE USE OF ICTS 2021-2025, at 2 (Mar. 7, 2023), https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/ENG_Russian_statement_How_international_law_applies.pdf [https://perma.cc/4V6D-N77Y].

making this argument—such as Russia and Iran—are among those that have been publicly named as being behind multiple malicious cyber activities.[99]

Given this context, many of the public statements on State responsibility and cyberspace underscore that the word "attribution" may cover different types of acts that are not all coextensive with a claim of State responsibility under international law. These statements distinguish among attribution as a technical matter ("who did it?"); attribution for purposes of assessing an internationally wrongful act; and public attribution as a political act ("naming and shaming"), which may or may not include making a claim of legal responsibility and demand for reparations.[100]

One question that arises from the current state of play on these issues is what States can do to demystify cyberspace and provide greater transparency on attribution and State responsibility in this context, so that States can have confidence in their ability to use international law to protect their interests as a practical matter. This takes us back to the bigger picture of the interplay between international law and foreign policy.

INTERNATIONAL LAW AND THE FRAMEWORK OF RESPONSIBLE BEHAVIOR

Eight years ago, Brian Egan called for States to publicize their views on how international law applies in cyberspace in order to provide greater stability and predictability in cyberspace.[101] But this is not all States can do, or are doing, to promote international peace and stability in cyberspace. Earlier I mentioned the nonbinding framework for responsible State behavior in cyberspace, reflected in the 2015 GGE report.[102] The framework includes not just respect for international law, but eleven nonbinding norms of responsible behavior, as well as confidence-building measures and capacity building.

---

99. The Cybersecurity and Infrastructure Security Agency (CISA) at the Department of Homeland Security periodically issues cybersecurity advisories warning of specific cyber vulnerabilities and threats and provides information on how to mitigate and defend against these threats. *See Cyber Threats and Advisories*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/topics/cyber-threats-and-advisories [https://perma.cc/Q2SN-LRRH] (last visited Sept. 28, 2024). Its website lists nearly thirty cybersecurity advisories involving malicious cyber activities affiliated with the Russian State between 2016 and 2023, and twelve for Iran since 2020. *See Russia Cyber Threat Overview and Advisories*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/russia [https://perma.cc/ZRD5-U5WN] (last visited Sept. 28, 2024); *Iran Cyber Threat Overview and Advisories*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/iran [https://perma.cc/BY2V-JBM3] (last visited Sept. 28, 2024). There have also been numerous advisories concerning People's Republic of China threat actors. *See China State-Sponsored Cyber Threat: Advisories*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors/china/publications [https://perma.cc/43MY-S6BW] (last visited Sept. 28, 2024). Such advisories generally include detailed information on specific cyber threats, including tactics, techniques and procedures used by the threat actor, as well as ways to mitigate compromise. *See, e.g.*, *id.*

100. *See, e.g.*, Germany, *supra* note 20, at 40–41; IRELAND, *supra* note 46, ¶ 24; ITALY, *supra* note 24, at 5; Japan, *supra* note 20, at 47.

101. *See* Egan, *supra* note 7.

102. 2015 GGE Report, *supra* note 5, ¶ 13.

All of these elements are important, but I would like to touch briefly on the norms.

The eleven non-binding norms are voluntary expectations for responsible State behavior that are intended to supplement existing international law but do not themselves have the force of law.[103] Some of them may, in certain circumstances, overlap with standards of behavior that are required as a matter of international law.

Each of these norms represents an important consensus reached among UN Member States as to what constitutes responsible cyber behavior. We do not have time to discuss them all, but I would just flag a couple of them that may be of interest (recognizing that all this talk of "Norms" may make you feel as though you are in an episode of *Cheers*).

"Norm (c)"—named for the subparagraph of the GGE report in which it appears—states that "States should not knowingly allow their territory to be used for internationally wrongful acts using [cyber technology]."[104] This norm addresses situations where third parties may be conducting malicious cyber activities from the territory of one State that have harmful effects in another State. It reflects the expectation that States will not turn a "blind eye" to that kind of activity, and that when they become aware of it, they will take action to address it, including investigation and prosecution, as appropriate.[105]

"Norm (d)" contains the complementary expectation that "States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats."[106] An example is the International Counter Ransomware Initiative (CRI), established by the United States in 2021, and which now includes the International Counter Ransomware Task Force, bringing together policy, law enforcement, and operational agencies from around the world to combat ransomware.[107] The 2021 GGE report also includes suggestions for steps States can take to implement this norm.[108] This adds to preexisting efforts to promote cooperation on cybercrime, including the 2001 Council of Europe Cybercrime Convention, otherwise known as the Budapest

---

103. *See* Egan, *supra* note 7, at 179 (identifying four norms promoted by the United States, as well as eleven GGE norms).

104. 2015 GGE report, *supra* note 5, ¶ 13(c).

105. *See also* 2021 GGE report, *supra* note 86, ¶¶ 29–30. The proliferation of ransomware attacks on critical infrastructure provides a timely example of how this norm is relevant to real life circumstances. When ransomware actors in one State target critical infrastructure in another, it is incumbent on the first State to take action to investigate and mitigate that activity in line with the framework's norms. Yet some States, including Russia, continue to allow ransomware actors to operate from their territory with impunity. The United States condemns this irresponsible behavior and encourages all States to implement relevant norms in the interest of stability in cyberspace.

106. 2015 GGE report, *supra* note 5, ¶ 13(d).

107. *See International Counter Ransomware Initiative*, INT'L COUNTER RANSOMWARE INITIATIVE, https://counter-ransomware.org/ [https://perma.cc/67JH-CZYG] (last visited Sept. 28, 2024). Now with nearly sixty members, the CRI has grown rapidly in the past three years. Its growth underscores the global nature of the ransomware threat and the interest of the international community in coming together to mitigate it. Through cooperative efforts like the CRI, the United States and its partners are working to implement "Norm (d)."

108. 2021 GGE report, *supra* note 86, ¶¶ 32–35.

Convention, which has over seventy States party. The Budapest Convention and its recently concluded Second Additional Protocol are directed at ensuring States have harmonized measures addressing cybercrime at the national level and can provide cooperation to other States in investigating and prosecuting cybercrime.[109] Additionally, negotiations towards a new UN Convention Against Cybercrime are set to conclude later this year. If successful, this instrument could also establish required domestic law enforcement measures and mechanisms for international cooperation to combat cybercrime.[110]

Patterns of behavior we have seen in recent years also highlight the importance of "Norm (f)," which says that "[a] State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public."[111] Precisely what qualifies as critical infrastructure is for each State to decide; for instance, the U.S. Cybersecurity and Infrastructure Agency at the Department of Homeland Security maintains a list of what it considers critical infrastructure, such as transportation, communications, and water systems.[112] As the 2021 GGE report recommends, States should take appropriate measures to protect their critical infrastructure and to adopt relevant policy and legislative measures to promote implementation of this norm.[113] In late 2023, the United States issued a cybersecurity advisory (CSA) highlighting malicious cyber activity of Iranian Islamic Revolutionary Guard Corps (IRGC)-affiliated advanced persistent threat cyber actors targeting programmable logic controllers commonly used in the water and wastewater sector.[114] This CSA is an example of the United States' attempt to implement "Norm (g)" by protecting critical infrastructure, including by publishing information on how to mitigate threats posed by the cyber capabilities exploited by these actors.

Implementation of these and the other norms that are part of the nonbinding framework can go a long way toward supporting peace and stability in cyberspace, as well as the effectiveness and practical application of the existing international law rules that bind all States. The United States is committed to fostering the implementation of these norms, including through capacity-building. We support workshops and other training on the framework overall, as well as on international law specifically. We also support the creation of a new Programme of Action (POA) at the United Nations as a

109. Convention on Cybercrime, Nov. 23, 2001, E.T.S. 185.

110. *See generally Ad Hoc Committee To Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes*, U.N. OFF. ON DRUGS AND CRIME, https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home [https://perma.cc/5GDW-UGU7] (last visited Sept. 28, 2024).

111. 2015 GGE report, *supra* note 5, ¶ 13(f).

112. *Critical Infrastructure Sectors*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors [https://perma.cc/CWZ9-PFWU] (last visited Sept. 28, 2024).

113. 2021 GGE report, *supra* note 86, ¶ 46.

114. *See Joint Cybersecurity Advisory: IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems Facilities*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY ET AL. 1 (Dec. 1, 2023), https://www.cisa.gov/sites/default/files/2023-12/aa23-335a-irgc-affiliated-cyber-actors-exploit-plcs-in-multiple-sectors-1.pdf [https://perma.cc/UA5B-VY9D].

flexible and permanent venue where UN Member States can engage in practical discussions on the framework for responsible State behavior, including implementation of the norms and the need for States to respect international law in conducting cyber activities.[115]

CONCLUSION

Discussions of international law are part of the overall effort to promote responsible State behavior in cyberspace. Over the past twenty-five years, States have made tremendous progress in developing common understandings of how international law applies to what they do in cyberspace. Continuing these discussions and working to implement the framework of responsible State behavior in cyberspace will serve to further the shared goal of the United States and other UN Member States to promote international peace and security everywhere.

115. *See* Heidar Ali Balouji (Rapporteur), *Developments in the Field of Information and Telecommunications* in the Context of International Security, U.N. DOC. A/78/404 (Nov. 10, 2023). One-hundred-sixty-one States supported the POA in the UN General Assembly last fall. This broad-based affirmation demonstrates the international community's continued support for the framework as a guidepost for State behavior in cyberspace that promotes peace and stability and indicates the international community's desire to see the framework implemented.