94th REGULAR SESSION
February 18-22, 2019
Rio de Janeiro, Brazil

OEA/Ser.Q
CJI/doc. 578/19
21 January 2019
Original: English

INTERNATIONAL LAW AND STATE CYBER OPERATIONS: IMPROVING TRANSPARENCY

(Presented by Prof. Duncan B. Hollis)

1. The topic of international law and state cyber operations was raised for the first time during the Committee's 93rd Regular Session. The author was invited to present an initial report on the questions of international law's application to cyberspace and ideas for how the Committee might engage with the subject-matter.

2. My initial report surveyed the poor state of global cybersecurity and the financial, humanitarian, and national security costs of cyber-threats, with particular attention to those targeting critical infrastructure and electoral processes. It explored the increasing efforts by nation States to develop capacities to engage in defensive *and* offensive cyber operations directly. Other States appear to have deployed non-State actor "proxies" to engage in cyber operations under varying levels of State control or support.

3. With all this cyber activity, my initial report noted how little visibility international law has had in regulating State cyber-operations. Although governmental experts agreed in 2013 (and again in 2015) that "[i]nternational law, and in particular the Charter of the United Nations, is applicable" to cyberspace, efforts to agree on *how* it does so have faltered.[1] A 2017 GGE failed, reportedly because governmental experts from a few key States differed on whether certain fundamental rules of international law (e.g., self-defense, international humanitarian law, counter-measures, due diligence) applied to State cyber-operations.[2]

4. The International Committee of the Red Cross has offered its views on how international law applies to cyberspace in the specific area within its mandate – i.e., international humanitarian law (IHL).[3] And the two *Tallinn Manuals* offered the views of

---

[1] *See* U.N. Secretary-General, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, ¶ 19, U.N. Doc. A/68/98 (June 24, 2013); U.N. Secretary-General, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, ¶ 10, U.N. Doc. A/70/174 (July 22, 2015).

[2] *See, e.g.,* Arun M. Sukumar, *The UN GGE Failed. Is International Law in Cyberspace Doomed As Well?* LAWFARE, July 4, 2017.

[3] See ICRC, COMMENTARY (2016) ON THE FIRST GENEVA CONVENTION OF 1949, 91 ¶¶ 253–256, and 158-159 ¶¶ 436-437; and ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, report, 39-44 (Oct. 2015).

an independent (albeit NATO-funded) group of experts on how international law applies to cyber operations more generally.[4] Both Manuals are important reference works and governments were consulted in their drafting. But recent research suggests that States have left these Manuals "on the shelf" in their actual practice.[5] Indeed, there is little evidence that States are invoking international law in response to specific cyber incidents and only a few States have offered public statements on the application of international law generally.[6]

5. Reflecting on these experiences, my report suggested three sets of problems with respect to international law's regulation of State behavior in cyberspace. First, there are existential questions about whether certain international law rules or doctrines have any purchase in the cyber-context. Although they have not done so publicly, in the GGE context, experts for a few States reportedly resisted the application of international humanitarian law, self-defense, and due diligence doctrines to cyberspace.[7] Second, even where States accept the relevance of a particular international law concept—e.g., sovereignty, the duty of non-intervention—they diverge as to its proper "interpretation" in the cyber context.[8] Third, there is the aforementioned "application" problem, where States have done relatively little to employ international law with respect to actual cyber

---

[4] *See* Michael Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Tallinn, Estonia: NATO CCD COE, 2017); Michael Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Tallinn, Estonia: NATO CCD COE, 2013).

[5] Dan Efrony and Yuval Shany, *A Rule Book on The Shelf? Tallinn Manual 2.0 on Cyber Operations and Subsequent State Practice*, 112 AM. J. INT'L L. 583 (2018).

[6] *See, e.g.,* Jeremy Wright, QC, MP, *Cyber and International Law in the 21st Century*, May 23, 2018 (United Kingdom); Revue stratégie de cyberdéfense 82-84 (Feb. 2018) (France); Brian Egan, *Remarks on International Law and Stability in Cyberspace*, Berkeley Law School, Nov. 10, 2016 (United States); Harold Koh, *International Law in Cyberspace,* 54 HARV. INT'L LAW. J. 1, 7 (2012) (United States). There is one, recent notable exception to this pattern. In October 2018, the United Kingdom accused the GRU—Russia's military intelligence arm—of responsibility for a series of cyber-operations, including targeting the Organization for the Prohibition of Chemical Weapons (which was investigating the use of a nerve agent against a former Russian spy and his daughter in Salisbury, U.K.). The U.K. Foreign Secretary attributed the Russian behavior as reflecting a "desire to operate without regard to international law or established norms" while a related press release described the GRU's operations as a "flagrant violation of international law." Press Release, Foreign Commonwealth Office, *UK exposes Russian cyber attacks*, 4 Oct. 2018; NCSC, *Reckless campaign of cyber attacks by Russian military intelligence service exposed*, Oct. 4, 2018.

[7] *See, e.g.,* Sukumar, *supra* note 2.

[8] For example, with respect to sovereignty, *Tallinn Manual 2.0* envisions sovereignty as a rule that States may violate directly by their cyber-operations. See *Tallinn Manual 2.0*, *supra* note 4, Rule 4 ("A State must not conduct cyber operations that violate the sovereignty of another State."). The Dutch government appears to support that approach. Bert Koenders, Foreign Minister, Neth., Remarks at The Hague Regarding Tallinn Manual 2.0 (Feb. 13, 2017). In contrast, the UK Attorney General has questioned that view (as has the chief lawyer for the U.S. Cyber Command, albeit while writing in his personal capacity). *See* Wright, *supra* note 6 ("Some have sought to argue for the existence of a cyber specific rule of a 'violation of territorial sovereignty' … Sovereignty is of course fundamental to the international rules-based system. But I am not persuaded that we can currently extrapolate from that general principle a specific rule or additional prohibition for cyber activity beyond that of a prohibited intervention. The UK Government's position is therefore that there is no such rule as a matter of current international law."); Gary Corn, *Tallinn Manual 2.0—Advancing the Conversation*, Just Security (Feb. 15, 2017).

incidents.[9] As a result, there is little international legal accountability for State behavior in cyberspace today.

6. The Committee received the first report favorably. It agreed the topic was an important one that fit within the Committee's mandate, adding it to its regular agenda and appointing the present author Rapporteur. That said, the Committee's focus on cyber operations remains relatively narrow – rather than formulating the Committee's views on how international law applies to cyberspace, the Committee believes a more fruitful first step would involve increasing the transparency of how OAS Member States view this issue. In short, the Committee supports the idea that Member States need to formulate *and* publicize their views on these questions.

7. Doing so would have clear benefits. As a legal matter, understanding how States view international law and cyberspace will permit a mapping of State practice – identifying areas where states have a general and uniform view of what international law requires. With sufficient support, these views may help elaborate how customary international law regulates State cyber operations. But even if States turn out to have differing—or even conflicting—views, it is just as important to publicize such differences. Otherwise, there is a risk that States with differing baseline understandings of what international says might inadvertently escalate a conflict (i.e., where State A assumes its operation would not cross the armed attack threshold but the victim State B understands it to have done exactly that). Knowing where States disagree would highlight areas in need of further dialogue, whether to close these gaps, articulate clarifications, or to seek modifications to ensure that international law can be more effective in regulating actual State behavior in cyberspace.

8. The Committee's efforts on international law and cyberspace will thus focus on *transparency* – on soliciting, collecting and publicizing the views of OAS Member States on how international law applies in the cyber context. The Committee authorized the author to prepare a questionnaire for Member States to obtain their views on some of the most prominent international legal questions associated with cyberspace to date.

9. On August 15, 2018, the author presented the Committee's transparency project during its meeting with OAS Member State Foreign Ministry Legal Advisers. The project was received quite positively by all attending. Suggestions were made to shorten the list of questions posed (the original report had annexed twenty potential questions). In addition, one Legal Adviser's representative suggested that the Committee endeavor first and foremost to collect any prior public statements made by OAS Member States relevant to the application of international law generally.

10. Since the Committee's August meetings, new efforts in multilateral and multistakeholder fora have continued to emphasize the application of international law to cyber-space, including having human rights that exist off-line apply on-line as well.[10] At

[9] *See supra* note 6 and accompanying text.

[10] See *Paris Call for Trust and Security in Cyberspace*, Nov. 12, 2018 ("We also reaffirm that international law, including the United Nations Charter in its entirety, international humanitarian law and customary international law is applicable to the use of information and communication technologies (ICT) by States. We reaffirm that the same rights that people have offline must also be protected online, and also reaffirm the

least two regional organizations—ASEAN and the European Union—have affirmed the view that international law applies to cyberspace and signaled support for further elaboration on how it does so.[11] The European Union, moreover, endorsed the idea that *all* UN Member States "should submit national contributions on the subject of how international law applies to the use of [information and communication technologies] by States" in order to advance "the global understanding on national approaches which is fundamental to maintaining long-term peace and security and reducing the risk of conflict in cyberspace."[12] Thus, the Committee's approach is consistent with the views of other regional organizations.

11. In the meantime, the United Nations General Assembly has endorsed the conclusion of earlier GGEs that international law applies to cyberspace.[13] It also agreed to commence two new processes related to global cybersecurity – (i) a new Open Ended Working Group to discuss cyber-security in a relatively open and standing forum; and (ii) a new GGE that will be formed and begin meeting later in the Spring or early Summer of 2019.[14] With respect to the new GGE, the UN General Assembly requested

> [T]he 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, and to submit a report on the results of the study, including an annex containing national contributions of participating governmental experts on the subject of how international law applies … to the General Assembly at its seventy-sixth session.[15]

12. Taken together, it appears that there is growing momentum to have States express their views on international law's application to cyberspace. Such support—including in the United Nations—reinforces the importance and timeliness of the Committee's work on this subject matter. The GGE will be comprised of experts from 20

---

applicability of international human rights law in cyberspace."); Please note that, in addition to my membership on the Committee, I serve as an external consultant to Microsoft on issues of international law and cyberspace, including its work with the French Government to launch the Paris Call.

[11] *See* ASEAN-United States Leaders' Statement on Cybersecurity Cooperation (18 November 2018) ("Reaffirm that international law, and in particular the Charter of the United Nations (UN), is applicable and essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT environment and recognise the need for further study of how international law applies to the use of ICTs by States); EU Statement – United Nations 1st Committee, Thematic Discussion on Other Disarmament Measures and International Security (October 26, 2018) ("the EU recalls that 'International law and in particular the UN Charter, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment.'").

[12] EU Statement, *supra* note 11.

[13] UNGA Res. 266, U.N. Doc. A/RES/73/266 (2 Jan. 2019) ("Confirming the conclusions of the Group of Governmental Experts, in its 2013 and 2015 reports, that international law, and in particular the Charter of the United Nations, is applicable and essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful information and communications technology environment").

[14] See U.N. Doc. A/RES/73/27 (re the OEWG, which will be open to all UN Member States with plans to include consultations with industry); U.N. Doc. A/RES/73/266 (2 Jan. 2019) (re the GGE).

[15] U.N. Doc. A/Res/73/266, at ¶3.

to at most 25 States. Less than a handful of these will be OAS Member States. The Committee thus has an opportunity to survey and gather a larger—and more diverse—set of views from among *all* OAS Member States than the GGE process will allow. Moreover, as other regional organizations encourage their Member States to elaborate views on the application of international law, it is important that the OAS Member States have an opportunity to advance their views, lest other regions have an outsized voice in delineating the boundaries and contents of international law in the cyber-context. As such, it is critical that the Committee gather and share OAS Member State views not only within the region but with other regional international organizations and within the U.N. system.

13. It is important to note, moreover, that GGE's own important efforts will be constrained by its mandate to certain, limited topics. As a product of the First Committee, the GGE will focus only on questions of international law vis-à-vis issues of disarmament and security. The Committee's mandate, in contrast, is broader, and State responses to its questionnaire can touch on a broader range of subjects, including all matters of public and private international law implicated by State cyber operations. Thus, the Committee can improve transparency across the entire range of international law subjects.

14. Since producing my first report, I produced a summary call for OAS Member States on this topic along with a revised—and shorter—list of questions. The Committee questionnaire ended up comprising 10 questions:

- The first question responds to the suggestion of one of the Foreign Ministry Legal Advisers that the Committee solicit and compile existing statements on international law and cyberspace.
- The second question is geared towards existential questions – asking States to confirm or deny whether certain extant rules of international law do (or do not) apply in the cyber context.
- The third question focuses on the use of force (the *jus ad bellum*) with particular attention to what criteria a State uses to identify a cyber operation as a use of force or an armed attack.The fourth and fifth questions ask about how States understand the assignment of international legal responsibility for non-State actor behavior.
- The sixth and seventh questions address international humanitarian law and two of the critical outstanding issues, namely the definition of an "attack" in the cyber-context and the question of whether cyber operations that only target data would constitute such an attack (note: these questions were revised substantially from the original proposal in light of suggestions and comments provided by the International Committee of the Red Cross).
- The eighth question seeks States views on whether sovereignty comprises its own distinct rule for State behavior in cyber space or is, instead, a background principle that informs the content of other rules.
- The ninth question makes a similar inquiry with respect to due diligence.
- Finally, the tenth question invites States to identify additional areas of international law on which the Committee should focus improving

transparency in the cyber context.

15. The revised Questionnaire was finalized with able assistance from the Committee Secretariat. A report on relevant responses to the Committee Questionnaire will be prepared in advance of the Committee's next Regular Session. Once a sufficient body of responses has been received, the Committee will need to discuss whether to follow up with further questions or to simply approve their circulation to the General Assembly with a recommendation that it approve their distribution within the region and beyond.

INTER-AMERICAN JURIDICAL COMMITTEE
QUESTIONNAIRE FOR MEMBER STATES
INTERNATIONAL LAW & STATE CYBER OPERATIONS: IMPROVING TRANSPARENCY

Cyberspace has become an integral component of civilian life in all its social, economic, cultural and political aspects. At the same time, "cyberthreats" to information and communication technologies (ICTs) have become ubiquitous. Cyber operations have generated significant financial losses, violated human rights, and threatened national security. States have responded by regulating cybercrime and building capacity, whether directly or through proxies, to engage in defensive *and* offensive cyber operations. The increase in capacities—and activities—of States in cyberspace has led to wide-spread calls to clarify what rules regulate State behavior. In 2013 and 2015, a Group of Governmental Experts (GGE) convened by the U.N. General Assembly's First Committee confirmed that "International law, and in particular the Charter of the United Nations, is applicable" to cyberspace.[1] Earlier this year, the United Nations General Assembly endorsed this conclusion.[2]

Unfortunately, however, States have not been able to agree on *how* international law applies. Only a few States have offered public views on the matter.[3] And although independent experts (most notably via two *Tallinn Manuals*[4]) have tried to fill in this

[1] U.N. Secretary-General, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, ¶ 19, U.N. Doc. A/68/98 (June 24, 2013); U.N. Secretary-General, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, ¶ 10, U.N. Doc. A/70/174 (July 22, 2015).

[2] UNGA Res. 266, U.N. Doc. A/RES/73/266 (2 Jan. 2019) ("Confirming the conclusions of the Group of Governmental Experts, in its 2013 and 2015 reports, that international law, and in particular the Charter of the United Nations, is applicable and essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful information and communications technology environment").

[3] *See, e.g.,* Jeremy Wright, QC, MP, *Cyber and International Law in the 21st Century*, May 23, 2018 (United Kingdom); Revue stratégie de cyberdéfense 82-84 (Feb. 2018) (France); Brian Egan, *Remarks on International Law and Stability in Cyberspace*, Berkeley Law School, November 10, 2016 (United States); Harold Koh, *International Law in Cyberspace,* 54 HARV. INT'L LAW. J. 1, 7 (2012) (United States). The International Committee of the Red Cross has also expressed views on the application of international humanitarian law to cyberspace. See ICRC, COMMENTARY (2016) ON THE FIRST GENEVA CONVENTION OF 1949, 91 ¶¶ 253–256, and 158-159 ¶¶ 436-437; and ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, report, 39-44 (Oct. 2015).

[4] MICHAEL SCHMITT (ED.), TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (NATO CCD COE, 2017); MICHAEL SCHMITT (ED.), TALLINN MANUAL ON THE INTERNATIONAL

information gap, States have not done so. To date, States have refrained from invoking international law both in general and in response to specific cyber incidents.

A new UN GGE will be convened later in 2019. Its mandate will encourage experts to elaborate on how their States understand the application of international law to cyberspace.[5] The new GGE will, however, have a small membership with only a limited set of voices from the Americas. The Inter-American Juridical Committee (IAJC) supports the UN GGE's past and future work. Nonetheless, it believes that there is room for complimentary efforts to increase transparency on how States understand international law's application to cyberspace. Moreover, this is a view shared by other regional organizations, including ASEAN and the European Union.[6]

The attached questionnaire represents the first step in the IAJC's effort to solicit, compile, and publicize Member State views on international law's application to cyber operations. It reflects some of the most important or discussed issues that have arisen to date. The Committee does not anticipate offering its own views on these questions. Rather, the goal is to provide a forum in which State views may be collected and publicized for purposes of advancing mutual understanding in the Region. To the extent Member State responses conform to existing statements on international law offered at the UN GGE or elsewhere, these responses would make an important contribution to elaborating the current international legal rules. It is, however, just as important to identify areas where State views diverge. Doing so will allow States to appreciate how other States may perceive offensive or defensive cyber-operations, setting expectations for their future interactions and providing a baseline for further dialogue.

Thus, the Committee would welcome all Member States to respond to the following questions. Ideally, Member States would respond to all ten questions posed. Member States may, however, opt to provide a more limited set of responses if there are particular questions where its Government has not yet formulated a view (or it has a view that it is not yet prepared to make public). As the final question indicates, the Committee would also welcome Member State views on additional questions or topics where more transparency would benefit the application of international law to cyberspace.

QUESTIONS:

LAW APPLICABLE TO CYBER WARFARE (NATO CCD COE, 2013). Although funded by NATO's Cyber Defense Centre of Excellence, *Tallinn* represents the work of an independent group of experts.

[5] See UNGA Res. 266, U.N. Doc. A/Res/73/266, ¶3 (2 January 2019).

[6] *See* ASEAN-United States Leaders' Statement on Cybersecurity Cooperation (18 November 2018) ("Reaffirm that international law, and in particular the Charter of the United Nations (UN), is applicable and essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT environment and recognise the need for further study of how international law applies to the use of ICTs by States); EU Statement – United Nations 1st Committee, Thematic Discussion on Other Disarmament Measures and International Security (October 26, 2018) ("UN Member States … should submit national contributions on the subject of how international law applies to the use of ICTs by States" to advance "the global understanding on national approaches which is fundamental to maintaining long-term peace and security and reducing the risk of conflict in cyberspace.").

1. Has your Government previously issued an official paper, speech, or similar statement summarizing how it understands international law applies to cyber operations? Please provide copies or links to any such statements.

2. Do existing fields of international law (including the prohibition on the use of force, the right of self-defense, international humanitarian law, and human rights) apply to cyberspace? Are there areas where the novelty of cyberspace excludes the application of a particular set of international legal rights or obligations?

3. Can a cyber operation by itself constitute a use of force? Can it constitute an armed attack that triggers a right of self-defense under Article 51 of the UN Charter? Can a cyber operation qualify as a use of force or armed attack without causing the violent effects that have been used to mark such thresholds in past kinetic conflicts?

4. Outside of armed conflicts, when would a State be responsible for the cyber operations of a non-State actor? What levels of control or involvement must a State have with respect to the non-State actor's operations to trigger the international legal responsibility of that State?

5. Are the standards of State responsibility the same or different in the context of an armed conflict as that term is defined in Articles 2 and 3 common to the 1949 Geneva Conventions?

6. Under international humanitarian law, can a cyber operation qualify as an "attack" for the rules governing the conduct of hostilities if it does not cause death, injury or direct physical harm to the targeted computer system or the infrastructure it supports? Could a cyber operation that produces only a loss of functionality, for example, qualify as an attack? If so, in which cases?

7. Is a cyber operation that only targets data governed by the international humanitarian law obligation to direct attacks only against military objectives and not against civilian objects?

8. Is sovereignty a discrete rule of international law that prohibits States from engaging in specific cyber operations? If so, does that prohibition cover cyber operations that fall below the use of force threshold and which do not otherwise violate the duty of non-intervention?

9. Does due diligence qualify as a rule of international law that States must follow in exercising sovereignty over the information and communication technologies in their territory or under the control of their nationals?

10. Are there other rules of international law that your government believes are important to highlight in assessing the regulation of cyber operations by States or actors for which a State is internationally responsible?