95th REGULAR SESSION
July 31- August 9, 2019
Rio de Janeiro, Brazil

OEA/Ser.Q
CJI/doc. 594/19
July 24, 2019
Original: English

THIRD REPORT
INTERNATIONAL LAW & STATE CYBER OPERATIONS: IMPROVING TRANSPARENCY

(Presented by Dr. Duncan B. Hollis)

1. This is my Third Report on the topic of improving transparency with respect to how Member States understand the application of international law to State cyber operations. My first report examined the increasing number of cyber incidents associated with States and their proxies as well as their economic, humanitarian, and national security implications.[1] It highlighted how little visibility international law has had in regulating State cyber-operations. To be sure, many States have confirmed the applicability of international law to their behavior in cyberspace.[2] Moreover, although the OAS has not, three major international organizations—ASEAN, the European Union, and the United Nations have done so as well.[3] To date, however, efforts to delineate *how* international law applies to cyberspace have born little fruit.

2. My second report highlighted several areas where questions of how international law applies to cyber operations has generated controversy or confusion, including the use of force and self-defense, international humanitarian law, counter-measures, sovereignty, and due diligence.[4] States have been largely reticent about explaining their views on whether and how these (and other) areas of international law apply in cyberspace. Indeed, States appear quite reluctant to invoke the language of international law in making accusations about other State's cyber-operations.[5] A handful of States have

---

[1] *See* Duncan B. Hollis, *International Law and State Cyber Operations: Improving Transparency*, OEA/Ser.Q, CJI/doc. 570/18 (9 August 2018) ("Hollis, First Report").

[2] *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) ("[i]nternational law, and in particular the Charter of the United Nations, is applicable" to cyberspace); 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*, ¶ 24, U.N. Doc. A/70/174 (July 22, 2015) (same).

[3] *See* 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"); 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.").

[4] Duncan B. Hollis, *International Law and State Cyber Operations: Improving Transparency*, OEA/Ser. Q, CJI/doc 578/19 (21 January 2019) ("Hollis, Second Report").

[5] *See, e.g.,* 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). The most notable exception was the United

offered general statements on such topics, including most recently comments by the President of Estonia.[6] But the number and specificity of such statements has not been sufficient to rely on them as evidence of state practice or *opinio juris* in this important area.

3. With the Committee's support, my second report detailed a plan to focus on *transparency* with respect to how States understand international law's application to cyber operations. The Committee supported my asking States for their views on some of the most relevant international legal questions. Doing so has several clear benefits for the region. Mapping OAS Member State views on international law and cyber operations can help identify how much convergence (or divergence) there is on key questions, ranging from self-defense to sovereignty to counter-measures. Knowing where States agree may provide much-needed evidence to delineate States' customary international law responsibilities in cyberspace. At the same time, identifying disagreements may be just as important. Publicizing such differences can mitigate the risk of States operating from different base-line assumptions in ways that could escalate a conflict (if, for example, one side views its cyber-operation as a non-forceful counter-measure, but the State against which the operation is directed perceives it as an armed attack, entitling it to respond with kinetic acts of self-defense). It would also highlight areas in need of further dialogue, whether to reconcile conflicting positions, clarify the law's contents, or, perhaps even, pursue changes to it.

4. Beyond its regional impacts, elaborating the views of multiple OAS States may also help illuminate the state of international law globally. Publicizing such views will coincide with global efforts at the United Nations First Committee, specifically the upcoming U.N. Group of Governmental Experts, to be chaired by a governmental expert from Brazil.[7] Among other things, the new GGE will reportedly invite its government experts to offer national views on international law in the information security context. Four of the GGE's 25 members hail from the region: Brazil, Mexico, the United States, and Uruguay. The Committee's efforts will allow additional States to weigh in with their views without competing or conflicting with the GGE's work. Indeed, the Committee's efforts should supplement and support the GGE's project, providing a fuller range of views from across the region on international legal issues, improving our understanding of international law in cyberspace, and its efficacy in regulating State relations therein. This approach is, moreover, consistent with that proposed in other regional organizations. The European Union, for example, has suggested 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."[8]

5. As detailed in my Second Report, with the help of the OAS Department of International Law and input from the International Committee of the Red Cross, I prepared a questionnaire for Member States. The OAS International Law Department circulated the Questionnaire in January 2019.

Kingdom's willingness to suggest that Russian cyber-operations constituted a "flagrant violation of international law." The United Kingdom did not, however, specify precisely which cyber-operations did so (their accusation listed several attributed to the Russian Federation) nor which international laws were violated. *See* 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.

[6] *See* Kersti Kaljulaid, President of Estonia, Opening Remarks for CyCon 2019, 29 May 2019; *see also* 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).

[7] See U.N. Doc. A/RES/73/266 (2 Jan. 2019) paragraph 3 (on the GGE's mandate). In addition, to the new GGE, there will also be a UN-sponsored Open Ended Working Group (OEWG) that will look to operationalize the work of prior GGEs, and in some cases revisit or even revise the outcomes of that work. *See* U.N. Doc. A/RES/73/27.

[8] EU Statement, *supra* note 3.

It contains 10 questions:

- The first question solicits existing national statements on international law and cyberspace from each Member State.
- The second question asks Member States to confirm whether they have identified certain extant rules of international law that do (or do not) apply in the cyber context.
- The third question focuses on the use of force (the *jus ad bellum*), asking 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, in particular the extent of State "control" required.
- The sixth and seventh questions address international humanitarian law (the *jus in bello*) and two of its critical outstanding issues, namely the definition of an "attack" in the cyber-context and the question of whether cyber operations that only target data constitute such an attack.
- 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. There is currently a division of views among States on this topic.
- 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.

6. To date, the Committee has received six responses to its Questionnaire from Bolivia, Brazil, Costa Rica, Ecuador, Guatemala, and Peru. Brazil's response highlighted its pending work at the UN GGE (which will be chaired by a Brazilian expert). Another response by Costa Rica, highlighted the need for further capacity building on how international law applies to cyber operations as well as the possibility of the Committee undertaking work to develop domestic legal regulations for cyber threats. The other four responses addressed the Committee's questions specifically. I have annexed all six responses to this Report for review by the Committee.

7. In this Third Report, I am not offering any substantive analysis or summation of the responses received to date. Rather, my aim is merely to update the Committee on where things stand. I would also invite Committee members from States that have not yet responded to the Committee Questionnaire to encourage their national governments to do so.

8. I understand that other States are continuing to work on and prepare their responses. As such, I believe it would be better to have a fuller set of responses before undertaking any analysis of how OAS Member States understand international law applies to cyberspace generally, or cyber operations in particular. Moreover, the OAS Secretariat of the Inter-American Committee against Terrorism (CICTE) is holding consultations with the United Nations Office for Disarmament Affairs 15-16 August 2019.[9] Those consultations are likely to address the utility of the Committee's efforts as well as some of the substantive international legal issues on which it seeks greater transparency. As such, they offer an additional rationale for waiting before offering a detailed analysis of Member State views.

[9] This is one of a series of consultations ODA is hosting this summer with various regional organizations across the globe, including the OSCE, ASEAN, and the EU.

9. In my next report, I do plan to summarize how responding Member States understand international law applies to State cyber-operations. I will attempt to do so with an eye to ongoing efforts at the UN (including the GGE, which will begin meeting formally in December, but also a new Open-Ended Working Group (OEWG) that will commence in September 2019), asking how—if at all—they may impact our understanding of Member State responses.

10. As at the outset, I do not anticipate this project will result in either an effort to codify or progressively develop international law (nor even an effort to identify best practices or general guidance). Rather, the goal remains a modest one – to provide OAS Member States a platform to be more transparent on how they understand international law applies to cyberspace and the information and communication technologies from which it derives. I look forward to hearing the Committee's views and advice on how to ensure more transparency on what is widely recognized as one of the highest priorities for nation States today.