96th REGULAR SESSION
2-6 March 2020
Rio de Janeiro, Brazil

OEA/Ser.Q
CJI/doc. 603/20 rev.1
5 March 2020
Original: English
* Limited

IMPROVING TRANSPARENCY
INTERNATIONAL LAW AND STATE CYBER OPERATIONS:
FOURTH REPORT

(Presented by Prof. Duncan B. Hollis)

1. This is my fourth report on the topic of improving transparency with respect to how Member States understand the application of international law to State cyber operations. It reviews responses received to date from the Committee's questionnaire to Member States on international law and State cyber-operations. In doing so, it aims to contribute to a broader trend in international relations seeking more transparency on how nation States understand international law's application to cyberspace.

2. My first report highlighted how little visibility international law has had in regulating State cyber-operations, despite their increasing number and economic, humanitarian, and national security implications.[1] Many States *have* confirmed the applicability of international law to their behavior in cyberspace.[2] And, although the OAS has not, other international organizations—ASEAN, the European Union, and the United Nations—have done so as well.[3] To date, however, efforts to delineate *how* States understand international law's application to cyberspace have had limited success.

3. As my second report highlighted, there is outstanding controversy and confusion on whether certain existing international legal regimes apply to cyber-operations, including self-defense, international humanitarian law, countermeasures, sovereignty (as a standalone rule), and due diligence.[4] More importantly, States appear reluctant to invoke the language of international law in making

---

[1] *See* Duncan B. Hollis, *International Law and State Cyber Operations: Improving Transparency*, OEA/Ser.Q, CJI/doc 570/18 (August 9, 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); ASEAN-United States Leaders' Statement on Cybersecurity Cooperation (Nov. 18, 2018), at https://asean.org/storage/2018/11/ASEAN-US-Leaders-Statement-on-Cybersecurity-Cooperation-Final.pdf ; EU Statement – United Nations 1st Committee, Thematic Discussion on Other Disarmament Measures and International Security (October 26, 2018), at https://eeas.europa.eu/delegations/un-new-york/52894/eu-statement-%E2%80%93-united-nations-1st-committee-thematic-discussion-other-disarmament-measures-and_en. Both the G7 and G20 have made similar affirmations. *See, e.g.,* G7 Declaration on Responsible States Behavior in Cyberspace (Luca, April 11, 2017) at https://www.mofa.go.jp/files/000246367.pdf; G20 Antalya Summit Leader's Communique (Nov. 15-16, 2015) 26, at http://g20.org.tr/g20-leaders-commenced-the-antalya-summit/.

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

accusations about other State's cyber-operations.[5] In one notable exception, in 2018 five states (Australia, Canada, the Netherlands, New Zealand, and the United Kingdom) accused the GRU—Russia's military intelligence arm—of responsibility for a series of cyber operations, including those targeting the Organization for the Prohibition of Chemical Weapons (OPCW) and the World Anti-Doping Agency (WADA). The U.K. Foreign Secretary suggested that Russia had a "desire to operate without regard to international law or established norms" while the Netherlands suggested, more broadly, that these Russian activities "undermine the international rule of law."[6] Unfortunately, these accusations did not delineate whether all of the GRU's alleged operations violated international law or if only some did; nor did they elaborate which international laws the accusers believed were violated.

4. In recent years, a number of States have begun to offer *some* elaborations on how international law applies in cyberspace. Beginning in 2012, the United States began to offer its views in a series of speeches and statements.[7] In 2018, the United Kingdom's Attorney General made an important statement of U.K. views.[8] In the ensuing years, a number of other States have begun to offer their own detailed

[5] *See* Dan Efrony and Yuval Shany, *A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyber-Operations and Subsequent State Practice,* 112 AJIL 583, 594 (2018); Duncan B. Hollis & Martha Finnemore, *Beyond Naming and Shaming: Accusations and International Law in Global Cybersecurity,* EURO. J. INT'L L. (forthcoming 2020).

[6] Press Release, Foreign Commonwealth Office, *UK exposes Russian cyber-attacks* (Oct. 4, 2018); NCSC, *Reckless campaign of cyber attacks by Russian military intelligence service exposed* (Oct. 4, 2018), at https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed; Netherlands Ministry of Defense, *Netherlands Defence Intelligence and Security Service disrupts Russian cyber operation targeting OPCW* (Oct. 4, 2018), at https://english.defensie.nl/latest/news/2018/10/04/netherlands-defence-intelligence-and-security-service-disrupts-russian-cyber-operation-targeting-opcw.
Canada's accusation incorporated both formulations. Press Release, Global Affairs Canada, *Canada Identifies Malicious Cyber-Activity by Russia* (Oct. 4, 2018) at https://www.canada.ca/en/global-affairs/news/2018/10/canada-identifies-malicious-cyber-activity-by-russia.html (Russian activity demonstrates "a disregard for international law and undermine[s] the rules-based international order."). In contrast, Australia and New Zealand accused Russia of "malicious cyber activity" without referencing international law at all. *See, e.g.,* Press Release, New Zealand Government Communications Security Bureau, *Malicious Cyber Activity Attributed to Russia* (October 4, 2018), at https://www.gcsb.govt.nz/news/malicious-cyber-activity-attributed-to-russia/; Media Release, Prime Minister of Australia, *Attribution of a Pattern of Malicious Cyber Activity to Russia* (Oct. 4, 2018), athttps://www.pm.gov.au/media/attribution-pattern-malicious-cyber-activity-russia.

[7] *See, e.g.,* Brian Egan, *Remarks on International Law and Stability in Cyberspace* (Nov. 10, 2016), *in* DIGEST OF U.S. PRACTICE IN INT'L LAW. 815 (2016); *U.S. Submission to Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (Oct. 2016), *in* DIGEST OF U.S. PRACTICE IN INT'L LAW. 823 (2016); *U.S. Submission to Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (Oct. 2014), *in* DIGEST OF U.S. PRACTICE IN INT'L LAW. 732 (2014); Harold Koh, *International Law in Cyberspace* (Sept. 18, 2012), *in* DIGEST OF U.S. PRACTICE IN INT'L LAW. 593 (2012).

[8] Jeremy Wright, QC, MP, *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 ("U.K. Views").

perspectives, including Australia,[9] Estonia,[10] France,[11] and the Netherlands.[12] Although a welcome development, the number and specificity of these statements has not (yet) been sufficient to rely on them as evidence of general state practice or *opinio juris*.[13]

5. Several non-State actors have sought to fill in this information deficit by offering their own views on how customary international law regulates State cyber-operations. The two most prominent sets of voices are undoubtedly those of the International Committee of the Red Cross (ICRC) and the Independent Group of Experts who authored the *Tallinn Manuals*.[14] It is clear, however, that not all States regard their contents as reflecting international law.[15]

6. 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. Specifically, I proposed—and the Committee approved—circulating a questionnaire to OAS Member States on some of the most relevant international legal questions. The project has three discrete goals:

a. To identify areas of convergence in how States understand which international legal rules apply and how they do so. When combined with existing statements from States outside the region, their uniformity of views may provide further evidence for delineating the relevant customary international law rules.

b. To identify divergent views on what international laws apply and how they do so. This may help

---

[9] *Australian Mission to the United Nations, Australian Paper—Open Ended Working Group on Developments in the Field of Information and Telecommunications in the context of International Security* (Sept. 2019) https://s3.amazonaws.com/unoda-web/wp-content/uploads/2019/09/fin-australian-oewg-national-paper-Sept-2019.pdf ("Australian Views").

[10] Kersti Kaljulaid, President of Estonia, *Speech at the opening of CyCon 2019* (May 29, 2019) https://www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/index.html ("Estonian Views").

[11] Ministère des Armées, *Droit international appliqué aux operations dans le cyberspace* (9 Sept 2019) https://www.defense.gouv.fr/salle-de-presse/communiques/communiques-du-ministere-des-armees/communique_la-france-s-engage-a-promouvoir-un-cyberespace-stable-fonde-sur-la-confiance-et-le-respect-du-droit-international ("French Ministry of Defense Views"). I have not labeled these as "French views" as at least one scholar has pointed out that the document is authored by the French Ministry of Defense and its contents may not be attributable to the French State as a whole. See Gary Corn, *Punching on the Edges of the Gray Zone, Iranian Cyber Threats and State Cyber Responses,* JUST SECURITY (Feb. 11, 2020) ("it should be noted that despite numerous assertions to the contrary, the French document does not claim to be the official position of the French government. It was written and published by the French Ministère des Armées (MdA), in the same vain as the DoD Law of War Manual which does not necessarily reflect the views of the U.S. Government as a whole.").

[12] *Letter from Minister of Foreign Affairs to President of the House of Representatives on the international legal order in cyberspace*, July 5, 2019, Appendix 1, at 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 ("The Netherlands Views").

[13] *See, e.g.*, Egan, *supra* note 7, at 817.

[14] *See, e.g.,* ICRC, *Position Paper on International Humanitarian Law and Cyber Operations during Armed Conflicts* (Nov. 2019) ("ICRC Position Paper"); MICHAEL N. SCHMITT (ED.), TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (2017) ("*Tallinn 2.0*"); *see also* ICRC, *Report on International Humanitarian Law and the Challenges of Contemporary Armed Conflict*, 70th Anniversary of the Geneva Conventions (Nov. 2019) ("2019 ICRC Report"); ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts,* 32nd International Conference of the Red Cross and Red Crescent (Oct. 2015) 39-43 ("2015 ICRC Report").

[15] Egan, *supra* note 7, at 817 ("Interpretations or applications of international law proposed by non-governmental groups may not reflect the practice or legal views of many or most States. States' relative silence could lead to unpredictability in the cyber realm, where States may be left guessing about each other's views on the applicable legal framework. In the context of a specific cyber incident, this uncertainty could give rise to misperceptions and miscalculations by States, potentially leading to escalation and, in the worst case, conflict.").

set a baseline for further dialogue, whether to reconcile conflicting positions, clarify the law's contents, or, perhaps even, pursue changes to it. In addition, providing more transparency on a State's views can inform other States' behavior to limit risks of inadvertent escalation or conflict.

c. To afford OAS Member States an appropriate voice in global conversations about international law's application. Last year, the UN General Assembly tasked a new U.N. Group of Governmental Experts to invite national views on international law.[16] With only four OAS Member States participating in the GGE (Brazil, Mexico, the United States and Uruguay), the Committee's work offers an opportunity to other Member States to provide a fuller range of views from across the region. This aligns with a European Union call 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."[17]

At the same time, it is important to reiterate what this project is *not* designed to do. It does not aim to codify or progressively develop international law (nor even to identify best practices or general guidance). Nor does it aim to offer a comprehensive or overarching perspective on international legal issues in the cyber context. The goal is more modest. These questions were designed to elicit State views on how international law applies to cyberspace in areas where the most discussion (and discord) has appeared to date. It thus aims to afford OAS Member States a platform to be more transparent on how they understand international law's relationship to cyberspace and the information and communication technologies (ICTs) from which it derives.

7. With the Committee's approval, I prepared a questionnaire on these issues with input from the OAS Department of International Law and the International Committee of the Red Cross. The questionnaire was circulated to Member States in January 2019. My third report provided an update on the questionnaire's contents and asked for an extension to the response deadline.[18] A copy of the original questionnaire is included as Annex A to this report.

8. Subsequent to my third report, I had the opportunity to participate in consultations held by the OAS Secretariat of the Inter-American Committee against Terrorism (CICTE) with the UN Office for Disarmament Affairs on August 15-16, 2019, during which time I addressed participants on the Committee's work on this topic. In December, I participated (in my academic capacity) in the informal inter-sessional meeting of the Open Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security. There, I had a number of informal consultations with States and other stakeholders to describe the Committee's interest in promoting transparency in how States understand international law's application to cyberspace. In both contexts, I received uniformly positive feedback and encouragement, suggesting that there is widespread interest in affording States one or more fora for expressing their opinions and further strengthening the rule of law in cyberspace.

9. In this report, I briefly survey the responses to the Committee's ten questions on international law and cyberspace. To date, the Committee has received nine responses. Eight of these are substantive as Bolivia, Chile, Costa Rica, Ecuador, Guatemala, Guyana, Peru provided specific responses[19] while

---

[16] *See* UNGA Res. 266, *supra* note 3, ¶3 (on the GGE's mandate). In addition, to the new GGE, there is also a UN-sponsored Open Ended Working Group (OEWG) that looks 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.

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

[18] See Duncan B. Hollis, *International Law and State Cyber Operations: Improving Transparency: Third Report*, OEA/Ser.Q, CJI/doc 594/19 (July 24, 2019) ("Hollis, Third Report").

[19] *Note from the Plurilateral State of Bolivia, Ministry of Foreign Affairs, OAS Permanent Mission to the OAS Inter-American Juridical Committee*, MPB-OEA-NV104-19 (July 17, 2019) (containing responses to IAJC Questionnaire from Bolivia's Office of the Commander-in-Chief of the State Inspector General of the Armed Forces) ("Bolivia Response"); *Response submitted by Chile to the OAS Inter-American Juridical Committee Questionnaire* (Jan.14, 2020) ("Chile Response"); *Communication from Carole Arce Echeverria, Costa Rica,*

the United States directed the Committee to its prior statements issued between 2012 and 2016.[20] The ninth response—from Brazil—was non-substantive; it highlighted Brazil's pending work at the UN GGE (where its expert serves as Chair) as the forum where it planned to address issues of international law's application to cyberspace.[21] All nine responses are enclosed with this report at Annex B.

10. Before reviewing the responses, question-by-question, I must emphasize three overall reactions. *First* and foremost, it is apparent that all the responding States have an abiding interest in the rule of law, including the role international law can play in regulating State behavior in cyberspace. This is an undoubtedly welcome development and bodes well for Member State cooperation and coordination on international legal issues in this context going forward.

11. At the same time, however, I must highlight a *second*, less positive, reaction to the questionnaire responses. When considered collectively, they reveal just how *uneven* Member State capacities are distributed at present. By "capacity" I am not just referring to variations in what operational capabilities States have to deploy cyber operations, although that variation is very real. Rather, I am also referring to how much OAS Member States appear to understand the relevant technical and legal issues that have garnered so much attention in other geopolitical contexts like the United Nations. To be sure, several States' responses evince a deep knowledge of the various ways States may employ cyber-operations, both as a substitute for things States have done in the past as well as a novel tool to achieve objectives, scales or effects not seen previously. At the same time, however, other States appear more limited in their understanding of what States may achieve in cyberspace. Their understanding is further complicated by a lack of a shared language; States employ very different terms and definitions in their responses.[22] Similarly, when it comes to international law, several States are clearly familiar with the various dividing lines that have dominated conversations for the last several years, while other States demonstrate much less familiarity with the underlying international legal rules and the particular questions their applications generate in the cyber context.

12. Such disparities suggest that the Committee might consider whether, in addition to surveying State views, the OAS should engage in more legal and technical capacity building. OAS's CICTE already has an excellent track record in assisting Member States on building capacity, whether by helping them devise "national" cybersecurity strategies or standing up computer security incident response teams (CSIRTs).[23] There have also been several programs in the region designed to educate Member State foreign ministries on the relevant legal questions and the terms of ongoing debates.[24] Nevertheless, the current responses suggest that more can—and should—be done. This is, moreover, a view that comes

---

International Organizations, Department of Foreign Policy, Minister of Foreign Affairs and Worship to OAS, (April 3, 2019) (including letter no. 163-OCRI2019 from Yonathan Alfaro Aguero, Office of International Cooperation and Relations to Carole Arce Echeverria, which includes a reply from the "relevant authority"—the Costa Rica Criminal Court of Appeals) ("Costa Rica Response"); *Verbal Note 4-2 186/2019 from the Permanent Mission of Ecuador to the OAS* (June 28, 2019) ("Ecuador Response"); Note Of. 4VM.200-2019/GJL/lr/bm, from Mr. Gabriel Juárez Lucas, Fourth Vice Minister of the Interior Ministry of the Republic of Guatemala to Luis Toro Utillano, Technical Secretariat, Inter-American Juridical Committee (June 14, 2019) ("Guatemala Response"); *Note No: 105/2019 from the Permanent Mission of Guyana to the OAS* (July 30, 2019) ("Guyana Response"); *Response Submitted by Peru to the Questionnaire on the Application of International Law in OAS Member States in the Cyber Context* (June 2019) ("Peru Response").

[20] *See* note 7.

[21] Response by Brazil to CJI OEA Note 2.2/14/19 (July 1, 2019).

[22] For example, States employ different definitions for cyberspace. *Compare* Guyana Response, *supra* note 19, at 2 (using a definition drawn from U.S. Naval Academy web-site) with Peru Response, *supra* note 19, at 2 (using a definition drawn from Kristen Eichensehr, *The Cyber-Law of Nations,* 103 GEORGETOWN L. J. 323, 324 (2015) which draws, in turn, from the *Oxford English Dictionary*).

[23] For more on CICTE's activities see http://www.oas.org/en/sms/cicte/prog-cybersecurity.asp.

[24] Canada and Mexico, for example, co-hosted a workshop with the OAS on May 30, 2019 that targeted OAS countries for a discussion of international law's application to cyberspace.

across in several of the Member States' own responses. Costa Rica's response was particularly eloquent in this respect. It cited –

> the urgent need for opportunities for study and analysis to be able to address successfully and effectively all problems that cyber operations might generate, not only to address attacks and how they should be countered, prevented, and punished, but also for study and analysis of the responsibility of States, even vis-à-vis non-state actors.
>
> In that regard, we wish very respectfully to indicate the need to join forces to create appropriate opportunities so that countries like Costa Rica and others become involved in the study of this subject and make proposals, not only for international but also for domestic law, that can take a step towards dealing with a virtual reality with cross-border implications and the capacity to impact fundamental rights of the world's citizens.[25]

Given such views, I would invite the Committee's input on whether and how the OAS might engage in more international legal capacity building in this space. I am particularly interested in ways to ensure Member States have the necessary legal and technical background knowledge necessary to engage in ongoing discussions and debates—and to reach their own conclusions on them—in an informed manner.

13. *Third*, the response rate to the Committee's questionnaire remains under-representative of the region as a whole. The time and effort States put into substantive responses is appreciated (and tremendously valuable). And yet, the responses received so far represent less than 25% of the OAS's Membership. To acquire a more accurate reflection of how the region understands international law's application to cyberspace suggests a need for more Member State responses. I invite the Committee's ideas on whether further efforts seeking (and obtaining) such responses would be useful or feasible.

14. With these caveats in mind, I reproduce below each of the Committee's questions, accompanied by a short summary of the responses received to date.

Question 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.

15. This first question solicited existing national statements on international law and cyberspace. The idea was to make sure the Committee was aware of any prior views of Member States. It also allowed States to avoid having to respond to the questions if they had already taken relevant substantive positions. Of the eight responses, however, only the United States indicated that it had previously made statements and speeches on how international law applies to cyberspace, including 2012 and 2016 speeches by the then-Legal Advisers to the U.S. Department of State and the 2014 and 2016 U.S. Submissions to meetings of U.N. Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security.[26]

16. Other States indicated that they were unaware of any prior positions on their views on international law's application in the cyber context.[27] Several States took the opportunity, however, to

---

[25] Costa Rica Response, *supra* note 19, at 2

[26] For citations, *see supra* note 7. Note, however, that the U.S. Response indicated that these were only "some of" the documents indicating U.S. views. Thus, there may be others that warrant attention. In particular, it might be useful to know how much the U.S. Department of Defense *Laws of War Manual* reflects the views of the United States as a whole. *See* Office of General Counsel, U.S. Department of Defense, *Department of Defense Law of War Manual* (June 2015, updated December 2016) ("DOD Manual").

[27] *See, e.g.,* Ecuador Response, *supra* note 19, at 1 ("We are not aware of any official paper the Government of Ecuador has issued on cyber operations."); *see also* Guyana Response, *supra* note 19, at 1 (same).

highlight their internal efforts to establish relevant organizations or regulatory regimes for addressing ICT issues.[28]

17. The dearth of prior official statements confirms the hypothesis on which this project rests – that States have said relatively little to date about how international law applies to State behavior in cyberspace. It also confirms that most domestic efforts relating to cybersecurity to date have centered on national cybersecurity strategies or policies as well as domestic cybercrime and other ICT regulatory efforts.

Question 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?

18. Although a recent U.N. General Assembly Resolution[29] suggests that there is now widespread support for international law's application to cyberspace, earlier efforts at the United Nations revealed that certain States have deep reservations about the applicability of certain international legal regimes. Indeed, these reservations reportedly led the 2016-2017 U.N. GGE to fail to produce any final report.[30] Thus, there is a continuing need to identify whether the existence of certain areas of international law in cyberspace is contested, and, if so, which ones. This second question was designed to solicit each State's views on any extant international law that it considered inapplicable (or where the application might at least be problematic) in the cyber context.

19. Overall, the questionnaire responses reflected extensive support for the application of existing fields of international law to cyberspace. As Chile's Response summarized, "current international law provides the applicable legal framework … including rules relating to *jus ad bellum,* international humanitarian law, human rights, and those governing the international responsibility of States."[31] Other States affirming international law's application included Ecuador, Peru, and the United States.[32] Along with the *jus ad bellum* and the *jus in bello,* Peru's response emphasized the validity in cyberspace of various human rights, including "the right to privacy, freedom of information, freedom of expression, free and equal access to information, elimination of the digital divide, intellectual property rights, free flow of information, the right to confidentiality of communications, etc."[33] The U.S. echoed the application of international human rights law, while touting the overall application of existing

---

[28] Bolivia Response, *supra* note 19, at 1 (citing a new 2015 law); Chile Response, *supra* note 19, at 1 (listing the Ministry of Defense's March 2018 "cyber-defense policy"); Guatemala Response, *supra* note 19, at 1 (emphasizing its "national cybersecurity strategy" and new cybercrime law); *see also* Costa Rica Response, *supra* note 19, at 1.

[29] *See* UNGA Res. 266, *supra* note 3.

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

[31] Chile Response, *supra* note 19, at 1 (As a result, Chile notes that the "planning, conduct, and execution of operations in cyberspace must adhere strictly to respect for public international law, with particular consideration to international human rights law and international humanitarian law").

[32] Ecuador Response, *supra* note 19, at 1 ("The fields of international law do apply to cyberspace"); Peru Response, *supra* note 19, at 1 ("bearing in mind the fundamental role of the Charter in terms of how it relates to other international instruments … it would be reasonable to conclude that no area of international relations lies outside the scope of the aforesaid principles… Bearing in mind that cyberspace is becoming an everyday setting for international interaction, the actors in such interactions are required to observe their higher obligations under international law, including the prohibition on the use of force, the right of self-defense, and respect for human rights and international humanitarian law."); Koh, *supra* note 7, at 594 ("Yes, international law principles do apply in cyberspace . . . Cyberspace is not a 'law-free' zone where anyone can conduct hostile activities without rules or restraint.").

[33] Peru Response, *supra* note 19, at 1.

international law as the "cornerstone" of U.S. cyberspace policy.[34]

20. Bolivia also offered a positive response. But its answer focused on the international law "to be applied in armed conflicts," offering views on how to differentiate when international humanitarian law (IHL) would (and would not) apply.[35] As such, it is not clear whether Bolivia's positive response extends to the application of other sub-fields of international law beyond the *jus ad bellum* and the *jus in bello*.

21. Guatemala and Guyana both expressed positive support for international law's application. Yet, both offered caveats about how universally the extant law might apply. Without offering any examples, Guatemala noted that there could be areas where "the novelty of cyberspace does preclude the application of certain international rights or obligations."[36] Guyana, meanwhile, noted that "cyber operations do not fit into traditional concepts" and pointed out that "a raging debate as to whether existing fields of international law apply to cyberspace"[37] Acknowledging the prior work of the GGE, Guyana "respectfully submitted that while it is acknowledged that international law should or ought to apply to cyberspace, it is difficult to easily apply existing principles" such as the use of force which "traditionally implies some physical element and armed attacks which traditionally imply some sort of weapon."[38]

22. Thus, even as the overall application of international law to cyber-operations appears well entrenched, these last two responses suggest the need for further dialogue and discussion. It would be useful to identify *which* particular areas of international law's application give certain States pause and why. Doing so would help illuminate just how much convergence (or divergence) of views exist on how international legal regimes govern State and State-sponsored cyber operations.

Question 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?

23. Most (but not all) States appear to accept the application of international law on the use of force (*e.g.*, the *jus ad bellum*) to their cyber operations. This question sought to identify which States in the region adhere to this dominant view versus alternative positions. At the same time, additional application questions have arisen among States who accept the *jus ad bellum* in cyberspace, most notably the extent to which thresholds for the "use of force" or "armed attacks" require analogous "violent" effects to those deemed to pass those thresholds in the past. The issue is how to handle novelties in the scale or effects of cyber operations (*i.e.*, those operations that are not akin to *either* past kinetic operations—which surpassed the use of force threshold—nor economic or political sanctions—which did not). How should international law regard such cyber operations? Should they be placed, by default, below the use of force threshold or above it? Or, is further investigation and analysis needed to bifurcate cyber operations in this new "grey zone," treating some of these novel operations as above, and others below, relevant thresholds?[39] Thus, this question sought to acquire State perspectives on whether to define cyber operations as uses of force (or armed attacks) entirely by analogy to previous cases or to devise some new standard for doing so.

---

[34] 2014 US GGE Submission, *supra* note 7, at 733 (application of international law comprises the "cornerstone" of US view, taking into account its distinctive characteristics); Egan, *supra* note 7, at 815 (same); on the application of human rights, *see* Koh, *supra* note 7, at 598; Egan, *supra* note 7, at 820; 2016 US GGE Submission, *supra* note 7, at 824.

[35] Bolivia Response, *supra* note 19, at 2-7. Thus, Bolivia suggested that IHL would not govern cyber-operations involving national security, propaganda, espionage, manipulation of strategic critical infrastructure, cyber operations with political objectives, or those hacking into private systems putting at risk the state's economic and social operations. *Id*. at 3-7.

[36] Guatemala Response, *supra* note 19, at 1-2.

[37] Guyana Response, *supra* note 19, at 1-2

[38] *Id.*

[39] *See* Michael N. Schmitt, *Grey Zones in the International Law of Cyberspace,* 42 YALE J. INT' L. 1 (2017).

24. Bolivia, Chile, Guatemala, Peru, and the United States are all clear that both the prohibition on the use of force and the inherent right of self-defense in response to an "armed attack" may be triggered by cyber operations alone.[40] As Guatemala explained:

> [A] cyber operation in and of itself can qualify as a use of force, since "use of force" does not exclusively mean physical force; it also covers threats to and violations of the security and protection of third parties . . . there is a right of legitimate defense against a cyber attack or operation against a country's sovereignty.[41]

The 2014 U.S. Submission to the GGE emphasized its understanding that the "inherent right of self-defense potentially applies against any illegal use of force" suggesting a single threshold for both rules.[42] This stands in contrast to States that view all armed attacks as uses of force but not all uses of force as armed attacks (the latter are said to involve only the "most grave" forms of a use of force).[43] The United States also emphasized that its inherent right of self-defense can be triggered by cyber activities that "amount to an actual or imminent armed attack" and "regardless if the attacker is a State or non-State actor.[44]

25. In contrast, Guyana's response expressed doubts about the applicability of the *jus ad bellum* to cyber operations alone. Relying on *Black's Law Dictionary* for a definition of force as "power dynamically considered," Guyana indicated that a cyber operation "by itself may not constitute a use of force."[45] Similarly, it defined an armed attack as involving "weaponry" and to the extent "no physical weaponry is involved" in a cyber operation, it may not be considered an armed attack triggering self-defense.[46] At the same time, Guyana did emphasize that cyber operations could be used in armed conflicts and governed international humanitarian law (IHL).[47]

26. With respect to whether a cyber operation could cross the use-of-force threshold (or that for an armed-attack[48]) without having violent effects, State views were mixed. Most responding States continue to find power in drawing the relevant thresholds by analogizing cyber operations to kinetic or other past operations that did (or did not) qualify as a use of force or armed attack. Some States, however, hinted

---

[40] Bolivia Response, *supra* note 19, at 2-7 Chile Response, *supra* note 19, at 1 (Chile will refrain from using force "through cyberspace" in a manner that is against international law and will exercise "its right to self-defense against any armed attack carried out through cyberspace"); Guatemala, *supra* note 19, at 2; Peru Response, *supra* note 19, at 1-3; Koh, *supra* note 7, at 595 (Stating the U.S. view that (a) "Cyber activities may in certain circumstances constitute uses of force within the meaning of Article 2(4) of the UN Charter and customary international law"; and (b) "a State's national right of self-defense, recognized in Article 51 of the UN Charter, may be triggered by computer network activities that amount to an armed attack or imminent threat thereof."); 2014 US GGE Submission, *supra* note 7, at 734; Egan, *supra* note 7, at 816 (suggesting 2015 UN GGE also endorsed the right of self-defense). Ecuador also responded to the question affirmatively, but cited the definition of "armed attack" used in Article 92 of *Tallinn 2.0*, which defines that term in the context of an armed conflict (*i.e.,* the *jus in bello*) – a distinct usage of the term from its expression in UN Charter Article 51 and the *jus ad bellum*. *See* Ecuador Response, *supra* note 19, at 1.

[41] Guatemala, *supra* note 19, at 2. *Accord* Peru Response, *supra* note 19, at 3 (citing the ICRC and Michael Schmitt for the idea that uses of force are not limited to kinetic force).

[42] Koh, *supra* note 7, at 597.

[43] *See Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. U.S.)* [1986] ICJ Rep. 14, ¶¶176, 191 (June 27) (describing armed attacks as "the most grave forms of the use of force.").

[44] 2014 US GGE Submission, *supra* note 7, at 734-5. The submission also reiterates the "unwilling or unable" test for engaging in self-defense against a State without its consent where "a territorial State is unwilling or unable to stop or prevent the actual or imminent attack launched in or through cyberspace." *Id.* at 735.

[45] Guyana Response, *supra* note 19, at 2.

[46] *Id.*

[47] *See id.* at 3, 5.

[48] This assumes, contra the U.S. view, that there may be two different thresholds. *See supra* notes 42-43, and accompanying text.

at the potential to move beyond such analogies. Chile, for example, suggested that cyber operations analogous to the threshold of severity necessary to satisfy the requirements established by international law to be an armed attack" can give rise to a right of self-defense.[49] At the same time, however, Chile's response may have left room for defining armed attacks more broadly, suggesting that "cyberattacks directed against its sovereignty, its inhabitants, its physical or information infrastructure" could qualify as such.[50]

27. Peru more openly admitted the "possibility of a cyber operation that does not cause violent effects being classed as a use of force or an armed attack."[51] It did so, however, based on the idea that kinetic weaponry in the past might have also been employed without causing violent effects and yet still constituted a use of force (*i.e.*, firing a missile across another State's territory even if it does not land in that State).[52] Overall, Peru emphasized the need to differentiate "cyber-attacks" (which "cause damage to a militarily significant target, resulting in its total or partial destruction, capture, or neutralization") from "cyber disruptions" that "cause inconvenience, even extreme inconvenience, but no direct injury or death, and no destruction of property."[53] As such, the specifics of Peru's response emphasized evaluating the legality of cyber operations in the use of force context based on whether they "cause death or injury to persons or property."[54]

28. Guatemala's response adopted a different approach, suggesting a willingness to rethink what qualifies as "violent effects" because a cyber operation's consequences "can be greater and more lasting, in that they threaten such sectors as health, security, and others."[55] It suggested that in the cyber context, consequences that produce "death, anxiety, and poverty" should be considered violent.[56]

29. Bolivia's response suggested that the threshold might be difficult to apply in practice since the "effects of cyber-attacks will not always be immediately known" making it hard to check if there's been a use of force. At the same time, Bolivia indicated that it would evaluate the threshold based on analogies to the kinetic context, *i.e.,* an "armed attack" arises where "the cyber virtual attack uses unconventional means that have the same impact [as] an armed attack."[57]

30. Finally, the United States did not respond to the questionnaire itself. Nonetheless, its previous statements shed some light on its views. In his seminal 2012 speech, Harold Koh indicated the U.S. preference for a contextual approach to identifying uses of force (albeit with the aforementioned caveat that the U.S. definition also would identify armed attacks):

> In assessing whether an event constituted a use of force in or through cyberspace, we must evaluate factors including the context of the event, the actor perpetrating the action (recognizing challenges of attribution in cyberspace), the target and location, effects and intent, among other possible issues.[58]

At the same time, Koh clearly viewed the test as requiring an analogy, asking "whether the direct

---

[49] Chile Response, *supra* note 19, at 2.
[50] *Id.* at 2.
[51] Peru Response, *supra* note 19, at 3.
[52] *Id.*
[53] *Id.* at 2.
[54] *Id. at* 3.
[55] Guatemala, *supra* note 19, at 2.
[56] *Id*.
[57] Bolivia Response, *supra* note 19, at 2-7 (Bolivia emphasized that the right of self-defense also encompasses "pre-emptive self-defense," which is only available when the threat is imminent and the need for self-defense is immediate (rather than retaliatory)).
[58] Koh, *supra* note 7, at 595 (Cyber activities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force"). The U.S. has maintained this view subsequently. 2014 US GGE Submission, note 7, at 734. The 2014 US GGE Submission was also appended to the 2016 US GGE Submission, suggesting continued support for its contents.

physical injury and property damage resulting from the cyber event looks like that which would be considered a use of force if produced by kinetic weapons."[59] He also has cited specific examples of cyber operations that would constitute uses of force: (i) a nuclear plant meltdown caused by cyber activity; (ii) cyber operations that "open a dam above a populated area causing destruction"; and (iii) a cyber operation that disables "air traffic control resulting in airplane crashes."[60] To the extent all these examples involve some form of "violence" it would appear that the United States favors a use of force threshold analogous to the one applied in the kinetic context.

Question 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?

Question 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?

31. States are responsible not only for the behavior of their own organs and agencies in cyberspace, but also for any non-state actor that they endorse or control.[61] 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. As is well known, cyber threats may be authored not just by States directly but also by a range of non-state actors, including hacktivist groups and cybercriminal organizations. In some cases, States may seek to employ these non-State actors as proxies for conducting various cyber operations.

32. Tying a proxy back to a principal in cyberspace can be technically quite challenging (although perhaps not as difficult as some supposed in the past). At the same time, a factual linkage is not enough, there must be legal attribution as well – *i.e.*, a sufficient connection between a State and a non-State actor for the former to assume legal responsibility for the latter's behavior. A State may, for example, endorse a non-state actor's behavior after the fact, thereby assuming legal responsibility for it.[62] Alternatively, States are legally responsible for non-State actor behavior that they control. Precisely how much control is, however, often unclear. In the *Nicaragua* case*,* the ICJ indicated that international law contains a rule imposing responsibility on a State for acts of those non-State actors over which it has "effective control" (*e.g.*, ordering the behavior or directing an operation).[63] But, a few years later, the International Criminal Tribunal for the Former Yugoslavia (ICTY) adopted a looser standard of "overall control" for the purposes of IHL. As the ICTY put it, this test requires "more than the mere provision of financial assistance or military equipment or training" but not going so far as to insist on the "issuing of specific orders by the State or its direction of individual operations."[64] The ICC later endorsed the "overall control" standard.[65]

33. The ICJ, however, has continued to insist on its "effective control" formulation in the use of force context. At the same time, it signaled that the "overall control" test might be appropriate in the IHL context, raising the possibility of a consensus on "overall control" in the IHL context and "effective

---

[59] Koh, *supra* note 7, at 595.
[60] *Id.*
[61] *See* ILC, "Draft Articles on the Responsibility of States for Internationally Wrongful Acts" in *Report on the Work of its Fifty-first Session* (May 3-July 23, 1999), UN Doc A/56/10 55 [3] ('ASR'); *accord Tallinn 2.0, supra* note 14, Rule 15.
[62] ASR, *supra* note 61, Art. 11; HEATHER HARRISON DINNISS, CYBER WARFARE AND THE LAWS OF WAR 52 (2012).
[63] *Nicaragua Case*, *supra* note 43, at ¶115.
[64] *Prosecutor v. Dusko Tadić aka 'Dule'* (Judgment) ICTY-94-1-A (15 July 1999) ¶¶131-145, 162.
[65] *Prosecutor v. Lubanga*, Case No. ICC-01/04-01/06, Trial Chamber, Judgement (Int'l Crim. Court, March 14, 2012).

control" in other contexts.[66] Given this possibility, the questionnaire asked about state responsibility both generally and in the IHL context based on the existence of some armed conflict as that term is used in the Geneva Conventions.

[66] *Case concerning application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)* (Judgment) [1997] ICJ Rep. 43, 208–09, ¶¶402-407 (indicating that the overall control test "may well be . . . applicable and suitable" for IHL sorts of classifications).

34. In terms of their responses, several Member States emphasized the difficulty of attribution in cyberspace.[67] Others focused less on the question of liability for proxy behavior and more on the State's responsibility to take care its territory was not used by non-State actors to launch attacks.[68] Thus, Peru commented that "if there is inertia on the part of a State in controlling a nonstate actor that unleashed a cyber attack against another State, despite having the capacity to control them, then that could give rise to their conduct being attributable to the State."[69] For its part, Bolivia emphasized that States should not bear responsibility where they lack the technological infrastructure to control non-State actors. [70] And the United States emphasized that the "mere fact that a cyber activity was launched from, or otherwise originates from, another State's territory or from the cyber infrastructure of another State is insufficient, without more, to attribute that activity to that State."[71]

35. For those States whose responses focused on the question of proxy actors, the Articles of State Responsibility ("ASR") loomed large. Chile, Guyana, and Peru all based their response on ASR Article 8:

> The conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct.[72]

The ASR, however, did not offer an opinion on which type of "control" the State needs to exhibit, suggesting it is "a matter for appreciation in each case."[73] This tracks U.S. views, which endorse State responsibility for "activities undertaken through 'proxy actors' who act on the State's instructions or under its direction or control" while only saying that the degree of control exhibited must be "sufficient."[74] The United States has also acknowledged that a State may later acknowledge or adopt a non-State actor's cyber operation as its own.[75]

36. However, one State, Chile, did offer its views on the level of control required to trigger legal responsibility. Citing the *Nicaragua* and *Genocide* cases, Chile opined that the "The degree or level of control or involvement of a state in the operations of a non-state actor, required to trigger its international responsibility is that of effective control."[76] Chile, moreover, took the view that the standards of State

---

[67] Guatemala, *supra* note 19, at 3 (finding "clear responsibility" for a cyber attack is "by no means an easy task"); Peru, *supra* note 19, at 4 (noting great "uncertainty in attribution, and levels of attribution, of cyber attacks" making it harder "to control those who use cyberspace to unleash attacks over the Internet").

[68] Ecuador, *supra* note 19, at 1 ("States cannot be held liable for an attack by a non-state actor, but there should be some way [for them] to collaborate to find the perpetrators. Furthermore, a state is responsible for regulating/setting standards for services to prevent territory belonging to a state from being launch [sic.] an attack."); Guatemala, *supra* note 19, at 3 (answering in terms of due diligence of the host State rather than the amount of control over proxy actors).

[69] Peru Response, *supra* note 19, at 4 (citing ASR Article 11).

[70] Bolivia *supra* note 19, at 3-7. On the question of proxies, Bolivia's response was indirect, although it did suggest a link between a State and non-State actors associated with its defense policy objectives and/or strategies of a State in a situation of armed conflict. *Id*.

[71] 2014 US GGE Submission, *supra* note 7, at 738.

[72] ASR, *supra* note 61, Art. 8; Chile Response, *supra* note 19, at 2; Guyana Response, *supra* note 19, at 3; Peru Response, *supra* note 19, at 4. Chile and Peru's responses also appear based on ASR Article 5 assigning State responsibility to "[t]he conduct of a person or entity which ... is empowered by the law of [a] State to exercise elements of the governmental authority … provided the person or entity is acting in that capacity in the particular instance." *See* Chile Response, *supra* note 19, at 2; Peru Response, *supra* note 19, at 4.

[73] ASR, *supra* note 61, at 48 (Commentary to Art. 8).

[74] Koh, *supra* note 7, at 595; 2014 US GGE Submission, *supra* note 7, at 738 (same); Egan *supra* note 7, at 821; 2016 US GGE Submission, *supra* note 7, at 826.

[75] Egan *supra* note 7, at 821; 2016 US GGE Submission, *supra* note 7, at 826.

[76] Chile Response, *supra* note 19, at 2.

responsibility are the same in the context of armed conflicts.[77]

37. With respect to IHL, Peru took a similar stance, favoring a uniform rule of State responsibility both in and outside of armed conflicts. While recognizing the ASR contemplates being supplanted by *lex specialis,* it indicated that doing so requires an integrated analysis. And in this case, "[a]n examination of the Geneva Conventions does not disclose any difference with respect to the provisions on international responsibility set down in the Draft Articles on Responsibility of States for Internationally Wrongful Acts; therefore, it cannot be argued that the draft articles have a different scope of application."[78] As noted, however, the ASR standard of responsibility only references "control" generally, without differentiating whether it must be "effective" or "overall."

38. Other States had more trouble answering the fifth question. Guatemala suggested that "international forums must continue their discussions on the uniquely different aspects that a conflict in cyberspace would entail, particularly regarding such issues as attribution and territorial considerations."[79] Other States read this question to ask about differing standards of responsibility between international and non-international armed conflicts.[80]

Question 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?

39. The sixth question is the first of two addressing how international humanitarian law (IHL or the *jus in bello*) applies to cyber-operations. It focuses on an issue that has divided States and scholars to date – how to define an "attack" for IHL purposes. Much of IHL, including its fundamental principles of distinction, proportionality, and precautions, are largely framed in terms of prohibiting certain types of "attacks" (*e.g.*, those targeting civilians or civilian objects) while permitting others (*e.g.*, those targeting military objects).[81] As the ICRC recently noted, "[t]he question of how widely or narrowly the notion of 'attack' is interpreted with regard to cyber operations is therefore essential for the applicability of these rules and the protection they afford to civilians and civilian infrastructure.[82] Indeed, to the extent an operation *does not* constitute an "attack," it may be conducted in an armed conflict without regard to most IHL rules.[83]

40. Under IHL, an "attack" is defined by customary international law (as codified in Article 49 of Additional Protocol I to the Geneva Conventions (API)) as "acts of violence against the adversary,

---

[77] *Id.* at 3.

[78] Peru Response, *supra* note 19, at 4-5.

[79] Guatemala Response, *supra* note 19, at 3.

[80] *See, e.g.*, Bolivia Response, *supra* note 19, at 4-7; Guyana Response, *supra* note 19, at 3. Ecuador's Response simply emphasized that States "are responsible for complying with the rules in armed conflicts, even where there are parties that are not party" to those Conventions. Ecuador Response, *supra* note 19, at 2.

[81] For example, the principle of distinction is regularly framed as a prohibition on making civilians the object of an attack. *See, e.g.,* Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Armed Conflict (Protocol I) (June 8, 1977), 1125 UNTS 3, Art. 51(2) ("API"); Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (Dec. 12, 1977), 1125 UNTS 609, Art. 13(2); Rome Statute of the International Criminal Court (July 17, 1998), Art. 8(2)(b)(f); Convention (IV) Respecting the Laws and Customs of War on Land and its Annex: Regulations concerning the Laws and Customs of war on Land (Oct. 18, 1907), 36 Stat. 2277, Art. 8(2)(b)(i)-(ii); JEAN MARIE HENCKAERTS & LOUISE DOSWALD-BECK, 1 CUSTOMARY INTERNATIONAL HUMANITARIAN LAW (ICRC, 2005) Rules 1, 7, 9, and 10.

[82] ICRC Position Paper, *supra* note 14, at 7.

[83] Even outside of attacks, States must still exercise "constant care" in an international armed conflict to avoid "unnecessary effects" on civilians and their objects. AP I, *supra* note 81, Art. 57(1); *Tallinn 2.0, supra* note 14, at 476.

whether in offence or defense."[84] As *Tallinn Manual 2.0* explains, moreover, "the consequences, not its nature, are what generally determine the scope of the term 'attack'; 'violence' must be considered in the sense of violent consequences and is not limited to violent acts."[85] The ICRC has noted, moreover, "[i]t is widely accepted that cyber operations expected to cause death, injury or physical damage constitute attacks under IHL."[86] As is well known, however, some cyber operations (*e.g.*, ransomware) are novel in that they offer an opportunity to "render objects dysfunctional without physically damaging them."[87] This raises the question whether cyber-operations that do not produce such effects (*e.g.*, disrupting the functionality of a water treatment facility without necessarily causing physical damage) can constitute an attack? Diverging views have emerged to date including among the *Tallinn Manual 2.0*'s Independent Group of Experts.[88]

41. A majority of the *Tallinn Manual 2.0*'s experts took the view that violence required some physical damage, including "replacement of physical components" such as a control system.[89] Others interpreted damage to include cases where no physical components require replacing and functionality can be restored by reinstalling the operating system, while a few other experts believed an attack could occur via the "loss of usability of cyber infrastructure" itself.[90] For its part, the ICRC has argued that during an armed conflict an operation designed to disable a computer or a computer network constitutes an attack under IHL, whether the object is disabled through kinetic or cyber means.[91]

42. The sixth question was thus designed to see if Member States likewise view IHL's attack threshold in terms of violence (or violent effects) of if they would consider that the "attack" label applicable to cyber operations based on loss of functionality rather than more traditional concepts of physical damage or destruction.

43. The questionnaire responses reveal support for the applicability of IHL generally and the idea that cyber operations can constitute an attack in that context.[92] Responses were more mixed, however, with respect to whether a cyber operation could qualify as an "attack" under IHL if it fails to cause death, injury, or direct physical harm. Chile, Peru, and the United States all gave negative responses.[93] Chile cited Article 49 of Additional Protocol 1 to the Geneva Conventions (API) to insist that IHL attacks must involve "effects or consequences arising from the act itself" that are "violent."[94] In particular, it suggested that to qualify as an attack, its result must require the affected State to "take action to repair or restore the affected infrastructure or computer systems, since in those cases the consequences of the attack are similar to those described above, in particular physical damage to property."[95] Peru's response suggests for there to be an "attack" there must be "people" or "public or private property" that is "physically

---

[84] AP I, *supra* note 81, Art. 49.
[85] *Tallinn 2.0*, *supra* note 14, at 415.
[86] *See* ICRC Position Paper, *supra* note 14, at 7.
[87] 2015 ICRC Report, *supra* note 14, at 41.
[88] *Id.*
[89] *Tallinn 2.0, supra* note 14, at 417.
[90] 2015 ICRC Report, *supra* note 14, at 43; see also 2019 ICRC Report, *supra* note 14, at 21 ("IHL rules protecting civilian objects can, however, provide the full scope of legal protection only if States recognize that cyber operations that impair the functionality of civilian infrastructure are subject to the rules governing attacks under IHL.")
[91] *See* ICRC Position Paper, *supra* note 14, at 7; 2015 ICRC Report, *supra* note 14, at 43 (arguing that international law must treat as attacks those cyber operations that disable objects since the definition of a military objective includes neutralization (suggesting that neutralizing objects falls within the ambit of IHL)).
[92] *See, e.g.,* Bolivia Response, *supra* note 19, at 3-7; *id.* at 4-7 (noting two views on whether a cyber operation alone can give rise to an armed conflict subject to IHL); Chile Response, *supra* note 19, at 3. Guyana Response, *supra* note 19, at 3; Peru Response, *supra* note 19, at 1; Koh, *supra* note 7, at 595 (U.S. view).
[93] Guyana Response, *supra* note 19, at 4.
[94] Chile Response, *supra* note 19, at 3.
[95] *Id.*

harmed."[96] The United States, meanwhile, has emphasized that the IHL "attack" threshold requires looking at "*inter alia,* whether a cyber activity results in kinetic and irreversible effects on civilians, civilian objects, or civilian infrastructure, or non-kinetic and reversible effects on the same."[97] The implication is that if a cyber operation produces non-kinetic or reversible effects, it will not "rise to the level of an armed attack."[98] This would seem to exclude, for example, ransomware exploits that are not kinetic themselves or where the data they interrupt can be restored.

44. In contrast, Guatemala and Ecuador both responded positively to the idea of delimiting attacks based on functionality losses rather than death, injury or destruction of property. Guatemala indicated that among cyber operations that can be considered an attack are those "that only produce a loss of functionality."[99] Ecuador opined that "[a] cyber operation can qualify as an attack if it renders inoperable a state's critical infrastructure or others that endanger the security of the state."[100]

45. Bolivia and Guyana's responses were more equivocal. On the one hand, Bolivia emphasized that IHL would define attacks to include those cyber operations "intended to be able to cause loss of human life, injury to people, and damage or destruction of property."[101] On the other hand, it suggested that a cyber operation "could be considered an attack when its objective is to disable a state's basic services (water, electricity, telecommunications, or the financial system").[102] Guyana noted that "[w]hen a cyber operation produces a loss of functionality, it may or may not constitute an attack."[103] Like Chile, it referenced API Article 49, tying the attack concept to a need for violence (whether in terms of means or consequences): "a cyber operation which does not result in death, injury, or physical harm cannot constitute an attack" under IHL.[104] On the other hand, it also suggested that "cyber operations that undermine the functioning of computer systems and infrastructure needed for the provision of services and resources to the civilian population constitute an attack" among which it included "nuclear plants, hospitals, banks, and air traffic control systems."[105] Such responses suggest a need for further dialogue on how proximate the death or destruction must be to the loss of functionality. In other words, does the loss of functionality to an essential service alone constitute an attack or must there be some attendant (or reasonably foreseeable) death or injury to people or property?

Question 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?

46. IHL clearly requires "attacking" States to distinguish between civilian and military objects, permitting attacks on military objectives while prohibiting those against civilians and civilian objects.[106] When it comes to cyberspace, however, it is not always clear what constitutes an "object" to which this principle applies. The primary debate has centered on "data." Does the non-physical nature of "data" mean it will not constitute an object so that militaries need not distinguish it and exclude it as a target in

---

[96] Peru's response is, however, a bit ambiguous, as it appears to rely on *jus ad bellum* materials to identify the standards for an IHL attack, including citing the U.S. contextual approach favored by Harold Koh. Peru Response, *supra* note 19, at 6.
[97] 2014 US GGE Submission, *supra* note 7, at 736.
[98] Egan, *supra* note 7, at 818. Egan's speech did not mention the reversible/irreversible criterion but emphasized instead "the nature and scope of those effects, as well as the nature of the connection, if any, between cyber activity and the particular armed conflict in question." *Id.*
[99] Guatemala Response, *supra* note 19, at 3.
[100] Ecuador Response, *supra* note 19, at 3.
[101] Bolivia Response, *supra* note 19, at 4-7.
[102] *Id.*
[103] Guyana, *supra* note 19, at 3.
[104] *Id.*
[105] *Id.* (citing API Art. 54(2)).
[106] When a particular object is used for both civilian and military purposes (so-called "dual-use objects"), it becomes a military objective (except for separable parts thereof). For sources codifying this principle of "distinction" see *supra* note 81.

their cyber operations? Or should at least some "data" qualify as an "object" to which the principle of distinction and relevant IHL rules apply?

47. A majority of the *Tallinn Manual 2.0*'s Independent Group of Experts adopted the former view: the "armed conflict notion of 'object' is not to be interpreted as including data, at least in the current state of the law."[107] That said, the experts did agree that a cyber operation against data could trigger IHL's rules where it "foreseeably results in the injury or death of individuals or damage or destruction of physical objects" since the latter individuals and objects would be protected by relevant IHL rules like distinction.[108] The ICRC has, in contrast, suggested a more expansive definition of data via the term "essential civilian data" (*e.g.*, medical data, biometric data, social security data, tax records, bank accounts, companies' client files or election lists and records). It has pointed out that "[d]eleting or tampering with essential civilian data can "cause more harm to civilians than the destruction of physical objects."[109] Although it recognizes that the question of whether data can constitute a civilian object remains unresolved, the ICRC has suggested that IHL should do so or otherwise face a large "protection gap" inconsistent with IHL's object and purpose. The seventh question sought Member State views on this important issue.

48. None of the States that responded to this question took the position that civilian data is directly subject to the principle of distinction in armed conflict. Indeed, several States emphasized the principle of distinction without offering an opinion on the status of data as an object.[110] Chile's response suggested, however, that the principle of distinction could apply to cyber operations against data indirectly based on the knock-on effects of such operations. It cited the Commentary to API for the idea that objects must be "visible and tangible" which means that "under current international humanitarian law the aforementioned data would not qualify as objects, in principle, because they are essentially intangible, without prejudice to the physical elements containing the data—hardware, for example."[111] At the same time, Chile emphasized that "an attack directed exclusively at computer data could well produce adverse consequences affecting the civilian population," citing as an example the possibility of a cyber operation eliminating a State's social security database.[112] It concluded that "[t]he principle of distinction must therefore be taken into consideration in the context of cyber operations, whereby a state should refrain from attacking data in case it could affect the civilian population, unless such data are being used for military purposes."[113] Guyana's response adopted a similar lens. Noting that "the deletion, suppression, corruption of data may have far reaching consequences," it focused on the effects of the cyber operation rather than whether the data targeted qualified as an object or not.[114]

49. Peru's response did not address the potential of data to qualify as a civilian object, but focused

---

[107] *Tallinn 2.0*, *supra* note 14, at 437.
[108] *Id.* at 416.
[109] ICRC Position Paper, *supra* note 14, at 8; *accord* 2019 ICRC Report, *supra* note 14, at 21 ("Moreover, data have become an essential component of the digital domain and a cornerstone of life in many societies. However, different views exist on whether civilian data should be considered as civilian objects and therefore be protected under IHL principles and rules governing the conduct of hostilities. In the ICRC's view, the conclusion that deleting or tampering with essential civilian data would not be prohibited by IHL in today's ever more data-reliant world seems difficult to reconcile with the object and purpose of this body of law. Put simply, the replacement of paper files and documents with digital files in the form of data should not decrease the protection that IHL affords to them."); 2015 ICRC Report, *supra* note 14, at 43.
[110] *See* Bolivia Response, *supra* note 19, at 5-7; Ecuador Response, *supra* note 19, at 2; Guatemala Response, *supra* note 19, at 3.
[111] Chile Response, *supra* note 19, at 4.
[112] *Id.*
[113] *Id*.
[114] Guyana Response, *supra* note 19, at 4 ("As it relates to data…regard should be had to whether the cyber operation that targets data has produced such a loss of functionality that it may constitute an attack").

(affirmatively) on its potential to qualify as a military objective. It characterized certain "data" (*e.g.*, software allowing troop communications in the field, synchronization of a missile arsenal or location of enemy aircraft) as lawful "military objectives" while suggesting other data systems used in conflicts (*e.g.*, "a data system that enabled the operating room of a field hospital treating war wounded or civilians to function") were not subject to attack.[115]

Question 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?

50. Sovereignty is undoubtedly the core architectural feature of the current international legal order, providing States with both rights and responsibilities.[116] Sovereignty serves as a foundational principle for some of the international legal rules already mentioned (*e.g.*, the prohibition on the use of force, the right of self-defense, State responsibility). Moreover, in certain contexts, sovereignty exists as more than a background principle, as an independent rule directly regulating State behavior (*i.e.*, a foreign aircraft entering another State's airspace without permission violates its sovereignty).[117] It is not yet clear, however, whether sovereignty operates as a rule in cyberspace. *Tallinn Manual 2.0* indicated that it constitutes a rule that operates to constrain a State's cyber operations that do not rise to the level of a use of force or constitute a prohibited intervention.[118] In 2018, however, the U.K. Attorney General took the view that sovereignty was a principle that informed other rules not a rule of international law itself.[119] Since then, the French Ministry of Defense and the Dutch government have both expressed support for sovereignty as a stand-alone rule.[120]

---

[115] Peru Response, *supra* note 19, at 6. Peru explained that attacks in the first case could cause significant military harm to opposing forces while an attack on the data in the field hospital would "not create a legitimate military advantage." *Id.*

[116] *Island of Palmas (Netherlands v. United States of America)*, 2 R.I.A.A. 829, 839 (1928) ("Sovereignty in the relations between States signifies independence. Independence in regard to the portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State. . . . Territorial sovereignty, as has already been said, involves the exclusive right to display the activities of a State. This right has as corollary a duty: the obligation to protect within the territory the rights of other States, in particular their right to integrity and inviolability in peace and in war.").

[117] *See, e.g.,* Michael N. Schmitt and Liis Vihul, *Respect for Sovereignty in Cyberspace,* 95 TEXAS L. REV. 1639, 1640 (2017). In addition to Article 2(4)'s prohibition on the use of force, there is widespread agreement on a duty of non-intervention in international law that is applicable to cyberspace. *See, e.g., Case Concerning Armed Activities in the Territory of the Congo (Democratic Republic of the Congo v. Uganda)* (Jurisdiction and Admissibility) [2006] ICJ Rep. 6, [46]-[48]; *Nicaragua Case*, *supra* note 43, at ¶205; Declaration on Principles of International Law concerning Friendly Relations & Co-operation among States, UNGA Res. 2625 (XXV), U.N. Doc. A/RES/25/2625 (Oct. 23, 1970). The 2015 UN GGE endorsed it among the applicable rules of international law in cyberspace. 2015 GGE Report, *supra* note 2, ¶¶26, 28(b). And Rule 66 of *Tallinn 2.0* posits that "A State may not intervene, including by cyber means, in the internal or external affairs of another State." *Tallinn 2.0, supra* note 14, at 312. As with the use of force, however, questions remain about how this duty operates in cyberspace and what cyber operations it prohibits or otherwise regulates.

[118] *Tallinn 2.0, supra* note 14, Rule 4 ("A State must not conduct cyber operations that violate the sovereignty of another State.").

[119] *See, e.g.,* U.K. View*, supra* note 8 ("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.").

[120] *See* French Ministry of Defense Views*, supra* note 11, at 6 ("Any unauthorised penetration by a State of French systems or any production of effects on French territory via a digital vector may constitute, at the least, a breach of sovereignty"); the Netherlands Views, *supra* note 12, Appendix, at 2 ("According to some countries and legal scholars, the sovereignty principle does not constitute an independently binding rule of international law that is

51. The eighth question sought to solicit Member State views on the question of sovereignty-as-principle versus sovereignty-as-rule. It was focused on the constraining function of sovereignty, *i.e.*, whether and how it limits a State's ability to conduct cyber operations outside of its territory. Interestingly, many of the responding States took the question as an invitation to reaffirm sovereignty's enabling function – *i.e.*, according State's authority to regulate ICTs within their own territorial jurisdiction. Bolivia and Guyana, for example, both cited sovereignty as authorizing States to exercise jurisdiction over cyber infrastructure or activities in their territory.[121] Ecuador, in contrast, cast doubt on the ability of States to exercise their sovereignty in cyberspace given its "intangible" characteristics, while affirming States do have sovereignty over "Cyber infrastructure" and activity related to that infrastructure in their territory.[122] Chile and the United States also echoed the power sovereignty accords States over ICTs in their territory, but noted that this power must operate within limits. Both cited the need for States to exercise their sovereignty consistent with international human rights law.[123]

52. On the question of whether sovereignty operates as a stand-alone rule in cyberspace, three States—Bolivia, Guatemala, and Guyana—affirmed its status as such.[124] Guyana, for example, indicated that sovereignty protections are "not limited to activities amounting to an unjustified use of force, to an armed attack, or to a prohibited intervention."[125] Thus, it took the view that a State "must not conduct cyber operations that violate the sovereignty of another State" with the existence of such violations depending on "the degree of infringement and whether there has been an interference with government functions."[126] Guatemala adopted a similar stance, indicating that "a State participating in a specific cyber operations violates a country's sovereignty if, in the course of a cyber attack, it takes certain information from another State's cyber realm, even when no harm that could affect equipment or the human rights of a person or persons is caused."[127]

53. Other State's responses where quite equivocal. Peru simply cited sovereignty as "one of the fundamental pillars of international society" without opining on its status as an independent rule.[128] Ecuador suggested that the "rule" authorizing States to control their own cyber infrastructure "does not prevent a state from engaging in cyber operations" without offering an opinion on whether it might regulate how they do so vis-à-vis other sovereign States.[129]

---

separate from the other rules derived from it. The Netherlands does not share this view. It believes that respect for the sovereignty of other countries is an obligation in its own right, the violation of which may in turn constitute an internationally wrongful act."). A recent scholarly treatment questions if France clearly falls in the sovereignty-as-rule camp. *See* Corn, *supra* note 11 ("although the MdA does state that cyberattacks, as it defines that term, against French digital systems or any effects produced on French territory by digital means may constitute a breach of sovereignty in the general sense, at no point does it assert unequivocally that a violation of the principle of sovereignty constitutes a breach of an international obligation. To the contrary, obviously aware of the debate, the document is deliberately vague on this point and simply asserts France's right to respond to cyberattacks with the full range of options available under international law...").

[121] Bolivia Response, *supra* note 19, at 5-7; Guyana Response, *supra* note 19, at 5.

[122] Ecuador Response, *supra* note 19, at 2.

[123] Chile Response, *supra* note 19, at 4-5 (recognizing sovereignty authorizes protection and defense of a State's "critical information infrastructure" as long as those sovereignty based measures "do not violate the rule of international law – for example, those contained in international human rights law or international humanitarian law."); 2014 US GGE Submission, *supra* note 7, at 737-8 (noting that the exercise of jurisdiction of a territorial State "is not unlimited; it must be consistent with applicable international law, including international human rights obligations" and citing, in particular freedom of expression and freedom of opinion).

[124] Bolivia Response, *supra* note 19, at 5-7; Guatemala Response, *supra* note 19, at 3; Guyana Response, *supra* note 19, at 5.

[125] Guyana Response, *supra* note 19, at 5.

[126] *Id.*

[127] Guatemala Response, *supra* note 19, at 3.

[128] Peru Response, *supra* note 19, at 6-7.

[129] Ecuador Response, *supra* note 19, at 2.

54. Chile's response described sovereignty as a "principle" that "States carrying out cyber operations must always take … into account."[130] Thus, "every time a state considers carrying out a cyber-operation, it must consider ensuring it does not affect the sovereignty of another."[131] The use of "principle" may suggest something other than a concrete rule, although the use of "must" creates more obligatory expectation. Moreover, Chile did suggest that:

> every state has an obligation to respect the territorial integrity and independence of other states and must faithfully discharge its international obligations, including as regards the principle of nonintervention. Cyber operations that hinder another state from exercising its sovereignty therefore constitute a violation of that sovereignty and are prohibited under international law.[132]

The last sentence suggests sovereignty might constitute a stand-alone rule unless one reads the reference to intervention with another State's exercise of sovereignty as equivalent to the *domaine reservé* protected by the duty of non-intervention.[133]

55. The U.S. position is murkier. In 2014, then-legal adviser Harold Koh indicated that "State sovereignty . . . must be taken into account in the conduct of activities in cyberspace, including outside of the context of armed conflict."[134] It's not clear, however, whether taking "State sovereignty . . . into account" signals U.S. recognition of sovereignty as a standalone rule. In his own speech in 2016, then-Legal Adviser Brian Egan made clear that "remote cyber operations involving computers or other networked devices located on another State's territory do not constitute a per se violation of international law."[135] At the same time, he conceded that '[i]n certain circumstances, one State's non-consensual cyber operation in another State's territory could violate international law, even if it falls below the threshold for the use of force." In any case, Egan indicated 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, and it is one that ultimately will be resolved through the practice and opinio juris."[136] Most recentl recently, however, the General Counsel for the U.S. Department of Defense indicated that "[f]or cyber operations that would not constitute a prohibited intervention or use-of-force [i.e., those that might be covered by a rule of sovereignty], the Department believes there is not sufficiently widespread and consistent State practice resulting from a sense of legal obligation to conclude that customary international law generally prohibits such non-consensual cyber operations in another State's territory."[137] It is unclear, however, how widely shared this view is across the U.S. government as a whole.

Question 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?

---

[130] Chile Response, *supra* note 19, at 5.
[131] *Id.*
[132] *Id.*
[133] *See* note 117.
[134] Koh, *supra* note 7, at 596: *Accord* 2014 US GGE Submission, *supra* note 7, at 737; 2016 US GGE Submission, *supra* note 7, at 825.
[135] Egan, *supra* note 7, at 818. Among other things, Egan indicated that the United States does engage in intelligence collection activities overseas and that such activities may violate the domestic laws of other States, but that there is no "per se prohibition on such activities under customary international law." *Id.*
[136] *Id.* at 819.
[137] *See* Paul C. Ney, "DOD General Counsel Remarks at U.S. Cyber Command Legal Conference, March 2, 2020, at https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/.

56. Due diligence is a principle of international law that requires a State to respond to activities that it knows (or reasonably should know) have originated in its territory or other areas under its control and that violate the right(s) of another State.[138] It is an obligation of effort, not result – where a State knows or should know of the conduct, it must employ "all means reasonably available" to redress it.[139] As a principle, due diligence currently regulates State behavior in a number of contexts, most notably international environmental law, where it is the basis for requiring States to stop pollution in their territory that serves as a source for transboundary harm to other States' territories.

57. Like sovereignty, there are competing views on whether due diligence is a requirement of international law in cyberspace. The 2015 UN GGE report listed it among the "voluntary" norms of responsible State behavior rather than listing it under applicable international law principles.[140] Several States, including France and the Netherlands, have characterized it as a legal rule in cyberspace.[141] In doing so, however, the Netherlands noted that "not all countries agree that the due diligence principle constitutes an obligation in its own right under international law" and the United States is widely thought to be among those contesting its status as such.[142] The ninth question thus sought to obtain Member State views on the status of due diligence with respect to a State's obligations under international law in cyberspace.

58. Chile, Ecuador, Guatemala, Guyana, and Peru all took the position that the due diligence principle is a part of the international law that States must apply in cyberspace.[143] As Chile explained, "[f]rom a cyber-operations standpoint, a state must exercise due diligence to prevent its sovereign territory, including the cyber infrastructure under its control, from being used to carry out cyber operations that affect another state's rights or could have adverse consequences for them."[144] Guatemala adopted a similar stance, while noting that since "cyberspace" is such a broad term, performing due diligence can be extremely complicated.[145] Still, to the extent due diligence "derives from the principle of sovereignty," Guatemala opined that "each State should exert the control necessary to halt all harmful activities within its territory and be obliged to take preventive measures, establish a CERT, adopt information security policies, and raise awareness about information security."[146]

---

[138] *See, e.g., Corfu Channel Case; Assessment of Compensation (United Kingdom v. Albania)* [1949] ICJ Rep. ¶22 (April 9). *Trail Smelter Case* (United States-Canada), UNRIAA, vol. III, 1905 (1938, 1941).

[139] *See Application of the Convention on the Protection and Punishment of the Crime of Genocide (Bosnia v. Serbia)* (Judgment) [2007] ICJ Rep. 1, ¶430.

[140] 2015 UNGGE, *supra* note 2, ¶¶13, 26-28.

[141] French Ministry of Defense Views, *supra* note 11, at 10 ("Under the due diligence obligation, States should ensure that their sovereign domain in cyberspace is not used to commit internationally unlawful acts. A State's failure to comply with this obligation is not a ground for an exception to the prohibition of the use of force, contrary to the opinion of the majority of the Tallinn Manual Group of Experts."); The Netherlands Views, *supra* note 12, Appendix, at 4 ("the due diligence principle requires that states take action in respect of cyber activities: - carried out by persons in their territory or where use is made of items or networks that are in their territory or which they otherwise control; - that violate a right of another state; and - whose existence they are, or should be, aware of"). Although it did not describe due diligence as a specific rule of international law, Estonia has catalogued its contents as a requirement for State behaviour. Estonia Views, *supra* note 10 ("states have to make reasonable efforts to ensure that their territory is not used to adversely affect the rights of other states. They should strive to develop means to offer support when requested by the injured state in order to identify, attribute or investigate malicious cyber operations. This expectation depends on national capacity as well as availability, and accessibility of information.").

[142] The Netherlands Views, *supra* note 12, Appendix, at 4.

[143] Chile Response, *supra* note 19, at 6-7; Ecuador Response, *supra* note 19, at 2; Guatemala Response, *supra* note 19, at 4; Guyana Response, *supra* note 19, at 5; Peru Response, *supra* note 19, at 7.

[144] Chile Response, *supra* note 19, at 6-7. Ecuador simply stated: "due diligence is applicable to what happens with technological resources within national territory." Ecuador Response, *supra* note 19, at 2.

[145] Guatemala Response, *supra* note 19, at 4.

[146] *Id.* at 2, 4.

59. Bolivia offered a more equivocal response. Without opining one way or another on the legal status of due diligence, it did opine that a State may not be held responsible for a cyber-attack when it lacks technological infrastructure to control a non-State actor.[147] This view could be consistent with having due diligence as an international legal rule for cyber operations as due diligence generally has required States to "know" about the activities in question, which may not be possible for States lacking the requisite technical infrastructure.[148] On the other hand, the inability to "control" cyber activities of which it has knowledge might suggest Bolivia does not accede to the due diligence doctrine in cyberspace. Without further clarification of Bolivia's response, it is difficult to reach a conclusion one way or another.

60. Similarly, prior public U.S. statements have not addressed the international legal status of due diligence directly. It is notable, however, that the United States has tended to describe any obligations to respond to requests for assistance in non-binding terms.[149] The lack of any public U.S. endorsement of due diligence as a legal rule in either the GGE context or elsewhere may be indicative of U.S. doubts as to its legal status.

Question 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?

61. The final, tenth, question invited States to identify additional areas of international law on which the Committee should focus improving transparency in the cyber context. Responses focused on different issues. Bolivia called for more attention to protecting people's "fundamental rights" wherever they operate, including in cyberspace.[150] Several other responses focused on cybercrime, particularly the Council of Europe's Budapest Convention.[151] Others emphasized the contributions of the *Tallinn Manuals*.[152]

62. Two States – Ecuador and Guyana indicated that there may be a need for new international law in the cyber context. Ecuador emphasized establishing how "to regulate attacks against military and/or civilian targets that affect the huge sections of the population, such as the case of critical infrastructure, hospitals, public transportation, and other infrastructure affecting state security."[153] Guyana suggested that "it might be prudent to have a set of international law principles that are tailored to the special nature of cyberspace," noting that existing legal principles were developed for a different time and context.[154]

* * *

63. With the Committee's approval, I would propose publication of my report (and the responses) so that States, both inside the region and across the globe may benefit from the positions and views expressed herein. It would also be an opportunity to seek additional views from States that have yet to respond to the questionnaire.

---

[147] Bolivia Response, *supra* note 19, at 3-7.
[148] See *Tallinn 2.0*, *supra* note 14, at 40.
[149] 2014 US GGE Submission, *supra* note 7, at 739 ("A State *should* cooperate, in a manner consistent with domestic law and International obligations, with requests for assistance from other States in investigating cybercrimes, collecting electronic evidence, and mitigating malicious cyber activity from its territory.").
[150] Bolivia Response, *supra* note 19, at 6-7.
[151] Guatemala Response, *supra* note 19, at 4; Bolivia Response, *supra* note 19, at 6-7.
[152] Costa Rica Response, *supra* note 19, at 2 (emphasizing Costa Rican interest in joining the Budapest Convention); Guatemala Response, *supra* note 19, at 4 (citing the Budapest Convention).
[153] Ecuador Response, *supra* note 19, at 3.
[154] Guyana Response, *supra* note 19, at 5-6 (emphasizing anonymity as a particular challenge to applying existing law).

64. As always, I would also welcome the Committee's views and reactions to the responses received to date and whether it would be worthwhile to seek additional responses. I would further welcome Committee feedback on how we might address the uneven technical and legal capacities this project has identified.

65. Finally, I would value Committee input on the next steps, if any, for this project. On the one hand, I could simply receive feedback from Member States on this report and revise it as necessary prior to its final approval. Alternatively, I could attempt in my next report to expand the analysis, whether by adding in additional Member State responses, or (if none of those are forthcoming), comparing Member State views with the views of States outside the region. Increasingly, there is greater evidence of State views than in the past and it could be useful to compare those views to the responses surveyed here. Or, should the project retain its original focus and attend only to the transparency of OAS Member States on questions of international law's application to cyber operations?