Informal Multi-stakeholder Cyber Dialogue

INTERNATIONAL LAW
04 December
SESSION REPORT

GENERAL SUMMARY

There were a total of 286 participants who joined the event from Zoom and the Livecast including government representatives, non-governmental organisations, academia, and private sector stakeholders. The Livecast attracted viewers from 28 countries and 41 cities around the world.

SESSION OUTLINE

Takeshi Akahori (co-chair, Ministry of Foreign Affairs of Japan) kicked off the session with an explanation of the content of the 2013 and 2015 GGE consensus reports and of the pre-draft report under consideration by the OEWG on applicability of international law in cyberspace. He particularly highlighted language in the pre-draft concerning state responsibility, self-defense and international humanitarian law.

Dapo Akande (co-chair, Oxford University) set the scene of the session by explaining (i) how as a general matter international law applies to the activities of States and non-state actors in cyberspace; and (ii) attempts to clarify - outside the UN processes - the applicable international law rules. On (i) he mentioned why it is that international law applies by default to state activity whether in cyberspace or elsewhere as well as how international law applies to activities of non-state actors, focusing on rules of attribution and the due diligence obligation of States to prevent harmful cyber activities by non-state actors. On (ii) he mentioned the Tallinn Manual and the recent work that Oxford and others have been engaging in to clarify the rules with regard to particular types of harmful cyber operations.

Marietje Schaake (Cyber Peace Institute) indicated that while cyberattacks often stay below the thresholds of intervention or armed conflict, creating ambiguity, there is a wide range of laws and rights that might be at stake below those thresholds, including human rights, non-proliferation, counterterrorism, crime fighting, etc. Introducing the work of the Cyber Peace Institute, she stressed that enough information in the public domain was necessary for accountability to become the goal. She thought that in addition to the United Nations, groups of like-minded nations could work together for example on the rule of law principles and look at how they could crack some politically sensitive issues. She also recognized the need to build capacity and institutions for attribution.

Liis Vihuul (Cyber Law International) pointed out that the international community has had an expectation that countries would start articulating what kind of practical implementation of the international law, rights and obligations can and should be expected of States in the cyber context but that progress was modest. She believed that international peace and security would be better served if countries would be more willing to accept that international law provides substantial prior restrictions that take off the table, certain types of cyber operations. With regard to States that feel that the international legal debate lacks inclusivity, in part because

those countries do not have the capacity to fully and meaningfully participate in the international negotiations concerning international law, she said that to a great extent, “the ball was in their court” because in many countries there was room for improvement with regard to internal coordination.

Harriet Moynihan (Chatham House) suggested that to make progress in discussions on how international law applies, more States needed to put on record their views on how particular principles of international law apply, where possible with reference to concrete examples. She gave a few examples of areas on which it would be good to have States' views. Those areas were non-intervention (could interference in elections, cyberattack on medical facilities constitute intervention and was the victim state entitled to take countermeasures?), peaceful settlement of disputes (do the Security Council and the ICJ provide a basis?).

Tilman Rodenhäuser (ICRC) recalled that international humanitarian law (IHL) applies to cyber operations during armed conflict. On the pre-draft under consideration in the Open-Ended Working Group he said that ICRC attaches great importance to some of the statements or the findings, including that “IHL reduces risk and potential harm to both civilians and combatants in the context of armed conflict”, and that “IHL neither encourages the militarization nor legitimizes resort to conflict in any domain.” (paragraph 29), and that there is a need to fully clarify questions relevant to how the principles of IHL, such as principles of humanity, necessity, proportionality, distinction and precaution apply to ICT operations in the context of an armed conflict (paragraph 32). ICRC believed that finding agreement among States on how international law, including IHL, restrict cyber operations during armed conflict is of utmost importance. He encouraged States to deepen their discussions on how IHL applies in cyberspace and indicated that the ICRC and other multi-stakeholder entities were available to contribute to these discussions as needed.

Jan Neutze (Microsoft) recalled that the first United Nations organized multi-stakeholder meeting on trust and security in cyberspace held a year ago in New York in the context of the Open-Ended Working Group which included a formal role for non-state organizations to contribute to the discussions was a remarkable milestone. He explained that since then there were a number of additional positive steps such as the UN Secretary General’s Roadmap on Digital Cooperation, the increase in organizations endorsing the Paris Call for trust and security in cyberspace which was originally adopted in 2018, and the Oxford University research project and its three statements. He emphasised that governments need to be the ones that that agree on norms and apply them with data and other input from companies and that the world in many ways is running out of time before offensive cyber capabilities are applied against a critical infrastructure target and will cause significant impact and consequences. He urged all digital citizens to get involved.

The above statements were followed by active interaction with other participants. Issues raised included the importance of publishing national position papers, how to maintain a peaceful cyberspace, cyberattacks on medical facilities and IP theft on medical research projects, whether disinformation constitutes intervention, criminal responsibility of non-state actors under international law, the right of taking collective countermeasures.

MAJOR THEMES / AREAS OF CONVERGENCE

As affirmed in the 2013 and 2015 GGE reports, international law applies in cyberspace. The ongoing OEWG and GGE are expected to further clarify how international law applies in cyberspace. At the same time, considering that there is a realistic limit to what can be agreed

by States in the OEWG and GGE, efforts by like-minded countries or discussions involving the multi-stakeholder community are also important. Academia also plays an important role in such discussions and can provide in-depth studies and research.

States are urged to publish their position papers on how international law applies in cyberspace. Differences in national positions on how international law applies in cyberspace will not harm the common understanding that international law applies in cyberspace.

Civil society has an important role to play in discussions concerning how international law applies, including by providing data and examples.

AREAS FOR FURTHER DISCUSSION

Is there a need to establish an international attribution mechanism? Could existing mechanisms including the Security Council and the International Court of Justice be used in disputes involving cyber activities?

RECOMMENDATIONS

The OEWG report should devote some lines to the impact of the COVID-19 pandemic on discussions related to application of international law in cyberspace.