Informal Multi-stakeholder Cyber Dialogue

REGULAR INSTITUTIONAL DIALOGUE
09 December 2020
SESSION REPORT

GENERAL SUMMARY

The United Nations' Open-ended working group (OEWG) on developments in the field of information and telecommunications in the context of international security has provided UN Member States with an open and inclusive forum to discuss international cybersecurity. Identifying a regular mechanism to continue dialogue on this subject is an urgent priority and may represent one of the OEWG's most significant outcomes.

This session, co-organised by France, Egypt, Women's International League for Peace and Freedom (WILPF), and Kaspersky, invited discussion and inputs from non-governmental stakeholders on the topic of regular institutional dialogue (RID). The main purpose was to discuss different possible types of frameworks and institutional settings in which the global community can continue to address threats associated with the use of information and communications technologies (ICTs) in the context of international security and peace, including with a possible of meaningful engagement and participation by relevant non-governmental stakeholders.

The session attracted a broad participation of 150 people who joined the event from Zoom and the Livecast. The Livecast attracted viewers from 17 countries and 32 cities around the world.

SESSION OUTLINE

Brief opening remarks were provided by representatives of the four co-organisers: Bassem Hassan, Counsellor, Permanent Mission of Egypt to the United Nations; Allison Pytlak, Programme Manager, WILPF; Henri Verdier, Ambassador, Digital Affairs, Ministry for Europe and Foreign Affairs, Government of France; and Anastasiya Kazakova, Public Affairs Manager, Kaspersky.

The session was moderated by Camille Morfouace-de Broucker, Ministry for Europe and Foreign Affairs, France.

A set of guiding questions was distributed in advance in order to inform the contributions of participants. The questions were organised under two themes: Ideas for a regular Institutional Dialogue; and Stakeholder participation—lessons learned and challenges.

Following the opening remarks, participants were invited to respond to a Mentimeter poll that asked, "What topics should future regular institutional dialogue aim to cover?" Participants could select multiple responses from the answers provided.

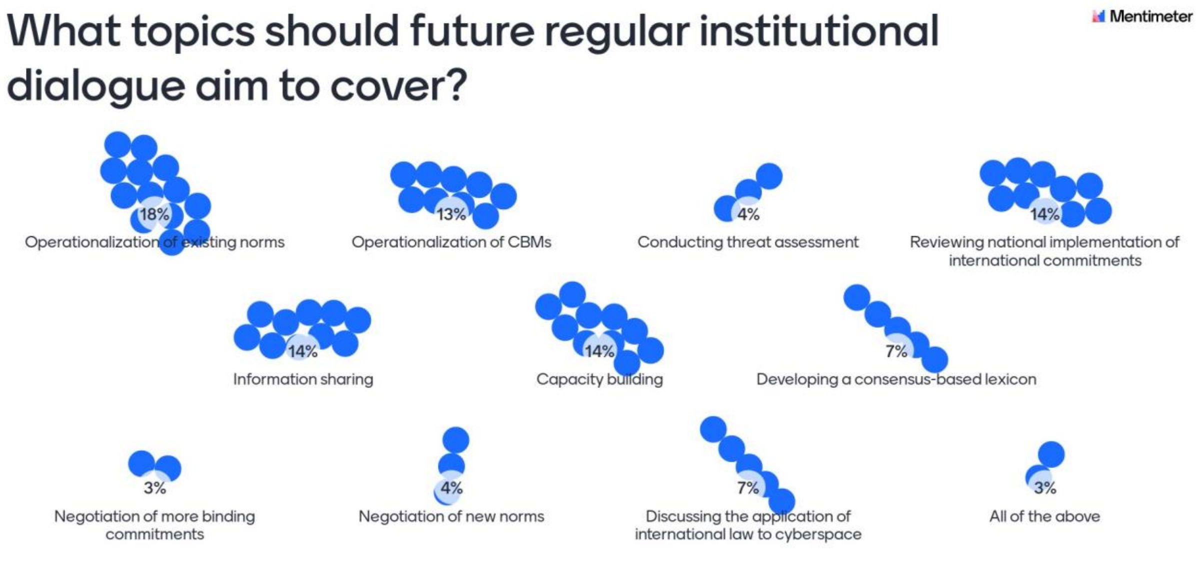
The moderator then opened the floor for discussion and questions. Some participants asked questions of the speakers while others took the floor to express views and/or positions on key themes. These questions and points were either conveyed through the chat function, including by individuals watching the livestream, or asked directly on video. Toward the end of the session, Ms. Kazakova shared the results of the poll. They are presented in the next section of this summary.

MAJOR THEMES / AREAS OF CONVERGENCE

As noted by the panellists of Egypt and France, there is growing convergence among UN Member States around five key characteristics that future RID should account for: (i) be inclusive, i.e. allowing all countries to participate and contribute; (ii) be regular with a timetable for the meetings; (iii) be institutional with clear points of reference and rules of procedures; (iv) be consensus-driven to ensure universality of a platform and adherence to its outcomes; and (v) be action-oriented in order to move further to practical outcomes after several years of discussion of key theoretical and fundamental principles.

All participants who spoke during the session, as well as the panellists, seem to agree on two important topics for future RID to focus on: ***national implementation of previously agreed non-binding norms*** (including the monitoring and reviewing the national implementation efforts) and ***capacity-building*** (for ensuring that the UN Member States have enough capacity for norm implementation). The panellists all emphasised the importance of transparency and inclusivity. There was also wide acknowledgement that ***multi-stakeholder participation*** plays a crucial role in the operationalisation of norms and confidence-building measures (CBMs) as states cannot alone achieve international security and peace in relation to the use of ICTs. However, it was noted that the current set-up of the OEWG does not always allow for non-governmental actors to meaningfully participate and support the discussions between UN Member States. Therefore, it is important for the future dialogue to move from discussions on 'if' the multi-stakeholder engagement is possible to 'how' this can be organised.

The poll results reflect the views of the speakers:


What topics should future regular institutional dialogue aim to cover?

However, roles are different within the international community, both between governments and non-governmental stakeholders, but also among different stakeholder groups. Particularly, the private sector and industry, as noted by Kaspersky, seems essential in the operationalisation of norms related to critical infrastructure protection, ensuring the integrity of supply chains, responsible reporting of vulnerabilities, and discussing cooperative mechanisms for a global response in the event of a significant cyber incident or attack. The role of the civil society, as stressed by WILPF and many participants, is to bring forward the voices of those that are affected by the issue as well as bring those stakeholders who have the necessary expertise for the discussions. WILPF shared examples of how non-governmental stakeholders engage and participate in other multilateral and UN fora on international security issues.

Finally, as expressed by all panellists, it is time to achieve more practical outcomes. In this regard, a proposal that is now cosponsored by 47 UN Member States and supported by many other Member States to establish a Programme of Action[1] (PoA) has been initiated by the delegations of France and Egypt. This proposal was discussed as an instrumental way for RID that can move UN discussions on international cybersecurity forward. To a question from one non-governmental participant on how the PoA can be implemented practically, the panellists from Egypt and France explained that there is currently a lack of knowledge about national implementation of the UN cyber norms which makes such a PoA a unique opportunity to monitor implementation and identify the gaps in implementation, the normative base, and capacity. As one possible option for a standardised reporting template, national implementation could be also conducted through the national survey, such as proposed by Mexico and Australia during OEWG discussions.[2] In the chat, one governmental participant shared that it and another Member State have submitted to the OEWG an overview of how each country implements the norms. France also noted that for the future RID, although implementing the cyber norms is crucial, reaching a global treaty is not a priority as the discussion of the treaty only hinders the actual implementation of norms and having one treaty only would hardly allow to face the multitude issues in cyberspace.

Some questions and remarks from participants raised issues that may require further consideration, elaboration, or work. Some examples include: how to gain support for a PoA from countries like Russia, China, and the United States; how the timeline to potentially negotiate and adopt a PoA will align with the forthcoming (second) OEWG, as well forums like the Internet Governance Forum (IGF) and the Paris Call; what a PoA can do to guard against the militarisation of cyber space and avoid becoming an instrument that regulates cyberwarfare; accounting for the lack of an attribution framework; if the UN is the best place to coordinate cyber capacity-building; and what specific modalities are needed to ensure *meaningful* participation of non-governmental stakeholders.

RECOMMENDATIONS

The following points reflect substantive suggestions and recommendations made by panellists or the participants in the course of written or spoken comments and questions. They do not constitute formal recommendations, unless presented as such.

From organisers/panellists:

- Be inclusive of all UN member states and allow for meaningful participation by non-governmental stakeholders. Openness and transparency are important considerations. This was emphasised variously by all panellists.

[1] *The future of discussions on ICTs and cyberspace at the UN*, https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-the-future-of-cyber-discussions-at-the-un-10302020.pdf.

[2] *Joint Proposal*, 16 April 2020, https://front.un-arm.org/wp-content/uploads/2020/04/final-joint-oewg-proposal-survey-of-national-implementation-16-april-2020.pdf.

- It’s time for action-oriented dialogue and/or processes, and a move away from deliberative processes like Groups of Governmental Experts and the OEWGs on theoretical and fundamental questions. These types of fora are not designed to take the kind of action that is needed on this issue at this juncture, such as reviewing or monitoring national implementation of the UN cyber norms, as one example. Additional thematic tracks of work could potentially be based on those that have been established within other initiatives such as the Paris Call.
- A global framework is needed, to pull together and give impetus to what exists regionally, or otherwise.
- Learn from good practices in non-governmental engagement in other international security fora. This includes modalities that enable stakeholders to engage in real-time, rather than in a single allocated session; enable space for side events or expert panels; and agree on standing rules for participation, as part of rules of procedure.
- Continue working on the consensus-based guidance for the implementation of the previously agreed norms (including norms on critical infrastructure protection, supply chain integrity, and responsible reporting of vulnerabilities); resolve questions about what a “cyber conflict” is, among other key concepts; and develop a consensus-based lexicon including on dispute-settlement, despite the challenges of doing so.
- Learn from other PoAs and their implementation. For example, they can eventually lead to legal instruments if needed; they can bring a diverse patchwork of existing regulations under one umbrella; and national implementation needs to be the priority.

From participants:

- The forum created by the PoA could serve for consultation and provide a dispute settlement mechanism, but to do so in a timely way it would have to be able to convene as required and not just in an annual meeting. The PoA could also evolve into a UN Cyber Security Committee, supported by a UN Office of Cyber Affairs.

- It was noted that the Human Rights Council’s Universal Periodic Review (UPR) process, which is comprised of state reports and independent review, provides an interesting model for promoting and supporting implementation of agreed norms, even those that are “voluntary and non-binding” such as those contained in the 2015 GGE report. The PoA could consider developing a similar mechanism as a result, or part, of the PoA, such as one non-governmental participant has already proposed.

- It was asked if the PoA could establish a mechanism for emergency and current risks, such as the current threats to a vaccine supply chain, for example. The same participant noted that this would not need be like the UN Security Council, but more operational.

- A participant wrote that a programme of work is needed, rather than a programme of action. This participant encouraged reaching a balanced normative framework and common understanding on how international law applies; after which a legally binding framework is needed “to achieve real accountability and legal deterrence.”

- One participant suggested that the PoA should also report progress to the IGF throughout the year.

- It was suggested to establish a “committee of peaceful digital space in United Nations to develop [an] international treaty on Data, Governance, Security, Crime” which could be modelled on the International Civil Aviation Organization or inspired by the

UN Convention on the Law of the Sea or the Committee on the Peaceful Uses of Outer Space (COPUOS).

- While this dialogue series is important, it shouldn't become the norm for non-governmental stakeholders and supportive governments to organise dialogue opportunities outside of what is happening at the UN in order to be involved in the discussions. Such dialogue should be institutionalised in any future mechanism.
- Make space for the technical community. This community makes not only attribution possible, but other cyber security assurances too. As well, the PoA should bear in the mind the cadence of what regional organisations are already doing—how can meetings of regional organisations facilitate aspects of what the PoA eventually includes, for example.
- Remember that the participation of the technical community and industry is a "two-way street." This community can provide insights on new threats and techniques, but it can also gain information from these conversations about how technology is being used and misused in different contexts around the world.