Informal Multi-stakeholder Cyber Dialogue

RULES NORMS AND PRINCIPLES

07 December

SESSION REPORT

GENERAL SUMMARY

There were a total of 319 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 22 countries and 32 cities around the world.

SESSION OUTLINE

The session opened with a scene setter by Sirine Hijal and Daniel McBryde of Global Affairs Canada (GAC). Sirine Hijal presented the 11 norms of State behaviour in cyberspace agreed by the UN Group of Governmental Experts (GGE) in its 2015 report. Dan McBryde then outlined the 2016-17 GGE draft text on norms and Canada's proposed norms guidance text at the current OEWG.

The scene setting remarks were followed by statements by Sheetal Kumar, Global Partners Digital (GDP) and Veronica Ferrari, Association for Progressive Communications (APC) made on behalf of stakeholders who submitted input to the OEWG on the norms non-paper proposals. GPD and APC's statement emphasized three key comments on the norms text from the joint stakeholder input: a) humans are the ones impacted by state behaviour in cyberspace and therefore a human-centric and rights-based approach to norm implementation is needed 2) cyberspace isn't equal: cyber incidents impact people in a differentiated manner, c) Relevant discussions, including regarding implementation, need to be open, inclusive and transparent.

Nemanja Malisevic shared the industry perspective on the issues at stake. Microsoft's statement reiterated the importance of multistakeholder initiatives and called for a more systematic involvement of all relevant stakeholders. It further invited states to reaffirm the validity of the 11 norms recognized by the 2015 UNGGE in their entirety. It also encouraged states to explain what the implementation of these norms is expected to look like, and stressed that states should strive to turn these politically binding commitments into legally binding rules.

The statements were intended to provide context for the open discussion which followed and which was based on the following four questions:

1. In the non-paper, there is guidance for the implementation of the eleven agreed norms. Are there any elements missing in this guidance?
2. The focus so far in the non-paper is on the 11 agreed norms, but are there other issues that should be considered?
3. What challenges do you see in taking forward the proposals included in the non-paper, including in any of the relevant norms guidance text?

4. With respect to the draft “Norms" section of the OEWG the pre-draft report, are there any notable omissions, additions, or statements with which you support or disagree? (see paragraphs 38-44) In particular, do you think there is sufficient reference to non-governmental stakeholder engagement? If not, how could this be improved?

MAJOR THEMES / AREAS OF CONVERGENCE

- *The implementation of what has already been agreed is of primary importance*: It was widely agreed that there should be no ‘unravelling’ the existing agreed 11 norms. Norms guidance, like that provided by Canada and other states, as well as other stakeholders, is important at this stage for operationalisation of the norms.
- *Inclusivity of stakeholders in the implementation of norms:* the operationalisation of norms should not be ‘top-down’. Stakeholders, including the technical community and civil society, should be involved. For example, they possess information necessary to ensure the stability and security of the internet. Input from all relevant stakeholders should be systematic, rather than ad-hoc.
- *International law and norms are complementary:* Voluntary norms do not affect the obligations states already have under international law; instead the norms and international law are complementary. Implementation of the norms can support state’s compliance with their international legal commitments.
- *Accountability is needed:* When agreed cybernorms are not respected or violated, there currently isn’t sufficient accountability for those who violate the norms. This is important for the implementation of cyber norms; otherwise, the norms fail to have real-world impact without frameworks that ensure they are implemented and not violated. Engaging participants from the multistakeholder in implementation efforts can support those efforts.
- *A human-centric and bottom-up approach should support the implementation of the agreed norms:* as it is humans who are impacted by state behaviour and cyber incidents, it is important for states to ensure that human rights are a core part of norm implementation. The implementation of norms should also take into consideration that cyber incidents impact people in a differentiated way because of existing inequalities. Women, as well as people of diverse sexualities and gender expression, are more often targets of online violence. Increasingly, disinformation campaigns further alienate minority groups.
- *Regional organisations play an important role in norms implementation:* Regional organisations can play a range of roles in supporting norm implementation, including through developing frameworks for implementation that are tailored to regional context and gathering of best practices. They can complement what is being done at the UN/global level. However, in supporting member states to implement cyber norms, they should engage all stakeholders.

Areas for continuing discussion:

- **Norm elaboration:** There was discussion regarding whether the guidance related to norms on critical infrastructure could be further elaborated, specifically to include reference to electoral and health infrastructure. There were different views expressed: some felt that referring to

electoral and health infrastructure would be singling these sectors out, and would therefore give the impression that other sectors should not be understood to be protected in the same way. However, others felt that the inclusion of language such as "including, but not limited to" would be sufficient to ensure that any interpretation of the norms on critical infrastructure would not be limited to specific sectors only. In addition, a question was raised regarding the "public core" norm which has been proposed by the GCSC, how it is perceived and whether it is seen as key to norm implementation.

- **Norm implementation vs a binding agreement**: There was some discussion as to whether the implementation of the norms is sufficient to guide State behaviour in this space, or whether the current framework needs to be supplemented by the elaboration of either a legally binding instrument or additional norms. While there was no agreement on this, a point was made that continuing implementation of the norms could reveal any potential gaps and thereby potentially help identify new norms that may be needed. Some States and participants in the event indicated that they believe that the current framework of law and norms is not sufficient and that a treaty or binding instrument is needed to regulate State behavior in this space, but they recognized that such a treaty is unlikely to be adopted anytime soon, given that a majority of States continue to oppose such an approach.
- **International law thresholds and impact on norm implementation**: A question was raised regarding what thresholds need to be reached for specific elements of international law to apply and how the understanding of what these thresholds are impacts norm implementation. While not discussed in-depth, this could merit further discussion as it could help clarify the interplay between existing agreed norms and international law.

RECOMMENDATIONS FROM STAKEHOLDERS

- States should prioritise the implementation of the existing agreed 11 norms, utilising guidance developed within the OEWG and engage other stakeholders in doing so. However, in doing so, they should not discard the necessity of exploring whether additional norms may be needed at some point or how such norms may be turned into legally binding commitments in the future.
- Mechanisms set up to support implementation of the norms should institutionalise stakeholder engagement, including involvement of the technical community, civil society and industry.
- The OEWG report should include reference to the role of non-governmental stakeholders, including civil society, academia, the technical community and industry, in supporting the implementation of norms, rules and principles.
- The OEWG's report recognises the differential impact of cyber incidents on marginalised groups, but it should further elaborate on these concerns.
- States should consider the links between human rights and cyber norms and comply with their obligations under international human rights law when operationalising cyber norms.