The OEWG First Annual Progress Report: The role and contributions of stakeholders must be recognized across the priority areas

The CyberPeace Institute’s comments on the draft versions of the first annual progress report of the UN Open-Ended Working Group on security of and in the use of information and communications technologies 2021-2025 (OEWG).

The third substantive session of the OEWG will be held from 25 July to 29 July 2022. Resolution 75/240 mandates the OEWG to submit, for adoption by consensus, annual progress reports to the General Assembly. In accordance with this obligation, the Chair published a Zero Draft of the first annual progress report of the OEWG on 22 June 2020¹ as a starting point for the discussions, and a revised draft on 20 July 2022 reflecting on preliminary views expressed by delegation,² with an objective to adopt the progress report by consensus at the end of the substantive session.

The CyberPeace Institute has reviewed the Zero Draft and the revised draft of the first annual progress report and commends the efforts of the Chair and his team for drafting the text. Drawing on the Institute’s Statement on the value of multistakeholder engagement in the OEWG process (2021-2025)³ and recommendations for Member States participating in the OEWG⁴, we would like to bring the following comments into consideration.

Introduction

The CyberPeace Institute appreciates that the role of stakeholders, including businesses, nongovernmental organizations and academia, is mentioned in the Zero Draft and the language is further reinforced in the revised draft. Recalling the extensive discussions on the contributions of the multistakeholder community, the importance of a meaningful stakeholder participation in the OEWG process, as well as any progress made to date on this issue, should be a key focus of the first annual progress report.

The report must address the discussions and negotiations that took place around stakeholder modalities. Modalities are not a mere procedural matter, but they significantly impact the substantive discussions and the ways in which stakeholders interact. The importance of the discussions on this topic, the reason why they arose, and how the matter was settled needs to be

---

reflected in the text to achieve that the report clearly shows the progress — or lack of it — on the issue of stakeholder participation. We therefore welcome that the revised draft stipulates that the OEWG is committed to engaging stakeholders in a systematic, sustained and substantive manner and that different views were expressed on the preferred modalities to be adopted.

While we appreciate the revisions in the draft report, we also note that references to stakeholders’ involvement in the report remain selective and limited and the text does not capture the value of stakeholders’ participation and the ways of engagement sufficiently across all six priority areas. The progress report ought to recognize the full scope and depth of stakeholders’ contribution for the work of OEWG.

Existing and Potential Threats

States previously highlighted the importance of continued exchange on addressing threats to the healthcare sector emanating from cyberspace during the first and the second substantive session of the OEWG. The recognition of this problem needs to be reflected in the progress report. The protection of the healthcare sector from cyber harm is an urgent and essential matter that necessitates cooperation of all relevant stakeholders. In order to understand the impact of cyber threats, the Institute has been studying attacks against the healthcare sector that can help to inform the work of Member States. Reflecting on the practical examples of the bodies of knowledge summarized in the Cyber Incident Tracer #HEALTH and the Addendum to the Strategic Analysis Report ‘Playing with Lives: Cyberattacks on Healthcare are Attacks on


People\textsuperscript{8}, the recommendation of sharing risk assessments and technical information between States, including threat intelligence and compendiums, should be extended to non-state actors.

Threats outlined in the report need to include concerns about the threats of cyberattacks targeting humanitarian organizations, as expressed by States.\textsuperscript{9} The recent submission of the CyberPeace Institute to the OEWG on the protection of the humanitarian sector\textsuperscript{10} illustrates the impact that malicious activities in cyberspace have on humanitarian action. The evidence-based, forward-looking and action-oriented contribution – based on an analysis of 157 cases of cyber incidents that impacted NGOs over the past two years – proposes policy recommendations that inform all relevant areas of the OEWG work and demonstrate the value of stakeholders' participation in the process.

Rules, Norms and Principles of Responsible State Behavior

The importance of exchanging views on the protection of the healthcare sector should be further outlined in the area of norm implementation, while emphasizing stakeholders’ contributions to these discussions. As an example, the CyberPeace Institute, the Government of the Czech Republic, and Microsoft partnered together to identify critical gaps that need to be addressed to protect the healthcare sector from cyber harm. This partnership reflects our shared commitment to advance the implementation of UN cyber norms through concrete action as well as our belief that a multistakeholder approach to protect the healthcare sector is the only way to meaningfully increase its resilience.

The Compendium on Protecting the Healthcare Sector from Cyber Harm, which will be launched during the third substantive session, is a practical example of a cooperation between stakeholders on issues of critical importance to the OEWG and the richness of perspective and experience that they can bring to the process. As a model, this cooperation could be scaled up to include other areas of Critical Infrastructure (CI) and Critical Information Infrastructure (CII), including other partners from among States and non-state actors.

The recommended next steps in this part should include suggestions that States consider exchanging in focused discussion with interested stakeholders, including businesses, non-governmental organizations and academia to inform the implementation of cyber norms, to develop common understanding of the gaps in current norms implementation and exchange knowledge of the potential effects that these proposed rules, norms and principles may have.

International Law


The CyberPeace Institute welcomes the mention of inviting experts to make presentations on relevant topics and the specific mention that the OEWG discussions around the development of common understandings on international law could benefit from expert briefings.

We appreciate that the revised draft clarifies that experts from the UN, as well as interested stakeholders including businesses, non-governmental organizations and academia may be considered to contribute to these discussions. However, we encourage the Chair to include this clarification consistently throughout the report to ensure that briefings from interested stakeholders with demonstrated expertise will be considered across the priority areas.

Stakeholders bring valuable contributions by informing the discussions on how international law applies in cyberspace, thereby helping to reach a common understanding on this matter. For instance, the CyberPeace Institute has been mapping and analyzing unlawful ICT activities by different States, in connection to the war in Ukraine, and monitoring the harm to civilians from cyberattacks as part of the Cyber Attacks in Times of Conflict Platform #Ukraine.\(^\text{11}\)

The text on capacity-building efforts on international law should further include that States can draw from the experience and best practices from stakeholders, as a complementary engagement to coordination with regional organizations. The corresponding recommended next steps should mirror the capacity of stakeholders to inform the discussions on applicability of the international legal framework in cyberspace. The list of steps should include that wherever possible, States could consider stakeholder engagement in the proposed initiatives and opportunities to meet their potential needs and gaps in capacity-building in the area of international law as well as on existing capacity-building initiatives and opportunities.

**Confidence-Building Measures**

The Institute considers the mention of the part that stakeholders play in confidence-building measures and their potential future engagement as an important recognition of their work in this area. Sharing current threat information that informs present and future confidence-building initiatives is important and should also include references to the specific knowledge and expertise that non-state actors can bring to the discussion. The reference to establishing Points of Contact in the private sector is promising and in line with strengthening practical cooperation with relevant stakeholders.

Cooperation in the area of confidence-building measures could also benefit from further focused consultations – facilitated by the Chair or by Member States – to foster dialogue with the goal of providing more in-depth discussions on the outlined topics. The private sector, civil society, academia, and the technical community can assist in facilitating such consultations and engagement. The outcomes of such thematic discussions could be presented during the substantive sessions.

Capacity Building

The report’s acknowledgement that stakeholders have an important role in capacity building programmes and initiatives through partnerships with States together with the list of possible activities is a positive sign of the commitment to the efforts towards strengthening coordination and cooperation between States and non-state actors. Other relevant areas for cooperation with civil society can include, but not be limited to, awareness-raising, training and educational activities, closing the cybersecurity workforce gap, and operationalising principles for capacity building.

Concerning the respective recommended future actions, the report should add that States could consider inviting interested stakeholder to provide the UN Secretariat with information on forthcoming capacity-building programmes and initiatives. The UN Secretariat could make this information available on the OEWG website.

Regular Institutional Dialogue

The CyberPeace Institute was proud to partner with Canada and the Kingdom of the Netherlands to co-organize the first multistakeholder event on the Advancing the Cyber Programme of Action (PoA).12 The participants of this workshop highlighted their support for the proposal to establish a PoA as an inclusive, consensus-based and action-oriented international instrument to advance responsible behavior in the use of ICTs in the context of international security. It was generally agreed that a PoA should not be limited to capacity building efforts but should include a variety of issues that would benefit from practical implementation and a meaningful multistakeholder participation in the initiative.

In conclusion, the draft report offers a good starting point for assessing the progress made so far and developing a roadmap for future work of the OEWG that considers the value and importance of a variety of stakeholders. The CyberPeace Institute believes that the proposed recommendations can inform discussions that precede finalization of the annual progress report, and, in line with its mission and expertise, the Institute stands ready to continue contributing and informing the OEWG process.