Submission to OEWG informal intersessional meetings
Submitted by Allison Pytlak, Stimson Center

This submission is being made in response to a request from the Chair of the Open-ended Working Group (OEWG) on information and communication technologies (ICTs), H.E. Burhan Gafoor, in the context of an informal dialogue with non-governmental stakeholders held on May 22, 2023. The Chair is requesting non-governmental stakeholders to make suggestions for “concrete outcomes” that should be captured in the Group’s second Annual Progress Report (APR), which is expected to be adopted at the Fifth Substantive Session in July 2023.

Below are several relevant suggestions that correspond to the standing agenda items of the OEWG. Many are based on recent developments and the status of OEWG discussions within these agenda items as well as the assumption that the second APR will, like its predecessor, provide a roadmap for future work in the OEWG. Broadly speaking, these suggestions outline ways in which the APR could lay a foundation for more focused discussions within standing OEWG agenda items and move toward more concrete outputs and/or initiatives. It is vital that any recommended next steps or progress toward concrete outputs be undertaken in an inclusive manner, recognizing the valuable role of non-governmental stakeholders in these undertakings.

Existing and Potential Threats
Under the OEWG’s ongoing consideration of Threats, the APR could mandate future OEWG sessions to pursue this topic in greater detail and move away from general expressions of concern and pursue specific initiatives. For instance, the APR could recommend dedicated sessions on specific threats that member states agree are a priority and invite subject matter experts, including from non-governmental stakeholders, to provide briefings. During the Fourth Substantive Session in March 2023, a significant number of member states raised artificial intelligence and ransomware as threats of high concern; topics such as these could form a focus for future dedicated sessions.

The APR could also set out a roadmap to explore in more detail some of the concrete proposals that have been made recently, such as Kenya’s proposal to establish a
repository of common threats, vectors, and actors; and the Philippines’ suggestion of a portal, modelled after the Cybercrime Repository under the UN Office on Drugs and Crime and building on the existing Cyber Policy Portal of the UN Institute for Disarmament Research (UNIDIR). Duplication of existing efforts and platforms should be avoided and working with stakeholders encouraged in any future work in this area.

**Rules, Norms and Principles of Responsible State Behaviour**

The 2022 APR included recommendations that states submit on a voluntary basis, working papers that contribute to the “development of guidance, checklists and share national views on technical ICT terms” along with other tools that would aid in developing common understandings about the rules, norms, and principles. Going forward, the 2023 APR should at minimum maintain this encouragement but also build out time for more detailed discussion about proposals made subsequently. In this regard, France’s suggestion to create a practical guide on due diligence to facilitate the implementation of norms 13C and 13H is noteworthy.

The APR should again encourage states to submit their annual views to the UN Secretary-General on developments in the field of ICTs in the context of international security and make use of the National Survey of Implementation. An evaluation of how well and to what extent the Survey is being utilized would also be helpful in determining its impact to date.

**International Law**

The APR could build on past recommendations to convene focused and dedicated sessions about specific aspects of international law or legal principles, as began in 2023. These could continue to take place in future formal OEWG sessions or occur through virtual or hybrid dedicated session(s). The Fourth Session demonstrated there is broad interest in exchanging views about this, whether on the topics covered in March (UN Charter, peaceful settlement of disputes, IHL, and state responsibility) as based on the joint Canada-Switzerland proposal and the 2022 APR. Or it could be expanded to include new ideas that have more recently been put forward, such as India’s suggestion to discuss convergence and gaps in member states’ common understanding and interpretation of international law. There is appetite and need for more focused exchange in this area, and a need to include legal experts from within and without government and build on the work of relevant initiatives, such as the Oxford Process.

An area that deserves further discussion is the question of enforcement of the states’ obligations, such as in relation to recent points made by Switzerland in relation to the citing the International Court of Justice and the work of Liechtenstein within the International Criminal Court (ICC) on the application of the Rome Statute of the ICC to cyberwarfare. While international law and the voluntary norms provide a framework for state behavior in cyber space there has not been sufficient attention to issues of
accountability and enforcement, whether in the context of consequences for malign behavior or affirmation of implementing good practice to reduce vulnerability and build resilience.

**Accountability**
The Stimson Center is implementing a project on cyber accountability to research lessons learned from non-cyber threats and identify possible good practice or models with relevance for cyber, including to support implementation of the UN Framework. Both states and non-governmental actors have observed various accountability gaps in this regard, including in relation to the cyber norms (both the restrictive/negative norms and the proactive/positive norms). The APR could encourage states to outline views on the subject of accountability, including gaps and possible response mechanisms or procedures that the OEWG might study in the next phase of its work. This could occur as part of discussions on most of the OEWG’s standing agenda items and thus be mainstreamed, given that the accountability is relevant to not only norms and law, but also capacity building and as a component of confidence-building measures, and has links to activities like the National Survey and annual submissions to the UNSG.

**Gender, human-centric approaches, and stakeholders**
Since the first substantive OEWG session was convened in 2019, there has been a more robust and regular engagement in discussing the gender dimensions of cyber security, particularly within cyber capacity building, and a reinforcement by many states about the importance of human-centric cyber security.

It would be important that the APR not only capture relevant progress made in both areas since the adoption of the 2022 APR but also continue to stake out ways forward in order to avoid backsliding. The APR should call for continued gender diversity among representatives to future OEWG sessions, including the meaningful representation of women, but also mainstream gender across its agenda items. Several suggestions have been made in the last year by states and stakeholders about practical ways that the OEWG could continue to advance gender-sensitive cyber capacity building, a principle endorsed in the final report of the 2019-2021 OEWG, and about how states can raise awareness of the gender dimensions of security of and in the use of ICTs. The next APR is an opportunity to deepen and concretize the discussion in this area.

Lastly, the APR should reinforce that all stakeholders have a meaningful role to play in implementing the agreed UN Framework. While the overall ability of non-governmental stakeholders to access OEWG sessions has improved somewhat in the last year, obstacles remain. Many of the actors who play an important role in operationalizing the UN cyber norms are being denied accreditation, which impacts the credibility and real-world impact of the OEWG.