STIMSON

16 April 2020

To: Ambassador Jűrg Lauber, OEWG Chair

Excellency,

We appreciate the opportunity to comment on the pre-draft of the report of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security ("OEWG").

Suggestions for Further Strengthening of Statements

The historical perspective on the evolution of UN concern over information and communications technologies (ICTs) is notable and appreciated in the draft. ***Further emphasis might be given to the purpose of the OEWG and its mandate under 2018 UN General Assembly resolution 73/27,*** in particular "to further develop the rules, norms and principles of responsible behaviour of States listed in paragraph 1 above, and the ways for their implementation; if necessary, to introduce changes to them or elaborate additional rules of behaviour; to study the possibility of establishing regular institutional dialogue with broad participation under the auspices of the United Nations…"[1]

The Stimson Center has traditionally worked with multiple stakeholders in addressing international security issues and has found that the perspectives of diverse stakeholders can significantly contribute to identification of good outcomes in the development of effective policy. For this reason, we support the comments that many UN Member States and others have made regarding continuing an OEWG that engages multiple stakeholders in working to better international security. It was particularly heartening to see so many States that have not been part of the Governmental Group of Experts' deliberations actually be part of this OEWG process, both to the benefit of those States as well as to the benefit of international cybersecurity in our interconnected world. ***We suggest that those statements in the draft report recommending the continuance of some form of inclusive OEWG process be amplified to include more discussion of how business, non-governmental organizations and academia can contribute.***

- States *and other stakeholders* should increase exchanges on standards and best practices, especially regarding critical infrastructure – and should include attention being given to industrial control systems and new evolving technologies such as artificial intelligence that affect IT/OT and overall enterprise risk management.[2]
    - Exchanges should include the development of concrete tools States could adopt to better secure cyber space, as proposed by Croatia, Finland, France and Slovenia in the Non-Paper. The need for capacity building is indeed critical, as so many noted.

[1] https://undocs.org/en/A/RES/73/27

[2] The resolution notes that critical infrastructure and supply chains are primary concerns, thereby implying that ICT be defined most inclusively.

- Standards and security requirements should be collected not just from States but also from *legal/technical/other specialists* in non-governmental organizations, academia and businesses. In many aspects of ICT, these latter stakeholders are in the vanguard of the latest technologies. The uniquely important perspectives they bring should be highlighted by more discussion in the pre-draft report.

The fact that so much of the discussion veered beyond a narrow interpretation of the First Committee's traditional mandate might be noted by acknowledging the cross-cutting nature of ICT and the need for future OEWG work to more directly coordinate with the efforts of others, including UN groups, addressing these issues.

- **A new/continuing OEWG should clarify and prioritize its work.** This dialogue might include a directive to recognize and gain from other related efforts within and outside the UN.[3]
  - Given the limited resources available to the UN, the Secretary-General could find it beneficial to leverage or outsource some of the recommended work that has already been started by others, such as developing points of contact at the policy, diplomatic, legal and technical levels and expanding development of Computer Emergency Response Teams.
  - Given conflicting views, the OEWG and/or Secretary-General might want to explore various organizational mechanisms to ensure coordination among efforts and avoid duplication in developing continued institutional dialogue.

Suggestions for Further Study

It would be beneficial to strengthen the suggestions States and others have made of ways to operationalize the norms (listed in Resolution 73/27 and noted in past Governmental Groups of Experts recommendations) and to further develop and implement these and other norms and to support international security**.** ***To this end, some additional background work should be undertaken to support any continuing work of the OEWG****.* For example:

- **Exploring conflicting approaches/views:** Given the conflicting State opinions on some topics, areas of disagreement should be more clearly identified with a recommendation that individual States or groups of States might be called upon to engage think tanks and/or academia in collaboration with the private sector to pursue additional unbiased research on those issues in support of future OEWG discussions. *The goal should be to develop analytical frameworks for States to better assess options.* Such issues might include:
  - *On existing norms and laws:* Case studies of how some States or groups of States have applied international law to ICT matters and an analysis of the alternative approaches would help some States build capacity. As Canada noted, it would be useful for States

[3] As noted by the Chair, the UN has a number of related efforts (see: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/01/background-paper-on-existing-un-bodies-processes-related-to-mandate.pdf), and as noted by some participants, some points of contact and best-practice dialogues already are being pursued in other venues.

to have "a repository of national practices regarding international rules, norms and principles of responsible behaviour" to support norm development and implementation.[4] Further, a template for compliance with norms could be developed as a complement to the UNIDIR Cyber Policy Portal; this could be approached in a manner similar to the one the UN 1540 Committee used, with its experts developing matrices in which State compliance could be demonstrated.[5]

- *On development of new norms and laws:* Many suggestions for new norms and laws have been put forward. These should be more systematically assessed, analyzed and vetted among States both for their potential impacts on risk and for their likelihood of being supported and implemented.
- *On vulnerability disclosure policies:* Policies of States and of hardware and service provider could be posted on a website, with related information on how a third-party entity should proceed if a vulnerability is discovered.
- *On attribution and definitions, including of war-like acts:* A State has the prerogative to attribute a malicious cyber operation – and some have called for a better lexicon of terms, including for what constitutes a "cyber-attack." States need to define with more nuance what acts are considered State-based/supported and which rise to war-like act. This is important not only to the development of norms and the application of international law but also to assist the private sector, e.g., for insurers in considering policy exclusions for war-like acts. Lessons can be taken from other areas where accountability is important, e.g., on international cooperation for identifying the origin and history of nuclear material found out of regulatory control.

- **Learning from Existing and New Efforts:**
  - *On capacity-building and confidence-building measures:* In addition to coordinating and assessing current cooperative outreach programs promoting cyber hygiene, the possibility of building up new efforts cooperatively to address cybercrime should be considered. Efforts to identify and prosecute threat actors are important to international peace and security - and the First Committee - as well as other UN bodies. Consideration should be given to developing a Global Network of Cybercrime Centers to more efficiently and effectively address emerging threats and as a capacity- and confidence-building measure.[6]

[4] https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/03/canada-responses-to-oewg-chair-questions-Feb-26.pdf

[5] https://www.un.org/en/sc/1540/national-implementation/1540-matrices.shtml

[6] See, for example, the Albright-Gambari Commission's report and update in last year's follow-on report for recommendations for building on INTERPOL's Global Complex for Innovation and including a new standby roster of expert cybercrime fighters within INTERPOL's new Cyber Fusion Centre out of Singapore. http://www.platformglobalsecurityjusticegovernance.org/publications-resources/an-innovation-agenda-for-un-75. https://www.interpol.int/en/News-and-Events/News/2014/INTERPOL-Global-Complex-for-Innovation-opens-its-doors.

- *On organizational design and mandates:* Other organizations from the International Atomic Energy Agency to the International Maritime Organization have already embarked on efforts to share information, promote best practices and provide guidance documents. Any new OEWG looking at the UN developing/coordinating cyber efforts should take lessons from the experiences of such other organizations.

Please consider including the informative meeting notes of David Koh, Chair of the informal intersessional consultative meeting of the OEWG, as an addendum to the report.[7]

We commend the Chair and the Secretariat for its excellent facilitation of this complex process involving many stakeholders and hope that you may continue productive work during these challenging times.

Sincerely,

Debra Decker, Senior Advisor
The Stimson Center
Innovative Ideas Changing the World
1211 Connecticut Avenue NW | 8th Floor
Washington, DC 20036
www.stimson.org
Cyber Security Project

[7] https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/01/200128-OEWG-Chairs-letter-on-the-summary-report-of-the-informal-intersessional-consultative-meeting-from-2-4-December-2019.pdf