Estonia's comments to the "Initial "Pre-draft" of the report of the OEWG on developments in the field of information and telecommunications in the context of international security"

Estonia welcomes the comprehensive pre-draft of the Open Ended Working Group (OEWG) report and would like to thank the OEWG Chair Ambassador Jürg Lauber and his team for an excellent organisation of the meetings as well as the preparation of the pre-draft report. We express our gratitude for a thorough overview of different ideas expressed during the meetings in New York in September 2019 and February 2020. The comments below capture several aspects in the thematic order that we consider important to be reflected in the future versions of this report.

General comments

1. Estonia welcomes the presentation of the elements of the discussion in the initial OEWG pre-draft that include international law, the rules, norms and principles of responsible state behavior, confidence-building measures and capacity-building, which are interrelated and mutually reinforcing. As an important next step in the Group's activities, we should be moving towards implementation of these measures. A single global repository of implementation activities with voluntary contributions from UN Member States could enhance this endeavor.

2. Estonia appreciates the reflections on international law discussions that have taken place during the first and the second substantive sessions of the OEWG. The pre-draft report noted that international law, particularly the UN charter in its entirety, applies and remains essential for ensuring peace and stability in cyberspace. The principles of existing international law, voluntary norms of responsible state behavior and confidence building measures create a normative framework that increases transparency and predictability.

3. Estonia has reiterated in its statements that in addition to the UN Charter in its entirety, also the international humanitarian law, international human rights law and customary rules of law of state responsibility are applicable to state conduct in cyberspace. It is vital that international legal rules apply to state conduct in cyberspace as they apply to state conduct in conventional sense.

4. An important addition during the OEWG discussions have been informal intersessional consultative meetings that broadened the debate with multi-stakeholder perspectives from the private sector, academia and civil society. The conclusions of these discussions could also be reflected in the final report.

On Existing and Potential Threats

5. We welcome that the concept of "technology-neutral" has been included to the report. We have witnessed rapid developments of technologies, which will continue at rapid pace. In order to assure a non-exclusive language in the report, focus should be on responsible use of these technologies, not each technological development individually (Article 18).

6. Whereas cyber threats directed towards the critical national infrastructure pose a challenge that all UN Member States should address, it remains less clear what are the "transborder and transnational critical infrastructures at risk" (Article 19). Majority of critical information infrastructure resides within national jurisdictions, although there might be different levels of criticality of this infrastructure. We suggest to consider changing the wording in this respect.

7. Some of the elements mentioned under the Existing and Potential Threats discussion could be aggregated to a more generic notion that is based on agreed UN language as found in the

2010, 2013 and 2015 UN GGE reports. For example, harmful hidden functions and the integrity of global ICT supply chains were mentioned in the UN GGE 2015 report norm 13(i) (Article 15).

8. We welcome the fact that the OEWG pre-draft has recognised the effects of threats on different actors, including on youth, the elderly, women and on vulnerable populations, particular professions, and other categories of actors, as well as on States with different levels of ICT security and resilience. The cyber threats during the ongoing global health crisis illustrate this notion (Article 17).

On International Law

9. Estonia supports the statement that further discussion is necessary amongst states to provide a better understanding on how provisions of international law apply. These areas should include agreements on international human rights law, international humanitarian law, and law of state responsibility. However, we support the idea that the current framework – based on applicability of existing international law, and supported by the voluntary and non-binding norms of responsible state behavior – is sufficient. The main question for this Group is how this framework will be implemented among all States globally.

10. The pre-draft report has noted that, in particular, the international humanitarian law in cyberspace aims to reduce risks and potential harm to civilians and combatants in the context of armed conflict. Estonia reiterates its long standing position that IHL sets boundaries for state's activity by offering protection to civilian infrastructure, and it acts as a constraint, not facilitator of conflict. There has been an agreement at the UNGA level that major principles of IHL - humanity, necessity, proportionality and distinction, are applicable in cyberspace. This is important element to stress in the report of the OEWG (Articles 25, 27).

11. Estonia would like to recall the OEWG discussions where majority of states stressed the need to adhere to the rules of existing international law. The recommendations of the report could contribute significantly to the development of a common understanding on how international law applies. In addition, Estonia would like to see a stronger emphasis on what most of the states during the meeting brought forward –there is currently no need for an additional legal instrument as majority of UN Member States agree that existing international law applies. In the current report, Estonia finds a slight imbalance between how discussions are reflected on existing international law applying to state use of ICTs as only very few states called for a new legally binding instrument (Articles 26-29).

12. The pre-draft report addresses the proposals to create a legally binding instrument on the use of ICTs by States due to the quickly evolving nature of the threat environment and the severity of the risk. We do not see a value in the discussions on a new instrument, and would like to draw the attention to the link between technologically neutral approach and the need to address the state behavior in general, not technological achievements individually (Article 27).

13. Estonia supports the call to states to present their views on how international law applies to state use of ICTs. In addition, we see that there is a possibility to add further text on capacity building on international law matters and to link this with the possibility to present national positions, e.g. in a repository. This could be achieved through a Cyber Policy Portal of a repository, which would provide access for States that seek guidance on international legal positions (Article 30).

14. The pre-draft refers to developing a common approach to attribution but fails to recognise that attribution should remain a sovereign decision of each individual state. In order to increase states' capacities to conduct attribution activities, we encourage states to share their best practices regarding attribution (Article 32).

15. While ILC contributes to international law discussions regarding various bodies of international law, Estonia does not see the need to add international law applicable to state use of ICTs to the agenda of the ILC. Given that the national positions are still developing and only a handful of states have declared their positions publicly, the state practice is yet too scarce for the ILC to carry out a meaningful analysis. Our position on this proposal is to keep relevant discussions in the GGE and the OEWG and refrain from adding an additional layer to ongoing exchanges between states (Article 68).

On the Rules, Norms and Principles for Responsible State Behaviour

16. Estonia sees the voluntary and non-binding norms from the 2010, 2013 and 2015 UN GGE reports to form a foundation for responsible state behavior, together with the existing international law, and supports their further implementation to promote international peace and security. At this point, we see more value in the implementation of the already existing norms than in developing new ones (Article 38).

17. As mentioned in the pre-draft report, voluntary, non-binding norms reflect the expectations of the international community regarding the behaviour of States. Additionally, it should be noted that the norms support and do not replace nor alter international law; in addition, norms do not change the applicability of international law.

18. Awareness of the existing norms should be further promoted among all UN Member States. Estonia supports sharing of best practices on how some states have already operationalised these voluntary and non-binding norms. A global repository with voluntary written contributions by Member States could facilitate information sharing on how States have already implemented the norms (Article 37, 68b).

19. The pre-draft report mentions the importance of partnerships and joint efforts with the private sector and notes that all stakeholders have responsibilities in their use of ICTs. These partnership relations could also be used to build capacities and increase awareness among the Member States (Article 40).

20. The question on how norms will be implemented should not hinder States' economic development; at the same time, including human rights and gender perspective would have the potential to contribute to creating more stabile societies and economic growth. Estonia supports mainstreaming elements of human rights and gender perspective in the implementation process (Article 34). In this case, we would like to draw the attention to the recently adopted Freedom Online Coalition statement on Human Rights Impact of Cybersecurity Laws, Practices and Policies and its recommendations, which addresses key elements of ensuring and protecting fundamental rights and freedoms.

On Confidence-building Measures

21. Estonia re-affirms the notion of interlinkages between norms and confidence-building measures as the latter may often support the effective implementation of the voluntary and non-binding norms. Operationalisation of confidence-building measures – in a way that could allow a region-specific approach – could effectively increase security and stability in these regions as well as potentially address inequalities and the existing digital divide between Member States.

22. Estonia is supportive of the idea of establishing national Points of Contact as it would increase the effective implementation of CBMs regarding policy/diplomatic, legal and technical questions. Some regional organisations (e.g. the OSCE) already have started with the

operationalisation of PoC network that this initiative could take into account and share information about to other regional organisations (Article 44).

23. Estonia would be supportive of an idea to add to the global repository a list of confidence-building measures adopted at regional and sub-regional levels to enable the sharing or exchange of information and best-practices on confidence-building measures; e.g. a global registry of national points of contacts that could enhance the global political/diplomatic and technical network and expertise in cybersecurity (Article 45).

On Capacity-building

24. Estonia fully supports the idea that all UN Member States need to build capacities to identify and protect national critical infrastructure (Article 49).

25. Additionally, further capacity-building efforts should focus on all elements of the 2013 and 2015 GGE reports varying from international law, policy/diplomatic, technical and regulatory areas (Article 48-50).

26. The variety and volume of capacity building projects has created a requirement for better global coordination between the existing initiatives. In order to improve efficiency and avoid duplication in coordination efforts, Estonia supports using the existing global capacity-building coordination platforms, such as the Global Forum of Cyber Expertise (Article 55).

27. We support the inclusion of human rights and gender perspective to capacity building efforts, these two elements should also shape the approach to capacity-building to ensure more stable societies and economic growth (Article 56).

On Regular Institutional Dialogue

28. The dialogue in the UN First Committee should be guided by the existing consensus to implement the voluntary and non-binding norms, confidence-building measures, as well as address capacity-building, and to elaborate on how States interpret international law's applicability to cyberspace (Article 58). The format of the dialogue should support the goal to strengthen international peace and stability, and conflict prevention in cyberspace.