Latvia’s submission to the UN Secretary General’s call for contributions to report under resolution 78/237 “Developments in the field of information and telecommunications in the context of international security” adopted by the General Assembly on 22 December 2023 (note verbale of UNODA: ODA/2024-002/)

30 April 2024

The framework of responsible State behaviour in the use of information and communications technologies (ICTs) for a long time – since 2003 – has been on the UN GA First Committee’s agenda and discussed at several Groups of Governmental Experts (GGEs), as well as Open-Ended Working Groups (OEWGs), emphasizing the increasing importance of responsible use of ICTs to maintain international stability and security. Cooperation among States is vital to effectively address growing threats in cyberspace and to build confidence among States. For these reasons, it is time to decide on establishment of a permanent mechanism within the UN to address cybersecurity matters in a long-term manner.

Cyber-attacks are becoming more sophisticated, destructive and frequent than ever in modern interconnected world. Cyber landscape is evolving constantly. Cyber-attacks against critical infrastructure, politically motivated attacks, ransomware attacks and malicious use of artificial intelligence (AI) are on the rise. Therefore, relevance of cybersecurity is undeniable in the international security debate.

In order to tackle the unprecedented level of malicious activity in cyberspace, Latvia is increasing its own cybersecurity and resilience. Among other things, Latvia organises and conducts cyber threat hunting operations both nationally and within the European Union (EU), our governmental institutions share knowledge and experience with citizens, public and private entities. In 2023 and 2024 Latvia, along with other EU Member States, has repeatedly publicly condemned malicious cyber activities, including cyber-attacks targeting democratic processes and institutions.

Proposal to establish a “regular institutional dialogue” under auspices of the UN has been discussed previously in the UN First Committee and is noted in the final report of the OEWG 2019-2021.1 The OEWG 2019-2021 concluded that any future mechanism for regular institutional dialogue should be “an action-oriented process with specific objectives, building on previous outcomes, and be inclusive, transparent, consensus driven, and results-based”2. In the 2023 Annual Progress Report of the OEWG 2021-2025 States agreed on common elements, most notably, on single-track, State-led, permanent mechanism.3

Growing cyber threats require that energy and resources of States are focused on enhancing cooperation and trust among States in long-term rather than on discussions regarding modalities of a new mechanism taking place every few years and risking future progress fragmentation. Latvia as a small State supports a single-track approach which would facilitate effective use of limited resources.

Responding to the call for establishment of a permanent mechanism to advance responsible State behaviour in the use of ICTs in a coherent and long-term approach, a Programme of Action

---

1 Final report of the OEWG 2019-2021, Regular Institutional Dialogue.
2 Final report of the OEWG 2019-2021, paragraph 74.
(PoA) has been proposed⁴. The UNGA Resolution 77/37⁵ on the PoA in 2022 and the UNGA Resolution 78/16⁶ on the PoA in 2023 received a broad support by the States at the GA and this initiative has been developed in a transparent, inclusive and incremental manner.

**On the PoA as a permanent UN mechanism**

Latvia believes that by the Resolutions 77/37 and 78/16 the UNGA has granted a strong mandate to proceed with establishment of the PoA. The PoA should be a permanent, inclusive, action-oriented, State-led mechanism within the UN First Committee and a platform for all States to participate. Its overarching objective would be to contribute to the strengthening of international peace and security and to the prevention of conflicts and misunderstandings among States. The scope of the PoA should be matters related to the use of ICTs in accordance with the international law and the implementation of the UN framework of responsible State behaviour in cyberspace. As noted in UNGA Resolution 77/37, the PoA would “take into account the consensus outcomes adopted”⁷ by the OEWG 2021–2025.

Stability and security in cyberspace will be advanced by supporting the implementation and further development, if appropriate⁸, of the framework for responsible State behaviour, based on the international law, including UN Charter in its entirety. As agreed in the UN GGE reports in 2013, 2015, 2021 and UN OEWG reports in 2021, 2022, the international law, including the international humanitarian law, is applicable and essential to maintaining peace, security and stability in cyberspace.

In order to advance implementation of the framework for responsible State behaviour, the PoA would support relevant and needs-based capacity-building activities. **It is important to advance collective work on capacity-building and to share our experience and best practices to improve both national and global resilience against cyber threats.**

The PoA could hold annual formal sessions. In between the formal sessions work of the PoA could be organised within technical working groups dedicated to specific issues. For example, a technical working group could work to further enhance an understanding on how international law applies to the use of ICTs. The formal sessions would adopt recommendations prepared by the technical working groups. Periodically, further priorities of the PoA should be reviewed during Review Conferences.

The technical groups could be created and terminated by decisions of the formal sessions. The technical working groups must be inclusive and open to all States, ensuring that national experts can participate offline or online (hybrid format). Decisions on the technical groups and on their working modalities should be made considering capacity and resources of small States.

Regular and full-fledged dialogue with stakeholders – civil society, private sector, academia – is essential and should be facilitated through the PoA. Their expertise in ever-evolving cyber domain is invaluable and thus their input is relevant for advancement of implementation of the responsible State behaviour. Furthermore, the stakeholders themselves “have a responsibility

---

⁵ UNGA Resolution A/RES/77/37, Programme of action to advance responsible State behaviour in the use of information and communications technologies in the context of international security.
⁶ UNGA Resolution A/RES/78/16, Programme of action to advance responsible State behaviour in the use of information and communications technologies in the context of international security.
⁷ UNGA Resolution A/RES/77/37, PP 27.
⁸ UNGA Resolution A/RES/76/19, PP10.
to use ICTs in a manner that does not endanger peace and security”9 as well as they are the ones driving development of the new technologies.

Further focused discussions at the remaining sessions and intersessional meetings of the OEWG 2021-2025 should be organized in 2024 and 2025 to continue to elaborate the different aspects of the PoA, including modalities for establishment of the PoA. The PoA should be operational upon conclusion of the OEWG 2021-2025.

---