

**Programme of action (PoA) to advance responsible State behaviour in the use of ICTs in the context of international security**

**Estonia's submission to the UNSG report**

**As mandated by the UNGA Resolution 77/37, Estonia would like to submit a national position on the Programme of Action (PoA).**

Over the recent years, threats in the use of ICTs in the context of international security have continued to intensify and evolved significantly in the current challenging geopolitical environment. Increasing threats in the use of ICTs are leading to growing challenges concerning the negative effects on economic and social development, as well as implications on national and international stability. These implications continue to be at the forefront of multilateral discussions, as illustrated by the work of the United Nations Group of Governmental Experts (GGE) and the Open Ended Working Group (OEWG). Estonia would like to share the following remarks on the establishment of a regular institutional dialogue in the format of the PoA. We believe the PoA would serve as a useful vehicle for continuing discussion to advance responsible State behaviour in the use of ICTs, and thereby contribute to reducing tensions, preventing conflict and promoting their peaceful use.

- 1. The PoA should be based on the existing *acquis* and the framework of responsible State behaviour, focusing on State use of ICTs in the context of international peace and security.** Estonia believes that ICTs must be employed consistent with the objectives of maintaining international stability and security and in accordance with the agreed *acquis* and the framework of responsible State behaviour. We underline that Member States should be guided in their use of ICTs by the GGE 2010, 2013, 2015 and 2021 reports and the 2021 OEWG report. The PoA mechanism should be built on these premises and be guided by the objective of preserving an open, stable, secure accessible and peaceful ICT environment. Estonia finds that several existing or proposed initiatives, such as the global Point of Contact directory, would offer instrumental support to the effective functioning of the PoA format.
- 2. The PoA should be a neutral format providing for institutional stability.** From the perspective of a small State, it is necessary to have clarity and institutional stability regarding the further processes related to the discussions on State use of ICTs. Estonia thus advocates for establishing a single permanent structure for furthering the OEWG discussions, after the end of the current OEWG ending in 2025. We support furthering discussions on the structure, modalities and timeline for establishing PoA as a mechanism for advancing responsible State behaviour in the use of ICTs, taking into account the views from all Member States. Estonia supports the the option of establishing the PoA via an international conference, as proposed in the UNGA resolution 77/37. We would also like to underline that the PoA mechanism should be founded on the principle of consensus. Estonia believes that the proposed PoA framework would remove the need for UNGA to debate the creation of new cyber processes every two, three or four years. It is our hope that the PoA framework would

be seen as a useful and neutral framework by Member States and there would be no need for parallel processes.

3. **The PoA should offer a holistic framework for advancing various topics proposed during the OEWG in an inclusive manner.** We welcome the increasing interest of Member States to contribute to various topics which are focused upon during the ongoing debates of the OEWG sessions. The current OEWG discussions have been substantial, with a range of ideas proposed by different Member States. We believe that the PoA framework could offer a “go-to” venue for Member States to raise issues related to ICTs and international peace and security. Thereby the PoA could provide for a holistic framework for these ideas to be brought forward and analysed in greater detail. The PoA should also include clear and transparent modalities for the substantial involvement of the multistakeholder community to further benefit from their expertise and knowledge.
4. **The format of the PoA should allow for focused discussions.** Estonia suggests that the elements of the PoA mechanism could be based on focused discussion – for example, held in working groups open to all interested participants, including on, but not limited to, threats, capacity building, confidence building, norms as well as international law. Another option could be focusing these working groups on more thematic topics such as critical infrastructure protection. With an increasing number of Member States reflecting their views as well as an evolving threat landscape, PoA would allow for a more flexible, yet, focused format for continuing these discussions. Equally, we would like to underline that the design of the PoA framework should also take into account the challenges regarding limited capacities of small States and thereby be built on reasonable expectations as regards to projected workload. In that regard we support the idea of annual conferences broadly addressing State use of ICTs, supplemented with more focused working groups.
5. **PoA should offer an inclusive framework for the discussions on international law.** Estonia welcomes the increasingly active and substantial discussions on international law and how it applies to the State use of ICTs. International law is evolving in time and Member States would benefit from a deepened understanding and shared views on how existing rules apply, and a more detailed analysis of any possible gaps. PoA would be well positioned as offering an inclusive venue for continuing these discussions.
6. **PoA should be action-oriented and with a strong focus on capacity building.** An integral part of the future discussions should be the implementation of the agreed upon framework of responsible State behaviour. This can be supported by a practical and transparent approach to mapping as well as responding to the need and requests for capacity building. PoA should take stock of existing capacity-building initiatives in a well-coordinated and complementary manner. For example, designing PoA should take note of existing mapping exercises and resources, such as the Cybil portal and the EU CyberNet’s mapping of EU Member States’ cyber capacity-building projects.