As mandated by the United Nations General Assembly Resolution 78/237, Estonia would like to submit a national position on the future regular institutional dialogue (RID) on the security of and in the use of information and communications technologies.

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).

Following the broad support of a cross-regional group of countries to establish a Programme of Action (PoA), we support the PoA as a permanent institutional mechanism under the First Committee with a focus on the implementation of the agreed framework of responsible State behaviour in cyberspace, while also allowing for the further development of the framework, if appropriate. We believe that such a regular institutional dialogue would contribute to reducing tensions, preventing conflict and promoting their peaceful use.

This national position is an update of Estonia’s national contribution included in the Secretary-General report A/78/76 on the PoA which builds on inter alia the progress reflected in UNGA resolution 78/16 and discussions within the 2021-2025 OEWG.

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 further processes related to the discussions on State use of ICTs. Estonia thus advocates for the establishment of 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 option of establishing the mechanism via an international conference, as agreed in the UNGA resolution 77/37 by no later than 2026. Estonia believes that the proposed PoA format would remove the need for the 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.

4. **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. Engaging the multistakeholder community will support Member States in implementing the framework for responsible State behaviour and designing as well as delivering needs-driven capacity building efforts to increase cyber resilience globally. Equally, the PoA could also enhance regional engagement through cooperation with regional and thematic organisations to leverage and build upon relevant existing initiatives.

5. **The PoA should allow for more flexible, yet, focused format** for continuing the discussions on the framework of responsible State behaviour. Estonia 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.

   a. We suggest that the elements of the PoA mechanism could include annual plenary meetings addressing topics under the main pillars of the framework of responsible State behaviour.

   b. We also support focused discussion in the format of 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. The participation in the working groups
should be voluntary and the creation of such work streams would be decided by States in annual plenary meetings.

c. We also support the organisation of review conferences (for example, in every four years) which would allow to take stock of progress and consider any further possible amendments to the mandate as well as organisation of work or the PoA.

6. Among other topics, 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. 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. In particular, the PoA could offer a platform for the following elements in discussing international law: 1) continuing discussions on how international law applies to cyberspace; 2) sharing national views; 3) dedicated meetings on how international law applies in the use of ICTs, focusing on specific topics to allow for more detailed elaboration; 4) expert briefings; 5) scenario-based discussions; 6) capacity-building on international law.

7. 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. PoA could also encourage voluntary reporting of national implementation efforts which would contribute to many goals such as confidence building, transparency, as well mapping capacities and needs. 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.