North Macedonia's submission to the UN Secretary General's report on the Programme of Action

Submission of the Government of the Republic of North Macedonia to the United Nations Secretary General report on the Programme of Action (PoA) towards implementing the framework and building resilience in line with the United Nations General Assembly Resolution 77/37.

The discussion on the principles related to the PoA is crucial in enhancing our ability to address challenges and ensure a secure cyberspace.

Our view is that regional and global collaboration can significantly enhance the pace and effectiveness of state actors' efforts to improve their response capabilities.

In countries comparable to North Macedonia, where there is a shortage of standards and resources for defence, individuals, businesses, and organizations are very susceptible to cyber threats. Therefore, the PoA should establish a permanent and unified institutional structure to address cyber issues. This structure should have a clear and well-defined mandate and sufficient resources to confront the constantly evolving landscape of threats.

Inter-Organizational cooperation including cross-regional collaboration of institutions that are dealing with this subject matter of their relevant structures involved into the cyber security should also be considered to strengthen coordination, which can be added value for further exchange of experiences and with aim to build coherent front that can address all emerging challenges.

To promote widespread involvement in respect to this, the PoA must provide a malleable framework that can be adjusted as required. One possible solution is for the PoA to hold annual or biannual plenary sessions, which would be available to all governments, where decisions will be based on the efforts of specialized working groups during the intersessional period.

These plenary sessions could also establish task forces and utilizing the knowledge of both States and pertinent stakeholders.

While the established framework for responsible State behaviour should serve as the basis for the PoA's work, there should also be a room for updating the framework as necessary. One way to accomplish this is through periodic plenary meetings or review conferences, during which States can reassess the framework and decide to enhance it if deemed necessary. To ensure the effectiveness of these reviews, dedicated working groups could inform them during the intersessional period.

A major priority for the PoA should be to provide significant support for the implementation of its efforts. This level of support can come in the form of voluntary reporting of implementation efforts by participating States, which would help to identify the most pressing needs and challenges.

The PoA should also provide updated, practical recommendations on a continuous basis to guide States in their implementation efforts. Additionally, it should offer support for capacity-building activities to further enable effective implementation.

We believe that the PoA is to be comprehensive and suitable for each country. One of the challenges is that the needs, and capacities of different countries can vary significantly. Therefore, it is important that the PoA is flexible enough to accommodate these differences and can be tailored to the specific needs and circumstances of each country. This can help to ensure that the implementation is feasible and effective in each context.

The PoA must prioritize inclusivity, not only for participating States but also for the stakeholder community. With regards to stakeholders, the PoA should affirm that States hold the primary responsibility for matters related to international security, and thus retain decision-making power. However, the PoA should also provide modalities that enable all stakeholders to attend formal meetings, make statements, and submit written inputs. This approach will ensure that the voices and perspectives of all relevant parties are considered, while still acknowledging the central role of States in matters of international security.