Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Foreign Affairs FDFA

State Secretariat
International Security Division ISD

Resolution 77/37 “Programme of action to advance responsible State behaviour in the use of information and communications technologies in the context of international security”

I. Introduction

1. For more than 20 years, States have been discussing at UN level existing and potential threats to international peace and security by States’ use of information and communications technologies (ICTs) and how to address those threats. Those discussions, held in varying, time-limited formats, have incrementally made considerable progress. The consensus recommendations of the 2010, 2013, 2015 and 2021 UN Group of Governmental Experts (UNGGE), the consensus recommendation of the 2021 UN Open-ended Working Group (OEWG) and the 2022 consensus Annual Progress Report of the OEWG 2021-2025 have developed and consolidated a framework for responsible behaviour of States in cyberspace. The framework for responsible behaviour of States in cyberspace comprises the application of international law to cyberspace, voluntary norms of responsible State behaviour, confidence building measures and capacity building.

2. UN Member States, through General Assembly Resolutions A/RES/70/237 and A/RES/76/19 have agreed by consensus to be guided in their use of ICTs by the 2015 and 2021 GGE Reports as well as the 2021 OEWG report that outline the framework, affirming the so called “acquis”.

3. The proposed “Programme of action” builds firmly on this agreed framework and the acquis.

II. Scope and objective of the UN Programme of action (PoA)

4. The Programme of action (PoA) would contribute to the shared goal of an open, free, peaceful and secure cyberspace. It would provide a permanent structure for regular institutional dialogue at UN level to support member States in their national efforts to implement and operationalize the framework for responsible State behaviour in cyberspace.

5. It would be action-oriented, inclusive, transparent, consensus driven and results based.

6. Its action-oriented nature is a core element of the PoA. The PoA would assist States in putting in place cooperation and capacity-building activities adapted to their needs. It would provide a permanent platform for exchange of knowledge, best practices and expertise, thereby contributing to building and strengthening trust and transparency.

7. The PoA should also be flexible enough to allow States to address future threats. In this regard, it should regularly convene States to review the framework and where necessary to further develop the framework as appropriate, on basis of consensus.

III. Structure and content

8. An annual formal meeting would be held as part of the PoA. States would be invited to conduct, on a voluntary basis, an assessment of their progress and challenges in implementing the framework. This could be done either by creating its own reporting system or by promoting

existing mechanisms (such as the “National Survey of Implementation of United Nations recommendations on responsible use of ICTs by states in the context of international security”[1]). Based on these assessments, the specific needs, positive lessons learned, challenges and priority areas could be identified. At the annual formal meeting, member States would adopt decisions and recommendations by consensus. Also at the annual formal meeting, member States would establish technical working groups by consensus.

9. During the intersessional period, technical working group meetings could be held, as established at the annual formal PoA meeting. The findings and recommendations of those meetings would feed back into the annual formal meeting. The technical working groups would focus on priority areas as identified at the annual meeting. These technical areas could include operationalisation of specific voluntary norms through development of concrete guidance and exchange of best practices; advancing discussion and common understanding on how international law applies to cyberspace; presentation of concrete capacity building needs and provision of concrete support.

10. Regular exchanges with regional organisations as well as relevant international bodies such as the ITU should also be envisaged to share best practices and to support coordination with relevant international and regional initiatives. Where such exchanges already exist, the PoA should build on corresponding experiences and structures, as appropriate.

11. On a regular basis (for example every 4, 5 or 6 years), a review conference could be held, to update the PoA as appropriate.

12. All decisions taken within the PoA should be taken by consensus.

13. States bear the primary responsibility for the maintenance of international peace and security, including in cyberspace. At the same time, they are not the sole actors relevant to achieve this goal. This is especially true in cyberspace, where most of the infrastructure is owned and operated by private actors. Multi-stakeholders play an integral role in its operation; possess valuable insights and expertise beyond that of States. Actors such as civil society, the private sector, academia and the technical community also have their respective roles and contributions to make, especially in supporting States in their implementation of their commitments under the framework for responsible behaviour of States in cyberspace. Moreover, their expertise is important for capacity building efforts. It is essential for States to harness this knowledge and to benefit from a rich pool of ideas.

14. Decision-making and negotiation within the PoA should remain the prerogative of member States. In addition, the PoA should allow for broad and meaningful participation and contributions of the multistakeholder community in the annual formal meetings, review meetings and technical working group meetings. Modalities for the proceedings of PoA meetings and working groups should therefore allow stakeholders to attend formal and informal sessions, deliver statements and provide oral and/or written inputs for consideration of member States.

IV. Preparatory work and modalities for establishment of the PoA

15. As recommended by the 2021 GGE and OEWG reports, the PoA should be further elaborated including at the 2021-2025 OEWG process. Therefore, there should be within the current OEWG process dedicated sessions on the PoA. Outcomes of these sessions should be reflected in the respective annual progress reports of the OEWG.

[1] Available at the UNIDIR Cyber Policy Portal https://nationalcybersurvey.cyberpolicyportal.org/

16. In addition, intersessional multistakeholder consultations should be held to gather their views and suggestions on the PoA and its establishment.

17. Establishment of the PoA should be based on a decision/resolution by the UN General Assembly, on the basis of the preparatory work done including in the 2021-2025 OEWG. Member States may wish to hold a dedicated UN conference to establish the PoA.

18. The PoA should be <u>operational after conclusion of the 2021-2025 OEWG</u>.