

National contribution to the Secretary General's report on the cyber Programme of Action

The Kingdom of the Netherlands

April 2023

Introduction

The Netherlands continues to be deeply concerned by the growing risk of the malicious use of ICTs by State and non-State actors to international security and stability, economic and social development, and the safety and well-being of individuals. It is also noted that different levels of capacity for ICT security among States can increase vulnerability in an increasingly interconnected world.

To address these challenges, States have developed, through the work of a series of intergovernmental processes, a cumulative and evolving framework for responsible State behaviour in the use of ICTs in the context of international security. The General Assembly has repeatedly endorsed this framework through consensus resolutions.

To build on these achievements, the Netherlands underlines the need to establish a regular institutional dialogue after the conclusion of the current Open-ended working group on security of and in the use of information and communications technologies 2021-2025 (OEWG), established pursuant to General Assembly resolution 75/240. To this end, the Netherlands supports the initiative to establish a future Programme of Action to Advance Responsible State Behaviour in the Use of Information and Communication Technologies in the Context of International Security (PoA), welcomed by the General Assembly in its resolution 77/37.

In accordance with operative paragraph 3 of this resolution, this submission contains the Netherlands' views on the desired scope, structure and content of the PoA, as well as the preparatory work and modalities for establishment. In particular, it proposes a practical mechanism to facilitate capacity-building within the PoA.

Scope and objectives

The Netherlands, reaffirming the operative paragraph 1 of General Assembly resolution 77/37, is of the view that the main scope of the PoA should be (a) to support States' capacities and efforts to implement and advance commitments to be guided by the framework for responsible State behaviour; and (b) to discuss, and further develop, if appropriate, this framework on the basis of consensus. While maintaining its focus on matters related to international peace and security, the PoA should also enhance synergies with other relevant efforts, including those related to cybercrime, connectivity, cyber capacity-building and digital development.

Structure

The Netherlands shares the view that the programme of action should be an inclusive, transparent, consensus-driven and results-based process. The PoA's mandate could be derived from a founding document affirming States' political commitment to be guided by the framework for responsible State behaviour in cyberspace, and establishing a mechanism to further operationalize its objectives.

The PoA should be inclusive, open to participation by all UN Member States, permanent observers, intergovernmental and other organizations and specialized agencies. Furthermore, while States have the primary responsibility for the maintenance of international peace and security, the PoA should also allow for the meaningful participation, including in formal settings, of relevant non-governmental stakeholders, including the private sector, academia and civil society.

The structure of the PoA could comprise of regular meetings to adopt decisions and recommendations by consensus, as well as work undertaken in technical work groups, open to participation of relevant stakeholders, dedicated to specific issues, including, *inter alia*, to study how new and emerging technologies impact international peace and security in cyberspace.

Content

Facilitating capacity-building within the PoA will bolster and streamline international cooperation to advance the worldwide implementation of the normative framework. The PoA could also build synergies with existing capacity-building resources on a broader set of cyber-related issues, such as connectivity, countering cybercrime, as well as broader efforts to bridge the digital divide.

The Netherlands proposes a practical mechanism to facilitate capacity-building within the Programme of Action. The proposal is based on a four-step cycle of (1) developing a set of PoA Areas of Capacity Building (ACBs); (2) self-assess and identify needs; (3) matching needs with resources; and (4) a feedback loop.

Step 1: developing a set of PoA “Areas of Capacity Building”

Under the Programme of Action, States could together develop a set of PoA-endorsed “Areas of Capacity-Building” that are instrumental to the implementation of the framework for responsible State behaviour. A similar approach has been taken with the “Areas of Assistance” identified in the PoA to Prevent, Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons in All Its Aspects (PoA SALW). The Areas of Capacity Building, or ACBs, would build on the rich practical guidance for implementation provided in the consensus OEWG and GGE reports and would be reviewed periodically to remain up-to-date. The ACBs would provide a common framework that translates the consensus outcomes to practical action on, for example, critical infrastructure protection, incident response, policies and strategies, CERTs, etc. They should also be flexible to ensure they can be adapted to the diverse contexts and priorities of each State. In identifying the Areas of Capacity-Building, States could draw from the work undertaken by UNIDIR on *Unpacking Cyber Capabilities Needs: a Threat-based Approach* and the Singapore-UNODA Norms Implementation Checklist, as well as tools developed by other stakeholders, such as the Cybersecurity Capacity Maturity Model for Nations developed by the University of Oxford.

Step 2: self-assessment and identification of needs

Based on the Areas of Capacity Building and the accompanying tool, States can voluntarily conduct a self-assessment to identify their cooperation and capacity-building needs and gaps. This would ensure national ownership and a needs-based approach to capacity-building. The UNIDIR Survey of National Implementation provides a useful tool to undertake such a self-assessment. States can then choose to share the outcomes of their self-assessment in the PoA, for example at a technical working group.

Step 3: matching needs with resources

As a next step, the PoA would provide a convening platform to match the identified capacity-building needs with resources. The PoA would serve as a hub where providers of capacity-building can exchange with States seeking capacity-building resources to address the capacity-gaps identified in the ACBs. Providers of capacity-building would be encouraged to make available resources dedicated to the ACBs, thereby helping to mobilize more resources for capacity-building with a common purpose. The Secretariat could support States by maintaining an online overview of capacity-building needs and available resources. This overview would integrate existing tools such as the Cybil Portal of the GFCE, as well as other potential UN portals or repositories proposed by several Member States in the 2021-2025 OEWG. An easily accessible overview could also help States find available resources of cyber capacity-building in areas adjacent to international security (e.g. cybercrime, digital development, connectivity, etc.). This includes capacity-building work undertaken by, amongst others, regional organizations, ITU, Interpol, UNODC and the GFCE.

Capacity-building efforts as part of the PoA framework should be undertaken in accordance with the principles for capacity building agreed in the 2019-2021 OEWG.

Step 4: feedback loop

After capacity-building needs have been identified, successfully matched with resources and capacity-building is underway, the PoA platform would facilitate a feedback loop to report progress, share best practices and identify areas where the normative framework could be further developed.

The preparatory work and modalities for establishment of the PoA

Resolution 77/37 provides an initial roadmap towards establishing the PoA. Recalling the recommendations contained in the final reports of the 2019-2021 OEWG and 2019-2021 GGE that the PoA could be further elaborated in the 2021-2025 OEWG, the Netherlands welcomes further discussions on the scope, structure and content of the PoA within the OEWG, and welcomes operative paragraph 2 of resolution 77/37 stating that the “programme of action is to take into account the consensus outcomes adopted by the open-ended working group 2021-2025.” In that regard, the Netherlands would encourage further intersessional and dedicated sessions of the 2021-2025 OEWG to continue elaborating the PoA. The Netherlands also welcomes the General Assembly’s request to the Secretary General, contained in resolution 77/37, to convene series of regional consultations to share views on the PoA.

In 2025-2025, after the conclusion of the Open-ended Working Group, the Netherlands envisages an international conference, open to non-governmental stakeholders, building upon the preparatory work done including in the 2021-2025 OEWG, to be held to adopt the founding document.