Working paper for a Programme of Action (PoA) to advance responsible State behavior in the use of ICTs in the context of international security

From the General Assembly's first discussions recognizing that information and communication technologies (ICTs) both provide broad positive opportunities for the development of civilization, and can potentially be misused for purposes inconsistent with the objectives of maintaining international security, through six Groups of Governmental Experts (GGE) and one Open-Ended Working Group (OEWG) on Developments in the Field of ICTs in the context of International Security, the General Assembly has elaborated a framework for responsible State behavior in ICTs in the context of international security, which includes international law, non-binding norms, rules and principles, and confidence-building measures, supported by cooperation and capacity-building measures. This framework has been endorsed notably by UNGA resolution 70/237 and the consensus final report of the OEWG established pursuant to resolution 73/27.

While continued engagement in constructive dialogue at the United nations is welcome, to further the discussions on the norms applicable to the use of ICTs, there is now also a need for concrete action to effectively tackle the rising international security threats in cyberspace, and to make concrete progress in the implementation of the agreed framework, bearing in mind in particular that "the international community's ability to prevent or mitigate the impact of malicious ICT activity depends on the capacity of each State to prepare and respond"[1]. It is crucial to strengthen international cooperation and support the capacities of all States in an inclusive, coordinated and efficient manner.

To that end, a proposal for a UN Programme of action (PoA) is currently co-sponsored by 54 States[2]. This proposal is aimed at advancing responsible State behavior in the use of ICTs, and ultimately strengthening international security and stability in the cyber domain, through actionable proposals and enhanced support for tailored capacity-building efforts. The PoA would be established as a permanent, action-oriented, inclusive, transparent, and results-based mechanism, building on previous outcomes and in line with the evolving framework. It could work in a complementary and coordinated fashion with other relevant UN processes, such as the OEWG established pursuant to resolution 75/240.

This proposal has been noted in both the Final consensus report adopted in March 2021 by the OEWG established pursuant to resolution 73/27, and the Final report adopted in May 2021 by the GGE established pursuant to resolution 73/266, as a prominent proposal to support the capacities of States in implementing their commitments in their use of ICTs and advance responsible State behavior in cyberspace. As recommended by these reports, the co-sponsors wish to further elaborate this proposal, taking into account the views and needs of all States, as well as the input of other stakeholders, with a view to the possible establishment of a UN PoA.

This paper is meant to provide (I) elements of a vision for the PoA's structure and content, and (II) modalities for its establishment and organization, to serve as a basis for further discussion.

I/ **Elements of vision for the PoA**

The PoA would be based on a political declaration *(see below for modalities of adoption)*, which would recall existing and emerging threats to international security related to the malicious uses of ICTs, building notably on the threat assessments contained in GGE and OEWG reports, and reaffirm States' commitment to the framework agreed in successive GGE reports and the 2021 OEWG report. The PoA

[1] Paragraph 54, Final report of the 2019-2021 OEWG.

[2] Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Chile, Colombia, Croatia, Republic of Cyprus, Czech Republic, Denmark, Ecuador, Egypt, Estonia, France, Finland, Gabon, Georgia, Germany, Greece, Guatemala, Hungary, Iceland, Ireland, Italy, Japan, Latvia, Lebanon, Liechtenstein, Lithuania, Luxembourg, Malta, Monaco, Montenegro, Morocco, Netherlands, Norway, Poland, Portugal, Republic of Korea, Republic of Moldova, Republic of North Macedonia, Romania, Salvador, Singapore, Slovakia, Slovenia, Spain, Sweden, Switzerland, Ukraine, United Arab Emirates, United Kingdom.

could also support the implementation of additional norms, rules and principles which may be agreed in the future *(see below)*.

The PoA would function as an action-oriented instrument to advance the implementation of this framework, in particular by (1) identifying the diverse challenges faced by States and promoting relevant actionable recommendations and cooperation to respond to these challenges, (2) providing concrete support for capacity-building efforts including through a working group dedicated to it, (3) fostering meaningful multi-stakeholder engagement.

In addition, the PoA would provide a periodic opportunity to assess whether additional actions are needed to respond to challenges in a rapidly evolving ICT environment *(see below)*.

(1) Identify the challenges and promote relevant actions as well as cooperation

The PoA would firstly aim at precisely mapping the specific needs and challenges faced by diverse States to effectively implement the framework. States would be encouraged to report on their national implementation efforts (possibly by using tools such as the "National survey of implementation of UNGA resolution 70/237") and conduct gap analyses, to determine their needs and the priority areas for action. Such reports and gap analyses could be conducted on a rotating basis, to avoid overburdening States, which could also consider clustering and aligning their processes to benefit from each other's experiences and efforts.

To address these challenges and promote actionable solutions suited to the diverse needs of States, the PoA would also serve as a platform to exchange best practices and actionable recommendations, to be implemented at the national, regional and international level (e.g. in terms of adaptation of the legislative and administrative framework, identification and protection of critical infrastructure, etc.). The PoA could include an annex which would list relevant initiatives taken by regional organizations.

The PoA would also take practical steps to further international cooperation and transparency, by establishing a repository of national point of contacts, and creating a portal for States to share their national positions and contributions regarding their understanding of how international law applies to the use of ICTs. UNIDIR's Cyber security portal may be used to that end. *[Other stakeholders' working papers could also be welcome on such a portal : see below.]*

(2) Provide concrete support for capacity-building efforts including through a working group dedicated to it

The PoA could leverage existing and potential capacity-building efforts, increase their visibility and improve their coordination. The PoA could consider utilizing relevant existing tools put in place by regional organizations or the civil society, to share data, information and best practice on global capacity-building efforts[3]. The PoA could also support the mobilization of resources and assist with pairing available resources with requests for capacity-building support and technical assistance.

PoA meetings would also provide an opportunity to exchange on ongoing capacity-building efforts and identify areas where additional action is needed. The PoA could contribute to strengthening capacity-building efforts with a dedicated funding mechanism, and/or by relying on existing or new instruments, such as the World Bank cybersecurity multi-donor trust fund. Capacity-building actions supported by the PoA would be consistent with the principles set out in paragraph 56 of the OEWG final report.

The PoA could create a special working group to examine, develop, coordinate or/and expand diverse initiatives projects for capacity building.

[3] Examples of such tools, that States may consider leveraging as appropriate, could include initiatives such as the Cybil portal developed by the Global Forum Cyber Expertis (GFCE), EU CyberNet, etc.

(3) Foster meaningful multi-stakeholder engagement

While the PoA would remain a State-driven process, cooperation with the multistakeholder community brings practical benefits for security, lifts capacity, and takes forward development. Therefore the PoA will allow for regular consultations with relevant stakeholders, including the private sector, academia and the civil society, to consider and provide their unique perspectives uponrelevant issues.
The Chair could convene a day of consultative meetings open to interested parties, prior to each Review Conference and Annual Meeting, to share views on relevant issues, and stakeholders may be invited by the Chair as participants or observers to the Review Conference and/or other meetings, without prejudice to States' prerogatives.

The multi-stakeholder community could also be encouraged to submit working papers to PoA meetings and could be consulted on specific topics when appropriate. A web portal could also be created for the multi-stakeholder community to share its views and suggestions.

The PoA could encourage States to cooperate with other stakeholders in particular to : develop coordinated government and corporate policies to improve the security of the ICT supply chain, and build trust; harmonize mechanisms for the responsible disclosure of vulnerabilities and prevent the proliferation of malicious tools and techniques; encourage research in relevant areas; enhance capacity building efforts based on needs and existing gaps; promote a culture of cybersecurity in the larger public.

II/ <u>Possible Modalities for the establishment and organization of the PoA</u>

(1) Establishment of the PoA

Inclusive consultations will be conducted to seek States' views on the Programme of action. Consistent with the recommendations contained in paragraph 77 of the OEWG final report and paragraph 97 of the 2021 GGE final report, consultations could take place within the OEWG created pursuant to resolution 75/240. Informal consultations and other events would also be organized, including with other stakeholders.

Venues for consultations and events may include :
- The Internet Governance Forum (December 2021) ;
- The OEWG established pursuant to resolution 75/240 (December 2021) ;
- The World Summit on the Information society (WSIS) 2022 (May-June 2022).

Consultations would be conducted at the regional level as well.

These consultations would also provide opportunities to share and discuss further options for modalities as well as analysis and lessons learned from previous PoAs, such as the PoA to Prevent, Combat, and Eradicate the Illicit Trade in Small Arms and Light Weapons (SALW). Learning from the experiences of comparable instruments, the PoA could ensure clarity on its goals and scope from the outset, ensure built-in flexibility and ability to keep up with the pace of technological change and allow for meaningful stakeholder participation.

At the end of these consultations, a resolution could be adopted at the First Committee of UNGA to establish the PoA.

(2) Meetings

Reviewconferences. Review conferences could be held for a duration of five to ten working days. They would examine the state of implementation of the framework, identify main priorities for action in the following years, and consequently adopt a Programme of work for subsequent meetings *(see below)*. Review conferences may also decide to update the framework by including new principles, recommendations and commitments in the event that UNGA, by consensus, endorses a report of a relevant UN process, and/or by consensus agreement during a PoA Review Conference. The PoA could therefore support the implementation of additional norms, rules and principles which may be agreed in the future.

Periodic meetings. These meetings would follow up on the Programme of work adopted by the Review conference. The participation of relevant technical experts from governments would be encouraged to foster substantive works. Intersessionnal meetings may be held, or informal working groups may be created to focus on specific aspects of the Programme of work.

(3) Rules of procedure

The UN PoA shall function under the rules of procedure relating to the Main Committees of the General Assembly with such modifications as the Member States may deem necessary, and ensure that decisions on substantive issues are adopted by consensus, including updates to the Political Declaration.

(4) Secretariat

UNODA could provide Secretariat services for the PoA.

(5) Sponsorship programme

To foster inclusivity, equal gender participation, capacity-building and achieve the widest possible participation from States, a sponsorship programme funded by voluntary contributions could be established to help experts attend relevant meetings.

Recognizing the gender dimensions of cyber security, the PoA will promote the full, equal and meaningful participation of women and address the gender aspects of cyber security in its work.

(6) Coordination with other relevant UN processes

The PoA would act as complementary and coordinated with other relevant UN processes. The PoA is not intended, nor designed to duplicate or replace any other negotiation format on the use of ICTs in the context of international security within the UN system.

The substance of the PoA's work would focus on the implementation of the agreed acquis as it resulted from the work of the UN GGE and OEWG mechanisms. The recommendations of both the 2021 report of the OEWG and the GGE refer to a PoA.

The work of the PoA is fully compatible with any subsequent consensus agreement on the governance of cyberspace within the OEWG or other mechanisms. The PoA holds an open-ended mandate which could be used to support implementation of any such agreements in the future.