Multistakeholder Feedback on the Current State of the Program of Action on Cybersecurity

July 2023

In December 2022, the UN General Assembly adopted the resolution 77/L.73 which welcomes the proposal to establish a Programme of Action (PoA) to advance responsible State behaviour in the use of information and communications technologies in the context of international security, calling for further discussion in this regard. The zero draft of the OEWG's second Annual Progress Report, as released by the Chair in June 2023, provides further details on the general scope and objectives of the future permanent mechanism and outlines a work agenda running up to 2025.

Currently, intergovernmental negotiations on the scope, structure and content of the Cyber PoA are therefore still in the early stages. In light of this, the UN Office for Disarmament Affairs has endeavored to gather input from States and regional organizations over the past months, which will be compiled into a report commissioned by the Secretary General. Alongside this effort, the Paris Peace Forum, acting as the secretariat of the Paris Call for Trust and Security in Cyberspace, has joined forces with the Global Forum on Cyber Expertise (GFCE) and the Cybersecurity Tech Accord to foster coordination within the stakeholder community and ensure that the discussions on the Cyber PoA are reflective of their collective concerns and aspirations.

This common position paper was conceived following an online consultation launched in June 2023. Respondents from across the multistakeholder cybersecurity community, were asked to answer a series of questions ranging from mechanisms of implementation of the Cyber PoA, to capacity building and confidence building measures within the mechanism. This consultation and its initial findings shall be regarded as a minimum baseline upon which each endorsing organization may build on, according to its own priorities or specific areas of expertise. This process will be taken further as States will be moving forward with the establishment of the Cyber PoA, with regular milestones at the occasion of the OEWG sessions.

Among the 33 written inputs received as part of this first step, 15 of them came from the private sector (45.5%), 3 from the technical community (9.1%), 10 from the civil society and academia (30.3%) and 5 from public authorities and international organizations (15.2%). The below summarizes the responses received during the consultation period.

I – Structure and scope of the PoA

- States should first and foremost strive to leverage rather than to duplicate existing bodies, mechanisms and other existing initiatives on cyber and digital policy, as this may lead to damageable fragmentation of efforts by the international community to secure cyberspace. The articulation of the Cyber PoA with such established bodies, mechanisms and initiatives, including within the UN system, should be precised as clearly as possible. Particular attention should be given to processes emanating from regional organizations and non-governmental, multi-stakeholder initiatives – which will be key in the buy-in of all stakeholders worldwide – in addition to those developed under the auspices of international organizations

- States should draw lessons from existing PoAs and other comparable permanent, multilateral mechanisms - including beyond the field of disarmament and international security as covered by the First Committee of the United Nations General Assembly. A precise identification of the structural strengths, weaknesses and pitfalls of such mechanisms should inform States' discussions when developing the Cyber-PoA.

- The work undertaken in the framework of the Cyber PoA should be organized around precise and clearly defined issues addressed to achieve specific, tangible outcomes. This methodical approach will enable States to comprehensively consider all relevant aspects associated with each issue, including local and regional specificities when reflecting on the implementation phase, while mitigating the potential risks of excessive politicization.

- The Cyber PoA should be a privileged platform for States to proactively share their national doctrines regarding responsible behavior in cyberspace overall as well as on their use of both defensive and offensive cyber capabilities.

- The cyber PoA should consider existing digital development agendas in the framework of the United Nations and focus on the nexus between digital development and international cyber security. To that end, it should focus on cyber capacity-building with all relevant actors.

II – Substance of the PoA

- The Cyber PoA should clearly prioritize the clarification of existing States' positive and negative obligations based on international law as well as the implementation of the already agreed framework on responsible State behavior - as enshrined in relevant GGE and OEWG reports as well as UNGA resolutions. In the same spirit, the Cyber PoA should strive to develop effective mechanisms to build a sense of accountability and means of verification where relevant. This is especially true when considering the protection of critical infrastructures, for which clarification of the very concept should also be prioritized considering possible impacts on populations. In this regard, the work could especially focus in the first place on information sharing and emergency mechanisms.

- The Cyber PoA should be a preferred platform for States to exchange perspectives on actual and emerging threats to the ICT environment, as well as the impact of emerging technologies to cyber security.

- In order to enhance accountability with regards to the agreed framework, the Cyber PoA should create the incentives for transparency through effective review procedures based on agreed-upon goals and metrics, such as standardized reporting tools, a yearly report of implementation or other peer review processes. International Human Rights Mechanisms might serve as a useful point of reference when designing such review procedures. Furthermore, the cyber PoA's review procedures should not only allow for significant involvement from non-governmental stakeholders but also require their support in raising awareness and assisting States in reporting.

- Advancing the implementation of the agreed framework of responsible State behavior in the ICT environment will only be possible if the Cyber PoA also serves as a vehicle for streamlining cyber capacity-building efforts worldwide in a way that would be needs- and context-driven, when relevant to international security. The Cyber PoA thus shouldn't duplicate existing

mechanisms in this field, but should rather aim at building on existing initiatives, identifying the needs and matching them with available resources while relying on and engaging trusted stakeholders. This effort should be carried out according to clear goals, timelines, and sustained by regular impact reviews. One expected goal of such endeavor could for instance be to facilitate the development of clear blueprints for public-private partnerships for cyber security.

- The Cyber PoA should allow for the design and operationalization of Confidence Building Measures (CBMs) in order prevent the escalation of tensions, improve mutual understanding and trust, and thus enhance the overall security in, and stability of cyberspace. States could build on existing CBMs proposed as part of previous GGEs and OEWGs reports as well as from regional organizations by seeking to implement them, especially by prioritizing those related to the protection of critical infrastructures and to vulnerabilities reporting. The Cyber PoA could also in this regard leverage the expertise of relevant NGOs, CERTs, Cybersecurity Centers, industry associations (such as ISACs).

III – Meaningful stakeholder inclusion in the PoA

- Meaningful stakeholder inclusion in the Cyber PoA should not be pursued as a matter of principle but draws on the objective contribution of the stakeholder community to intergovernmental processes related to international security. As the ICT environment is composed of infrastructures and technologies that are developed, owned and operated by private actors for a significant part, and as the Internet has been governed through a multistakeholder scheme since its foundation, non-governmental stakeholder bears both an irreplaceable experience and knowledge of cyberspace. They can also substantially contribute to better understanding dynamics at stake in, and in the use of the ICT environment while providing innovative inputs concerning the implementation of the agreed framework, and the elaboration of additional rules where relevant.

- Upstream, the stakeholder community can substantially contribute to the work of the Cyber PoA by:
    - Providing written inputs to publications or documents published by the Cyber PoA, as well as providing written contributions and substantial

elements in other relevant formats to specialized PoA working groups, or to all States at the occasion of plenary sessions;
    - Sharing specific information and knowledge that are key for the completion of the cyber PoA's mandate, including but not limited to threat intelligence, vulnerability disclosure and emergency response, with the full participation of the technical community;
    - Should an open-source repository of stakeholders PoC be established, many stakeholders have expressed their interest in remaining at the disposal of States to contribute on more precise questions upon specific request. Such open-source repository of stakeholders PoC could be operationally supported by the stakeholder community.

- Downstream, the stakeholder community can fruitfully be mobilized to advance the Cyber PoA goals by:
    - Contributing to create and maintain the necessary political momentum to get actual implementation of the agreed norms and principles;
    - Contributing to foster accountability through independent expertise and monitoring, based on publicly available resources and data;
    - Contributing to mainstreaming the outputs of the Cyber PoA and possible guidelines to regional and local communities, including but not limited to providing operational support, translations in non-UN languages, and training the relevant administrations at the legal, policy and technical level.

- Overall, modalities of the Ad Hoc Committee to Elaborate a Cybercrime Convention (AHC) which feature extensive and substantial input from the multistakeholder community both during intersessional organized by the Chair and during substantive sessions, should be considered as a baseline for the ones of the upcoming Cyber PoA.

The following organizations endorse this common position paper:

- APCO Worldwide
- Cybersecurity Tech Accord
- Global Forum on Cyber Expertise
- Paris Peace Forum
- Center for Multilateral Affairs
- CyberPeace Institute
- Digi Americas Alliance
- DXC Technology
- Global Partners Digital
- Hitachi America Ltd
- ICT4Peace Foundation
- MSD
- Summit V
- Telefónica

Organizations interested in supporting the text and joining this common effort may contact: pablo.rice@parispeaceforum.org