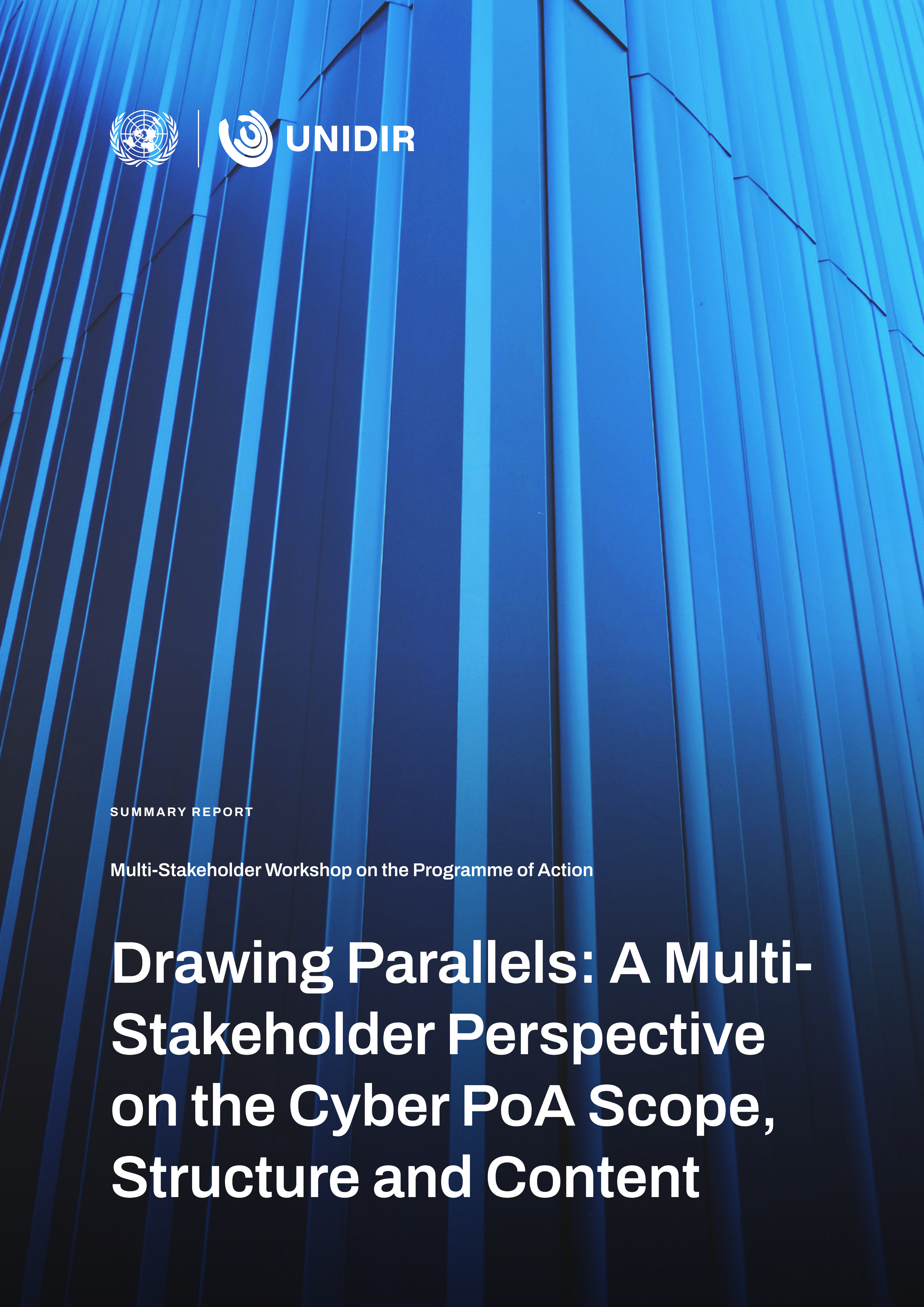


SUMMARY REPORT

Multi-Stakeholder Workshop on the Programme of Action

Drawing Parallels: A Multi-Stakeholder Perspective on the Cyber PoA Scope, Structure and Content

Acknowledgements

Support from UNIDIR core funders provides the foundation for all of the Institute's activities. This study is part of UNIDIR's Security and Technology Programme cyber workstream, which is funded by the Governments of Czechia, France, Germany, Italy, the Netherlands, Norway, Switzerland, and the United Kingdom, and by Microsoft.

About UNIDIR

The United Nations Institute for Disarmament Research (UNIDIR) is a voluntarily funded, autonomous institute within the United Nations. One of the few policy institutes worldwide focusing on disarmament, UNIDIR generates knowledge and promotes dialogue and action on disarmament and security. Based in Geneva, UNIDIR assists the international community to develop the practical, innovative ideas needed to find solutions to critical security problems.

Note

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries. The views expressed in the publication are the sole responsibility of the individual authors. They do not necessarily reflect the views or opinions of the United Nations, UNIDIR, its staff members or sponsors.

About the Author

This report was produced by **UNIDIR Security and Technology Programme.**

Photos by **Possessed Photography** on **Unsplash**.

Contents

1. Introduction and Overview of Workshop

Since the proposal for the Programme of Action for advancing responsible State behaviour in cyberspace (henceforth the ‘cyber PoA’) was first submitted to the Open-ended Working Group on security of and in the use of information and communication technologies 2021–2025, its envisaged mandate as a regular institutional dialogue mechanism has been a key issue of discussion.[1] Many different perspectives have been advanced over the years, from assisting States to implement the norms, rules and principles of responsible state behaviour through provision of capacity building, to providing a platform for further discussions on the development of new norms to address emerging and existing threats. Although most parties to the debate agree that the cyber PoA could be a practical, action-oriented implementation mechanism, they have yet to reach agreement on how the cyber PoA could be established, and on its scope, structure, and content.[2]

Pursuant to General Assembly resolution 77/37 requesting Member States’ views on the scope, structure, and content for the cyber PoA, and the preparatory work and modalities for its establishment, including at an international conference,[3] Member States of the United Nations had the opportunity to submit written inputs expressing their views on the cyber PoA and a series of regional consultations on this subject were organized by the United Nations Secretariat.[4]

To support the development of a shared understanding on the mandate and role of the cyber PoA, and acknowledging the critical role that the multi-stakeholder community already plays in the implementation of the framework of responsible State behaviour, UNIDIR offered a platform to non-governmental organizations, civil society organizations, academic institutions, and the private sector to share their perspectives on the prospects of establishing a cyber PoA.

This offer included a call for written inputs followed by a workshop to further elaborate on the development and operationalization of a PoA with a view to contribute to the discussions on this important topic in both the Open-ended Working Group and the First Committee.

[1] Summary of the Proposal: explore establishment of a Programme of Action for advancing responsible State behaviour in cyberspace with a view to ending the dual-track discussions (GGE/OEWG) and establishing a permanent United Nations forum to consider the use of information and communication technology by States in the context of international security; see https://front.un-arm.org/wp-content/uploads/2020/12/joint-contribution-PoA-future-of-cyber-discussions-at-the-un-2-2-2020.pdf.

[2] See “Concept-note on the organizational aspects of a Programme of Action for advancing responsible State behaviour in cyberspace”, https://front.un-arm.org/wp-content/uploads/2020/12/sponsors-oewg-concept-note-final-12-2-2020.pdf.

[3] General Assembly, “Programme of action to advance responsible State behaviour in the use of information and communications technologies in the context of international security”, UN document A/RES/77/37, 12 December 2022.

[4] Ibid.

The workshop “Drawing Parallels: A Multi-Stakeholder Perspective on the Cyber PoA Scope, Structure and Content” was convened to bring together experts and stakeholders to discuss and identify areas of convergence. The event provided a platform for participants to share their knowledge, experience and perspectives on scope, content, structure, and the most effective strategies and approaches for designing a PoA.

Based on the analysis of the workshop and written inputs, this report presents a consolidated set of considerations and options for action to inform States’ discussions on the PoA.

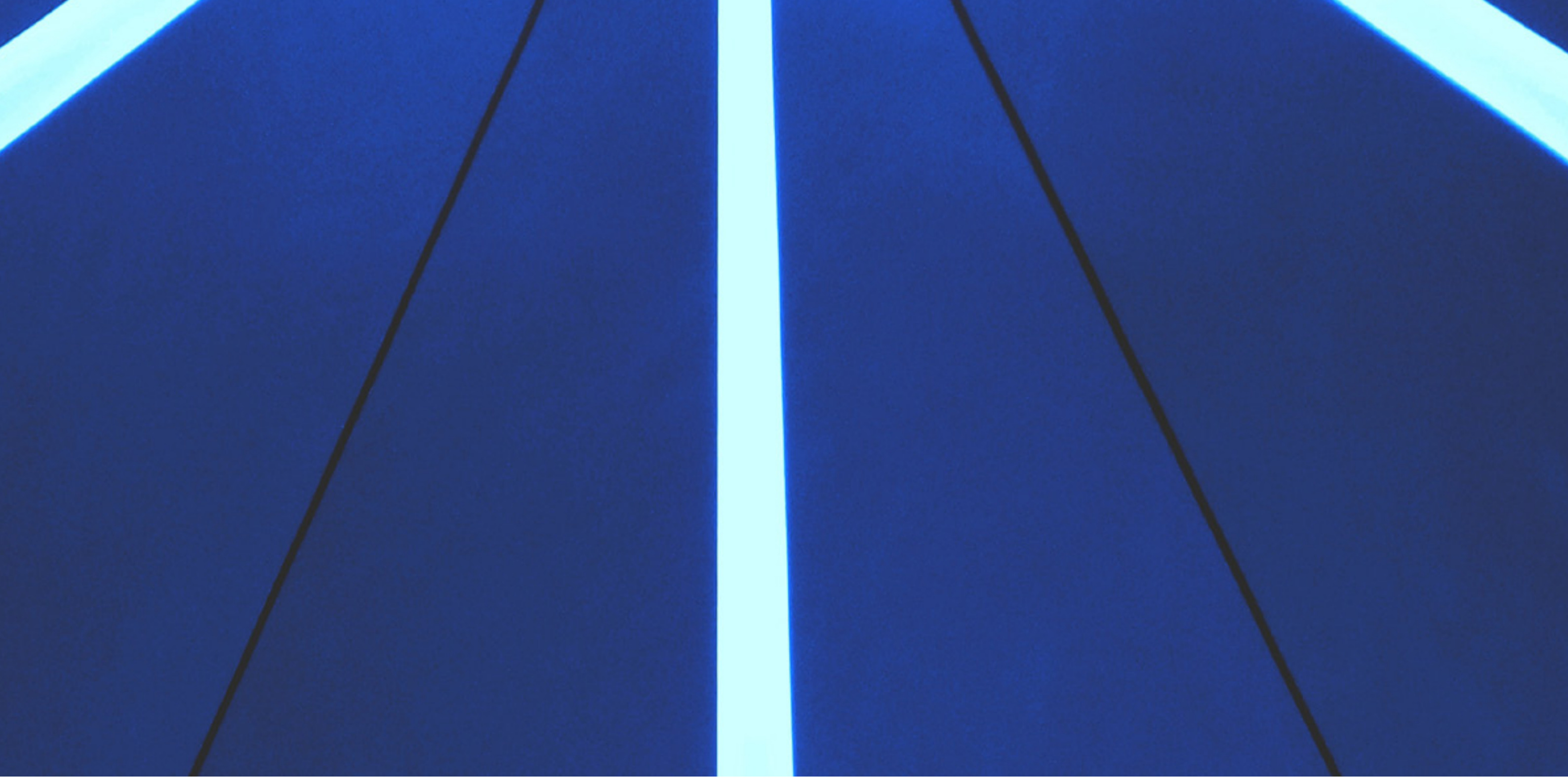
The workshop was divided into four sessions. The first session was dedicated to a presentation on existing United Nations Programmes of Action. The second and third sessions, convened under the Chatham House Rule, included a multistakeholder presentation and discussion on different capacities and competencies that a future PoA can leverage and a thematic discussion on scope, structure and content of the PoA. A series of guiding questions based on the preambular and operative paragraphs of the General Assembly resolution[5] were used to structure the discussion.

It is important to note that the views and written contributions included in this report are neither representative of the entire stakeholder community, nor should they be intended as being the product of consensus. Collectively, the contributions provide a wide range of concrete ideas for States to consider when elaborating the cyber PoA.

The collection of written inputs received by various stakeholders is provided as Annexure 2 to this report.

The report is structured into three sections. After this brief introduction, the second section reviews existing PoAs to offer insights into lessons learned, highlighting their relevance for States’ discussions on a cyber PoA. The third section on multi-stakeholder participation in the cyber PoA presents a concise summary of the inputs received during the workshop, encompassing perspectives from diverse stakeholders representing various sectors such as industry and civil society. Sections 4, 5, and 6 delve into the key takeaways for States to consider regarding the scope, content, and structure of the cyber PoA, drawing upon the analysis of workshop discussions and written contributions. Lastly, the report concludes with a final section on additional considerations.

[5] Ibid.



2. Review of Existing PoAS: Lessons Learned and Good Practice[6]

Reviewing the existing Programmes of Action may provide valuable insights and examples of good practices for the development and implementation of a cyber PoA. This section of the report provides an overview of the points raised by workshop participants in this regard.

2.1 What is a Programme of Action (PoA)

Lessons Learned

A PoA is an instrument, like a roadmap, which outlines concrete actions and activities to be implemented by endorsing parties to achieve shared objectives at various levels. It is non-legally binding.

[6] This section of the report is based on the presentation delivered by Ms Allison Pytlak, Program Lead of the Cyber Program at the Stimson Center, who highlighted key elements from some 10 PoAs that could be used to inform the design, implementation, and evaluation of the envisaged cyber PoA. For more information on options and lessons deriving from other Programmes of Actions, see also: Allison Pytlak, ***Advancing A Global Cyber Programme Of Action: Options and Priorities***, Women's International League for Peace and Freedom, May 2022.

Good Practice for the Cyber PoA

The cyber PoA can serve as a political instrument to demonstrate the political will and commitment of States in advancing the framework and addressing malicious use of information and communications technologies (ICT) impacting international security. It can create a sense of urgency in protecting cyberspace as a global common and mobilize support from stakeholders. The cyber PoA could be designed to be adaptable, allowing for revisions over time, encouraging wider stakeholder participation, promoting cooperation and collaboration without the need for legal agreements, and facilitating innovative approaches to achieve its objectives.

2.2 What are Common Elements of PoAs

Lessons Learned

There are seven common elements and characteristics of PoAs: a declaration, articulation of goals, action-oriented language, roles and responsibilities, mandate, relationship with the United Nations, and follow-up mechanisms.[7] Learning from existing PoAs in other fields can provide valuable examples of engagement between States and stakeholders, including the use of reporting mechanisms and the relationship with the United Nations.

Good Practice for the Cyber PoA

The cyber PoA presents an opportunity for States and stakeholders to provide inputs on each of the elements. Gender mainstreaming and the involvement of stakeholders were identified as important aspects that States could include in the text of the political declaration or the text of the cyber PoA. Regarding the relationship with the United Nations, participants supported complementarity with ongoing and future intergovernmental bodies under the United Nations's auspices. The cyber PoA could make recommendations on the establishment of United Nations bodies, such as Groups of Governmental Experts, and provide regular briefings to the First Committee on disarmament and international security. On the mandate, some priority activity areas could be included to promote responsible use of ICT, respect for human rights and fundamental freedoms in the use of ICT, the development of measures and mechanisms to hold malicious actors accountable and promote and strengthen discussions on how international law applies in cyberspace.

[7] Presentation by Allison Pytlak.

2.3 The Impact of PoAs

Lessons Learned

The impact of PoAs has to do with how they have contributed to the advancement of both discussion and action in their respective domains. The impact of PoAs on their subject matter has been significant. They have proven to be effective in mobilizing resources and support from various stakeholders, leading to funding, expertise, and collaboration. PoAs have also been successful in building partnerships, raising awareness, and translating broad goals into measurable activities.

Good Practice for the Cyber PoA

In the context of the cyber PoA, States could consider engagement of stakeholders who play a variety of roles including, but not limited to, incident response, development and deployment of ICT hardware and software, and the convening of stakeholders working across sectors to advise States as necessary. Participants also suggested that a funding mechanism for capacity-building and partnerships could be a strong feature of the cyber PoA especially for developing and small States.

2.4 The Impact of Stakeholders through PoAs

Lessons Learned

Stakeholders have played a crucial role in existing PoAs, particularly in raising awareness among victims or those affected, conducting research and analysis, and engaging in public outreach. The concrete involvement of civil society, religious leaders, the private sector, and youth in the PoA against racism serves as a good example of how the cyber PoA can proceed.

Good Practice for the Cyber PoA

A starting point could be a comprehensive stakeholder analysis of all relevant and interested stakeholders in the cyber PoA. The cyber PoA could urge different stakeholders to, as appropriate, develop and support action-orientated activities including research, promote and sponsor dialogues and partnerships in the case of civil society, and, for the private sector, consider developing voluntary codes of conduct. Such targeted roles if identified and included in the cyber PoA could facilitate greater awareness and better understanding of the scope of the problems associated with malicious activities in cyberspace.

3. Multi-Stakeholder Participation in the Cyber PoA: Civil Society, Academia, Industry and NGOs

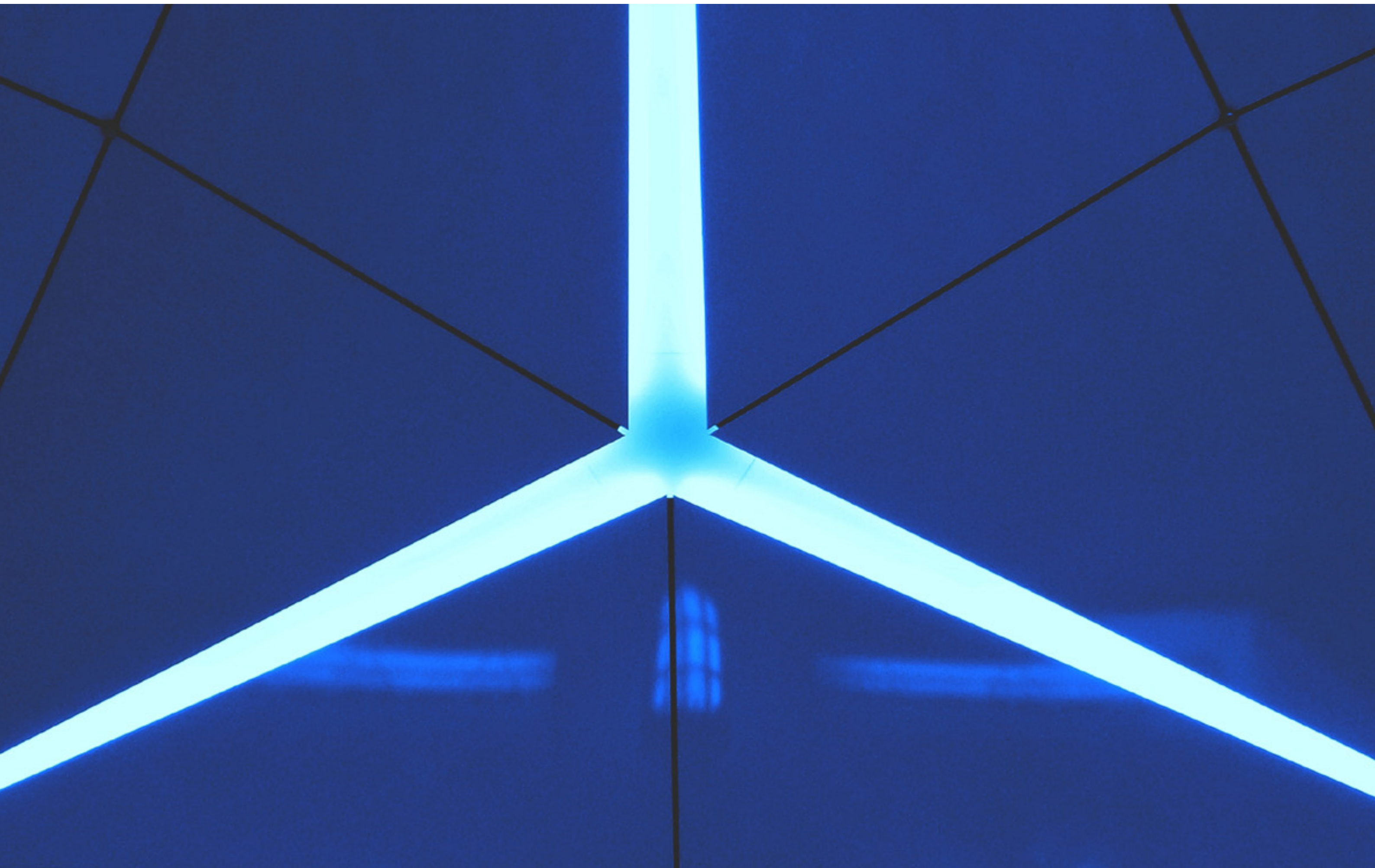
The non-State stakeholder ecosystem involves a wide range of actors, including Industry (cybersecurity companies, telecommunications companies, internet service providers, hardware and software manufactures) and non-governmental organizations (advocacy groups, humanitarian organizations, community base organizations). Each of these actors have different roles and responsibilities and interests in the cyber PoA. The challenge of having many actors in the ICT governance ecosystem is that it can be difficult to coordinate and be aware of the actions of multiple stakeholders with different interests and priorities.

Invited organizations highlighted the concern over the proliferation of malicious ICT tools and the differentiated impact they have on members of society. The organizations explained the work they are doing to address each area of concern and outlined functions that could be leveraged by States in a future cyber PoA. Subsequently, participants engaged in an open debate, highlighting the following issues:

- On malicious ICT tools, some stakeholders noted their unique capability to respond in the event of a malicious ICT incident and their insights into the tactics, techniques and procedures of malicious actors. This unique capability can be immediately leveraged in the cyber PoA by States in response to calls for access to early warnings, threat intelligence and response measures.
- Stakeholders reflected on the role of human rights advocacy to promote the protection of the digital rights of people and communities at risk by combining direct technical support and strategic advocacy for human rights in the digital age. The cyber PoA could be guided by a human-centric approach, which prioritizes the needs and well-being of people in the design, implementation, and evaluation of ICT policies. Practically, the cyber PoA could work to promote the protection of human rights, and activities of humanitarian and human rights organizations by mapping ICT threats in coordination with stakeholders that are already involved in this kind of work.
- To highlight the role of stakeholders to promote human rights in the digital environment, stakeholders noted that activities on capacity-building that include the development of toolkits for policymakers to assess State positions on use of ICT from a human rights perspective is a useful model that the cyber PoA could consider.
- There are several multi-stakeholder projects on ensuring a safe and ethical digital world. These multi-stakeholder ecosystems are consistently raising awareness on the importance of the framework for responsible State behaviour and sharing industry best practices and codes of

conducts—engaging and leveraging these entities could be priorities of the cyber PoA.

- The proliferation of malicious ICT incidents has inspired interest in understanding the impact on people. Stakeholders drew attention to proposed PoA activities which could include analysis of the human impact of systemic cyber threats, delivery of cybersecurity assistance, tracking of enforcement of international laws and norms, and forecasts of new threats to cyberspace. The expertise in working in proximity with the victims of cyberattacks and responding to requests for assistance can be leveraged in a cyber PoA to ensure that it remains up to date with developments in the use of ICT.
- To increase international collaboration, reducing overlap and duplication of efforts in the cyber capacity-building ecosystem, stakeholders also encouraged collaboration with entities already mapping capacity-building projects and matching providers and beneficiaries of capacity-building.



4. Considerations Regarding the Scope of the Cyber PoA

Under the general theme of the scope of the cyber PoA, participants focused the discussion specifically on purpose and objectives. Stakeholders agreed that having a shared and well-informed understanding of the purpose of the cyber PoA, which could be focused on promoting the implementation of the evolving and cumulative framework of responsible State behaviour[8] and consensus recommendations of the OEWG and GGEs while also embedding the participation and engagement of the multi-stakeholder community is important. The cyber PoA could be guided by the following objectives:

- **Promote the implementation of the framework for responsible State behaviour at the regional and global levels:** States could draft and endorse specific language in the preambular and operative paragraphs that welcomes and acknowledges the framework for responsible State behaviour, and the role of non-governmental actors and mainstream gender considerations at the national, regional and global levels.
- **Provide oversight for States' implementation of the framework:** The PoA could focus on establishing accountability measures and mechanisms for acts that undermine the framework, including activities that violate international law and undermine the norms of responsible State behaviour; monitor voluntary submissions of States' inputs on the implementation of norms; ensure effectiveness of initiatives established under the framework; and develop initiatives to improve cyber resilience of States.
- **Provide a negotiating platform for the discussion of potential gaps in the evolving and cumulative Framework**: This will serve a dual purpose of ensuring that the framework is responsive to emerging threats and developments in the use of ICT in the context of international security and provide an opportunity for an inclusive and transparent process of elaborating and adopting norms and confidence-building measures. The PoA platform could do this through regular briefings and engagement with the First Committee and recommend the establishment of an intergovernmental body and provide a roadmap of activities with specific focus on review or elaboration of new norms.

[8] The assessments and recommendations of the 2010, 2013 and 2015 consensus reports of the Groups of Governmental Experts (GGEs) and consensus reports of the 2021 and 2022 Open-ended Working Group on information and communication technologies on existing and emerging threats, norms, rules and principles of responsible State behaviour, international law, confidence-building and international cooperation and capacity-building, which together represent a cumulative and evolving framework for the responsible behaviour of States in their use of ICTs; see General Assembly, "Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security", UN document A/76/135, 14 July 2021.

- **Provide threat intelligence and access to incident response and recovery:** The PoA could provide a platform for States to access assistance for the prevention, mitigation and management of malicious ICT acts against critical infrastructure. The PoA platform could do this by providing threat intelligence information to States, and avenues of assistance for incident response and recovery.
- **Promote multi-stakeholder engagement and participation in international ICT security issues:** Parties to the PoA could conduct an in-depth multistakeholder analysis aimed at identifying dependencies and expertise, existing multi-stakeholder initiatives and potential for collaboration and cooperation to advance the framework.

5. Considerations Regarding the Structure of the Cyber PoA

Stakeholders agreed that the structure of the PoA could be linked to its objective to advance and promote the framework of responsible State behaviour. This section summarizes considerations on strategic and operational structures with insights on frequency and composition of meetings and resources.

- **Multi-stakeholder consultations on the cyber PoA rules of procedure:** There are several perceived advantages of outlining a structure of the PoA, which could provide accountability, clarify expectations, designate decision-making authority and foster collaboration between States and stakeholders. On the latter point, there is agreement that States could consult the multi-stakeholder community on rules of procedure for stakeholder participation in the cyber PoA and the elaboration of modalities for engagement in all structures of the PoA. The importance of the PoA to support consistent and structured engagement with global networks of research, academic, and think-tank institutions was highlighted. Stakeholders expressed that there is great potential in establishing a multi-stakeholder advisory body to provide insight on emerging threats.
- **Frequency of meetings could be responsive to developments in the use of ICT:** The frequency and structure of review meetings for the PoA would benefit from the clear understanding of the PoA scope. The proposals for review meetings every four years and annual intersessional meetings must be weighed against the need for the PoA to be responsive to developments in the use of ICT and time to monitor States' progress in implementing previous agreements.
- **Multi-stakeholder expert groups for consistent assessments:** The development of smaller, expert and data-driven multi-stakeholder working groups on thematic areas of implementation review, capacity-building and developments in technology would be an effective way to assess States' capabilities and gaps across the framework norms, confidence-building measures, and applicability of international law.
- **Reporting and feedback mechanisms to encourage consistency:** Reporting mechanisms could be a core feature of the PoA. National reports on implementation of the framework for responsible State behaviour could be analysed to identify gaps in States' capacities and identify areas and measures to help States address challenges.
- **Funding mechanism to be linked to commitments:** A funding mechanism could be developed as a permanent structure in the future cyber PoA. Some participants suggested that this mechanism could be linked to specific cyber PoA commitments, for example, projects, recipients, and eligible applicants, yet to be decided. In its formulation other factors may be considered including opening the mechanism to voluntary funding from contributions from private sector, including gender balance as a criterion for funding, and assessing existing funding mechanisms at regional and global levels to avoid duplication.

6. Considerations Regarding the Content of the Cyber PoA

Stakeholders agreed on the importance of mechanisms to improve States' awareness of the framework for responsible State behaviour and capacity to implement it, as well as mechanisms to support prevention, incident response and recovery from threats.

- **Multi-stakeholder mechanism for information-exchange:** Stakeholders discussed the development of cooperation mechanisms to enable States and the private sector to exchange information on malicious incidents against critical infrastructure, common threats, vectors and actors. Stakeholders highlighted that in consideration of threats, the PoA could pay attention to how threats disproportionately affect people in vulnerable situations and the differentiated impacts by gender. The inputs drew attention to the expanding threat landscape because of new technological developments such as artificial intelligence and quantum computing. Participants underlined the need for the cyber PoA to be proactive in understanding the dangers of technologies by collaborating with global networks of research, academic and think-tank institutions to provide cross-regional and multi-stakeholder perspectives on impacts on people and implications for the framework.
- **Inclusive process to assess threats to international security:** On specific threats, the cyber PoA could be guided by consensus reports of the GGEs and OEWG and other relevant intergovernmental bodies under the auspices of the United Nations. States could discuss existing and potential threats arising from developments in technology with an impact on international security. States' discussions on the assessment of threats implicating international security may be conducted in an inclusive manner that facilitates the sharing and incorporation of analysis and evaluation from a broad variety of stakeholders including to understand how threats evolve and may manifest.
- **Norms guidance to support implementation:** As elaborated in the GGE consensus report of 2021, greater clarity and guidance on norms can support their effective implementation.[9] Stakeholders added that the PoA could develop additional norms guidance through a multi-stakeholder consultation.
- **Link new capacity-building initiatives to existing programmes:** Streamlining global cyber capacity-building programmes at national and (sub)regional levels is important for the effective management

[9] General Assembly, "Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security", UN document A/76/135, 14 July 2021.

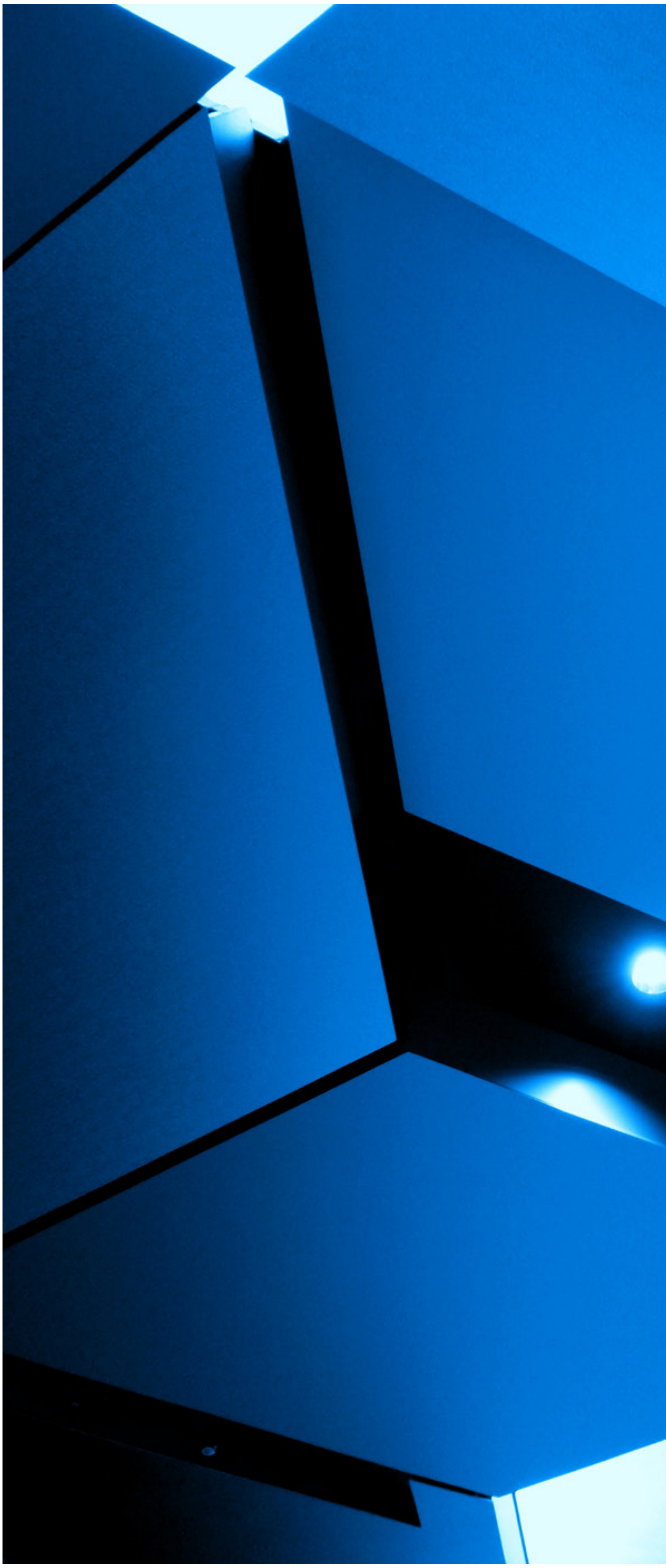
of resources. Stakeholders stressed the importance of mapping and leveraging relevant existing capacity-building programmes. Consideration must also be given to linking these programmes with digital capacity-building efforts on connectivity and access to the Internet. This indicates that cyber capacity needs cannot just be measured based on gaps identified through the framework but could also include other enablers and dependencies.

- **Regional organizations to support capacity-building measures**: Stakeholders echoed the discussions in the OEWG on a repository of confidence-building measures inspired by measures identified and adopted at the (sub)regional level. Cooperation with regional organizations will be critical to support State implementation.
- **Multi-stakeholder consultations at all levels of decision-making:** The PoA platform presents a unique opportunity for cooperation and collaboration between States and non-State stakeholders to be structured and sustainable. The Participants envision that this new era of engagement will include a commitment to engage all interested and relevant stakeholders, mindful of regional and gender representation within different structures of PoA and in decision-making structures when appropriate. This engagement could include collaboration on research, capacity-building implementation, briefings to Member States on agreed issues at review conferences, and intersessional meetings. Stakeholders could continue to provide external oversight to ensure that measures developed to counter threats in cyberspace respect and protect human rights and fundamental freedoms, both online and offline in accordance with their respective obligations.[10]
- **State-to-State peer learning for development and strengthening of national views on developments in ICT:** The submission of State views and assessments on developments in the field of ICT in the context of international security and use of the National Survey of Implementation would greatly benefit from a mechanism in which experienced States are paired with States hoping to do so. This peer-learning relationship will be based on the principles of capacity-building such as mutual trust, confidentiality, and tailoring to specific needs and contexts. The participants also highlighted that an addendum, to be developed, to the survey could include questions related to engagements and consultations with local non-State stakeholders in the completion of the survey. The cyber PoA could establish a dedicated strcuture that could also develop additional guidance for these submissions, set timelines, develop metrics and analyze national submissions.
- **Promotion of gender perspective:** Where the promotion of full, equal and meaningful participation and leadership of women in international ICT security governance is concerned, stakeholders agree on mainstreaming a gender lens on all issues under the mandate of the PoA and to contribute to ongoing research by commissioning research on gender-related cyber harms, and gender-related questions in reporting mechanism. Participants shared several

[10] Ibid.

proposals for the PoA including consideration of Security Council resolution 1325 on Women, Peace and Security (S/RES/1325) and national roadmaps, as well as the development of guidance notes for all activities and across all structures of the PoA.

- **Platform for further discussions on the applicability of international law**: To support the cyber PoA as a platform to discuss national views on how international law applies in cyberspace, dedicated structures could be developed to facilitate the exchange of views and for relevant and interested legal experts to brief Member States on how international law applies at the national, (sub)regional and global levels.
- **Good practices and standards:** Stakeholders stressed the development and sharing of good practices, standards and regulations that States could consider in the context of the cyber PoA to advance responsible State behaviour in cyberspace.



7. Additional Considerations and Courses of Action

To ensure the successful development of the cyber PoA, it would be crucial to initiate additional activities before and immediately after its adoption and leading up to the first review conference. Through discussions held during workshops and an analysis of written contributions, various options for action by States can be identified to inform the development of a cyber PoA:

- **Raise awareness about the PoA at national and (sub)regional levels**: In the lead up to the adoption of the cyber PoA, a series of meetings could be convened by current co-sponsors, in collaboration with other cyber inter-governmental and multi-stakeholder groups, to encourage State participation in ongoing discussions.
- **Establish a repository of resources:** Several guides and tools to facilitate national assessments and the compilation of national views on ICT developments in the context of international security have and are being developed; a database of these resources could be helpful to States in the lead up to the adoption of the cyber PoA.
- **Identify funding for projects and activities across all regions:** Current cyber PoA co-sponsors could already seek to identify existing funding and possible collaboration with existing funding mechanisms across all regions with the aim of engaging in discussions on how they can be leveraged in the future cyber PoA.

Stakeholders agree that not everything can be achieved at the same time. Accordingly, some activities and projects will be necessary at the outset to operationalize the PoA and some will be pursued later to support identified priorities. A funding mechanism is an example of a later project that could only be operational following resource mobilization and clarity around purpose and scope. The future of how the multi-stakeholder community can meaningfully engage in the process going forward, and what the next steps will be, requires the flexibility to explore several approaches. UNIDIR will continue to provide such a platform through workshops, seminars, research and joint projects.

8. Annexure 1: Guiding Questions for Written Inputs and Workshop

Scope

Should the Cyber PoA permanent mechanism focus on consensus report recommendation follow-up, development of new norms, capacity-building or confidence-building?

Should the PoA define States' and multi-stakeholders' rights and responsibilities – burden and credit-sharing modalities?

Should the PoA play a role in additional intergovernmental bodies under United Nations auspices that could be established by States?

Structure

Should the Cyber PoA engage with a knowledge partner agency including on research?

Should the PoA develop a funding mechanism? What kind of projects should the PoA consider?

Content

Should the Cyber PoA assist States in their efforts to implement the framework for responsible State behaviour and tackle emerging threats in the information and communications technologies?

Should the PoA support capacity-building and confidence-building between States? How?

Should the PoA facilitate and strengthen collaboration between States and when appropriate, with civil society, the private sector, academia and the technical community? How?

Should the PoA encourage States to, on a voluntary basis, survey or report on their national efforts to implement rules, norms and principles, including through the report of the Secretary-General as well as the National Survey of Implementation? How?

Should the PoA promote the full, equal and meaningful participation and leadership of women in decision-making processes? How?

Should the PoA advance multi-stakeholder discussions on the applicability of international law in cyberspace? How?

9. Annexure 2: Collection of Written Inputs by Various Stakeholders

The contributions received are attached without any editing and the responsibility for their content lies exclusively with the original authors.

- CyberPeace Institute
- Digital Society Institute Berlin (DSI)
- DXC Technology
- German Council on Foreign Relations (DGAP)
- Global Forum on Cyber Expertise (GFCE)
- Global Partners Digital
- International Federation of Information Processing (IFIP)
- LTC Flavio Augusto Coelho Regueira Costa - Cyber Advisor on Inter-American Defense Board
- Marchlewicz Marketing Management Agency
- Microsoft
- Paris Peace Forum
- Stimson Center
- Third Eye Legal

UNIDIR Cyber PoA - CyberPeace Institute's Written Contribution

Context

The Programme of Action to advance responsible State behaviour in the use of information and communications technologies in the context of international security (Cyber PoA) outlined in the resolution A/RES/77/37 reaffirms the commitment of States to implement the agreed-upon framework and to do so through an operative and action-oriented process.

The Cyber PoA aims to promote peace, security, and stability in cyberspace through a cooperative model that advances the exchange of knowledge and practices, avoids duplication of efforts, and assists in national and regional implementation efforts. This instrument is also an important opportunity for a comprehensive engagement of the multistakeholder community.

Scope

The Cyber PoA will allow for the continuation of previous consensus work in the Groups of Governmental Experts (GGEs) and Open-ended Working Groups (OEWGs) to consider, implement and advance responsible State behaviour in cyberspace and further build upon this work.

This initiative can create a single, dedicated, permanent forum for cybersecurity, which will not require renewed iterations, under the auspices of the UN First Committee where States bear primary responsibility in matters of international security. The Cyber PoA should centre around the implementation of the acquis, mapping and addressing the implementation challenges, and promoting continuous discussion and further development of the acquis.

The Cyber PoA should support the advancement of all pillars of the framework holistically and provide practical and needs-driven capacity building. Its mandate should consist of implementing cyber norms, building shared understandings of the applicability of international law and operationalizing confidence building measures (CBMs), and facilitating targeted capacity building efforts. It also needs to provide flexibility in addressing additional concrete issues that would benefit from information exchange, practical implementation, and multistakeholder engagement.

Content

Practical norm implementation necessitates the full inclusion of relevant stakeholders. Stakeholders can support States by advancing the interpretation and clarification of existing norms, assisting in identifying gaps in their operationalization, and promoting regular self-reporting. The model of the Cyber PoA could facilitate broad multi-stakeholder assistance in national and regional implementation efforts, including reporting on the progress.

The inclusion of relevant stakeholders in a dedicated forum would lend legitimacy and shape an instrument that reflects lived realities and addresses real threats that affect the safety, security and well-being of people. Stakeholders can assist States to build their capacity and understanding of how to apply norms on the practical day-to-day level. They are also well-positioned to connect different actors and build partnerships across a variety of communities and geographies to help in the practical implementation of cyber norms.

Clarifications related to the interpretation of international law are still required by States and civil society, academia, and other experts can be trusted partners in this regard. Several organizations have built a track record of elaborating how international law applies in cyberspace and thereby help to reach common understandings. The Cyber PoA should convene discussions on specific topics related to international law, international humanitarian law, and human rights law. This may include expert briefings and joint initiatives to consolidate common understandings on this subject.

States should meaningfully progress in operationalisation of CBMs as an essential component of international peace and security. The non-exhaustive list of measures towards building trust and transparency includes providing more clarity on what constitutes critical infrastructure under their national frameworks together with sharing information about cyber threats and vulnerabilities, national views on how international law applies in cyberspace, positive practices and existing capacity building initiatives, and national strategies and legislative frameworks related to the use of ICTs.

States are at different stages of implementation of the acquis, and it is imperative that they work together in cross-regional and multi-stakeholder partnerships to ensure that each State has the capacity to implement its commitments. The Cyber PoA can create a venue for needs- and context-driven capacity building that aligns with the assessments of threats and gaps in the implementation. Focused capacity building and multistakeholder initiatives can be particularly beneficial for smaller countries with limited resources to help them assess which infrastructure is critical and how to protect it while leveraging the model of public-private partnerships.

The PoA format needs to offer meaningful flexibility to reflect on the fast-developing field of international cybersecurity. States need to be able to decide on the substance for future meetings based on the identified needs and in a form that actively addresses building resilience against cyber threats. This can include expert briefings on selected topics, initiatives to promote the adoption of best practices and standards, joint exercises and simulations, and other forms of collaboration to benefit from the expertise and resources of various States and non-state actors.

The Cyber PoA should promote full, equal and meaningful participation of women in the process. This forum could include a call for gender diversity accompanied by practical steps, for example, in the form of programmes supporting women's participation in the meetings. There are already existing models, such as the Women in Cyber Fellowship that aims to ensure equal and effective representation of women diplomats from all regions in UN cyber negotiations, and on which accomplishments States can build and expand, for example, to include stakeholders. Moreover, understanding of the gendered impacts of cyber harm and gender-related practices in established actions should be increased and mainstreamed through this initiative. The Cyber PoA should increase understanding of the impacts of cyber threats that can be experienced differently based on multiple factors of vulnerability.

Modalities for stakeholder engagement

The final report of the first OEWG on ICTs acknowledges that *"the broad engagement of non-governmental stakeholders has demonstrated that a wider community of actors is ready to leverage its expertise to support States in their objective to ensure an open, secure, stable, accessible and peaceful ICT environment"*. However, the modalities for the participation of non-state actors in the OEWG fall short of allowing for an engagement of relevant non-governmental stakeholders. Given the multistakeholder nature of cyberspace, civil society, industry, academia, the technical community, and other experts, need to be part of the regular dialogue on cybersecurity. Their inclusion and participation can help to drive more impactful outcomes from dialogue and contribute to ensuring transparency and credibility of reached decisions as well as the sustainability of their implementation.

While States have the primary responsibility for the maintenance of international peace and security, non-governmental actors are their trusted partners. Collaboration with civil society, the private sector, academia and the technical community is essential for States to implement their commitments under the framework of responsible State behaviour in cyberspace. The PoA consultation should enable and encourage the participation of relevant stakeholders. Listing the possible roles of stakeholders under each part of the framework can help to mirror in the instrument the real-world collaboration that already takes place in the cybersecurity field.

Modalities for the proceedings of PoA meetings should therefore enable all relevant stakeholders to attend formal sessions, deliver statements and provide inputs, as is the case in other First Committee processes, such as the GGE on lethal autonomous weapons systems convened within the Convention on Certain Conventional Weapons (CCW). The modalities for stakeholder engagement can also be informed by processes in other Committees that have proven effective. Notably, the UN Ad Hoc Committee on Cybercrime has demonstrated an open and inclusive model that was agreed upon in the modalities of the participation of stakeholders in order to enable broad participation from civil society, the private sector, academia, and other relevant stakeholders.

The Cyber PoA should support implementation mechanisms at the national and regional levels, particularly to share best practices and expertise, and pursue engagement with regional fora. The regional consultations which are currently taking place in cooperation with the Organization of American States (OAS) and the Organization for Security and Co-operation in Europe (OSCE) are a good starting point for strengthened coordination.

Shaping a future mechanism for cybersecurity in the context of international security is a unique opportunity to advance accountability in cyberspace. The goal of the Cyber PoA should be to create an action-oriented framework, building upon previous actions and positive outcomes, and leveraging the respective strengths of States and relevant stakeholders. The CyberPeace Institute stands ready to engage in consultations on the instrument’s scope, structure, and content.

Drawing Parallels: A Multi-Stakeholder Perspective on the Cyber PoA Scope, Structure and Content

United Nations Institute for Disarmament Research (UNIDIR) Call for written contributions

By Heli Tiirmaa-Klaar[1], Līga Raita Rozentāle[2], Valentin Weber[3], Helene Pleil[4]

Scope:

1. **Should the Cyber PoA permanent mechanism focus on consensus report recommendation follow-up, development of new norms, capacity-building or confidence-building?**

The PoA should provide the First Committee with a permanent institutional mechanism to follow up on the implementation of the Framework for Responsible State Conduct in Cyberspace by providing and regularly updating sets of actionable recommendations and supporting relevant capacity-building projects. A clear focus on capacity building in the context of national efforts to implement the agreed framework should contribute to the overarching goal of achieving stability and resilience by identifying capacity building needs and addressing those capacity gaps. In addition, a focus on confidence building should contribute to the overarching objective of enhancing global cooperation. To this end, focal points should be identified in each state. The focus should not be on the development of new norms, but rather on the implementation of already agreed norms for responsible state behaviour in cyberspace. However, as technologies evolve, the need for new norms may arise, and the PoA should be the flexible and adaptable venue to discuss these in the future, as appropriate.

2. **Should the PoA define States' and multi-stakeholders' rights and responsibilities – burden and credit-sharing modalities?**

The PoA should provide a framework for the participation of various stakeholders - academia, civil society, the private sector, the technical community - as they have a critical role to play in implementing the framework for responsible state behaviour. However, the primary responsibility for the maintenance of

[1] Amb **Heli Tiirmaa-Klaar** (Ret) is the Director of the Digital Society Institute at the ESMT in Berlin, a knowledge hub on digital technology, regulation and cybersecurity issues, with a special focus on European technology policies and regulation.

[2] **Līga Raita Rozentāle** is an Independent Strategic Consultant, providing in-depth guidance for private and public sector, academia and international organizations on the influence of technology on the challenges of the future.

[3] **Dr. Valentin Weber** is a Research Fellow at the German Council on Foreign Relations (DGAP), a think tank based in Berlin. The opinions expressed in this contribution are solely those of the author and do not reflect the position of any affiliated organization.

[4] **Helene Pleil** is a Research Associate at the Digital Society Institute at the ESMT in Berlin, a knowledge hub on digital technology, regulation and cybersecurity issues, with a special focus on European technology policies and regulation.

international peace and security rests with States, which, guided by input from various stakeholders, are responsible for the final decision. The responsibility of these stakeholders could lie, in particular, in the provision of expertise and knowledge in the form of briefings and statements, as well as in the area of capacity building.

3. **Should the PoA play a role in additional intergovernmental bodies under UN auspices that could be established by States?**

The activities of the PoA could be informed by similar initiatives of other relevant UN bodies and agencies on digital development, critical technologies and the role of technologies in conflict. As the mandate of the PoA falls under the First Committee, it must serve its general objectives of maintaining and promoting international peace and security.

Structure:

1. **Should the Cyber PoA engage with a knowledge partner agency including on research?**

It would be advisable for the Cyber PoA to engage with a global network of research, academic and think-tank institutions to provide a truly cross-regional and multi-stakeholder perspective on the implementation of the framework for responsible state behaviour in cyberspace. The involvement of stakeholders from academia is crucial to enable them to conduct research related to the implementation of the framework and thus provide input to regular working groups on relevant issues, as well as expertise to identify needs and gaps in capacity building. Existing partners and networks should also be involved and efforts coordinated to avoid duplication.

2. **Should the PoA develop a funding mechanism? What kind of projects should the PoA consider?**

Given the resources required to implement the normative framework for state behaviour, states as well as international and regional organisations are advised to pursue a voluntary funding mechanism to support the necessary implementation activities. Inspiration for such a funding mechanism could be drawn from UNSCAR. As the majority of cyber resources are located outside governmental boundaries, the involvement of the private sector, academia and civil society should be encouraged in the establishment of the funding mechanism. The increased demand for cybersecurity assistance and training can also be met with contributions from the private sector and academia. The efforts of regional organisations such as the EU, OAS, ASEAN, AU as well as global mechanisms such as the World Bank Digital and Cybersecurity Fund, the Global Forum for Cyber Expertise (GFCE) and other similar coordination mechanisms could be integrated into the implementation efforts and a financing mechanism/multi-donor fund.

DSI | DIGITAL SOCIETY INSTITUTE BERLIN

ESMT BERLIN

Content:

1. **Should the Cyber PoA assist States in their efforts to implement the framework for responsible State behaviour and tackle emerging threats in the information and communications technology?**

The PoA should support States in their efforts to implement the framework for responsible state behaviour by providing structured support, a funding mechanism and a review process with benchmarks. UN Member States could benefit from an actionable cyber programme to help them achieve their goals of strengthening the cybersecurity of critical infrastructure, improving incident response and public-private partnerships for national cyber resilience, and achieving higher levels of cyber maturity.

In addition, the PoA could become a leading global platform for further discussions on cyber threat reduction. With regard to emerging threats, particular attention should be paid to the use of artificial intelligence for offensive cyber purposes, threats to complex systems, i.e. the Internet of Things, as well as potential threats related to the use of quantum computing.

2. **Should the PoA support capacity-building and confidence-building between States? How?**

The PoA should support capacity-building and confidence-building between States, building on existing co-operative activities. Existing regional CBMs, such as those implemented and monitored in the OSCE, should be recognized as best practices and extended globally. The regional organizations (OSCE, OAS, ASEAN) could assist in interregional and cross-regional cyber capacity and confidence-building efforts, as they have a more comprehensive overview of the state of implementation of the framework for responsible state behaviour in cyberspace in their respective regions. Regional organizations also serve as important forums for promoting regional cooperation and providing other confidence-building mechanisms for states.

3. **Should the PoA facilitate and strengthen collaboration between States and when appropriate, with civil society, the private sector, academia, and the technical community? How?**

While the PoA remains a government-led process, the involvement of the multi-stakeholder community to contribute to and drive action on practical steps, benefits and measures is essential for operational progress. All relevant stakeholders should be considered as contributing partners for the implementation of capacity-building partnerships and exchanges and to address any identified capacity gaps. Initiatives should involve multi-stakeholder actors where existing capacity-building mechanisms are already in place.

For capacity building related to education and training, academia should be considered as the primary provider of available capacity building options. A global network of academic organisations and training frameworks that can offer regular courses focused on cyber capacity building needs in the context of international peace and security could be envisaged. Such a network could provide the flexible and adaptable educational opportunities needed to meet the changing demands of policy negotiations and discussions.

Private sector participation should be built in to promote the local economic benefits of training and upskilling. For example, the private sector could provide overviews of the challenges/financial implications of malicious cyber activities for business. SME perspectives on responsibility in cyberspace should be encouraged to demonstrate the impact of cyber threats on local business.

The future of how the multi-stakeholder community can meaningfully engage in the process going forward, and what the next steps will be, requires the flexibility to explore more agile ways to collaborate on pilots, projects and other initiatives that can help anticipate challenges, gain insights and prioritise academic, NGO and private sector resources to support the PoA.

4. **Should the PoA encourage States to, on a voluntary basis, survey or report on their national efforts to implement rules, norms and principles, including through the report of the Secretary-General as well as the National Survey of Implementation? How?**

The PoA should encourage States to submit their national survey efforts in order to identify and map capacity-building needs. To encourage submissions, countries with stronger capacities could be paired with countries that lack capacity to become 'survey buddies'. Together they can work to identify and fill the gaps in the survey, for example by sharing best practices. These cooperation mechanisms could be linked to broader capacity building efforts. Such survey buddies could be paired at both interregional and intraregional levels.

5. **Should the PoA promote the full, equal, and meaningful participation and leadership of women in decision-making processes? How?**

Yes, in line with UN Security Council Resolution 1325 on Women, Peace and Security (S/RES/1325), the PoA should increase the representation of women in decision-making. By promoting diversity and inclusion in the decision-making and implementation processes of the PoA, a more inclusive and effective way forward will be developed. Inclusion and gender balance should be promoted by States at every stage of the development and implementation of a PoA - capacity-building activities should emphasise gender balance in the participation and leadership of such programmes, building on examples such as the joint Women in International Security and Cyberspace Fellowship (WIC) of Australia, Canada, the Netherlands, New Zealand and the United Kingdom. In developing a funding mechanism for the PoA, gender balance should be included as a criterion for funding.

6. **Should the PoA advance multi-stakeholder discussions on the applicability of international law in cyberspace? How?**

Multi-stakeholder actors have been crucial in advancing our understanding of how international law applies to cyberspace. The PoA should therefore actively involve academic and civil society experts to participate in the PoA, and also encourage the involvement of broader group of stakeholders beyond the accredited entities. The involvement of multi-stakeholder organisations could include inviting them to PoA sessions dedicated to international law. Multi-stakeholder actors could be invited to brief States on the current state of research on the application of international law to cyberspace and to provide input and statements in regular working groups.

UNIDIR Contribution: DXC Technology

The Multinational Company Perspective on Multi-Stakeholder Trust and Transparency

DXC Technology Company ("DXC") is a technology service provider located in over 70 countries. We provide IT services globally to thousands of customers, including to over 240 customers in the Fortune 500 and to a number of national governments. Services provided to customers include cybersecurity, but DXC also maintains a robust cyber program designed to protect its own internal systems, applications and proprietary data worldwide. At DXC, we firmly believe that we have a responsibility to be actively improving and challenging the tech sector and governments in order to facilitate a secure environment for NGOs and other stakeholders. We also believe it is critical that the private sector engage with international stakeholders as governments and their constituents work to establish international norms, laws and regulations applicable to cyber events. Accordingly, we have actively engaged as informal participants in the Open-ended Working Group on security of and in the use of information and communications technologies (OEWG) since 2019 and have been an active contributor to the Paris Call for Trust and Security in Cyberspace, as well as other industry interest groups and consortiums.

As an NGO supportive of the success of this UNIDIR event we submit this Contribution. We recognise that the UNDIR is one of several forums playing a critical role actively seeking to bring industry and government together. Focusing on the topic Drawing Parallels: A Multi-Stakeholder Perspective on the Cyber PoA Scope, Structure and Content, three points are immediately worth noting: Firstly, in the relationship between industry, government, and NGOs, trust is absolutely critical. DXC believes that every entity must be open in its dealings and should expect the same from others. Secondly, we need to be transparent. Because our clients and customers make up a sizeable part of the global population, we need to be transparent when we face attacks and in how we respond to attacks: no-one is made stronger by our fear to expose ourselves. Thirdly, we cannot be complacent. The threat of ransomware and other cyber attacks has certainly not gone away. With these messages in mind, DXC would like to contribute learnings from its own cyber attack experience. DXC will outline an example of a very real attack as a case study which emphasizes the need for government and all Stakeholders, including industry, to work together.

A Ransomware Case Study on Trust and Transparency:

On July 4th, 2020, a subsidiary of DXC, Xchanging, which provides technology-enabled business services to the commercial insurance industry, was subject to a ransomware attack. Xchanging plays an essential role in UK Critical National Infrastructure due to its significant work with the London Markets. While Xchanging's business is segregated from DXC's larger IT network, our specialists were concerned about whether the incident would have operational impacts on Xchanging and the wider company. The attack took place on a Saturday, with a very real risk of operational impacts to customers when the markets opened on Monday.

The attacker had sent the following message: "We have your data. We've encrypted your files. If you want to negotiate, we can talk on a secure tool or chat session." Our work ensured that engaging with the attackers was not necessary. Our team of specialists and experts worked through the weekend to verify that no data had been stolen, that only a handful of non-critical systems had been accessed, and that we were able to rapidly neutralise the threat.

On Sunday, we were able to fully clean and restore the impacted environment. By Monday morning, Xchanging and the London Market was able to open as planned and process global insurance policies and transactions. Critical to our success was trusting our governmental support and customers rather than working to resolve in a silo. Instead, we contacted and engaged the appropriate authorities and our customers early and with candor.

Too often, companies suffer ransomware attacks and engage with the attackers while withholding information from the authorities and their customer base. Legal counsel often advises this caution. Transparency is vital for creating trust for the wider supply chain and ensures that other companies can learn best practices from our steps to resolve the incident.

DXC identified five crucial lessons for consideration by multi-stakeholders including two of which are relevant to truth and transparency:

1. Know your infrastructure. Ensure all networks and firewalls have enterprise security tools in place to detect malicious behaviour. We were attacked using “Cobaltstrike”, a publicly available security testing tool. Knowing our infrastructure ensured that we were able to quickly detect when something was not right and identify where the network was compromised.
2. Involve senior leadership from the outset. We are a global company, spread across over 70 countries. To take rapid action, we would need to deploy staff in both the United Kingdom and India and engaging leadership teams was naturally critical. Good and tested governance, accountability, and clarity was essential.
3. Engage authorities and experts early. The attack took place on a holiday weekend in the USA (Independence Day). We had identified that the ransomware threat actor was utilising website domains in the United States to facilitate the attack. Good relationships ensured that we were able to contact law enforcement officials working on the holiday weekend, and we obtained a court order to take control of the attackers’ internet domains by that evening.
4. Gain leverage and do not pay. Our attackers wanted to negotiate; often, they will ask for money upfront in difficult to trace payments (cryptocurrency). We identified our strengths early: we knew we had stopped the attack; we knew they did not have our data, and we knew we had backups.
5. Be transparent. Openness is good practice. We shared details of the attack with hundreds of customers worldwide as well as several authorities in different jurisdictions. Medium to long-term, this has ensured that we continue to be regarded as a trustworthy and sincere company. In the short-term, it enabled us to move openly. An attack over a weekend is problematic; over a holiday weekend and it could have been critical. At the time, the average ransomware attack took down critical systems for sixteen days. Our transparency enabled us to move quickly, and it was resolved in time for markets to open on Monday.

The lessons outlined were important responsive actions that leveraged both acting preventatively and proactively. Companies like DXC are reliant on their entire supply chain (including experts and the government) implementing appropriate hygiene in their work.

Ransomware is a threat on a global scale. Increasingly cyber-aware groups and individuals can source ransomware tools with ease online and deploy them against companies and individuals at an unprecedented pace and scale. Public services across the world are especially at risk due to often running legacy IT and employing staff who, naturally, have responsibilities that preclude them from upskilling themselves digitally.

Perhaps most alarming, however, is the potential for nation-state attacks. The Ransomware Threat Assessment Model (NCSC-A/R/1197-22) identifies the 10 most prolific and dangerous ransomware strains. Nine are likely based in nation States (including Conti, regarded as responsible for the 2022 NHS attack). Seven of the ten have hit UK sectors in the past six months, including: technology, education, manufacturing, charities, transport, legal, financial, and academia. It has long been speculated that these attacks are endorsed by a specific nation State, highlighted by increased attacks in the build up to the invasion of Ukraine (none more notable than the 2017 NotPetya attack which caused havoc for Ukrainian critical national infrastructure). Indeed, NotPetya has been described by multiple outlets as an act of cyberwar. It had worldwide impact as unpatched systems were vulnerable to EternalBlue (an exploit also used in the WannaCry attack).

Modes of extortion are also becoming more challenging. The rise of cryptocurrency as an alternative payment, and one which is not tethered to any central bank or national currency, has created a ransom that is incredibly difficult to trace. This encourages gangs and individuals to target as many computers as possible in attacks, to maximise revenue. Extortion methods are, in turn, becoming more complex. Our personal experience, in 2020, saw the attacker gain access to a subsidiary's minor database and use that to attempt a ransom negotiation. The WannaCry attack saw computers themselves locked out in exchange for a payment. These forms of extortion encourage business to "lockdown" and not communicate externally, which then feeds into a cycle of success for the attacker. At DXC, we encourage businesses to learn from our experience: appropriate, prompt communication and transparency was key to our success. Indeed, we recommend this blog series on our approach to security.

International Lessons and The Drive for Cooperation through Trust and Transparency.

DXC's response focused on attacks from criminal gangs and individuals. To maximize global security, trust and transparency must exist across all stakeholders. The public sector, States and NGO's including industry, UNIDIR, OECD and the OEWG are effective resources for co-ordinating governments and large private sector companies to discuss emerging threats and how to respond. Individual States play a significant role in global cooperation and can lead through developing trust and transparency with Industry. For example, the UK Government has empowered the GCHQ, and others to engage with the private sector to continue sharing learnings and developing generally accepted best practices. Collectively these organisations need to ensure messages are cascaded appropriately and continue to work with NGO's including industry in forums such as this UNIDIR event.

Conclusion

An effective multi-stakeholder security program can be enhanced through the practice of the three proposed tools proposed in this contribution, trust, transparency and avoiding complacency. Our cyber attack hit at the worst possible time for an American-owned company: 4th July weekend. Staff were enjoying the national holiday for not only DXC but, crucially, regulators and clients. However, we had actively pursued relationships with the right regulators in relevant markets. DXC could stand up a response, as part of our tried and tested planning, on the worst possible day with great success. Regulators knew that, when we came to them and told them what we needed, or when they asked us to do something, **we were trusted to give them all the information**. We also trusted them to only ask for something that they genuinely needed. Secondly, we were transparent. The global insurance market could have been heavily exposed when the markets opened at 9:00 am on Monday. **We were transparent with our clients and, importantly, on social media.** Clients, prospective clients, and citizens were aware of what was happening and, importantly, our action to resolve the attack. Resolve it we did. Finally, this proves that **complacency cannot be allowed in government or in industry**. The market indicates there is no sign ransomware and similar attacks are over or substantially diminished. The impact of that one attack, had it worked, could have been devastating for companies and citizens across the globe. With millions of attacks undertaken globally every day, including by state-backed actors, the old saying is worth repeating: it only takes one to succeed.

DXC believes that we have a responsibility to challenge us all to be better. Multi-stakeholders, including industry, working together, have the right people to achieve success. With multi-lateral trust, transparency, and addressing complacency, together we have the ingredients to succeed.

DGAP
Advancing foreign policy. Since 1955.

Integration of Multilateral Export Control aspects of sensitive ICTs into the Cyber PoA

Dr Georgios KOLLIARAKIS

Advisor for Research Strategy, Technology Security Defence, German Council on Foreign Relations (DGAP)

RATIONALE

The laudable initiative by UNIDIR to engage stakeholders and experts for consulting on the scope, structure, and content of the “Programme of Action to advance responsible State behaviour in the use of information and communications technologies in the context of international security” (Cyber PoA) invites to consider potential synergies with existing ICT governance mechanisms to enhance international security.

It is a Hercules struggle, comprising several tasks, to harness the enormous potential of ICTs to support welfare and sustainability, while enhancing security and preventing misuse. The Cyber PoA should exploit in that respect synergies with existing frameworks, regimes, and initiatives, which respond to UNSCR 1540 (2004) with regard to countering proliferation of WMDs, as laid out in brief further below.

ICTs in the context of cyber security and defence resembles a double moving target: On the one hand, the shift in the direction of innovation transfer, which increasingly takes place from the Civil towards the Defence domain; related to that, the geometric proliferation of actors, from SMEs to Research and Technology Organizations that develop such technologies; also, the potential of ICTs to get re-engineered, and adjusted into components and equipment for malicious purposes also at a Technology Readiness Level of lower maturity (lower than 8 or 9); not least, the intangible nature of illicit, intended or non-intended transfer (as software, per email or cloud, in the form of technical assistance, or research collaboration), which makes control of sensitive aspects of the technology very difficult.

On the other hand, the intensifying geopolitical tensions among established and insurgent states give rise to a new securitization and weaponization of edge technology, many decades after the Cold War, rendering globally distributed value chains, but also national critical infrastructure, which is dependent upon ICTs, very vulnerable.

One of the crucial mechanisms to consider thereby is the strategic trade control of sensitive ICTs in order to minimize the risks out of their illicit diffusion and diversion with malicious purposes and misuse. Emerging Dual-Use ICTs pose one of the biggest challenges in terms of identifying their malicious uses and controlling their spread to actors who may misuse them, since their accessibility threshold, and the skillset needed for deploying them is, compared to those of nuclear or synthetic biology technologies, much lower.[1]

Responsible state behaviour needs to apply in a concerted manner policies both “upstream” (dealing with responsible R&D oversight, ethical self-constraints and codes of conduct), “downstream”, when it comes to innovation commercialization and industrial (trade & export) policies, and not least, human rights due diligence policies.

Following inputs to selected questions about the Cyber PoA are to be read against the above backdrop.

SCOPE
Question 3.

Should the PoA play a role in additional intergovernmental bodies under UN auspices that could be established by States?

According to UNSCR 1540 (2004), States shall refrain from providing any form of support to non-State actors that attempt to develop, acquire, manufacture, possess, transport, transfer or use nuclear, chemical or biological weapons and their means of delivery, in particular for terrorist purposes.[2] ICTs, while not explicitly referred to, play a key role in the means of delivery of the above. UNODA already undertakes activities, such as the facilitation and regional coordination of national implementation activities, the cooperation between international, regional and sub-regional organizations, and partnerships of key stakeholders including civil society, private sector and academia.

However, UNSCR 1540 does not prescribe which technologies or usages exactly should be monitored and sanctioned if transferred to the wrong actors. This task is undertaken, mostly by national export control regulations, and by a number of regimes, the most relevant of which for ICT is the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies (WA).
WA targets Cyber-Warfare Systems, Communications Surveillance, as well as military-grade offensive cyber-warfare technologies. Since 2011 successively intrusion software and IP network surveillance systems, certain cyber-surveillance items, offensive cyber-warfare technologies, and certain items related to the development of autonomous weapons have been taken up in the control lists (under Category 5 - Part 1 Telecommunications, and Part 2 "Information Security").[3]

The recent recast of the EU Regulation 2021/821 on the *export, brokering and technical assistance, transit,* and *transfer* of dual-use items, besides aiming at preventing the proliferation of Weapons of Mass Destruction (WMD), additionally refers to protecting public security, and safeguarding human rights.[4] That, reminiscent of the unprecedented challenge ICT are currently posing. The EU regulation, which is binding for the EU 27 Member States, and is followed by many more associated and partner states, includes risky items and services under Category 5 (Telecommunications and Information Security), but also Category 4 (Computers) and Category 3 (Electronics).

The Cyber PoA, with the proliferation and abuse of cyber surveillance technology being increasingly a global “wicked problem”, could establish a comprehensive forum at UN level to tackle the challenge from all aspects, including the export control one.

STRUCTURE
Question 1.

Should the Cyber PoA engage with a knowledge partner agency including on research?

The Cyber PoA should engage an array of knowledge agencies covering both technical aspects of the rapid developments of ICT R&D, as well as policy analysts and bodies tasked with monitoring policy developments in the application of those technologies in civil, space, and defence sectors, including critical infrastructure.

Question 2.

Should the PoA develop a funding mechanism? What kind of projects should the PoA consider?

The establishment of a funding mechanism would enable the targeted exploration of ICT risk use cases, with a particular emphasis on prospective (foresight-driven) use cases, conduct vulnerability assessments, and “red-flag” threat scenarios.

Furthermore, projects about the identification of (national) capability gaps and requirements of technical and policy nature, to foster a “whole-of-government” anticipatory governance approach on Cyber and ICT Security.

A third category of projects should deal with public outreach and stakeholder awareness raising, piloting also cross-sectoral multi-stakeholder formats.

CONTENT
Question 1.

Should the Cyber PoA assist States in their efforts to implement the framework for responsible State behaviour and tackle emerging threats in the information and communications technology?

The role of Cyber PoA in this context should be to advise and promote a mix of policy instruments with States, ranging from hard regulation (legislation and treaty-like international agreements), to soft regulation (such as ICT standards, R&D oversight mechanisms), and to self-regulation, such as self-constraint/codes of conduct.

Under the UN auspices, such efforts could overcome national/regional discrepancies, and move toward wider global sharing and support. Particularly with regard to emerging threats from ICT, such implementation assistance Framework for Responsible State Behaviour could serve to inter-connect existing international bodies and reduce discrepancies in awareness and approaches.

From the specific perspective of Multilateral Export Controls, key aspects should encompass

1. Licensing and authorization systems designed to ensure that controlled ICT items are not exported to countries or end-users that pose a risk of illicit proliferation.
2. End-use controls to ensure that controlled ICT items are not used for illegal or unauthorized activities.
3. “Catch-all” controls to prevent the illicit proliferation of dual-use ICT items and emerging technologies which are not explicitly on the export restriction lists.
4. Information sharing on exports and end-uses of controlled items with other States in order to improve transparency and consistency.
5. Targeted sanctions against individuals and entities that are involved in the illicit proliferation of particularly sensitive dual-use ICT items and technologies.
6. International cooperation, including with other countries, international organizations, and civil society to prevent the illicit proliferation of dual-use ICTs.

This recommendation is related also with the recommendation above under Scope, Question 3.

Question 3. **Should the PoA facilitate and strengthen collaboration between States and when appropriate, with civil society, the private sector, academia and the technical community? How?**

Inter-state but also cross-sectoral collaboration, including the industry, SMEs, research and academia should be one of the core tasks of the Cyber PoA.

Structured consultations ought to clarify divergences in interests and logics, and sensitize for the ultimate goal of national and international security and peace, public security, and human rights.

Bi-directional, co-creative consultation formats ought to raise awareness, and at the same time generate insights about possibilities for strengthening a "whole-of-society" approach in tackling Cyber threats at all stages of the ICT value chain.

Instrumental to the above can well be the recommendation above regarding Cyber PoA projects, under Structure-Question 2.

[1] For an overview see Kolliarakis, G. (2022): Anticipatory governance of emerging and disruptive technologies with dual-use potential. Multistakeholder Forum on Science, Technology and Innovation. UN Interagency Task Team on STI for the SDGs (IATT). Under https://sdgs.un.org/sites/default/files/2022-05/1.1.5-22-Kolliarakis%20-DualUseGov.pdf

[2] See under https://disarmament.unoda.org/wmd/sc1540/

[3] See under https://www.wassenaar.org/app/uploads/2022/12/List-of-Dual-Use-Goods-and-Technologies-Munitions-List-Dec-2022.pdf

[4] See under https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2021:206:FULL&from=EN

Contribution from the Global Forum on Cyber Expertise (GFCE)
May 2023

On behalf of the Board of the Global Forum on Cyber Expertise (GFCE) Foundation, we submit the following contribution to the UNIDIR Cyber PoA multistakeholder event on 1 June 2023. The GFCE would like to recognize the efforts of UNIDIR in providing a platform for the multi-stakeholder community to share their views and exchange ideas on the Cyber PoA.

The GFCE is a neutral, apolitical platform for international cooperation and exchange on strengthening cyber capacity and expertise globally. Established in 2015, its multi-stakeholder network comprises of over 190 organizations including governments, civil society, academia, industry, and international organizations. On this occasion, we respectfully provide input on the following guiding questions:

Structure Q2: Should the PoA develop a funding mechanism? What kind of projects should the PoA consider?

The PoA may consider developing a multi-donor, flexible funding mechanism to mobilize resources in support of the implementation of the PoA and existing framework of responsible State behavior in cyberspace. The funds should be allocated on a yearly basis for projects that demonstrate relevance to the goals of the PoA and with clear outputs and (sub)regional focus, for example in: capacity building assistance, training, awareness and education, research, policy and frameworks, incident response, information sharing, etc. Stakeholders such as UN partners, international organizations, NGOs and research institutes should be eligible to receive funding as important actors supporting the implementation of the existing framework of responsible State behavior in cyberspace.

Content Q2: Should the PoA support capacity-building and confidence-building between States? How?

The advancement of responsible State behavior in the use of ICTs in the context of international security must be underpinned by the essential pillars of capacity and confidence building. The PoA could support capacity building between States by encouraging those that require assistance to articulate their needs and priorities, and those with resources to provide tailored support. The PoA could also encourage States that are in a position to do so to invest more broadly in capacity building assistance.

The PoA may consider identifying which capacities are needed specifically and provide guidance on identifying individual priorities, for example by consulting UNIDIR's research on Unpacking Cyber Capacity-Building Capabilities. To utilize existing CCB knowledge and mechanisms, the PoA should connect with and leverage the GFCE ecosystem. In particular:

- the Cybil Portal, which contains mapping of over 800 capacity building projects and a repository of over 300 relevant resources.

- The mapping of countries' cyber capacity building needs conducted by the GFCE regional hubs.
- Knowledge modules on key capacity building topics which include the most relevant tools, guidelines, and practical knowledge.
- GFCE working groups, which facilitates dialogue on five prioritized capacity building themes between countries and experts/implementers.
- GFCE Clearing house mechanism, which involves identifying, defining and supporting capacity building needs with tailored assistance.

The PoA should reaffirm the basic principles of capacity building as agreed by the previous OEWG (2021) and seek to leverage existing capacity building initiatives and platforms such as those by regional organizations and the GFCE, and avoid duplicating existing efforts. The PoA could also promote transparency and open communication channels between States and encourage States to maintain an up-to-date Points of Contact directory, to contribute to building trust.

Content Q3: Should the PoA facilitate and strengthen collaboration between States and when appropriate, with civil society, the private sector, academia and the technical community? How?

The PoA should foster greater collaboration and cooperation between States and non-State actors by encouraging information sharing and building partnerships. The PoA could identify and outline the different roles stakeholders can play in implementing the normative framework and demonstrate good practices from multi-stakeholder collaboration.

If the PoA is to be an agile and functional instrument, it is essential it recognizes the important contribution of civil society, including non-governmental organizations and industry, in supporting States with implementing the existing framework of responsible state behavior in cyberspace and cyber capacity building efforts. For better efficiency, we encourage considering building on existing efforts that already are established and ongoing, such as the GFCE. With its broad membership base, track record, pragmatic approach to cyber capacity building, mapping of projects and Clearing House mechanism, the GFCE already works towards many objectives shared with the PoA.

Content Q5: Should the PoA promote the full, equal and meaningful participation and leadership of women in decision-making processes? How?

The PoA should include language that emphasizes the importance of gender diversity and inclusion. It should advocate for greater representation of women in cybersecurity-related decision-making processes at all levels, including in relevant PoA activities and working-level meetings, and promote a gender-sensitive approach to cyber capacity building, taking into account that women are often under-represented in initiatives or trainings.

The PoA should consider leveraging existing networks that support gender mainstreaming and empower women in the cyber field (such as the Women in International Security and Cyberspace

Fellowship and the GFCE’s Women in Cyber Capacity Building network), as well as women’s organizations, to amplify efforts and create an enabling environment for women’s meaningful participation and leadership.

UNIDIR consultation on the Cyber Programme of Action

Global Partners Digital submission
May 2023

About Global Partners Digital

Global Partners Digital is a social purpose company dedicated to fostering a digital environment underpinned by human rights.

Introduction

We welcome the opportunity to provide comments on the Cyber PoA as part of UNIDIR's consultation related to its event "Drawing Parallels: A Multi-Stakeholder Perspective on the Cyber PoA Scope, Structure and Content".[1] In our response we focus our comments on the questions in the consultation related to 'content'.

Response

1. **Should the Cyber PoA assist States in their efforts to implement the framework for responsible State behaviour and tackle emerging threats in the information and communications technology?**

Yes, the Cyber PoA should explicitly state (either through a political declaration or in the text of the instrument that comprises the basis of the PoA) that the implementation of the agreed framework for responsible State behaviour, as well as its evolution where agreed, is a key objective of the PoA. It should have a strong focus on supporting the implementation of the existing framework to ensure that it is 'action-oriented'.

2. **Should the PoA facilitate and strengthen collaboration between States and when appropriate, with civil society, the private sector, academia and the technical community? How?**

Yes, due to the nature of digital technologies and the internet, as well as the multiple roles that non-governmental organisation (NGOs), including civil society, play - the PoA should ensure meaningful participation and opportunities for collaboration

[1] https://unidir.org/events/drawing-parallels-multi-stakeholder-perspective-cyber-poa-scope-structure-and-content

between these actors and states. The PoA should focus on the implementation of the agreed framework, but also be flexible enough to allow for its adaptation through, for example, the development of new norms, CBMs or capacity building measures where agreed.

For the framework to be effectively implemented, it requires the engagement of stakeholders who play a variety of roles including but not limited to: incident response, development and deployment of ICT hardware and software; the convening of stakeholders working across sectors; working directly with marginalised and affected communities; the development of and implementation of evidence-based and human-centric, rights-respecting policy solutions to aid the implementation of the agreed framework[2].

The PoA should embed references to the importance of stakeholders in its operative paragraphs, drawing for example on other similar instruments like the DDPA (2001 Durban Declaration and Programme of Action against Against Racism, Racial Discrimination, Xenophobia and Related Intolerance). In this way, the PoA should reiterate the integral role of non-governmental stakeholders in fulfilling the entire mandate of the PoA. For this reason, it should adopt inclusive and transparent modalities for the participation or accreditation of NGOs - these could draw on the OEWG on Ageing for example (as outlined in the US reply to pursuant to resolution A/RES/77/37)[3] and transparency for the exclusion of any NGOs, drawing on the modalities for the Ad Hoc Committee on Cybercrime (as outlined in the UK submission pursuant to resolution A/RES/77/37)[4].

The text that is the basis of the PoA should include a preambular paragraph that welcomes and acknowledges the role played by non-governmental actors in the fulfilment of its mandate. As mentioned in the report (2022) published by the Women's League for International Peace and Freedom (WILPF) "its operative and action-oriented paragraphs could then refer to particular types of actors that will be relevant to implementation or advancing the action contained in any given paragraph or action points. This would serve to mainstream civil society engagement throughout the document in a way that mirrors real-world collaboration and cooperation"[5].

The PoA could encourage States to cooperate with other stakeholders in particular to: conduct briefings for member states; to conduct research in relevant areas related to the framework; enhance or conduct capacity building efforts based on needs and existing gaps identified. As the WILPF report also states, if the PoA sets up a system

[2] Further examples are provided in Sheetal Kumar (2021) "The missing piece in human-centric approaches to cybernorms implementation: the role of civil society, Journal of Cyber Policy", 6:3, 375-393, DOI: 10.1080/23738871.2021.1909090

[3]https://docs-library.unoda.org/General_Assembly_First_Committee_-Seventy-Eighth_session_(2023)/77-37-US-EN.pdf

[4]https://docs-library.unoda.org/General_Assembly_First_Committee_-Seventy-Eighth_session_(2023)/77-37-UK-EN.pdf

[5] Allison Pytlak (2022) ADVANCING A GLOBAL CYBER PROGRAMME OF ACTION: Options and priorities: https://reachingcriticalwill.org/images/documents/Publications/report_cyber-poa_final_May2022.pdf

for follow-up meetings and conferences (annual periodic meetings for example), then it will be important to consider how civil society can *meaningfully* participate in those convenings. This requires considering how the participation of stakeholders can be embedded in rules of procedure and which meeting formats are needed.
Civil society should be proactively consulted in this regard, for recommendations on rules of procedure and meeting formats that are inclusive of all stakeholders (this may include but not be limited to multiple ways of engaging - e.g through both oral and written inputs, hybrid and in-person access to both formal and informal meetings). This also includes stakeholders inclusion in preparatory consultations (including any relevant intersessionals of the OEWG) to develop the PoA, and for example an international conference to develop or finalise and adopt the text of a political declaration or the text of the instrument.

3. **Should the PoA encourage States to, on a voluntary basis, survey or report on their national efforts to implement rules, norms and principles, including through the report of the Secretary-General as well as the National Survey of Implementation? How?**

Yes, reporting mechanisms which help to identify capacity gaps, related for example to technical or policy capacity (e.g the existence of relevant institutions or processes) and foster mutual understandings of the framework and the status of its implementation should be part of the PoA. The PoA should also work with existing forums including regional bodies, through a consistent information sharing mechanism - e.g through regular briefings. It should incentivise working with other stakeholders in capacity building, for example by amending or adding to the UNIDIR national survey of implementation if that is used (e.g through a supplementary guidance note) to include questions and guidance that relate to engagement and participation with non-state stakeholders.

For example, it could ask:

- *Have you engaged other stakeholders in your country or region in supporting the implementation of the 11 norms? If so, how have they been engaged? What roles do they play?*
- *How have other stakeholders been engaged in supporting the implementation of the CBMs? What roles do they play?*
- *Have other stakeholders been engaged in the development of your national position(s) on the application of international law to the use of ICTs by states? If so, how?*
- *Can you provide examples of engagement with non-governmental stakeholders in implementing capacity building efforts, including in relation to the implementation of the rest of the framework (CBMs, norms, application of international law?)*

4. **Should the PoA promote the full, equal and meaningful participation and leadership of women in decision-making processes? How?**

Yes, we recommend the consideration and integration of the recommendations in the WILPF report previously cited (page 29).[6]

5. **Should the PoA advance multi-stakeholder discussions on the applicability of international law in cyberspace? How?**

Yes, the PoA should advance multi-stakeholder discussions on the applicability of international law in cyberspace and serve as a platform to deepen understanding of how international law appies. This could be done through:

- A dedicated intersessional workstream on the application of international law in cyberspace, including international humanitarian law and international human rights law.This workstream should be open to all relevant stakeholders, particularly the private sector, civil society and academia.
- Dedicated discussions at annual periodic meetings on international law to provide an inclusive venue on how existing rules apply and where further discussion is needed. It may also be beneficial to have a review conference on a periodic basis (4-5 years) to enable the international community to take stock of progress and deepen discussions on how interpretations have progressed which may not be possible at yearly intervals.
- The establishment of permanent and ongoing opportunities to identify areas for further engagement and common understanding (e.g through the national survey of implementation). The PoA can use the national survey as a means of encouraging states to share their positions on international law, which can be collected, disseminated, and facilitate dialogue and deepen understanding on how international law applies in cyberspace. The design of the PoA framework should take into account the challenges regarding limited capacities of smaller states and be built on reasonable expectations, which can be supported through multi-stakeholder involvement.

[6] Allison Pytlak (2022) ADVANCING A GLOBAL CYBER PROGRAMME OF ACTION: Options and priorities: https://reachingcriticalwill.org/images/documents/Publications/report_cyber-poa_final_May2022.pdf

ifip
the leading edge of information technology

23 May 2023

Submission by IFIP Working Group 9.10 ICT Uses in Peace and War Members to the UNIDIR Event “Drawing Parallels: A Multi-Stakeholder Perspective on The Cyber PoA Scope, Structure and Content”

This document is in response to the call for written submissions by stakeholders.

The International Federation of Information Processing (IFIP) is the leading multinational, apolitical organization for ICTs and is recognised by numerous world bodies, including the United Nations. IFIP represents IT professional societies and bodies from over 38 countries and has links with over 3500 scientists from both industry and academia. IFIP comprises of 13 Technical Committees with over 100 Working Groups. The IFIP Working Group 9.10 on ICT Uses in Peace and War has a multi-disciplinary member base from 19 countries. The aim of the working group is to bring together a range of stakeholders to “encourage dialogue by providing a platform for the presentation of research papers, current research or the result of research in progress, case studies, use cases, lessons learned, and risk assessment/impact assessment”.

Three members of the working group provided input, and this submission should be taken as the consolidated views of the individuals and not the organisation as a whole.

1. Scope of the PoA

1.1. Should the Cyber PoA permanent mechanism focus on consensus report recommendation follow-up, development of new norms, capacity-building or confidence-building?

The Cyber PoA can facilitate all of the focus areas: feedback of consensus reports, development of new norms, as well as inter-state capacity-building and confidence-building measures. However, it is suggested that capacity-building is prioritised (all three contributors supported capacity-building, and two contributors supported the other three focus areas).

1.2. Should the PoA define States’ and multi-stakeholders’ rights and responsibilities – burden and credit-sharing modalities?

Yes, the Cyber PoA should outline the rights and responsibilities for all stakeholder groups in order to provide a common understanding of the rights and responsibilities and to manage expectations of States and non-state stakeholders.

1.3. Should the PoA play a role in additional intergovernmental bodies under UN auspices that could be established by States?

Yes, but with possible limitations. The PoA can engage with existing bodies where relevant, for example the Internet Governance Forum. The PoA can play a role in establishing additional intergovernmental bodies under UN auspices (or assisting States in establishing such bodies); however, the Cyber PoA should not necessarily have a major role in the body once established.

2. Structure of the PoA

2.1. Should the Cyber PoA engage with a knowledge partner agency including on research?

Yes. As the multi-stakeholder inclusion has been seen to be a key component of the current processes, it will be important to engage with knowledge partners, and provide support for initiatives that advance the core scope of the PoA.

2.2. Should the PoA develop a funding mechanism? What kind of projects should the PoA consider?

Yes, a funding mechanism will provide a means of supporting initiatives aligned to the scope of the PoA. A wide range of projects from different stakeholders could be supported, and can be assessed on a case-by-case basis. The funding instrument does not necessarily need to fund projects only, but can be used to support diversity and inclusion initiatives, such as providing for multi-stakeholder groups who do not necessarily have the funds to attend relevant cyber diplomacy events in-person. As part of such engagements, a method to assist with visa applications can be considered to further facilitate inclusion. Some possible project areas can include:

- Collaborative capacity-building and knowledge-sharing related to cyber peace initiatives;
- Research projects from academia aimed at assessing norm adoption;
- Projects to facilitate inclusivity (e.g. North-South and South-South collaboration); and,
- Additional support to collaborative research projects funded by research funding agencies

3. Content of the PoA

3.1. Should the Cyber PoA assist States in their efforts to implement the framework for responsible State behaviour and tackle emerging threats in the information and communications technology?

Yes. The PoA should form a set of best practices (or a knowledge base) to cover a range of engagements and processes that states and stakeholders can then use to initiate their own processes to implement the framework and counter online threats. The PoA could provide guidance and other support for various mechanisms, including reporting and promoting inclusivity in participation. However, the implementation of the framework may be contentious and should be done in a manner whereby the framework becomes aligned and integrated into a State's national legislation, thereby promoting the ideals while maintaining issues such as human rights.

3.2. Should the PoA support capacity-building and confidence-building between States? How?

Yes. Both capacity-building and confidence-building measures are key aspects to advance international cyber policy and cyber diplomacy. The PoA can keep a repository of relevant information for capacity-building and confidence-building initiatives and related organisations, and facilitate initial engagements with the relevant stakeholders. In addition, support could be provided through the funding mechanism for projects on capacity-building and confidence-building. Using a knowledge base for best practices, the PoA can guide such initiatives to maximise return on investment.

3.3. Should the PoA facilitate and strengthen collaboration between States and when appropriate, with civil society, the private sector, academia and the technical community? How?

Yes. Through the Open-Ended Working Group, the importance of multi-stakeholder inclusion is apparent. The PoA can assist with a point of contact directory to allow for States and non-state stakeholders to initiate engagement. Virtual events can be held for possible collaborators to engage, and funding mechanisms can be used to support collaborative partnerships with multi-stakeholders. Existing events, such as the IGF conference, can be leveraged to include workshops or sessions to foster collaboration.

3.4. Should the PoA encourage States to, on a voluntary basis, survey or report on their national efforts to implement rules, norms and principles, including through the report of the Secretary-General as well as the National Survey of Implementation? How?

Yes. This is a key area to support confidence-building measures. The PoA efforts in this regard can be conducted through events (or sessions at related events), and in collaboration with the UNIDIR Cyber Policy Portal.

3.5. Should the PoA promote the full, equal and meaningful participation and leadership of women in decision-making processes? How?

Yes. Diversity and inclusivity are important in cyber security. As proposed above, part of the funding mechanism can focus on supporting diversity and inclusivity initiatives. This can include aid for women to participate in events and sessions. A possible process is to allow for mentorship programmes for the next generation of women to engage with the existing women decision-makers. This will be particularly important for the Global South, where there may be financial barriers preventing participation.

3.6. Should the PoA advance multi-stakeholder discussions on the applicability of international law in cyberspace? How?

Yes. International law creates the mechanisms for the regulation of international governance matters, and has gained an increased importance in the cyber context with states giving increased attention to the governance of cyberspace and governance in cyberspace; therefore, it will be important to advance discussion in this area. International law structures provide the ideal platform for states and international entities to collaborate through various limitations, requirements, and permissions.

The PoA can advance multi-stakeholder discussions by engaging with existing processes, civil society and academia to raise awareness and build capacity in this area. Through a funding mechanism, events can be supported where the intersection of international law and cyberspace are discussed (for example, a mini-track at an academic cybersecurity conference).

Your Sincerely,

Prof Brett van Niekerk
Chair: IFIP WG 9.10 ICT Uses in Peace and War; Associate Professor: Durban University of Technology

Prof Joey Jansen van Vuuren
Vice-Chair: IFIP WG 9.10 ICT Uses in Peace and War; Professor: Tshwane University of Technology

Dr Trishana Ramluckan
Member: IFIP WG 9.10 ICT Uses in Peace and War; Honorary Research Fellow: University of KwaZulu-Natal

LTC FLAVIO AUGUSTO COELHO REGUEIRA COSTA
CYBER ADVISOR ON INTER-AMERICAN DEFENSE BOARD

Scope:

1. Should the Cyber PoA permanent , capacity-building or confidence-building?

Considering the heterogeneity of participating countries, it would be interesting for the PoA to initially focus on building the capabilities of participants to establish a solid foundation for subsequently prioritizing confidence-building. Undoubtedly, trust is the most crucial aspect, but all countries must reach a minimum level of cyber maturity in a trusted environment.

2. Should the PoA define States' and multi-stakeholders' rights and responsibilities – burden and credit-sharing modalities?

The PoA should define all these aspects as responsibilities, burdens, and credit-sharing systems essential for fostering a fair, cooperative, and inclusive environment in information and communications. By clearly outlining these elements, we can ensure equitable distribution of obligations, encourage collaboration, and recognize the contributions made by various stakeholders towards cybersecurity.

3. Should the PoA play a role in additional intergovernmental bodies under UN auspices that could be established by States?

Considering that today there are non-governmental organizations that have a higher level of control over information and communications than states, it is vital to involve them in this process. In addition, the involvement of all parties would ensure responsible use by these organizations and the countries that oversee them.

Structure:

1. Should the Cyber PoA engage with a knowledge partner agency including on research?

The involvement of specialized partner agencies in the subject matter will ensure the program's success. Their expertise, combined with research capabilities, contributes to the maturity and effectiveness of the program's outcomes.

2. Should the PoA develop a funding mechanism? What kind of projects should the PoA consider?

Regarding the funding mechanism, it would be beneficial to support research projects related to technologies that identify misuse of communications and information by member countries and tools and technologies that can enhance mutual trust. In addition, the PoA should consider funding projects that focus on developing advanced cybersecurity measures, promoting information sharing, fostering international cooperation, and strengthening the capacity of member states to address emerging cyber threats. By investing in these areas, the PoA can contribute to building a more secure and trustworthy cyberspace for all stakeholders involved.

Content:

1. Should the Cyber PoA assist States in their efforts to implement the framework for responsible State behaviour and tackle emerging threats in the information and communications technology?

The Cyber PoA's assistance to states with lower cyber maturity would be precious in identifying threats to information and communications technology controls. Additionally, providing a supportive framework would help standardize the efforts of member countries in tackling emerging threats.

2. Should the PoA support capacity-building and confidence-building between States? How?

As mentioned earlier, capacity-building is essential for fostering a robust environment of trust. Trust can only be achieved through personal relationships among the members of the Programme. Therefore, it is crucial to organize conferences and workshops and conduct tabletop exercises to enhance engagement at all political and technical levels. These activities will facilitate knowledge exchange, skill development, and relationship-building, ultimately supporting capacity-building and confidence-building efforts between states.

3. Should the PoA facilitate and strengthen collaboration between States and when appropriate, with civil society, the private sector, academia and the technical community? How?

The primary objective of the PoA should be to enhance collaboration between states and various sectors, including academia, technical communities, and private enterprises. For that, it would be beneficial to establish a joint working group dedicated to studying the topic and fostering cooperation. Additionally, implementing a funding program for academic research and innovative products developed by companies that contribute to the responsible use of cyberspace would be valuable. These measures will facilitate knowledge-sharing, expertise exchange, and the development of practical solutions, ultimately strengthening collaboration and promoting responsible behavior in the cyber domain.

4. Should the PoA encourage States to, on a voluntary basis, survey or report on their national efforts to implement rules, norms and principles, including through the report of the Secretary-General as well as the National Survey of Implementation? How?

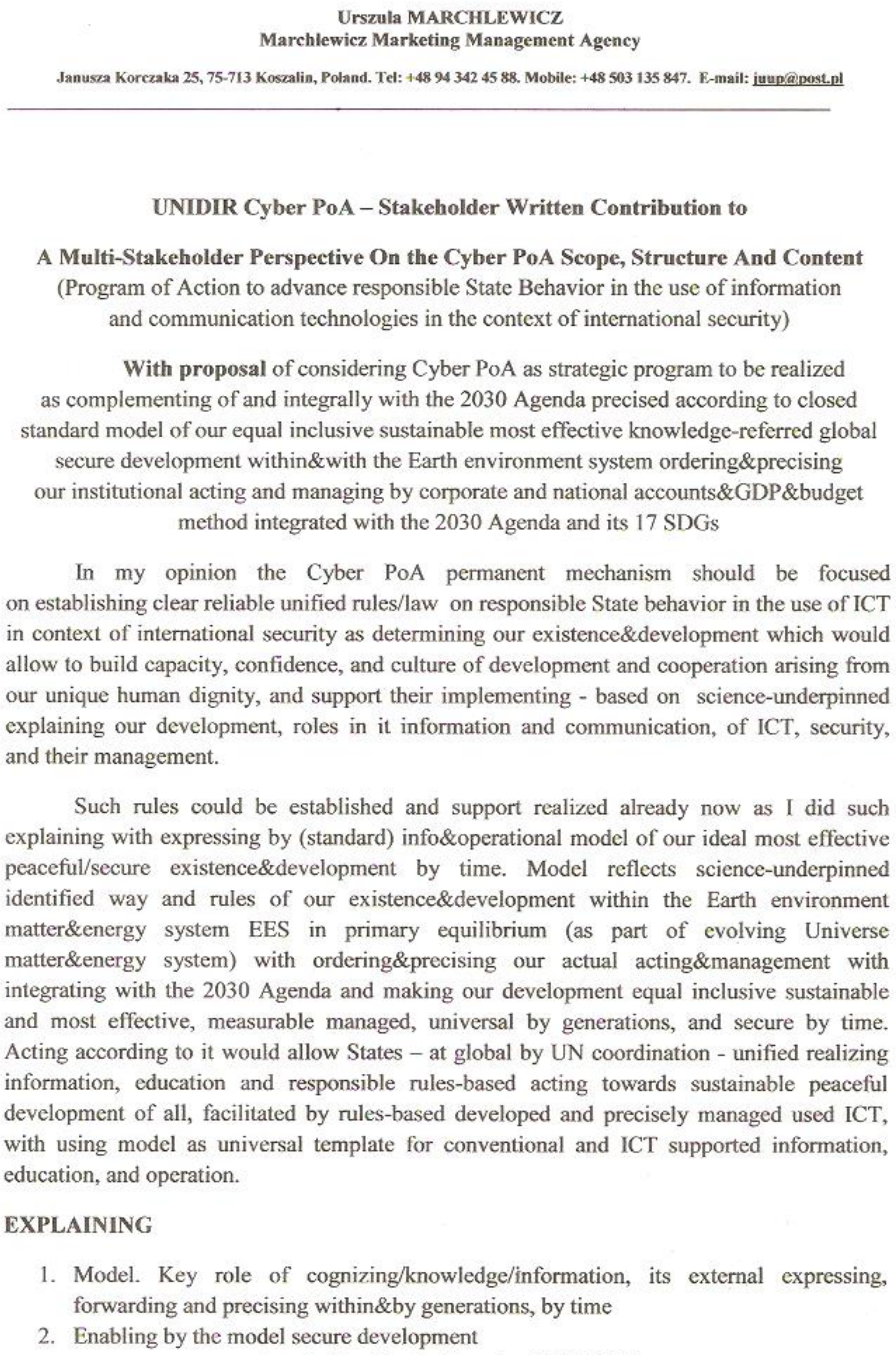
The program's success relies on each state's willingness to achieve the defined objectives. In this regard, the PoA should serve as an encourager by highlighting and showcasing on a dedicated platform those countries that have made significant progress in aligning with the established goals. In addition, the PoA can encourage states to voluntarily participate in surveys or reporting mechanisms, such as the report of the Secretary-General or the National Survey of Implementation, to demonstrate their national efforts in implementing rules, norms, and principles. Finally, recognizing and promoting the accomplishments of states that actively contribute to the PoA's objectives can inspire others to follow suit and create positive momentum toward responsible state behavior in information and communications technologies.

5. Should the PoA promote the full, equal and meaningful participation and leadership of women in decision-making processes? How?

The full, equal, and meaningful participation and leadership of women in decision-making processes should be consistently promoted within the PoA. Various international organizations focused on gender equality, particularly in technology, can support this purpose. Implementing academic research programs, fostering startups, and other initiatives targeting women can be valuable approaches. By actively involving women in critical roles, the PoA can incorporate diverse perspectives, expertise, and experiences into decision-making processes. Creating opportunities for women's engagement and leadership will contribute to more inclusive and effective outcomes within the context of the PoA.

6. Should the PoA advance multi-stakeholder discussions on the applicability of international law in cyberspace? How?

Regarding the applicability of international law in cyberspace, the PoA should engage with the CCDCoE, which is currently the leading authority in this field. This collaboration can involve sharing information, exchanging insights, and leveraging the expertise of the CCDCoE. Furthermore, the publication of the Tallinn Manual can serve as a valuable resource for advancing multi-stakeholder discussions on the topic. By actively interacting with the CCDCoE and utilizing the knowledge and guidance provided by the Tallinn Manual, the PoA can contribute to promoting and understanding international law in cyberspace.



Urszula MARCHLEWICZ
Marchlewicz Marketing Management Agency

Janusza Korczaka 25, 75-713 Koszalin, Poland. Tel: +48 94 342 45 88. Mobile: +48 503 135 847. E-mail: juup@post.pl

UNIDIR Cyber PoA – Stakeholder Written Contribution to

A Multi-Stakeholder Perspective On the Cyber PoA Scope, Structure And Content

(Program of Action to advance responsible State Behavior in the use of information
and communication technologies in the context of international security)

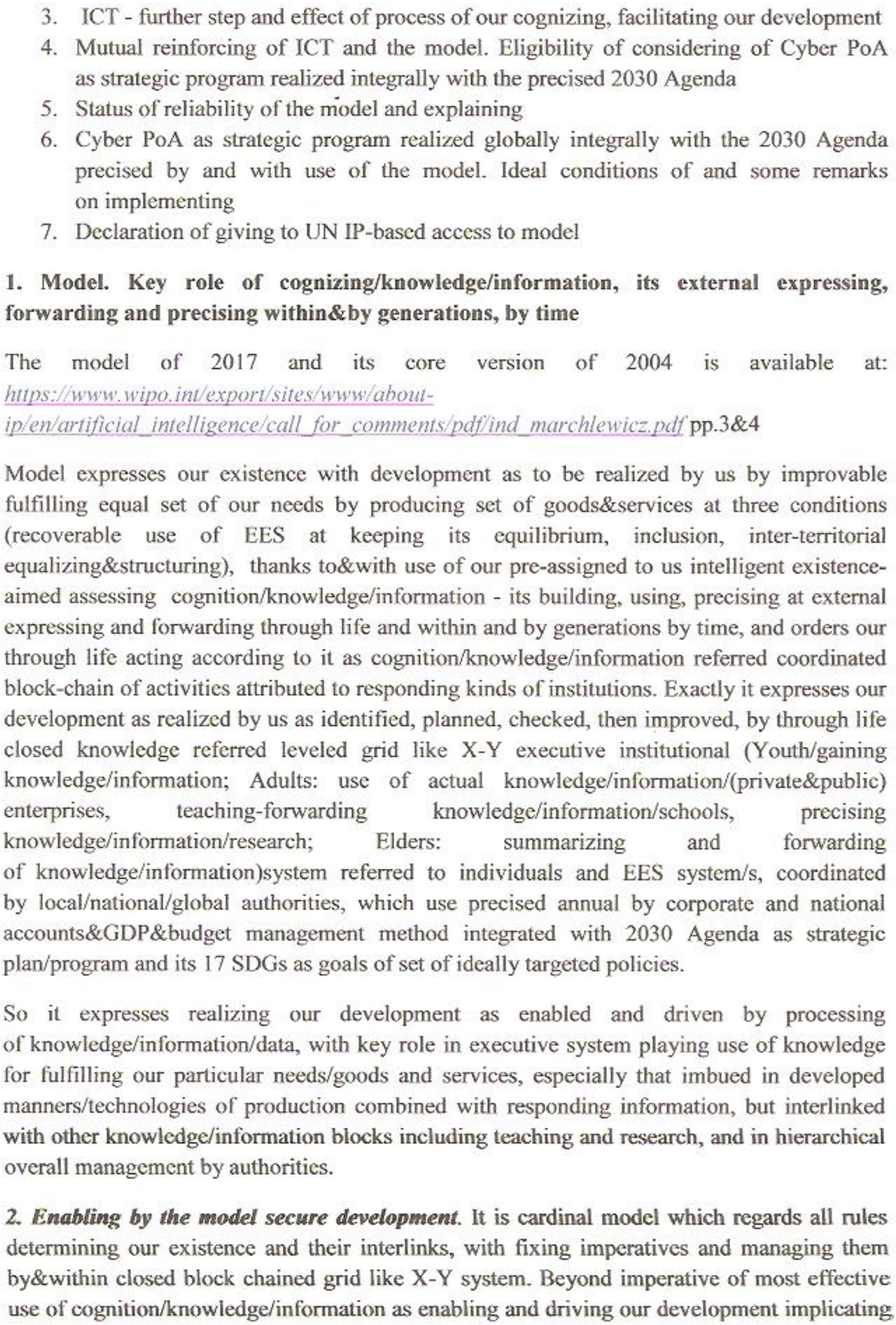
With proposal of considering Cyber PoA as strategic program to be realized
as complementing of and integrally with the 2030 Agenda precised according to closed
standard model of our equal inclusive sustainable most effective knowledge-referred global
secure development within&with the Earth environment system ordering&precising
our institutional acting and managing by corporate and national accounts&GDP&budget
method integrated with the 2030 Agenda and its 17 SDGs

In my opinion the Cyber PoA permanent mechanism should be focused on establishing clear reliable unified rules/law on responsible State behavior in the use of ICT in context of international security as determining our existence&development which would allow to build capacity, confidence, and culture of development and cooperation arising from our unique human dignity, and support their implementing - based on science-underpinned explaining our development, roles in it information and communication, of ICT, security, and their management.

Such rules could be established and support realized already now as I did such explaining with expressing by (standard) info&operational model of our ideal most effective peaceful/secure existence&development by time. Model reflects science-underpinned identified way and rules of our existence&development within the Earth environment matter&energy system EES in primary equilibrium (as part of evolving Universe matter&energy system) with ordering&precising our actual acting&management with integrating with the 2030 Agenda and making our development equal inclusive sustainable and most effective, measurable managed, universal by generations, and secure by time. Acting according to it would allow States – at global by UN coordination - unified realizing information, education and responsible rules-based acting towards sustainable peaceful development of all, facilitated by rules-based developed and precisely managed used ICT, with using model as universal template for conventional and ICT supported information, education, and operation.

EXPLAINING

1. Model. Key role of cognizing/knowledge/information, its external expressing, forwarding and precising within&by generations, by time
2. Enabling by the model secure development



3. ICT - further step and effect of process of our cognizing, facilitating our development
4. Mutual reinforcing of ICT and the model. Eligibility of considering of Cyber PoA as strategic program realized integrally with the precised 2030 Agenda
5. Status of reliability of the model and explaining
6. Cyber PoA as strategic program realized globally integrally with the 2030 Agenda precised by and with use of the model. Ideal conditions of and some remarks on implementing
7. Declaration of giving to UN IP-based access to model

1. Model. Key role of cognizing/knowledge/information, its external expressing, forwarding and precising within&by generations, by time

The model of 2017 and its core version of 2004 is available at: https://www.wipo.int/export/sites/www/about-ip/en/artificial_intelligence/call_for_comments/pdf/ind_marchlewicz.pdf pp.3&4

Model expresses our existence with development as to be realized by us by improvable fulfilling equal set of our needs by producing set of goods&services at three conditions (recoverable use of EES at keeping its equilibrium, inclusion, inter-territorial equalizing&structuring), thanks to&with use of our pre-assigned to us intelligent existence-aimed assessing cognition/knowledge/information - its building, using, precising at external expressing and forwarding through life and within and by generations by time, and orders our through life acting according to it as cognition/knowledge/information referred coordinated block-chain of activities attributed to responding kinds of institutions. Exactly it expresses our development as realized by us as identified, planned, checked, then improved, by through life closed knowledge referred leveled grid like X-Y executive institutional (Youth/gaining knowledge/information; Adults: use of actual knowledge/information/(private&public) enterprises, teaching-forwarding knowledge/information/schools, precising knowledge/information/research; Elders: summarizing and forwarding of knowledge/information)system referred to individuals and EES system/s, coordinated by local/national/global authorities, which use precised annual by corporate and national accounts&GDP&budget management method integrated with 2030 Agenda as strategic plan/program and its 17 SDGs as goals of set of ideally targeted policies.

So it expresses realizing our development as enabled and driven by processing of knowledge/information/data, with key role in executive system playing use of knowledge for fulfilling our particular needs/goods and services, especially that imbued in developed manners/technologies of production combined with responding information, but interlinked with other knowledge/information blocks including teaching and research, and in hierarchical overall management by authorities.

2. Enabling by the model secure development. It is cardinal model which regards all rules determining our existence and their interlinks, with fixing imperatives and managing them by&within closed block chained grid like X-Y system. Beyond imperative of most effective use of cognition/knowledge/information as enabling and driving our development implicating using it only for existence&development not for destroy, involving and equality of all and derivate equalizing and structuring, it has imbued imperative of most effective recoverable use of limited EES with keeping its primary construction&equilibrium arising from its fundamentally earlier established function for our existence&development.

Overarching imperative is observing all rules, imperatives and interlinks expressed by closed block-chained grid like X-Y system of realizing the precised 2030 Agenda, as their non-keeping results in development challenges being sources of local, national and global insecurity, as related with: migration, human rights, armament including nuclear ones, climate, urbanization, financing, women, equality, knowledge contributions, data, statistics, governance, which could be eliminated just by their observing. So with acting by the model enabling per se secure global peaceful existence and development.

3. ICT - further step and effect of process of our cognizing, facilitating our development.
The model explains fundamental mechanism of our cognizing and its use, but regards also its rules-based sequence, according to which ICT are further step and effect of our cognizing allowing us to use EES at precised (digital) way of expressing of cognition for facilitating and accelerating forwarding already built and expressed cognition/knowledge/information and followed development (and frontier technologies as AI, Metaverse - subsequent step and effect for facilitating and accelerating our own cognizing, based on way of our cognizing).

The above identification implicates conclusion, possibility and also imperative of developing and using ICT (also frontier technologies) for support realizing our existence according to the model, so by respective applying them for particular knowledge/information referred activities and to their overall coordination (and to attributed institutions).

4. Mutual reinforcing of ICT and the model. Eligibility of considering of Cyber PoA as strategic program realized integrally with the precised 2030 Agenda

The model with clear basic process&mechanism of our cognition and its coordination and its closed X-Y operational picture allows to develop and apply ICT to our particular knowledge/information referred activities and to the whole block-chained knowledge/information referred process of our development and its coordination (and to attributed institutions), with making them most adequate and effective for development.

From the other side - developing and applying ICT to the model would allow not only most effective realizing particular activities but coordination of all of them at the same time, with observing all rules, imperatives and interlinks (at collecting, storing and processing huge amounts of information at the same time) but also realistic achieving secure development (impossible by our conventional acting), with protection of the whole process and additionally of special one for easily identifiable neuralgic issues, and reactions on and prevention of its breaking. It could include using ICT in public communication function with identification of harmful information as done now, but considered as one of our needs, so being also existence-aimed and integrally managed.

Generally, ordering of our activities as aimed precisely at realizing set of precise goals, and their aware support, realizing, and management, through ICT, would allow more easy identification of harmful information, activities, also ICT (and frontier technologies), in their different phases, which would interfere our development, its management, security, and to undertake responding protecting and preventing means.

The applying of ICT to the acting ordered according to the model would have mutual reinforcing implications. It means that by applying ICT to acting according to model would allow fulfilling its function of peaceful development, while the model through its construction enables more effective protection of ICT themselves, with showing that their functions are integrated and mutually reinforcing.

Therefore it is eligible to consider the Cyber PoA as reliable strategic program realized globally integrally with the 2030 Agenda precised strategically by the model, moreover that the model with explaining was verified scientifically and or appreciated, by the EU (including by EU regional info&edu&development pilot by EU Programs projects) and the UN, and implementing would be realized with using existing UN (also EU) instruments and institutional structures.

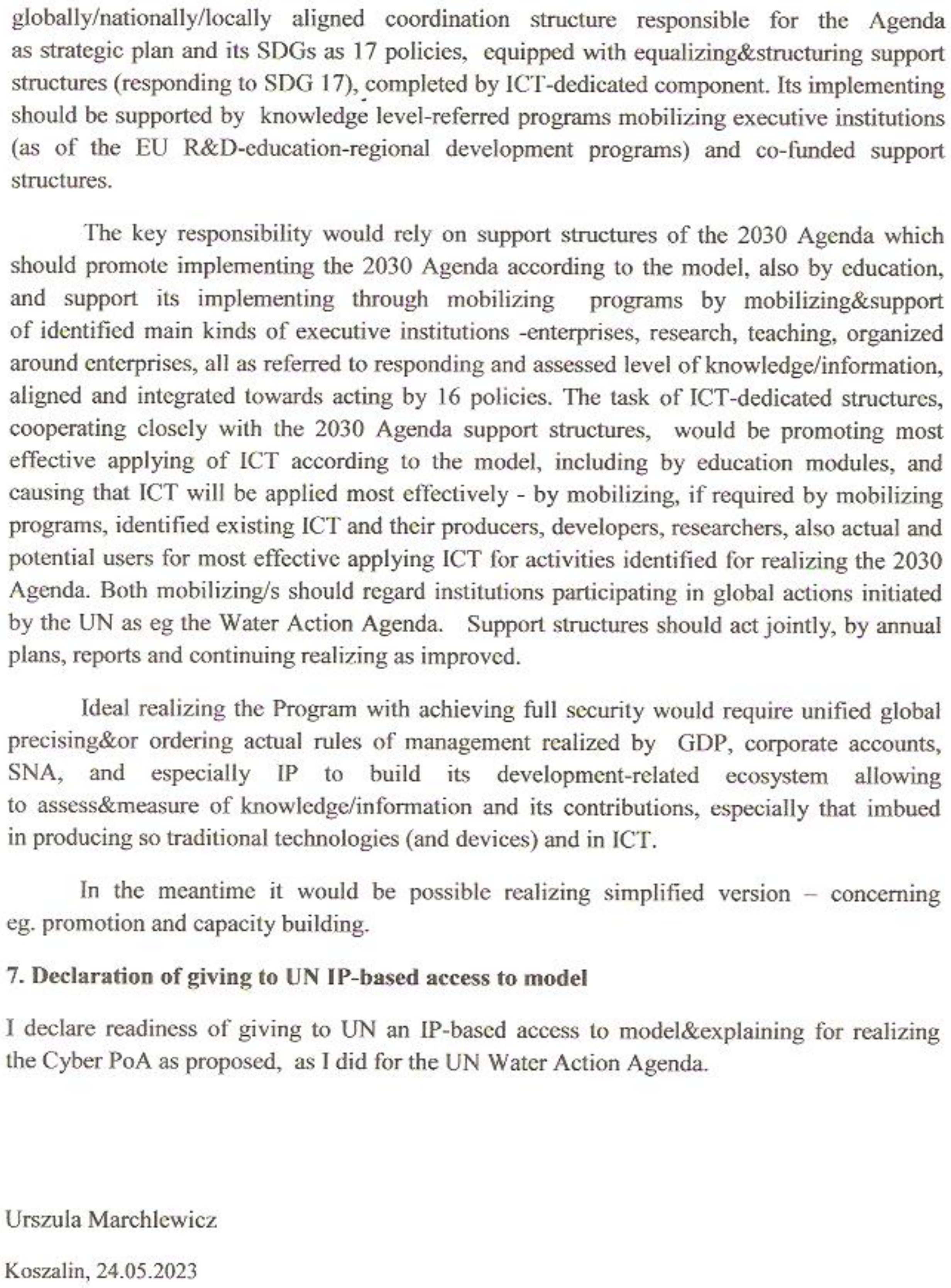
5. Status of reliability of the model and explaining

The model was built 2017 by further precising its core institutional version by GDP management integrated with the EU managing instruments (Lisbon Strategy, policies as in Treaties, knowledge-referred R&D/education/regional development programs) of 2004 verified scientifically by global higher education conferences involving also UNESCO, appreciated by Professor Nathan Rosenberg – Co-Author of Chain of Innovation, EY, accepted by EU&PL for realizing EU regional info&edu&development pilot by EU Programs projects I lead, through Koszalin University and its EU R&D Program Contact Point acting in national&EU network 2000-10.

Thanks to its actual final version and dedicated explaining/s promoted to the UN I was appreciated by UN by admitting myself to HL UN Processes as Global Compact for Migration (consultative status), UNGAs (as observer) on Nelson Mandela Peace Summit 2018 and on Eliminating Nuclear Weapons Threats 2018&2019, WIPO Conversation on IP and frontier technologies 5th Session (allowed intervention) 2022, UN 2023 Water Conference (special accreditation and organizing own side event). Final model assumes imperative keeping of EES equilibrium, with EES equilibrium confirmed by 2021 Nobel Winners in Physics.

6. Cyber PoA as strategic program realized globally integrally with the 2030 Agenda precised by and with use of the model. Ideal conditions of and some remarks on implementing

The Program should be realized as strategic one complementing program of realizing the 2030 Agenda according to the model, implemented jointly by annual plans (till 2030 with possible prolonging). It should have coordination structure based on built



globally/nationally/locally aligned coordination structure responsible for the Agenda as strategic plan and its SDGs as 17 policies, equipped with equalizing&structuring support structures (responding to SDG 17), completed by ICT-dedicated component. Its implementing should be supported by knowledge level-referred programs mobilizing executive institutions (as of the EU R&D-education-regional development programs) and co-funded support structures.

The key responsibility would rely on support structures of the 2030 Agenda which should promote implementing the 2030 Agenda according to the model, also by education, and support its implementing through mobilizing programs by mobilizing&support of identified main kinds of executive institutions -enterprises, research, teaching, organized around enterprises, all as referred to responding and assessed level of knowledge/information, aligned and integrated towards acting by 16 policies. The task of ICT-dedicated structures, cooperating closely with the 2030 Agenda support structures, would be promoting most effective applying of ICT according to the model, including by education modules, and causing that ICT will be applied most effectively - by mobilizing, if required by mobilizing programs, identified existing ICT and their producers, developers, researchers, also actual and potential users for most effective applying ICT for activities identified for realizing the 2030 Agenda. Both mobilizing/s should regard institutions participating in global actions initiated by the UN as eg the Water Action Agenda. Support structures should act jointly, by annual plans, reports and continuing realizing as improved.

Ideal realizing the Program with achieving full security would require unified global precising&or ordering actual rules of management realized by GDP, corporate accounts, SNA, and especially IP to build its development-related ecosystem allowing to assess&measure of knowledge/information and its contributions, especially that imbued in producing so traditional technologies (and devices) and in ICT.

In the meantime it would be possible realizing simplified version – concerning eg. promotion and capacity building.

7. Declaration of giving to UN IP-based access to model

I declare readiness of giving to UN an IP-based access to model&explaining for realizing the Cyber PoA as proposed, as I did for the UN Water Action Agenda.

Urszula Marchlewicz

Koszalin, 24.05.2023

Microsoft Corporation Tel 425 882 8080
One Microsoft Way Fax 425 936 7329
Redmond, WA 98052-6399 http://www.microsoft.com/

Microsoft

Microsoft’s Position Paper

Programme of action to advance responsible State behavior in the use of information and communications technologies in the context of international security

Over the past decade, Microsoft has closely followed and provided input to various United Nations (UN) initiatives and dialogues on cybersecurity. This has also included recent discussions to establish a permanent UN body on cybersecurity. In fact, Microsoft has consistently called for the establishment of just such a body to help address what we believe are growing international security challenges in cyberspace. We believe such a body is needed to drive the implementation, as well as further development of the existing UN framework for responsible state behavior in cyberspace – across norms, international law, capacity building and confidence-building measures.

Against this background, we supported, in principle, the concept of a Programme of Action (PoA), as proposed by France and Egypt and we acknowledge the significant support for the PoA resolution (A/RES/77/37) in the UN General Assembly. That said, it represents only the first step on the road to establishing a permanent venue for these challenging discussions. Many aspects of the PoA remain unresolved and this includes critical provisions on decision making and multistakeholder participation.

Microsoft has previously put forward a set of principles that we believe a permanent UN body on cybersecurity should be guided by, which include:

- Ensuring meaningful inclusion and participation of all relevant stakeholders, including those from private sector, academia, and civil society;
- Providing practical support, including funding, for implementation of existing commitments;
- Building upon existing agreements and effective international initiatives, such as the Paris Call for Trust and Security in Cyberspace and the Global Forum on Cybersecurity Expertise;
- Including robust human rights provisions:
- Retaining sufficient flexibility to be able to respond to rapidly evolving digital threats.

We elaborate on our substantive proposals for the PoA in more detail below for consideration by states, but suffice it to say that we believe that the international community needs to move from discussions into action. Commitments states make at the UN cannot remain mere words on paper. A permanent and inclusive UN body on the subject would allow the international community to set more ambitious goals for itself, support implementation across the globe, as well as periodically review the progress made.

We remain open to working closely with all partners who share our aspiration to establish an inclusive, flexible, forward-looking, action-oriented, and permanent UN body on cybersecurity.

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

Detailed proposals

Scope and general objectives

Microsoft supports the PoA's proposed objective, i.e., to strengthen international security and stability in the ICT domain, by establishing a permanent and inclusive UN mechanism to reinforce and advance the existing Framework. We strongly recommend this mechanism focuses on the most important threats emanating from cyberspace and the resulting challenges. For example, an early priority could be to encourage States to continue to define what they consider as critical infrastructure to establish further expectations for responsible state behavior and to develop practical guidance on critical infrastructure protection in different sectors. A focus on case studies may be conducive to reaching these objectives.

Importantly, however, States should also not shy away from expanding the framework to cover new areas to effectively respond to emerging cyber threats that can threaten international peace and security. The previous UN GGEs and the OEWG, as well as work in many regional organizations, such as e.g., the OSCE, have focused on the proverbial "low-hanging fruits". While such a focus was justified in the past, especially for time-bound initiatives such as the UN GGE and the OEWG, a permanent mechanism should not shirk away from focusing on the most important issues, even if they are the most challenging and could, potentially, take a long time to resolve.

Microsoft notes the idea that the PoA would provide a venue for engagement and cooperation with the multistakeholder community (academia, private sector, civil society). While we recognize the need to draft multilateral documents with diplomatic sensitivity and caution, we would also stress that, given the reality of ICT infrastructure, where responsibilities, expertise and resources are shared across all stakeholder groups, a reasonable argument can be made that the multistakeholder community can provide value to all topics that a new mechanism in this space would likely address. We therefore urge States to make the PoA as inclusive as possible of multistakeholder voices, including by facilitating stakeholder access to PoA working groups, e.g., in line with established practice of Geneva-based UN technical agencies.

Content and potential areas of focus

The PoA can potentially represent a positive contribution to UN processes on cybersecurity. Its establishment on its own would send a strong signal that states are committed to prevent, combat and eradicate threats emanating from cyberspace. Moreover, previous drafts envisioned it as a means to "*serve as a permanent, more structured yet flexible solution that allows for consensus driven, action-oriented and transparent regular dialogue between states, more multistakeholder engagement and acknowledges the importance of capacity building*". Such a structure would both ensure sustainable funding and incorporate prior processes into one permanent mechanism, thereby avoiding the need for a regular renewal of mandates, which always come with political risk.

Microsoft believes that the current OEWG identified important areas that need to be addressed when it comes to securing the common online environment. Indeed, many of these were highlighted in the original proposal for the PoA, as they stem from the mandate of the group (cooperation, confidence building measures, capacity building, norms, rules and principles, international law, threat assessment). While they should not be neglected, the OEWG and PoA should also not duplicate their efforts, in particular if the PoA is established with a focus on greater openness, transparency and collaboration with other groups. We urge states to consider the following areas of focus as priorities:

- **Implement agreed upon norms** by developing conceptual and practical guidance on how the existing framework could be operationalized. The PoA could also support and promote the implementation survey process, as envisioned as part of the previous OEWG, and build on the last GGE consensus report, which focused on critical infrastructure protection. For example, an early priority could be to encourage states to define what they consider critical infrastructure.

  The PoA could also build on similar existing international initiatives, such as the Paris Call for Trust and Security in Cyberspace. Efforts such as these have put forward potential models for multistakeholder cooperation for identification of good practices.

- **Encourage stakeholders to regularly measure progress made on norm implementation.** Technology will evolve as will our understanding on how to ensure stability and security of cyberspace. With that in mind we should ensure that implementation of cybersecurity norms is not a one-off investment, but a continuous process. The PoA could build on the implementation survey highlighted above to create a mechanism that would allow states to measure whether they are making progress in the implementation of norms, but more importantly in improving their security posture. Such a mechanism should be tailored to local contexts.

- **Identify new areas for engagement and potential development of new norms.** While the existing normative framework represents an important contribution to the stability of the online environment, it is Microsoft's view that there remain several gaps in the international cybersecurity framework that states continue to exploit. It is likely that as technology evolves, even more of these will become apparent. Given the PoA's aim to implement and reinforce expectations for responsible state behavior online, it must continue to identify new areas for action while consulting with a wider variety of stakeholders.

- **Drive greater understanding of how international law applies to cyberspace.** Norms are only part of the international cybersecurity framework that states need to abide by. International law, international human rights law, and international humanitarian law complete the puzzle. Indeed, it is widely acknowledged that these apply to cyberspace, but there has been limited consensus or understanding regarding *how* that occurs. With that in mind, the PoA should encourage states to articulate their positions on international law and then collect them, building a common understanding of this area.

  Similarly, the PoA should leverage existing multistakeholder processes looking to illuminate the application of international law to cyberspace and organize similar discussions as part of its mandate. For example, the Oxford Process on International Law Protections in Cyberspace has held numerous convenings and produced multiple statements of consensus, endorsed by hundreds of leading international lawyers from around the world, on how international law applies to key areas of daily life including the healthcare sector, vaccine research, electoral processes, and information operations. Similar topical discussions could help drive practical application of what is often a theoretical framework.

- **Provide a permanent structure to administer and evolve a database of points of contact** at various levels within governments and other stakeholder groups to support more rapid crisis management when attacks happen beyond borders. This database, which is currently being considered in the OEWG, could also be used to facilitate general information sharing and trust building among all relevant stakeholders before a real crisis hits.

- **Establish regional liaisons through cooperation with regional organization** to drive international collaboration in prevention, response and recovery efforts. This could facilitate coordinated initiatives down the line and offer tailored regional support for states.

- **Drive global cybersecurity capacity building**, in collaboration with stakeholders across sectors, in support of the Sustainable Development Goals, to allow for state implementation of international expectations in cyberspace. This could include the identification of gaps in cybersecurity capacity building efforts and help devise implementation solutions to fill those gaps, including potentially through the CyberPeace Institute and other NGOs.

Moreover, the PoA should encourage work with the Global Forum on Cyber Expertise (GFCE) as a donor coordinator given its existing function of capacity building and community efforts. The GFCE could be leveraged or used as model to coordinate assistance initiatives through a system for matching needs and resources.

- **Identify potential avenues to limit the use of private sector offensive actors** to mitigate risk. This work could start addressing current ambiguity around not just what tools and techniques should be banned, but also setting clear boundaries around intent, authority and intrusiveness.
- **Develop sustainable models for multistakeholder diplomacy**. The PoA by itself needs to be a multistakeholder initiative, but that does not mean it needs to be static. In fact, the PoA should dedicate time and effort to explore existing barriers to multistakeholder inclusion and identify good practices to mitigate exclusion – at international levels and domestically. Given the expertise non-governmental stakeholders have in cybersecurity, only by allowing for meaningful multistakeholder inclusion, does the PoA have a chance to make a meaningful contribution towards improving the security of the online world.

Since the PoA is envisioned as a permanent body that is expected to navigate a field that values speed and innovation, it is critical that it retains the flexibility for states to agree on new areas of work over time. The original proposal highlighted the possibility of states submitting working papers on specific thematic issues, but we believe that if the PoA wants to remain true to its commitment to working with the multistakeholder community, it must go a step further. As such, we encourage states to consult amongst each other, and with the multistakeholder community, on an annual basis to determine whether existing areas of priority remain relevant and whether new areas of work should be introduced. This should include the ability for non-governmental participants to propose new areas of action.

Structure - organizational considerations

The PoA's originally proposed periodic meeting schedule (i.e., review conferences every four years, followup meetings held every year and ad hoc thematic meetings, as appropriate) does not track with the speed of developments in cyberspace. Therefore, the PoA should consider adding more touch points throughout the year, such as bi-annual follow-up meetings and a minimum of two to three thematic meetings per year, especially given the rise and sophistication of cyber incidents.

We believe working groups with specific focus areas would also help drive collaboration and advancement of issues in this space. However, to ensure broad participation and engagement, the working groups should not be run concurrently. Proposed working groups could include:

- Analysis of emerging threats requiring the updating of existing framework;
- Promotion of norms and best practices;
- Protection of critical infrastructure across sectors;
- Application of international law to cyberspace;
- Expansion and mainstreaming of cybersecurity capacity building; and
- Development and implementation of confidence building measures.

Representatives from the working groups should meet at least once a year to track their progress on implementing the PoA, synchronize and recalibrate their efforts as needed.

Moreover, and regardless of the meeting cadence that will ultimately be selected, the importance of the intersessional period cannot be overstated. For the PoA to be successful, the intersessional period should be leveraged to hold additional discussions and drive the conversations forward as much as possible – and this should include all the relevant stakeholders.

We also hope the UN continues to leverage technology when it comes to live-streaming debates. While in-person meetings can be fruitful when it comes to building consensus and negotiating details, virtual meetings are also beneficial as they can be much more inclusive of non-governmental organizations, as many do not have representation in, or the budget to travel to New York. We therefore recommend that all formal meetings be live streamed, recorded, and published on the relevant UN websites.

Engagement with interested parties

Threats emanating from cyberspace cannot be tackled by states on their own. Clearly, multistakeholder diplomacy is essential considering the complex nature of the domain. On the UN side, this inclusion has already proven fruitful, not only through the OEWG's Intersessional Meeting in 2019, but through the plethora of informal consultations that have built trust amongst stakeholders since then. A recent example would be the UN negotiations on a new cybercrime convention which have allowed for meaningful multistakeholder participation and have significantly benefited from it.

In the context of the PoA, we believe that meaningful multistakeholder participation should be a key feature of the initiative. It is our belief that the multistakeholder aspect of the PoA would be one of its main strengths. What we hope for in the context of the PoA is for the multistakeholder community to be a core part of:

- The PoA's proposed periodic meetings;
- Consulting on proposals to take action with the multistakeholder community;
- Conferring through multiple channels, such as meetings or written responses to create multiple opportunities for groups to engage;
- Organizing side events and round tables, in cooperation with states and the secretariat;
- Exploring opportunities for the ongoing exchange of information to address pressing challenges.

With that in mind, we are also concerned that restrictive accreditation processes for multistakeholder participation and injudicious use vetoes in the current OEWG continues to run the risk of excluding organizations with valuable perspectives that may not be traditional participants in UN forums. Therefore, it is critical that any accreditation for cyber dialogues goes beyond the strict inclusion of groups that are already accredited at the Economic and Social Council (ECOSOC), or those that have a standing invitation to participate as observers at the General Assembly. One way to achieve this would be to leverage and further build on the modality for stakeholder inclusion used within the context of Ad Hoc Committee on elaborating a UN convention on countering cybercrime, which has proven to work well and is being increasingly leveraged across UN fora as a useful precedent.

While this is a relatively new area for this issue space, working with the multistakeholder community to drive implementation of international agreements is an established practice in fields such as development or environment. We would therefore recommend leveraging the models that emerged from those processes and which include steps that encourage broad participation.

Paris Peace Forum's Position Paper

Programme of Action to advance responsible State behavior in the use of information and communications technologies in the context of international security

Preliminary recommendations

Acting as the secretariat of the Paris Call for Trust and Security in Cyberspace, the Paris Peace Forum has long advocated for strengthening and sustaining multilateral processes to advance international norms for collective security in cyberspace. To this end, the Forum notably participates and provides inputs to the United Nations' Open-Ended Working Group on security of and in the use of information and communications technologies (OEWG) 2021-2025, as an accredited stakeholder.

The Paris Call was launched in 2018 with the view to best articulate international cyber policymaking with the traditional structure of internet governance, in particular by applying a multi-stakeholder lens to a range of policy concerns that were traditionally addressed from a strict inter-state perspective. This ambition led members of its 1,200 supporter's community to work jointly towards the elaboration of action-oriented recommendations aimed at "*Advancing the UN negotiations with a strong multistakeholder approach*". The study released in November 2021 notably suggested building on the achievements of existing international, permanent mechanisms, including Programmes of Action (PoAs) established in other fields, to advance intergovernmental discussions while ensuring a fair participation of the broader stakeholders community.

The Paris Peace Forum therefore welcomed the adoption of resolution (A/RES/77/37) by the UN General Assembly in December 2022, which endorses the proposal to establish a Cyber PoA and calls for further discussions in this regard. As the resolution merely envisages the future PoA as "*permanent, inclusive, and action-oriented*", it represents only the first step in the process towards establishing the mechanism - which still requires agreement on its concrete modalities. The Forum intends to support negotiations in this regard by mobilizing the Paris Call community in order to provide States with clear proposals on the scope, structure, and content of the Cyber PoA, in line with the Paris Call's underlying ambition of achieving greater inclusivity in multilateral dialogues on cybersecurity.

In this context, the Paris Peace Forum and the Global Forum on Cyber Expertise organized last March a roundtable discussion on the sidelines of the 4th substantial session of the OEWG on how to best mobilize the initiative in discussions on the Cyber PoA. The Forum will continue to engage with key partners in the coming months to strengthen coordination within the stakeholders community in the formulation of concrete proposals throughout the negotiation process. The following preliminary recommendations, produced as part of the UNIDIR event "*Drawing Parallels: A Multi-Stakeholder Perspective On The Cyber PoA Scope, Structure And Content*", should therefore not prejudge any conclusions that may be arise from a joint position of several stakeholders in the future.

Scope and objectives

The Paris Peace Forum supports the general goal of the Cyber PoA as proposed in the UN General Assembly resolution (A/RES/77/37), i.e. to strengthen international peace and security in the context of the use of ICTs by establishing a permanent, inclusive and action-oriented UN mechanism, whose action is guided by specific objectives and builds on previous outcomes in this field. While all of the specific purposes mentioned by the resolution (discussing existing and potential threats; supporting states' capacities and efforts to implement and advance commitments related to voluntary norms of responsible state behavior and to the application of international law to States' use of ICTs, developing new norms if needed, confidence and capacity building measures) are all relevant as part of such a mechanism, prioritization among these objectives is appropriate to maximize consistency and effectiveness.

In our view, a *permanent* mechanism main interest lies not primarily in a more efficient norms-making process with regard to the use of ICTs by States, especially if the development of such norms remains consensus-based. Rather, it allows to strengthen the dialogue not only among States but also with the inclusion of non-governmental stakeholders towards a smoother and more harmonious implementation of already agreed norms and frameworks. Implementation of existing norms should therefore come first, as this framework already provides a solid baseline for which there remain, however, major enforcement and accountability gaps. The full application of international law, as a binding body of norms applicable as a whole to cyberspace, remains particularly crucial and requires an ongoing dialogue for a progressive convergence among national positions.

This priority should go hand in hand, within the mechanism, with the elaboration, implementation and oversight of capacity building measures – in particular with regard to policy, institutional and legislative development among States. The involvement of trusted non-governmental stakeholders as designing and implementing partners should be particularly sought here, given the widely recognized expertise of some in this area. This may for instance includes the Global Forum on Cyber Expertise, Smart Africa or the Oxford Process on International Law Protections in Cyberspace. It should also be noted that certain regional organizations active in the cyber field have been developing such public-private partnerships for a long time and should be able to usefully inform intergovernmental discussions on this aspect.

When it comes to developing new norms of responsible behavior, we believe at this stage of the process that the realization of the above-mentioned priorities should not be obstructed by overwhelming negotiations under the PoA about expanding the framework. However, the necessary effectiveness of the future mechanism seems to require that it be endowed with a certain level of flexibility and not be deprived from the outset of any possibility to serve as a norms-making fora. Discussions on the desirability of developing new norms could therefore take place, if necessary, on the occasion of yearly or biennial meetings of States or during review conferences, provided that the later are not too distant in time. In any case, such discussions will have to be articulated with other intergovernmental bodies under the UN that may be created or extended by States in this regard, in order to avoid overlaps and fragmentation of efforts.

Transversally, and considering that cyberspace remains privately owned and operated for a significant part, we call on States to shape the Cyber PoA in such a way that the stakeholders community is able to contribute meaningfully in the work undertaken within it - in a more robust manner than in current multilateral fora. Although the definition of responsible behavior of States in the use of ICTs shall stem from a State-driven process, the resources and expertise of non-government stakeholders will effectively support the interpretation and implementation of such a framework while strengthening the accountability of private systemic actors led to cooperate. While a First Committee mechanism is not the most appropriate place to settle multi-stakeholders' rights and responsibilities, the rights and obligations of non-government stakeholders can nevertheless be addressed by clarifying any norms of international law that directly affects private actors, including parts of international humanitarian law and international criminal law, as well as indirectly by advancing due diligence in cyberspace.

Content

- Norms implementation efforts and accountability mechanisms

The achievement of the Cyber PoA's main objective would be usefully supported by the establishment of effective accountability mechanisms with regard to norms implementation by States. Alongside review conferences, this may include a self-assessment by States through national reporting, which has proven to be a useful accountability and transparency tool in numerous mechanisms related to disarmament and international security. It should be noted, however, that under the PoA on Small Arms and Light Weapons, the level, frequency and accuracy of reporting by States has varied over time, with significant disparities among regions of the world[1]. Targeted confidence-building and capacity-building measures should therefore be associated with this, in order to strengthen the practice of the States as a whole. UNIDIR could further support such national reporting efforts, as it is already doing through the National Survey of Implementation. States should also further consider more ambitious accountability mechanisms, such as mutual evaluation or cross-country reviews.

In terms of thematic priorities to be addressed with regards to norms implementation efforts, and while we understand that such priorities might be defined by States once the mechanism is established, we recommend to advance at first towards clear and common criteria for identifying critical infrastructures, building in particular on the final report from the 2019/2021 UN Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security.

- Coordination of cyber capacity-building efforts at the global level

The Cyber PoA provides a unique opportunity to create a vehicle for streamlining global cyber capacity-building efforts, in connection with existing public, private and multi-stakeholder initiatives and funding structures in this area. To maximize coherence and good use of necessarily limited resources, and considering that this mechanism will fall within the mandate of the First Committee of the UN General Assembly, we recommend that the capacity-building measures or programs that would be deployed or supported strictly respond to the objective of implementing the framework of responsible State behavior in the use of ICTs, in the context of international security. The operationalization of programs or measures decided within the PoA could rely on trusted implementing partners, whose identification will have to be done according to clear and transparent rules of procedure agreed upon by States while being informed by the stakeholders community.

- Strengthening multi-stakeholder collaboration

As mentioned above, we believe that the Cyber PoA should be designed from an organizational point of view to allow for strengthened participation of non-governmental stakeholders, while keeping in mind that States retain the central role in any UN mechanism aimed at maintaining international peace and security. From a substantive perspective, we also believe that the PoA should also address multi-stakeholder cooperation in cyberspace, including by sharing best practices in this regard while leveraging existing

[1] See, in this regard : Ivor Fung, "Programme of Action on SALW International Tracing Instrument: Trends, Challenges and Opportunities", UNODA, 2022; Sarah Parker, Christelle Rigual, "What the National Reports Reveal: Trends in UN PoA and ITI Reporting", Small Arms Survey Issue Briefs, 2015

initiatives in this field. As a multi-stakeholder initiative aimed at strengthening collective security in cyberspace, the Paris Call, in coordination with other initiatives, stands ready to support the work undertaken in the framework of the PoA on this and other aspects.

Structure

- Organization of work

Beyond structuring the Cyber PoA around review conferences and yearly or biennial meetings of States, as is traditionally the case for such mechanisms and for which we have no comments to make at this stage on the proposed periodicity, we recommend that States consider creating issue-specific workstreams that have the flexibility to be responsive to developments in the ICT environment while achieving meaningful multi-stakeholder engagement in this regard. This this is particularly critical to discuss existing and emerging threats, given the rapidly evolving technology landscape and the successful public-private collaborations that already exist in other fora - such as INTERPOL's Cyber Fusion Centre or Europol's European Cybercrime Centre[2]. This architecture could be usefully complemented by the establishment of permanent platforms for information sharing, such as a repository of common threats, vectors and actors as proposed by Kenya during the OEWG's last substantive session in March 2023. We also recommend that such a platform be created regarding critical infrastructure incidents, in order to foster cross-border cooperation in this regard, to strengthen the common understanding of the level of harms that cyber operations targeting them can actually produce, and to ultimately mitigate the damage to populations.

- Funding

As a permanent mechanism focused on concrete implementation of norms and capacity building, we believe that the Cyber PoA should be supported by sustainable financial resources, including extrabudgetary resources. In this regard, the establishment of a multi-donor trust fund specifically aimed at supporting activities undertaken under the PoA would be appropriate, in compliance with the UN Financial Regulations and Rules. States might also consider opening the trust fund to voluntary contributions from private actors, as is the case, for instance, for the UN Voluntary Trust Fund for Assistance in Mine Action. This fund could also provide some support for the attendance of non-governmental stakeholders with limited resources to formal meeting, rather than this support being the initiative of one or a few states as has been the case at previous substantive sessions of the OEWG II.

[2] See, in this regard: Compendium of Transnational Public-Private Partnerships Against Ransomware, Paris Call for Trust and Security in Cyberspace, 2022

STIMSON

INNOVATIVE IDEAS CHANGING THE WORLD

24 May 2023

Written Contribution:
UN Cyber Programme of Action

Submitted by Allison Pytlak, Stimson Center

This written contribution is being made in response to a request from the UN Institute for Disarmament Research (UNIDIR) about non-governmental stakeholder views on the scope, structure, and content of the proposed UN Cyber Programme of Action (Cyber PoA). A Cyber PoA could help to fill the current accountability gap between the existing UN Framework for State Behaviour in Cyberspace (UN Framework) and actual practice by solidifying commitments and introducing reporting or review mechanisms.

Diverse actors have raised the concern that there are few accountability or transparency mechanisms relating to implementation or compliance with the UN Framework, or that efforts in this area are patchy and disparate. The creation of a distinct and politically-binding instrument like a Cyber PoA is a unique opportunity to close this gap and foster greater transparency and accountability.

SCOPE

Q1. Should the Cyber PoA permanent mechanism focus on consensus report recommendation follow-up, development of new norms, capacity-building or confidence-building?

The Cyber PoA should focus on implementation of consensus report recommendations and in particular, the UN Framework. In this context, capacity- and confidence-building are also relevant objectives.

The Cyber PoA could be a way to foster better clarity and understanding about what the eleven UN norms for responsible state behavior are and provide practical and technical guidance to support their implementation. Despite being so foundational to the UN Framework, the norms themselves can be difficult to locate, identify, or explain to those not familiar with UN documentation and processes. Giving them a prominent place within the Cyber PoA and providing a series of recommended actions for implementing each norm, at all levels, would generate better awareness and understanding about what they are, thus improving the prospects for their implementation.

The possibility of developing of new norms has also surfaced as a topic for further consideration amongst member states. There are multiple dimensions to this issue: one is about “future proofing” the instrument so that the Cyber PoA can remain relevant while another dimension is political—all UN member states have endorsed the existing norms, but not all have participated in their development in the Groups of Governmental Experts (GGEs). Therefore, the possibility of being able to contribute to the development of new ones might be attractive to some member states and a motivating factor to support the Cyber PoA.

However, a PoA may not be the most appropriate pathway for developing new norms because a PoA is an instrument, not a negotiating forum. Attempting to negotiate new norms at PoA meetings risks politicizing the environment or could adversely affect PoA implementation. That said, Cyber PoA-endorsing member states could, at PoA meetings or via the UNGA, mandate the creation of a separate and temporary body such as a working group or GGE for new norm development if and when it is needed. Because PoAs are so operational in nature, they can be a good tool to detect gaps or new challenges that would require new norms. This possibility could be foreseen and reflected in the text of the Cyber PoA so as to ensure that it is accounted for at the time of its creation, given that new norms are a priority for some member states and ensure the long-term viability of the instrument.

Q2. Should the PoA define States’ and multi-stakeholders’ rights and responsibilities – burden and credit-sharing modalities?

Yes. PoAs can only be endorsed by states, who carry the primary responsibility for their implementation. Given the important role played by a range of non-governmental stakeholders in the ICT environment however, it will be vital that their functional role in PoA implementation is defined and clarified within the instrument.

An examination of other PoAs shows these instruments refer to the role of a wide range of stakeholders and describe their role in implementation and/or relationship to member states. These variously include UN organs or agencies; the UN Secretariat; regional bodies; intergovernmental organizations; technical experts or operators; civil society organizations; academia; legislators; and the private sector. Most of them refer to, or encourage collaboration with, specific types of actors throughout the instrument. This approach to the instrument’s text embeds and cements a cooperative, multistakeholder model within the text of these instruments and will help to facilitate engagement with stakeholders in national and regional implementation efforts.

The cyber PoA should also adopt this approach. The instrument could include a preambular paragraph that welcomes and acknowledges the role played by non-governmental actors. Its operative and action-oriented paragraphs could then refer to particular types of actors that will be relevant to implementation or advancing the activity contained in any given paragraph or action point and encourage collaboration between such stakeholders and member states.

STRUCTURE

Q2. Should the PoA develop a funding mechanism? What kind of projects should the PoA consider?

A funding mechanism to provide direct support for Cyber PoA implementation would be beneficial. However, it might make sense to develop and launch it after the PoA is established so that the mechanism can directly correlate to and support its provisions and commitments, which are still yet to be determined. It will be important to avoid duplication with other capacity-building activities, and to also bear in mind the capacity-building principles agreed to in the final report of the 2019-2021 OEWG. The text of the Cyber PoA could foresee this possibility in various ways, to ensure that it is a priority for endorsing member states to take up.

CONTENT

Q1. Should the Cyber PoA assist States in their efforts to implement the framework for responsible State behaviour and tackle emerging threats in the information and communications technology?

Yes, please see response to Question 1 under "Scope" for more on how the Cyber PoA could be linked to implementation of the Framework.

As an example of how this could work and look like in the Cyber PoA text, the final report of the sixth UN GGE adopted in 2021 provides context and additional understanding about each of the norms. That content would be a useful starting point for Cyber PoA content. In some places the GGE report content is more explanatory in tone, but other paragraphs provide guidance that would be suitable for inclusion in a PoA-type instrument. For example, paragraphs 22–28 of the GGE final report relate to norm 13(b) on attribution. Paragraphs 23–28 describe actions or activities that states can or should take in relation to attribution. In a PoA, those actions could each become their own paragraph or "action point" depending on how each is articulated. Some are national actions, whereas others require regional activity or international information exchange or cooperation. Another potential source for cyber PoA content in relation to the norms and framework would be the "norms guidance text" proposed by Canada during OEWG I, which was supported by several other delegations and developed with inputs from states and civil society.

Q3. Should the PoA facilitate and strengthen collaboration between States and when appropriate, with civil society, the private sector, academia and the technical community? How?

Yes. In addition to incorporating reference to the role of non-governmental stakeholders within the text of the instrument as outlined elsewhere in this contribution, PoA meetings and conferences, or subsidiary bodies, should be inclusive and engage non-governmental stakeholders in all aspects of its work. There are ample examples of how this has worked in other PoAs and UN forums, even though stakeholder access and participation to the Open-ended Working Groups has been challenging.

Q4. Should the PoA encourage States to, on a voluntary basis, survey or report on their national efforts to implement rules, norms and principles, including through the report of the Secretary-General as well as the National Survey of Implementation? How?

Yes, although "reporting for reporting's sake" alone should be avoided. Multiple instruments on diverse issues and topics have some form of national reporting built into them as a way to foster transparency and accountability, as well as share experience and knowledge and identify areas for capacity-building. But the experience across many of these instruments and their associated forums show that the general trend in reporting rates is either a decline over time or a lack of take-up at the outset, which sets a low bar for expectation and does little to advance aims of transparency, confidence-building, and information-sharing. This is often worse when the instrument is not legally-binding and reports are voluntary.

Encouraging an analysis or use for national reports could be helpful in offsetting these challenges and enable a true glimpse into national practice and impact of the instrument. For instance, if implementation of the UN Framework is the basis of the instrument then it would be very useful to see how member states are operationalizing the cyber norms, and clarify the value-add of stakeholders in that work. Probably it would be useful to base any Cyber PoA reporting provision on existing templates/formats such as the National Survey or annual reports to the UN Secretary-General, noting that these may require updating over time. The experience of updating the report templates of the UNPoA on small arms could be instructive. Member states could also seek to combine a Cyber PoA reporting provision with some of the proposals that have surfaced in the OEWG to improve accountability, such as peer review mechanisms.

Q5. Should the PoA promote the full, equal and meaningful participation and leadership of women in decision-making processes? How?

It would be both a step backward and detrimental to the eventual success and impact of the cyber PoA for it to not consider gender in a meaningful way. Consideration of gender should go beyond participation and representation and be gender-responsive in its design. Here are four suggestions:

- Highlight the significance of preventing and addressing gender-related cyber harms within the problem-framing or objectives portion of the Cyber PoA instrument.
- Mainstream gender throughout the operative parts of the instrument rather than limiting it to just one area.
- Innovate new action to fill policy gaps by suggesting actions such as additional research about the gendered impact of cyber operations, gender audits of standard setting bodies, or include gender-related questions within any reporting practices.
- Promote and call for gender equality in Cyber PoA meetings, subsidiary meetings, and the negotiation process.

For more on PoAs from Pytlak, see: *Programming action: observations from small arms control for cyber peace* (2021) and *Advancing a global cyber programme of action: options and priorities* (2022).

THIRD EYE LEGAL, INC. Website: https://thirdeyelegal.com

Third Eye Legal's Contribution to Cyber Programme of Action (Cyber PoA)

This is a compendium of contributions at various fora made by Third Eye Legal Consultancy in reference to Cyber Programme of Action (Cyber PoA)

1. Should the PoA facilitate and strengthen collaboration between States and when appropriate, with civil society, the private sector, academia and the technical community? How?

The need for "multi-stakeholder" initiatives through the development of principles and commitments under the Cyber PoA can help establish new networks for exchange, collaboration and cooperation that can be instrumental in implementing the programme of action.

2. Should the PoA support capacity-building and confidence-building between States? How?

Stakeholder capacity can be harnessed by making the resources available at the relevant UN bodies accessible in an inclusive and non-discriminatory manner. Coordination among states and stakeholders should be formulated in an actionable manner addressing capacity issues and filling gaps where necessary. Cyber PoA as a complementary initiative to the UN Cyber OEWG will be a key enabler in realising peaceful, secure and stable cyber space.

- Multi-stakeholder roles in a PoA: reflections on participation, structure and modalities

Multi-stakeholder participation can bring in diverse views across various segments in the cyber domain that include cyber crime, artificial intelligence, IOT and so on that include human centric approach and crafting converging ideas especially collating and bringing state's understanding of international law and international human rights law to the fore which can help devise a framework that can bind states to transpose it to national laws. Multi-stakeholder dialogue could form a multi-stakeholder advisory body to the UN with formal representations at the UN level with rotating seats of various stakeholder groups which can help achieve inclusivity leading to distributed (governments, private companies, citizens) global governance. For instance, distributed global governance especially in the use and deployment of Artificial intelligence, particularly safety of autonomous systems, globally, can help shape policy dialogue on AI at a multilateral level, that is human rights based, safe, peaceful and sustainable.

This will go long way in making Cyber PoA - future proof.

3. Should the PoA advance multi-stakeholder discussions on the applicability of international law in cyberspace? How?

Of particular importance to Third Eye Legal Consultancy are the aspects of international law, rules, norms and principles for responsible state behaviour as well as confidence building measures. Third Eye Legal affirms recommendations in the annual reports of the first, second, third and forthcoming APR of the fourth substantive session will help enable states develop their own understanding of how international law applies to the use of ICTs by States and to contribute to building consensus within the international community taking into account the proposals on norms made at the OEWG.

Specific principles of the UN Charter highlighted in the discussions of the OEWG include among others state sovereignty; sovereign equality; the settlement of international disputes by peaceful means in such a manner that international peace and security and justice are not endangered; refraining in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the purposes of the United Nations; respect for human rights and fundamental freedoms; and non-intervention in the internal affairs of other States.

It was recalled that international law is the foundation for stability and predictability in relations between States. In particular, international humanitarian law reduces risks and potential harm to both civilians and civilian objects as well as combatants in the context of an armed conflict. At the same time; states underscored that international humanitarian law neither encourages militarisation nor legitimises resort to conflict in any domain.

Some states expressed the view that due to the quickly evolving nature of the threat environment and the severity of the risk, an internationally agreed legally-binding framework on ICTs is needed. It was also suggested that such a binding framework may lead to more effective global implementation of commitments and a stronger basis for holding threat actors accountable for their actions especially with regards to threats to critical infrastructure and critical information infrastructure. Third Eye Legal Consultancy recommends that states agree to customary international law on "cyber" leading to a binding framework.

In order to inform UN Cyber OEWG, Third Eye Legal seeks potential collaboration with relevant stakeholders to develop comprehensive best practices on the classification and protection of Critical Infrastructure (CI) and Critical Information Infrastructure (CII) along with suggesting measures and initiatives to strengthen data security.

4. Should Cyber PoA assist States in their efforts to implement the framework for responsible State behaviour and tackle emerging threats in the information and communications technology?

In reference to norms, rules and principles, one peculiar aspect of conflict in cyberspace should be public declaration of cyber incidents and attribution in a global repository such as in the suggested Point of Contacts (PoC) directory portal or UNIDIR cyber policy portal. Where attribution is agreed upon, mitigating measures based on the 11 norms agreed as applicable notwithstanding technical, legal and political barriers would help contribute to Confidence Building Measures including acknowledgements from private companies and non-state actors in their contribution of vulnerabilities and the effort to mitigate harms based on transparency and cooperation to pacify the conflict such that peace can be assured even in times of uncertainty, in line with recommendation in para (c) of CBM section of the Annual Progress Report of the UN Cyber OEWG 2022.

States recognise in the PoA as well as in the deliberations of the UN Cyber OEWG that a guiding framework on the application of international law will pave the way to formulating confidence building measures and relevant stakeholders can engage and cooperate under the mandate of UN Cyber OEWG to achieve the objectives of peace and stability in the cyberspace.

Just as malicious actors share lessons, techniques and tactics to cause harm so should states, law enforcement, private sector and civil society must collaborate to defend cyberspace especially the critical information infrastructure and critical infrastructure before the onset of an attack through effective early warning mechanisms of sharing threat intelligence via CERTs and mitigate harm after an attack by way of sharing technical, legal and forensic information through joint collaboration of Critical Incident Response Teams.

UNIDIR's side event shared a project on taxonomy of malicious ICT incidents that measures implementation of norms, rules and principles of responsible state behaviour in their response to cyber incidents in cooperation with stakeholders; can be instrumental in providing an overview of threats against measures taken to mitigate them, thereby strengthening confidence building measures among states. This can also be achieved in close coordination with other bodies under the UN umbrella mandated to assist states in Critical Security Incident Response through CSIR Teams.

5. Should the PoA encourage States to, on a voluntary basis, survey or report on their national efforts to implement rules, norms and principles, including through the report of the Secretary-General as well as the National Survey of Implementation? How?

National Survey of Implementation is the only way to measure willingness of states to implement and measure progress on commitments made under the UN Cyber OEWG, to that end Cyber PoA will be instrumental in encouraging states to use that option rigorously as means of building confidence in the use of ICTs among states. Third Eye Legal Consultancy seeks to assist states in ensuring that international law principles and any deliberations of a binding framework emanating from proposals at UN Cyber OEWG and GGE are transposed to national laws, strategies and policies. Furthermore, accountability of national implementation of international law principles can be informed by stakeholders especially the private sector of which Third Eye Legal is a part of, in line with the 2030 Agenda for Sustainable Development. Assistance to states shall include advice and recommendations as well as in making informed choices in the judicious use of of voluntary implementation surveys available at the UN Disarmament Cyber Policy Portal.

6. Should the PoA promote the full, equal and meaningful participation and leadership of women in decision-making processes? How?

The challenge to multi-stakeholder consultation would be to reconcile diversity and differences especially participation of women and of marginalised communities in all fora to achieve shared values that can help achieve the trigger word “consensus” in international cooperation from bottom up to ensure equal and equitable representation in addition to achieving global inclusivity. Inadequate knowledge of UN processes would deter stakeholder’s ability to map the relevance and implementation of their proposals in the final negotiations, therefore, stakeholders must be informed of the processes that ensure their effective participation at higher fora and therefore the implementation and enforcement of their proposed recommendations.

UNIDIR

@unidir

/unidir

/un_disarmresearch

/unidirgeneva

/unidir

Palais de Nations
1211 Geneva, Switzerland

WWW.UNIDIR.ORG