Workshop on Advancing the Programme of Action
19-20 May 2022, Geneva
Event Summary

Day 1

Welcome Remarks from Co-Hosts

Speakers:
H.E. Nathalie Jaarsma, Ambassador at-Large for Security Policy and Cyber, Kingdom of the Netherlands
David Fairchild on behalf of H.E. Leslie Norton, Ambassador of Canada
Stéphane Duguin, CEO CyberPeace Institute

Ambassador Nathalie Jaarsma expressed her appreciation to see many different stakeholders involved in shaping the Cyber PoA, and the pleasure of partnering with the Government of Canada and the CyberPeace Institute for this exercise. Ambassador Jaarsma was also thankful to Egypt and France for their leadership of the Cyber PoA initiative. It was mentioned that everyone has a role to play when it comes to cyber and therefore involvement of all stakeholders is important. The implementation of the norms of responsible state behavior requires expertise, resources, and multistakeholder coordination. This will be a UN process, and as such it requires the engagement of all states. Ambassador Jaarsma also highlighted the need for the Cyber PoA process to be complementary to other ongoing processes, as a means to develop a common understanding. Several questions were posed to be addressed during the workshop, including how to ensure that the Cyber PoA can address national and regional priorities, how the PoA can facilitate concrete

capacity building with the support of non-state actors, and how do we ensure that states and stakeholders have the capacity to participate in the Cyber PoA.

David Fairchild delivered remarks on behalf of Ambassador Leslie Norton. He highlighted that the goal of the workshop is not to talk about the process, but rather, to talk about its content with key questions clarifying what the Cyber PoA is and how the multistakeholder community can make it work. He mentioned the growing pattern of disruptive cyber activity and the need to close the gaps in accountability for this disruption. It is hoped that the Cyber PoA will be established soon as a means to ensure the capacity of states as norm makers and actively engaged in discussion around the security of cyberspace.

Stéphane Duguin highlighted that the Cyber PoA is a unique opportunity to shape responsible behavior in cyberspace by implementation and multistakeholder cooperation. He emphasized the need to find a way to operationalize already agreed-upon norms to protect individuals and the enjoyment of their fundamental rights in cyberspace. Addressing cyber threats is an interconnected process and everyone has a stake in it. In line with this, the Cyber PoA is a chance for comprehensive engagement on these issues. He underlined the richness of experience that the multistakeholder community has to offer. This community is not a monolith⊠different entities vary in their starting points and views, and events like this are an opportunity to find the synergies within this community. He closed by mentioning that there is a need to recognize the value of the multistakeholder community and to act on it; because essentially peace and security is a collective goal that requires collective action.

Workshop overview and objectives

Speaker: Christian Ranger, Deputy Coordinator, Cyber Foreign Policy, Global Affairs Canada

Christian Ranger clarified that the purpose of this event is to go over the process and history of the PoA and to expand upon this knowledge to understand what it is trying to accomplish and how. He mentioned that the underlying goal is to craft a value proposal that includes what the role of stakeholders could look like and the value that this community can bring. He highlighted that cyberspace is a shared domain and everyone has a role to play.

Welcome Video from Past/Present Open-Ended Working Group Chair

Speakers: Ambassador Jürg Lauber, Permanent Representative of Switzerland to the United Nations and Other Organizations in Geneva [video remarks]
Ambassador Burhan Gafoor, Chair, Open-Ended Working Group on security of and in the use of information and communications technologies 2021-2025 [video remarks]

Ambassador Jürg Lauber highlighted the urgency to ensure the security of the use of technology and that efforts to move the Cyber PoA forward are necessary to reap the opportunities of the digital age. He mentioned that global acceptance of the norms is important, but now is the time to

operationalise commitments to achieve results. Building trust and confidence is more important than ever and concrete and pragmatic action is needed to secure rights online and offline. Part of this action is the need for capacity building for all states to mitigate threats, and for continued and regular institutional dialogue. Ambassador Lauber also highlighted the importance of building on what already exists in the multistakeholder community and mentioned that a Cyber PoA should not only be an inclusive and transparent process, but it needs to build on the respective strengths of various actors. Ambassador Lauber expressed his belief that the multistakeholder environment of international Geneva can play an important role in making a common vision of peaceful cyberspace a reality.

Ambassador Burhan Gafoor applauded the progress that has been made to move implementation forward, as expressed his hopes that the OEWG would be an action-oriented process from the beginning. He was pleased to see the level of ambition and initiative brought by the states, and highlighted the importance of having conversations to help all delegations to understand what the Cyber PoA is about and how it can be developed going forward. Ambassador Gafoor encouraged everyone to give careful thought on the complementarity of the OEWG and the PoA toward achieving the common goal of promoting responsible behavior in cyberspace. This is particularly important as many smaller states are concerned about duplicating processes, and we need to multiply action, not processes. The OEWG and the PoA need to succeed together with concrete outcomes and tangible results as the most important objectives. Ambassador Gafoor encouraged all to use the international, open-ended and transparent nature of the OEWG as an opportunity to continue to elaborate and build support for the PoA proposal. Ultimately, states need to show how the PoA can lead to results and action-oriented outcomes. The OEWG could serve as a venue to demonstrate the results of the PoA and to test out new ideas.

First Session: Scene Setting: What is a Program of Action (PoA)

Speakers:
Allison Pytlak, Programme Manager, Women's International League for Peace and Freedom (WILPF)
Katherine Prizeman, Political Affairs Officer, UN Office for Disarmament Affairs

Allison Pytlak presented research providing an overview of existing PoAs, the current status of the cyber PoA, and seven priorities for consideration. The report was conducted through desk research and conversations with experts and policymakers. She explained that PoAs are action plans or programmes that serve as roadmaps for implementation to achieve shared objectives. Some PoAs are stand-alone politically binding instruments whereas others are accompanied by political declarations, endorsed at the political level. There are seven common elements of PoAs: context setting and problem framing; goals, purposes, objectives; action-oriented language; roles and responsibilities; mandates and origins; relationship and integration within the UN; duration, universality, and follow-up.

Key questions for further discussions were stressed based on the research report. Regarding the goals, purposes and objectives, it is important to consider what will be the Cyber PoA's added value and common purpose. This is a matter of approach and substance for the international

community. Key questions include what mutual concerns will be addressed through this instrument and the scope and the form of the Cyber PoA, and whether a political declaration will accompany the Cyber PoA. Building on the history of PoAs while looking specifically at the cyber field, the Cyber PoA needs a more forward-looking perspective. Other questions for consideration include how the Cyber PoA will be situated in the larger UN framework, how it can help to close the digital divide, and how the Cyber PoA sees itself in relation to other processes and global goals.

Concerning the content of the instrument, two areas of work with the most support were identified, namely capacity building and norms implementation. Canada's norms proposal was mentioned as an example of how some of the already existing language can be transformed into a PoA format. Another area for cooperation is engagement with stakeholders. There is a strong indication to work with the multistakeholder community based on the experience of prior PoAs. It was also identified that the consultation should be inclusive, including on the substance. Most PoAs specifically refer to non-state actors and the Cyber PoA should implement this approach. Referring to stakeholders throughout the document could be one of the ways to help to mirror in the instrument the real-world collaboration that is happening in the cybersecurity field.

Another key aspect of the research paper was making the PoA gender-sensitive. She emphasized that a gender-blind instrument would be a step backward and included four recommendations to this effect. To begin with, the importance of gender-sensitive cyber harm should be highlighted. For example, this approach could be included in the preamble and mainstreamed throughout the document. It is equally important not to create silos and detach the topic into separate paragraphs. Understanding of the gendered impact of cyber harm and gender-related practices in established actions should be increased. Finally, the instrument could include a call for gender diversity accompanied by practical steps, for example, in the form of programmes for supporting women's participation in the meetings.

Katherine Prizeman provided an overview of the PoA process, including modalities and the implementation process and mechanisms. She mentioned that there is a consensus at the GGE and OEWG processes to support a Cyber PoA, indicating that there is an appetite to progress on several areas. From a UN perspective, PoAs are political instruments and negotiations must be inclusive and transparent. Regarding subsequent implementation, there needs to be a clear understanding of what framework is being established. PoAs are state-led initiatives outside of the UN, but the negotiations themselves are led at the UN premises. The mandates to negotiate the PoA instruments generally come from the UNGA. For example, the UN PoA on Small Arms and Light Weapons culminated in a UN conference. As negotiating a legally-binding document was not possible, an action-oriented and politically-binding document was achieved instead. The text can be then submitted back to the UNGA as a resolution, for the text to be endorsed. If the aim is to receive the maximum endorsement of the instrument, then it is important to think about where the mandate for the proposal will come from.

Ms Prizeman highlighted that the instrument is only as useful as its implementation. There are different options on this front, as support can come from various sources such as national reports,

funding mechanisms, or dedicated websites. The funding of the initiative is another point to consider, as if it will come from outside of the UN, it needs to receive support from the co-sponsoring states. The PoA on Small Arms and Light Weapons was offered as an example of how the implementation could work. The process has a review conference every six years, it is included in the UN budget, and it falls under the UNGA mandate. Follow up is part of the meetings, including as outcome documents, substantive reports from each meeting, and the scope for new commitments. The national, regional, subregional, and global implementation of the PoA should also be considered. States can also decide on the substance for new meetings, set funding mechanisms, trust funds, and scholarship mechanisms. Outcomes are adopted by consensus and the reporting is done annually and is available online.

Q&A with the Audience

The audience inquired about how the Cyber PoA could address ongoing cyber conflicts. The response mentioned that this would depend on what is in the instrument and how strong are its provisions. There is hope that the Cyber PoA would introduce accountability and clarity on the applicability of existing norms in cyberspace. It was also highlighted that the normative framework applies in a preventive sense but also to deter existing malicious use of ICTs.

The speakers were also asked to elaborate on the challenges with previous PoAs in terms of their implementation. It was stated that based on the example of the PoA on Small Arms and Light Weapons, one challenge is that the meetings and review conferences become politicized and take the attention away from the impact on the ground. It is important to test and update the instrument, for instance, to reference gender-related actions. National reporting was also a challenge as it is endemic across the UN system and adds to the reporting fatigue. However, there are options to incentivize reporting.

Another participant inquired about the most successful existing PoA regarding their outcomes, which PoAs led to results that would not be possible to reach without the instrument, and what were their attributes. The PoA on People with Disabilities was raised as a successful case, though it was emphasized that it is a different area than security. This PoA is part of a longer process to address the issue, and a convention was passed to supplement the PoA. A key attribute is that the process is time-bound in its nature.

The audience also remarked that it is important to focus on implementation and bringing everyone on board with the process. The speakers were asked to give examples of PoAs that have the capacity building element strongly included, such as for example, trust funds, and how it could work with the inclusion of the multistakeholder community. The UN's experience with trust funds was mentioned in relation to the PoA on Small Arms and Light Weapons. This PoA did not have a trust fund at first, and later it secured one as an initiative of the UN to support the implementation. However, this funding is specifically for NGOs and states are not eligible to apply for it. There is also a trust fund at UNODA which has country teams to focus on country-specific situations. This could be considered outside of the PoA. Regardless, it is important to consider the form, timeframe, and size to move forward.

Another participant asked about the unique feature of the Cyber PoA in its contribution to the cyber field and offered an example of the multistakeholder component. The speakers underlined that this depends on how the Cyber PoA will be established, but the hope is that the PoA would be practical and act as an instrument or platform for meetings. The underlying idea would be to transform the 11 existing norms into practical commitments that the endorsers commit to. Ultimately, they will be political commitments but still practically oriented. Alternatives in the approach to multistakeholder platforms are also important to consider. For example, the Cyber PoA can learn from other open-ended dialogue processes that can mandate actions and are inclusive.

Second Session: Current Status of Cyber Programme of Action (PoA)

Speaker: Ambassador Henri Verdier, Ambassadeur pour les affaires numériques [video remarks]

Ambassador Henri Verdier highlighted the need for an action-oriented approach, outlining that the Cyber PoA should be an inclusive and binding instrument. He emphasized the necessity to address escalating threats from cyberattacks, and the Cyber PoA's role in assisting with norm implementation, identifying gaps and improving capacity building, while acknowledging the role and responsibility of non-state actors in the implementation of norms and capacity development. He outlined that the goal of the Cyber PoA is to be dynamic and to support the capacity of states. The process should include practicalities such as a voluntary reporting structure, dedicated meetings, multistakeholder engagement and engagement with regional fora. In terms of the next steps, it will be important to refine the aspects of the Cyber PoA proposal based on feedback from outreach and consultations and to aim to have an annual progress report.

Ambassador Verdier also provided an overview of the workshop retreat convened by France on 18 May, emphasizing its complementarity with this workshop. The event was attended by 35 States from among 60 co-sponsors. The delegates discussed the substance of the Cyber PoA, with a regard to including capacity building, norms implementation, engagement with stakeholders, and reporting. The participants also received insights from disarmament experts, which were necessary to feed on the further elaboration of the Cyber PoA. Ultimately, this retreat helped to consolidate discussions in New York and Geneva, and to bring a common understanding of the building blocks of the Cyber PoA. There was broad consensus on taking action while the precise time frame will need to be agreed on to allow for the inclusion of as many states as possible.

Q&A with the Audience

The audience stressed the need to be mindful that implementation will require non-state actors. Reflecting on this, the process needs to be simple enough to allow them to take part. A particular consideration should be given to the mindset of certain states and regions for the Cyber PoA to succeed. It is key to answer how to ensure meaningful engagement of all stakeholders without creating contentious issues as part of the ongoing OEWG discussions. The Cyber PoA should

work for everybody and capacity building support for various parts of the world should be given special attention.

Third Session: What are our Priorities for a future Cyber Programme of Action (PoA)

Speakers:
H.E. Nathalie Jaarsma, Ambassador at-Large for Security Policy and Cyber, Kingdom of the Netherlands
G. Isaac Morales Tenorio, Coordinator for Multidimensional Security, Multilateral Affairs, Ministry of Foreign Affairs of Mexico

Ambassador Nathalie Jaarsma focused her intervention on ideas around capacity building and the implementation of the normative framework. She highlighted that states are at different stages of implementation, and it is imperative for them to work together to ensure that no state is left behind. She mentioned several areas that could use further clarification, for example, all countries must understand what international law means in cyberspace and what is needed to deliver on normative commitments such as the due diligence norm. The due diligence norm was further used as an example to show the importance of how things such as national legislation, local expertise, technical compliance frameworks, and vulnerability disclosure frameworks can help to implement the norms.

Ambassador Jaarsma also highlighted the need to protect strategic infrastructure, together with the support of private sector entities and the need to ensure that human rights are respected. Several suggestions were made about how the Cyber PoA could be organized and how it could support the monitoring of the implementation of the normative framework. She expressed support for the national implementation survey proposed by Australia and Mexico as part of UNIDIR's work, as this could be a good baseline for countries to see which gaps need to be filled. However, first, it needs to be understood whether and where states need help to fill out the questionnaire. She mentioned that the Cyber PoA should support implementation mechanisms at the national and regional levels, particularly to share best practices and expertise. This can be done by calling upon existing successful initiatives such as the GFCE to support the Cyber PoA.

Isaac Morales expressed his appreciation for the research paper put forward and highlighted it as a departing point for the current conversations, especially in an effort to learn from the lessons of previous PoAs. He also urged to look beyond PoA experiences to see if best practices could be borrowed from other fields. With this in mind, he highlighted five key priorities for this process. Coherence and complementarity to other processes outside the UN First Committee is a key element for ensuring future efficacy. The PoA should complement the OEWG and present ideas to advance concrete proposals. Inclusivity is another cornerstone, as the PoA is a chance to involve non-state actors from the start. He warned to avoid the conversation about precedence as it does not exist in the cyber field, and this should be used to the Cyber PoA's advantage. He advised not to delay in deciding on this topic and not to raise false expectations. He also reminded that regional representation at the table is important. Comprehensiveness related to implementation, in advancing CBMs and capacity building, should also be prioritized. Flexibility will be essential as the Cyber PoA needs to be able to address emerging and future threats.

Finally, there will have to be a balance of work, discussions, and deliverables, as well as a balance of the capacity building needs with the need to address challenges and threats. The link between prevention and accountability was discussed while the concluding message stressed the importance of having a framework of norms and laws to advance accountability.

Q&A with the Audience

A question from the audience inquired whether there is a role for the UN Security Council in what the Cyber PoA might deliver, keeping in mind current geopolitical conflicts. The answer outlined that the Cyber PoA should be a non-political instrument. The normative framework should allow for implementation by everyone. Overall, the UN Security Council is not a fitting approach for this.

Another question focused on the operationalization of norms that are mostly about restraint and turning them into actions. Reporting was mentioned several times, but this instrument has many limitations, and other ways could be explored. It was outlined that a neutral reporting of cyber incidents is important to create transparency of cyber activities. This is a step-by-step process, and the more that is known and the more collaboration there is, the better. Checks and balances are also important in this respect.

The participants also asked what could be done to convince states who are not among co-sponsors yet that the Cyber PoA would be a good thing, and what could stakeholders do to bring others on board. The speakers emphasized that clarifying the details of what to expect and what not to expect is important to encourage others to join. Another important aspect is to highlight the added value in relation to the OEWG, and the complementarity between the two initiatives. It is also important to consider the agreements coming out of other fora, such as the UN Security Council, and how they contribute to the topic.

The audience inquired about a role in capacity building for academic stakeholders in the Cyber PoA, and whether the UN university would be interested in opening a stream on cyber policy. The speakers confirmed that there is a distinctive role for academia. Some universities offer courses to study what states publish regarding their positions on the applicability of international law in cyberspace, for example, and this analysis can be used by MFAs. It was highlighted that there is a lot of collaboration between universities and scholars on joint research on capacity building and such research could be broadened in the future.

Another participant asked about involving young talents in the cyber field and what they can do to participate. Additionally, ideas around what is foreseen to be implemented in regard to victims of cybercrime and the needed assistance were explored. The answer raised the importance of making information about cyberattacks transparent, as well as the importance of drawing a clearer line between cybersecurity needs and concrete cybercrime prevention. The CyberPeace Institute was offered as an example for providing assistance to victims and working on how to better protect the healthcare sector and humanitarian organizations. It is important to remember that basic human rights are at stake, and they need to be respected. Regarding youth, they are a key group to engage with, and it is the responsibility of all to make the work of diplomats and technical

experts more visible to them as well as to encourage young people to become cyber diplomats. It was also noted that there is a skills gap in ICTs, and it is important to get children interested in this area.

Closing Remarks

Speaker: Klara Jordan, Chief Public Policy Officer, CyberPeace Institute

Klara Jordan summarized that the purpose of the first day was to set a level of understanding so that the group can explore the topic in more detail on the second day. The workshops will discuss the operationalization of the Cyber PoA and how to make the Cyber PoA outcome a success. The need to focus on the implementation of the normative framework was raised during the first-day discussions, as well as the importance that the Cyber PoA would be complementary to other processes. Some core issues raised throughout the day included how the PoA process can address national and regional priorities, how to ensure that stakeholders can support the process, and how to support capacity building across states. The goal of the Cyber PoA was mentioned as having a common understanding of what we must achieve, having an action-oriented framework, building upon previous actions and positive outcomes, and building upon our respective strengths. Highlights from the retreat organized by France included a broad consensus between states to take action and to gather insights from other disarmament processes to move ahead on the Cyber PoA.

Among other priority points, it was emphasized that the Cyber PoA needs to be forward-looking due to the nature of the cyber domain while building on the history of the PoA and other processes. There needs to be further clarity on what capacity building means in terms of implementation for all countries, while capacity building and norms implementation were highlighted as priority areas. There was a strong indication during the first day of the event and at the retreat to have a sustained involvement with the multistakeholder community, and many raised good examples of how the community was involved in past PoAs. Five priorities were outlined by the speakers, counting coherence and complementarity, inclusivity, comprehensiveness, flexibility, and balance. Overall, there were questions and hopes regarding how this instrument can be ambitious and forward-looking.

Day 2

Opening Session: Day 1 recap, Breakout session overview and objectives

Speakers: Allison Pytlak, Programme Manager, Women's International League for Peace and Freedom (WILPF)
Christian Ranger, Deputy Coordinator, Cyber Foreign Policy, Global Affairs Canada

Allison Pytlak summarized that the first day served as setting the background for the PoA process and setting the scene of where the cyber PoA is currently. With this growing momentum, there was an emphasis on substance, including from the OEWG Chairs, who urged for a forward-looking and action-oriented process. The presented research paper offered an overview of the

main points to be considered, procedural information, and the complementarity of the process. The French representatives provided an overview of the co-sponsors' event taking place the day before, and the Netherlands and Mexico outlined priorities for the process going forward. Some key themes emerged through these discussions, comprising the importance of complementarity with the OEWG, the need to keep in mind other relevant frameworks and forums, and the inclusivity of states and the multistakeholder community in the process. It was also highlighted that there is a lot to be learned from other processes but the cyber field has many unique features that the stakeholders need to consider and act on.

Christian Ranger emphasized that the PoA includes the implementation of the 11 norms of responsible state behavior, the applicability of international law, and capacity building and confidence building measures. He highlighted that the OEWG works on this framework, but the Cyber PoA is not in competition with the OEWG because the Cyber PoA acts as a to-do list. The negotiations are ongoing, but it is a standing list of tasks to complete and a forum to come together to understand the challenges and align on solutions. The goal of the second day is to craft a value proposition for the cyber PoA through discussions in small groups. The representatives of the Netherlands and Canada will go back to the co-sponsors with these proposals to help craft the next steps of the PoA.

Session 1: Aims and Objectives of a Cyber Programme of Action (PoA)

Moderator: Klara T. Jordan, Chief Public Policy Officer, CyberPeace Institute

Speakers:
Kathryn Jones, Head of International Cyber Governance, United Kingdom
Sheetal Kumar, Head of Global Engagement and Advocacy, Global Partners Digital
Anne-Marie Buzatu, Vice President and Chief Operating Officer, ICT4Peace Foundation

Klara Jordan stated that there is a distinction between aim and objective that needs to be made. The aim can be to prevent conflict, whereas the objectives include what we try to do with the to-do list for states and how we can achieve its implementation. She also made a call on the government representatives to encourage their national colleagues in civil society to take part in the process. Four guiding questions were presented for the breakout sessions: (I.) What would be the contribution of civil society that is needed by states? (II.) What is it that could not be done without the PoA mechanism? What will be possible with the Cyber PoA which would not be without the instrument? (III.) How can the objectives be met? (IV.) What are some ideas around monitoring the implementation?

Anne-Marie Buzatu emphasized that multistakeholderism is important to define and agree upon the aims and objectives. This is because different actors have different controls over the internet, and all norms necessarily require the contribution of stakeholders with control over these related areas. **Sheetal Kumar** highlighted the importance of defining the high-level aim and the more specific objectives of the PoA. She mentioned that consensus is needed for the role and implementation of stakeholders to build trust and craft policy documents and standards to support capacity building. **Kathryn Jones** underlined the importance of supporting states to support the norms that they have agreed upon, and that relevancy is crucial to help states who are struggling

with capacity. The intention is to help to bridge the international digital divide in an innovative way but based on what states have already found consensus on, as not all agree with the initial approach.

Breakout Session Summaries

Goals and Objectives of a cyber PoA

- Participants highlighted the interconnectedness of the topics of discussion (i.e., goals and objectives of the PoA, capacity building, norms).
- The expectation for the PoA is that it will become an actionable instrument.
- Hope was expressed that the PoA would help the international community with translating general objectives to the country/regional level and that it will help translate these objectives and goals into very concrete actions.
- Comments on the necessity to include developing countries gained a lot of support in the group discussion. The PoA should not be seen as a western initiative.
- Another specific comment that resonated with the group was a focus on youth.
- On the question of situating the PoA in relation to other UN frameworks, the group called for efforts to avoid further complexity and confusion as the PoA is an additional thing added to the already complex mix.
- The question of relation to the UN frameworks can only be clarified once it is decided whether the PoA is a First Committee process or a general instrument. As cybersecurity does not happen in silos, it clearly has relevance to SDGs – but procedural lines need to be decided first.
- There is a need to break the silos in the international multistakeholder community.
- It was raised by several groups that identifying overarching goals and objectives can be difficult as each norm will need specific objectives.
- It was mentioned that it should be easy for states to join the PoA later.
- Questions around commitments were raised, and the need for national-level commitments to implement.
- It was highlighted that the PoA should bring clarity to mandates and focus on the implementation of key mechanisms. The PoA should not become a negotiating body, but rather, should provide the evidence needed for states to go back to discussions of when key gaps have been identified.
- The PoA will ideally achieve a political declaration, but this might not be achievable in the short term. A political commitment from states is helpful to progress on the implementation of the norms and to help different groups to achieve their objectives.

How will the PoA address capacity building? What should it do?

- The PoA should provide a common vision for capacity development.
- Inclusivity was highlighted as important for capacity building initiatives, especially the inclusion of developing countries and the inclusion of youth.

- The group asked for there to be clarity on capacity building and other projects that the PoA could embed.
- The group raised the hope that the PoA will focus on strengthening capacities, rather than having a threshold of capacities in place for a state to join.
- It was emphasized that states should be able to progress on some parts but not all based on capacities, and they should not be ostracized for moving at different speeds. States should not be compared against each other based on their implementation and capacity to progress but should rather reflect where a country comes from and how to support its capacity.
- It was also highlighted that states have varying levels of cyber capacity, despite being more developed in other areas.
- The size of the secretariat and its function were discussed. It was raised that the PoA could follow the format of existing UN bodies such as committees and trust funds. The possibility of secondment of staff was also mentioned as a way to bring in people with expertise from diverse groups.

How will the PoA address norms implementation? How should it work?

- All states have unique needs, but every state needs more guidance on what the norms mean, especially in terms of the structures needed on the ground to implement them in practice.
- The PoA could provide a centralized platform for states and stakeholders alike to find and share information and track progress from all sides.
- The PoA could support States with implementation at the national and (sub)regional level. The group should identify venues for convening in the intersessional period of the OEWG.
- It was also raised that the OEWG discusses cyber in the context of peace and security but implementation at the national level also includes data security, cybercrime, and human rights. The PoA should take this into account when assisting with implementation at national and (sub)regional levels and should encourage States to participate in the OEWG, starting with having a look at regions with low participation.
- Regarding capacity building for the multistakeholder community, there should be a focus on awareness raising for all relevant stakeholders at national and regional levels to assist with access to the processes as the processes can be onerous, for example, because of lack of financial resources, and aim for continuous capacity building for all stakeholders to break the silos between different entities such as academia, civil society, industry, and others.
- There should be progress and monitoring via credible entities like UNIDIR, and support for the Cyber Policy Portal and self-assessment survey. Annual meetings for feedback would also be helpful.
- Reporting should be voluntary for states to participate and is a chance to report on what's going well and flag problems as they are encountered. It is a chance for states to raise their hand when they need help.

- It was also mentioned that the hope is for the PoA to be a safe space to understand how norms are being implemented and to ask for help as needed, for instance, if the state needs to set up a CERT or draft a national cyber strategy.
- In terms of progressing and monitoring, nothing new should be set up, but rather a trusted actor with a good relationship with states should be used e.g., UNIDIR.

Session 2: Operationalizing a Cyber Programme of Action (PoA)

Moderator: Nemanja Malisevic, Director of Digital Diplomacy, Microsoft

Speakers:
Nils Berglund, Outreach & Public Engagement Coordinator, EU Cyber Direct
Marjo Baayen, Director of the Global Forum on Cyber Expertise (GFCE) Secretariat

Nemanja Malisevic stressed the need for political will, resources and capacity, and accountability. He raised several questions including how to ensure that states implement the norms, whether deadlines should be set, how to incentivize the industry to participate, and how to stay relevant.

Nils Berglund mentioned two key considerations—pace and frequency. He raised that it is important to build convergence between countries on cyber diplomacy issues and to grow the multistakeholder community in global and regional debates. It is about trying to make the Cyber PoA realistic on a global scale. This means a critical mass of states is needed to support the initiative. In terms of operationalization, the group needs to consider the pace and frequency of meetings; needs to be careful not to overburden states and needs to establish a flexible and dynamic PoA. He raised concern about process fatigue as reporting tends to decline or not start from the outset. It was concluded that making the Cyber PoA accessible and interesting is of high importance.

Marjo Baayen shared the experience of the GFCE as a multistakeholder platform on cyber expertise. She emphasized key themes that resurface such as capacity building and knowledge and information sharing. The GFCE works along three pillars comprising coordination, knowledge sharing, and clearinghouse function. Coordination means clarifying who is doing what, and where. The GFCE organizes coordination meetings and connects actors. This work is inclusive and multistakeholder by design. As part of knowledge sharing, The GFCE brings together expertise and technical knowledge, offering a space for the community to share information on their projects to encourage transparency. The clearinghouse function means that the GFCE has regional offices around the world and works on national cyber risk assessments. They work with partners on response strategies, cybercrime legislation, and national cyber strategies. She emphasized the need to build trust, and for this initiative to be effective, the network needs to feel confident with each other. It is not about negotiations, but rather about working together on what is needed. If there is trust, then there can be real conversations.

Breakout Session Summaries

Multi-stakeholder involvement in confidence building measures

- UN Points of Contacts database with technical, legal and policy PoCs need to be established. The participants used an example of the OSCE PoC network that includes both MFA contact and national CERT contact for each country. NGO contact information should also be included since stakeholders, including critical infrastructure operators, often serve as first-responders in the case of ICT incidents.
- As a new CBM, the PoA could bring together stakeholders, either within regions or cross-regionally, for joint apolitical cybersecurity exercises to build community, trust, and muscle memory for responding to ICT incidents with cross-border impact. This may be particularly helpful for countries that are not part of existing regional organizations. It was also noted that exercises are neutral and do not drive specific political agenda, which makes participation easier for a greater number of countries.

Multi-stakeholder involvement in capacity building measures

- Different types of capacity building were discussed, including state institution building, legal and policy development, and the practical day-to-day cooperation involving stakeholders and the broader public. The PoA should provide a venue for both types of capacity building to be discussed and an exchange of good practices, models developed, gaps in expertise or resourcing identified. It should involve multiple ministries, stakeholders, and youth as they are all integral to practical implementation.
- Ensuring that an element of work in this area brings together existing efforts—like Cybil and UNIDIR—is important. We need more donors to be engaged in linking their priorities to the needs expressed as part of the work in both of these subjects.
- It was highlighted that work should not be duplicated, as organizations such as the GFCE are already doing a lot. In this line, smaller states should receive support when it comes to reporting, to ensure that they are able to participate.

Norms implementation

- Three fundamental questions that need to be addressed: (I.) What capacities do states need as foundational elements to cooperate on implementing and using the norms day-to-day, how to deal with defense against attacks as a collaborative effort? (II.) What the priorities or interlinkages are between norms in institutional/legal capacity terms, to produce better, faster norms implementation? (III.) What does implementation look like at the practical day-to-day level and who is involved/needed?
- Government and ministries, not just disarmament experts, need to be involved in order to achieve a practically valuable result on the ground. Norms implementation requires multiple ministries but also non-governmental stakeholders.
- An idea was expressed to focus first on a few priority areas and build up from there. For instance, critical infrastructure protection was cited by few participants.

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

- There should be regular, planned meetings for state and non-state actors. The inclusion of other industry actors is also important and the value of their participation should be emphasized.
- Other models could be followed such as the AHC cybercrime discussions and the OSCE implementation meetings. Stakeholders inform the work of states in these fora.
- The relevant working groups or processes should have mandates/objectives that are inviting to the multiple concerned ministries, as well as stakeholders, relevant to the conversation. Broader engagement would be welcomed more than the traditional disarmament and political constituencies currently focused on the OEWG.
- The PoA modalities should facilitate the involvement of stakeholders—ensuring that barriers to participation like travel costs are mitigated using electronic working methods. Face to face meetings are valuable and integral to the process but all should allow for full participation from remote participants.
- Special considerations should be given to bringing youth, and diversity in general, to the tables. It is key to have a clear goal for work on incorporating various stakeholders, so everyone can have a shared vision of what the goals are and what success looks like.
- To increase the participation of stakeholders and government experts from developing countries and promote global ownership, some PoA meetings such as implementation review and working groups could be held outside of Geneva or New York.
- Regional consultations are an important way to ensure inclusive discussions.
- Stakeholders should have access and ability to participate in the PoA meetings, especially at the level of working groups. The ITU model, where stakeholders can participate and contribute to conversations in all meetings, including at the level of study groups, was cited.
- Stakeholders should have an opportunity to submit written input. The PoA could also allow for submission of joint contributions of governments with other stakeholders from civil society and industry. Formal procedures could be established for the PoA to consider each contribution at the level of working groups.
- It was underlined that the multistakeholder community wants a voice in this process, not a vote.
- To ensure that stakeholder participation is accepted across the board, discussions should be kept as technical as possible, tied to real life and targeted in their scope, and separated on sectoral basis and reported back on.
- An idea raised was to have advisory groups or task forces to help policy makers to use this thinking at a higher level. These groups could also include stakeholders with specific knowledge to future-proof the initiative, and they can govern themselves for flexibility.
- More meaningful engagement was highlighted, such as having a conversation between actors about recommendations rather than just written contributions.The multistakeholder community also urged for more preparation time ahead of meetings, including seeing documents ahead of time, so that they can contribute more substantively.
- The instrument should be built to encourage states to consult nationally, and the instrument should be technical to avoid politicization of issues and allow for effective operationalisation.

- Widespread support was expressed for a permanent UN fund. Funding should extend to supporting developing countries, but also to universities and other research organizations in developing countries to support implementation and skilling. UN University, which now has a program on cyber diplomacy, could be linked to the PoA to provide training for PoA participating experts from developing countries.
- Keeping the instrument within the UN would help ensure its universality.

Reporting and transparency

- Reporting should not be a peer review mechanism, but rather should facilitate private, frank discussions.
- In terms of reporting and transparency, a national survey was recommended in the hope that CBMs will be raised at a global level.

Pace and Frequency

- The PoA should be defined with a clear mandate. The issue of state fatigue was also raised, including the concern of overburdening states, bringing sectoral discussions at a more regional level, and bringing perspectives together at an annual conference.

Session 2 Wrap-up and Overall Way Ahead

Speaker: Allison Pytlak, Programme Manager, Women's International League for Peace and Freedom (WILPF)

Allison Pytlak asked the audience to share things they learned and questions they still have. Many thanked the co-organizers for convening the workshop, and applauded the effort by the group to answer the question of how to develop a productive multistakeholder participation model for the PoA. Others encouraged the stakeholder community to reach out to other stakeholders across the world's regions to allow for a replication of this format of events in other places, and especially encouraged the participation of those who are less vocal in the UN processes with the idea to demystify the PoA and show it was a practical and action-oriented tool. Some highlighted that there are many existing initiatives to be aware of and as a group the community needs to strengthen its cooperation. They also mentioned the importance of cross-regional cooperation and the need to make engagement easier across stakeholder groups. The lack of diversity in the room and online was underscored as a challenge, and something that needs to be especially focused on in the future. Another challenge raised was the fact that the process is dominated by the English language—this is a challenge to encourage diversity and inclusion as well.

Allison Pytlak emphasized that a key takeaway is that there will need to be a mandate from the UNGA to propose to Member States, as they are working on a draft resolution for the upcoming UNGA session. She mentioned the need to continue to discuss and clarify the topics that emerged during the event, as many people were not present. These conversations also need to be widened to include more people. In terms of next steps, she urged everyone in the room to think about how to widen the participation and support for the Cyber PoA, and how governmental engagement and stakeholder involvement at the national level can be an important driver to this effect. She

also mentioned that there is space for further research on several outstanding issues, and existing work can be re-purposed so that it is more accessible to a variety of stakeholders.

Closing Remarks

Speakers: Christian Ranger, Deputy Coordinator, Cyber Foreign Policy, Global Affairs Canada
Ingmar Snabilie, Senior Policy Officer, Ministry of Foreign Affairs Netherlands

Christian Ranger thanked the co-organisers and applauded the stakeholder community for answering their call for support, and that the group has taken a step towards clarifying the PoA and its objectives. In terms of next steps, exchange of views between the multistakeholder community will be important as a new version of the working paper and formal agenda are prepared.

Ingmar Snabilie thanked the co-organizers and thanked everyone for sharing their views and reassured the group that they see a role for all stakeholders in this process. She concluded the event with a message that everyone has homework to do—to think about the future of the PoA.