Cyberspace Cooperation Initiative

Contribution from the Cyberspace Cooperation Initiative at the Observer Research Foundation America in the context of the seventh substantive session of the Open-ended Working Group on security of and in the use of information and communications technologies 2021-2025

March 2024

The Cyberspace Cooperation Initiative at Observer Research Foundation America (ORF America) expresses its support for the work of the Open-ended Working Group on security of and in the use of information and communications technologies 2021-2025 (OEWG) and welcomes the 2024 agenda. In following the substantive discussion of this OEWG and engaging with stakeholders from around the world over the last three years in virtual and in-person meetings including in Southeast Asia, Latin America and the Caribbean, Southern Africa, and the Western Balkans, ORF America would like to offer these observations:

The Cyberspace Cooperation Initiative at ORF America commends the chair of the Open-ended Working Group for his leadership and continued efforts to ensure participation and engagement from all interested stakeholders in this process. ORF America’s impetus for this submission on cyber cooperation is informed by our regional dialogues hosted in the Global South and have resulted in takeaways on the importance of implementing advances in these five areas: multistakeholderism, public private partnerships, norms, confidence building measures, and capacity building. ¹

First, ensuring multistakeholder participation and diverse perspectives is a key takeaway articulated by the expert participants in our dialogues. This means making certain that civil society, academia, and private sector entities’ viewpoints, concerns, and recommendations are given adequate footing and consideration along with states in the OEWG process. Continued conversation with all interested stakeholders remains vital and ORF America supports the Chair’s efforts in convening informal dialogues and other engagement opportunities going forward. Ongoing information exchange with diverse stakeholders to develop common understanding is essential to both protecting human rights and privacy, and also forging capacity and best practices development.

Simultaneously, sustaining and growing participation via inclusion is a critical issue. ORF America applauds the efforts that have been made to increase diversity and inclusivity, for example, through the Women in International Security and Cyberspace Fellowship program and applauds the increased

¹ ORF America, with support from the Ministry of Foreign Affairs of the Netherlands completed four virtual and five in-person regional multistakeholder meetings between 2021-2023 - in conjunction with regional governmental and civil society partners – to discuss pressing cyber policy issues, build trust and capacity and amplify voices from the Global South in international discussions on ICTs including in Southeast Asia, Southern Africa, Latin America and the Caribbean, and the Western Balkans (Meeting 1 & Meeting 2). More information can be found at www.orfamerica.org/technology-policy.
number of interventions made by women delegates in recent OEWG sessions. Our dialogues, however, emphasized that more needs to be done in this area, particularly to ensure equitable, sustainable, inclusive, and multistakeholder engagement from all regions, particularly the Global South.

Lastly, ensuring multistakeholder participation in future mechanisms was identified as a key takeaway, especially since all of society is needed to implement the normative framework. States are encouraged to consider how the multistakeholder community can be involved in future regular institutional dialogue, such as the Programme of Action.

Second, ORF America supports greater focus on **enhancing public private partnerships to better protect critical information infrastructure and critical infrastructure** more broadly. Our dialogue findings suggest that facilitating effective public private partnerships is a fundamental requirement for durable cross-sectoral cybersecurity to protect vital societal services such as electoral processes, healthcare delivery, electricity generation and distribution, transportation, and logistics. Participants have emphasized that sustained, targeted funding processes from public entities, reciprocity in information sharing and vulnerability disclosure, transparency in objectives, and advanced planning with multistakeholder consultation contribute to the efficacy, legitimacy, and durability of these partnerships to shape and secure cyberspace.

Third, maintaining momentum in the process of **implementation of norms and rules for responsible state behavior** with respect to ICTs is essential. A major takeaway from our dialogues is that the focus should be on operationalizing the norms and providing concrete guidance and assistance for countries to implement the framework for responsible state behavior. In this respect, ORF America welcomes the draft checklist on norms implementation. Our dialogues also found that intragovernmental coordination and information sharing among agencies and departments on a national level provides challenges. Greater internal coordination and communication among law enforcement, national security, and commercial regulators with cyber diplomats will help governments coordinate their policies, strategies, and aid practical implementation of commitments. This will also lead to a better understanding of the threat landscape and help countries identify gaps and priorities for capacity building, providing guidance to donors as to where assistance is most needed and resulting in more effective and sustainable norms implementation.

Additionally, there was consensus on the need for a permanent mechanism for regular dialogue, such as for example the Programme of Action, in order to ensure further operationalization of the framework. Finally, discussions also showed that sustainable development is inextricably linked to peace and security in the ICT context. It is crucial to acknowledge the links between development and ICT security to help bridge the digital divide, and to pursue future discussions and actions in ways that are mindful of these linkages.

Fourth, heightened geopolitical tensions and an increase of cyberattacks globally have underlined the need for **confidence building measures (CBMs)** and trust. The OEWG’s push toward the global Points of Contact directory, as well as practical implementation steps such as the June 2024 ping test, tabletop exercises, voluntary information sharing, and regular meetings is welcome. Findings from our dialogues also highlighted the importance of building on existing regional initiatives and amplifying and utilizing lessons learned from regional organizations. Greater coordination and cross-region information sharing on effective CBMs including, for example, the work of the ASEAN Regional Forum and ASEAN point of contact network, the Organization of American States’ working group on CBMs and the Organization for Security and Co-operation in Europe’s informal working groups and public resources on CBMs, will aid in trust facilitation and enhance cooperation and cyber stability.
Fifth, **capacity building** is foundational for all the above elements. ORF America welcomes the global roundtable meeting on capacity building in May 2024 and would like to emphasize the importance of information sharing, identifying synergies, building on and leveraging existing initiatives and avoiding duplication of efforts when discussing the capacity building agenda and priorities. Facilitating effective and sustainable capacity building lies at the core of addressing the full spectrum of issues, particularly for the Global South. All our dialogue meetings have provided takeaways that greater capacity, through training, exercises, workshops, and dialogues are essential to provide representatives in the technical, political, and diplomatic fields with the expertise and skills to frame strategies, facilitate engagement, and build on international and regional cybersecurity cooperation. Moreover, capacity building cultivates and facilitates cyber accountability and norms implementation. In addition to supporting capacity enhancement, effective donor coordination to deliver projects with tangible recipient input is paramount to ensure synergistic activities and minimize duplication. ORF America welcomes the role of organizations such as the Global Forum on Cyber Expertise (GFCE) and the activities it performs in bolstering this effort. The nascent UNIDIR portal can also serve an important function to coordinate and achieve cyber capacity building objectives.

Dialogue among experts and practitioners remains the foundation for generating consensus, strengthening norms implementation, and facilitating information sharing and capacity building. ORF America will continue to provide a trusted platform for dialogue among interested stakeholders and remains committed to the goal of supporting a free, open, and secure cyberspace.