United States Response to UNODA's Request for Views of the Landscape of Information and Communications Technologies (ICT) Capacity-Building Programs and Initiatives within and Outside the United Nations at the Global and Regional Levels

Through consensus endorsement of reports from the UN Group of Governmental Experts (GGE) and the Open-Ended Working Group (OEWG), UN Member States have coalesced around a framework for responsible State behavior in their use of ICTs ("the framework"). The success of the framework rests on States' adherence to and implementation of its elements. In its final report, the 2021 OEWG underscored that "increased cooperation alongside more effective assistance and capacity-building in the area of ICT security… can help States apply the framework."[1] The UN and its Member States have recognized the importance of international capacity building efforts in support of the framework, including in the most recent annual progress report of the OEWG in which States "proposed that the principles of capacity-building as adopted in the 2021 OEWG report should be further mainstreamed into capacity-building initiatives."[2]

The United States recognizes that many States still need to build awareness of the framework's elements and its importance. Many also have not yet adopted domestic cybersecurity practices that are foundational to implementing the framework. In several consensus UNGA resolutions, including but not limited to A/RES/58/199 and A/RES/64/211, the General Assembly has affirmed the necessity for states to adopt these domestic best practices, which include establishing a national computer incident response team, developing and implementing national cyber strategies, promoting public-private partnerships, protecting critical infrastructure, and building cyber workforces. International capacity building programs should support States' efforts to strengthen their national cybersecurity in line with these best practices and the framework.

The United States believes that international cybersecurity capacity building efforts should prioritize implementation of the framework and align with its cyber capacity building principles. In consensus OEWG and GGE reports, ongoing OEWG deliberations, and their overwhelming support for successive resolutions on a future POA mechanism, States have recognized both the UNGA First Committee's specific role in capacity building to address the international peace and security dimensions of cybersecurity. Within the UNGA First Committee, the OEWG and the Program of Action called for in General Assembly resolution 77/37 and 2023 First Committee Resolution 78/L.60 have a clear role in guiding States' implementation of the framework and raising broader awareness and understanding of its elements, including with respect to international law, norms, and confidence building mechanisms. The OEWG should consider how best to use capacity building resources to further awareness and adoption of the framework as well as how to gauge the relative maturity of States in implementing the framework domestically and subsequently determine capacity building needs and priorities.

UN Member States have affirmed the importance of involving various stakeholders "such as the private sector, academia, civil society and the technical community" in capacity building.[3] Specialized UN entities with related cyber mandates possess unique technical expertise that can be used in practical implementation of cyber capacity building efforts within those organizations' core competencies. For instance, the International Telecommunication Union (ITU), as the United Nations specialized agency for

[1] A/76/135
[2] A/78/265
[3] A/76/135

information and communication technologies, and UNODC, with its experience working on cybercrime issues, possess unique technical expertise within their core competencies that can be deployed in practical implementation of cyber capacity building efforts. The ITU Secretary General and the Telecommunication Development Bureau (BDT) are both currently undertaking a capacity building mapping exercise, and the United States encourages UNODA to coordinate its efforts, such as sharing the results of this survey, with the ITU so as to avoid unnecessary duplication and encompass key views.

International bodies other than the UN, such as regional organizations like the Organizations of American States, the Organization for Security Cooperation in Europe, the Association of Southeast Asian Nations and the ASEAN Regional Forum have also conducted highly effective cyber capacity building programs. In addition, development organizations such as the World Bank and global initiatives like the Global Forum on Cyber Expertise (GFCE) possess regional expertise and coordination functions in cyber capacity building efforts. The UN should take particular care not to duplicate or displace the work of these organizations, which possess valuable expertise.

The United Nations can play an important role in coordinating with and highlighting this wide range of actors actively engaged in capacity building on relevant cyber issues, as well as in implementing specific capacity building programs as directed by Member States. In compiling views on the landscape of ICT capacity-building programs, the United States encourages the UN to highlight the array of existing multistakeholder efforts and resources such as the Cybil Knowledge Portal for Cyber Capacity Building that identify ongoing cyber capacity building programs that complement and expand upon work being done by UN entities.