UNITED STATES COUNCIL FOR INTERNATIONAL BUSINESS

OEWG Stakeholder Consultation
July 27, 2022

The U.S. Council for International Business (USCIB) appreciates the Chair's decision to consult informally with non-governmental stakeholders to help inform the third substantive OEWG session. USCIB's corporate members include the leading U.S. providers of information and communication technology (ICT) products and services to the global community. We firmly believe that business, civil society, and the technical community provide the expertise required to ensure an open, secure, stable, accessible, and peaceful ICT environment.

Before offering our thoughts about capacity-building initiatives, USCIB would like to reiterate a point we made in earlier interventions because we feel it cannot be emphasized enough. That is, that a *holistic approach* to the consideration of ICT issues – involving dialogue among business, government, civil society, and the technical community -- is necessary and effective in lowering the risk of unintended consequences from policy decisions made by States alone.

One needs business and the technical community to inform policymakers what is commercially, economically, and technically feasible; civil society is needed to ensure that human rights are protected. This inclusive dialogue therefore increases the legitimacy of policies that are adopted because numerous parties have had a stake in their development.

With this in mind, we feel the need to express our disappointment that stakeholder participation in July 2022 phase of the OEWG process was not as fulsome as would be optimum. Many non-governmental stakeholders without ECOSOC accreditation who possess considerable expertise related to cyberspace were blocked from this phase of the OEWG process by a minority of UN member states.

In so doing, this minority limited the ability of organizations with unique insights into cybersecurity challenges to help advance our common goal of ensuring a safe and peaceful online environment for everyone. USCIB sincerely hopes that Member States will develop a sustainable solution that enables all relevant stakeholders to participate in UN discussions about ICT security.

With respect to the first set of guiding questions focused on capacity building, USCIB is pleased to share with you a few examples of the ways in which our members have shared technical information and developed and disseminated comprehensive best practices. These include, for example:

- Supporting the Global Forum on Cyber Expertise[1];
- Working to deliver sound national cybersecurity practices by informing development of the International Telecommunication Union's National Cybersecurity Strategy Guide[2];
- Partnering with the Alliance for Securing Democracy (ASD) and the Government of Canada to produce a Compendium on Countering Election Interference, which contained concrete recommendations and good practices critical to electoral infrastructure.[3] We note that Microsoft, a USCIB member, used the success of the ASD/Canadian effort to partner with the CyberPeace Institute (CPI) and the Government

[1] Global Forum on Cyber Expertise, https://thegfce.org/
[2] ITU, National Strategies, https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cybersecurity-national-strategies.aspx
[3] Multi-Stakeholder Insights: A Compendium On Countering Election Interference – Alliance For Securing Democracy (gmfus.org), April 2021

of the Czech Republic to craft a compendium of cybersecurity best practices to protect the healthcare sector from cyber harm; another critical sector highlighted by the first OEWG;
- Partnering with the United States Telecommunications Training Institute[4] to deliver training that equips officials from emerging economies with the skills needed to deploy wireless technologies, implement national cybersecurity strategies, support internet deployment, launch cloud services and ensure sound emergency communications plans, and importantly, to support the rule of law; and
- Supporting the efforts of the CPI's *CyberPeace Builders* program, which works to increase the resilience of non-profits around the world through a corporate network of volunteers.[5]

This is not an exhaustive list. However, it highlights dramatically, the awareness, interest, and willingness of USCIB members to step up and devote substantial corporate resources and expertise to building cybersecurity-related capacity throughout the world. In addition, we encourage UN members to consider how stakeholders are supporting such capacity building at the regional level, as well, with an eye toward leveraging, rather than duplicating these efforts.

In terms of types of capacity-building initiatives that present good opportunities for effective stakeholder contributions, USCIB encourages you to consider that there really are no limits to the types of projects that stakeholders have proven themselves willing and able to support.

These range from the hands-on provision of technical training to the creation of a compendia on election and healthcare sector cybersecurity, to participation in the multistakeholder *Let's Talk Cyber* Initiative, the latter benefitting from the invaluable support of Australia and Canada.

Going back to our earlier point, USCIB underscores the importance of diverse stakeholder participation in the OEWG discussions to enhance the perspective of UN members. Capacity-building contributions may vary across stakeholder groups, but they ultimately complement each other and lead to more comprehensive solutions to advance shared goals. Importantly, an inclusive approach to stakeholder participation would ensure that capacity building efforts are ongoing, and not simply uncoordinated, ad-hoc initiatives.

To this last point, I would like to highlight the Cyber Development Goals – modeled after the UN's Sustainable Development Goals – as one such stakeholder-proposed initiative that holds promise of enduring value to the UN and its members.

Proposed by the International Chamber of Commerce, of which USCIB serves as the US affiliate, the Cyber Development Goals define the necessary technical, legal, and policy framework and capacities needed by States for implementation of existing cybersecurity acquis and inspire collective action. By serving as a common capacity building instrument, the CDGs would bring clarity to what remains to be done to implement cybersecurity norms in all states and facilitate more targeted capacity building programs to address gaps.

USCIB strongly endorses the CDG concept and urges its active consideration as part of the OEWG process. We further lend our support to the important substantive contributions of the International Chamber of Commerce to these OEWG stakeholder consultations.

[4] www.ustti.org

[5] CyberPeace Institute (CPI), Cyber Builders Program, https://www.cyberpeaceinstitute.org/cyberpeacebuilders