DGAP
Advancing foreign policy. Since 1955.

**Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021-2025**

Informal Inter-Sessional Meetings

Thematic Session: Capacity-building, December 8, 2022

Thank you, Mr. Chair, for giving me the floor, and for allowing stakeholders to provide input to the discussions. I am Valentin Weber, a cybersecurity research Fellow at the German Council on Foreign Relations, which is a foreign policy think tank based in Berlin. Today we have heard a lot about education, funding, and complementarity of efforts, all of which is very important to strengthen our work in the area of capacity-building.

Chair, in your guiding questions you mentioned public-private partnerships, among the several ways of how to increase capacity-building. Think tanks, including the German Council on Foreign Relations, play an important role in providing a meeting ground for diplomats, experts and other interested publics to discuss areas of cybersecurity and state conduct. At the German Council on Foreign Relations, we strongly believe that having regular and dedicated subject-matter meetings largely increases the shared knowledge in a particular area. We therefore appreciate the opportunity to be able to participate in these meetings, as that allows us – as well as other think tanks and institutions – to organize also in the future, dedicated meetings on the subject matter.

At the same time, we believe that it is important to bring the issues of the OEWG, such as responsible vulnerabilities disclosure or supply chain resilience, to the broader public and to increase public literacy on it. We often think of stakeholders as not for profits or industry but the notion of multisakeholderism goes much farther. In our view it is crucial that the broader interested public is involved. And here again, I believe that stakeholders could play a role in bridging this gap.

The German Council on Foreign Relations especially is concerned about the increase of offensive measures in cyberspace, and has been rigorously arguing for defensive rather than offensive measures. But we know that cyberspace is by its nature an offense dominant environment, it is easier to launch an attack than to defend. Due to complex supply chains no country by itself will be able to increase security considerably by itself. Member states need to work together to fix issues such as open-source security, which is often upheld by volunteers. In addition to increasing security in critical infrastructure countries should also try to build cross societal resilience and to build capacity throughout society.

Here is where I see a huge value in the OEWG, in providing the space to discuss how we can increase this capacity to make the world a safer place for everyone. We know that this takes time, but we are happy to support this process, and you, Mr. Chair, in this endeavor.

Dr. Valentin Weber
*Cybersecurity Research Fellow*
*German Council on Foreign Relations (DGAP)*