CZECH REPUBLIC

Permanent Mission of the Czech Republic to the United Nations

---

77th Session of the General Assembly

4th substantive session of the
Open-ended Working Group on security of and in the use of information and telecommunications technologies 2021-2025

Statement by

Mr. Richard Kadlčák

Director of the Cyber Security Department, Ministry of Foreign Affairs of the Czech Republic

New York, 9 March 2023

One Dag Hammarskjöld Plaza
885 Second Avenue, 48th Floor, New York, NY 10017
tel.: +1 (646) 981 4001, fax: +1 (646) 981 4099, www.mzv.cz/un.newyork

Capacity building

Thank you, Mr. Chair.

The Czech Republic traditionally aligns itself with the EU statement delivered earlier and wishes to emphasize a couple of points in its national capacity.

We recognize the important function that cyber capacity building plays in global development, consequently also empowering all States to effectively participate in the technical and policy international discussions on cyber security. In this way cyber capacity building connects all of the discussions we´ve been having here this week. We take cyber capacity building as our priority in order to improve our collective global resilience against malicious cyber activities.

The discussion so far has shown that the OEWG represents an important platform for the exchange of views and ideas on cyber capacity building. From our point of view, the needs of States regarding cyber capacity building may significantly vary as they are often regional and national-specific. Many times sharing lessons learned on what did and what did not work can be as important, if not more, than the sharing of good practice. Together we can learn from our mistakes, even if success stories are sometimes difficult to replicate. Still, a few principles may be distilled as generally valuable:

- First, cyber capacity building must react to and fulfil the needs of its recipients, including in narrowing the digital divide, and the recipients should also manifest ownership over the delivered assistance.
- Second, cyber capacity building is a two-way street: we learn from each other, both the provider and receiver. Moreover, all states benefit from the improvement of a global cyber security.
- Third, stakeholders and public-private partnerships have an irreplaceable role in cyber capacity building. A number of cyber capacity building programs should therefore be carried out within the framework of a close cooperation between states and non-state entities, or civil society.
- Fourth, cyber capacity building must be fundamentally grounded in a clear respect for human rights and fundamental freedoms.

These principles are based on and build upon the principles already consensually adopted in the 2021 final report of the OEWG (OEWG 2019-2021 Final Substantive Report, paragraph 56)

The Czech Republic has long strived to develop capacity building based on the above-mentioned principles. We have held many consultations with other UN Member States in this regard, for example with Ghana, Senegal or Indonesia, which I believe have been mutually beneficial. But we do not want to do these things in isolation. We have always sought a broader cooperation. In the second half of last year, the Czech Republic held

the Presidency of the Council of the EU and precisely, coordination of outreach activities towards third countries was one of our top priorities in the field of cyber security.

However, the UN provides us with opportunities to coordinate capacity building in an even broader context. We believe that we should make the most of this potential. We strongly support and we are fully engaged in the development and strengthening of capacity building within the OEWG now. As for future development, we would like to especially highlight the idea already mentioned by the EU that the Programme of Action would perfectly fit as the primary future instrument to structure CCB initiatives, by coordinating donor efforts and mapping the needs of recipient countries.

Mr. Chair,

We should therefore integrate cyber capacity building into the already existing UN development programs – but, we could go further too and explore the setting of global targets for cyber development by the end of the decade, similar to how we have done for the SDGs – as was mentioned a couple of times at side-events accompanying our week's session.

The Czech Republic also welcomes the discussion on cyber capacity building in a context of the establishment of the Global POC Directory. In order for the Global POCs Directory to work and be sustainable in the long run, it is essential that all States can develop the capacity to participate in it - and for the POCs to be equipped adequately to fulfil their roles effectively. For example, we consider the online tutorial mentioned in the Chair Element paper to be a good example of such a cyber capacity building.

We also support an idea mentioned by Jordan and Argentina that the UNIDIR Portal could be efficient tool to support of our capacity building activities.

Thank you, Mr. Chair.