CZECH REPUBLIC

Statement by

Mr. Richard Kadlčák

Special Envoy for Cyberspace
Director of Cybersecurity Department

(check against delivery)

at the 2nd substantive session
of the
Open-ended Working Group on developments in the field of information and telecommunications in the context of international security

of the First Committee of the
the General Assembly of the United Nations

New York, 13 February 2020

Capacity-building

Mr. Chair, let me first express our appreciation for your efficient conduct of the OEWG and thank you for an opportunity to voice the Czech Republic's position concerning capacity building this morning.

Many delegations highlighted that the ongoing process of digital transformation is an opportunity for economic and social development, but that it also involves serious risks. We agree and add that cyber-security component of development assistance will be more important than ever going forward.

Cyber-security considerations are a critically important component of digital development cooperation. Furthermore, we should recognize that no government can achieve cyber-security alone - **we are all in the same boat**. Responsibility needs to be shared, among states, but also between states, private sector, academia, and civil society.

It is also obvious that no country has been spared cyberattacks and cybercrime. The Czech Republic firmly believes that we are all in this together. Through cyber-capacity building, we can, in fact, learn from one another. **We therefore see cyber-capacity-building as a two-way street.** Those providing assistance can learn as much from cyber capacity-building as those receiving assistance.

As for ensuring cyber security worldwide, the Czech Republic would like to point out one very important element - application of due diligence to the use of ICTs. As already mentioned by some of my colleagues in the segment on international law, and as recognized by the Czech Republic, States have a legal obligation to act against unlawful and harmful cyber activities emanating from their territory or conducted through cyber infrastructure under their governmental control, provided that they are aware of, or should reasonably be expected to be aware of, such activities. This is not an obligation of result, but rather an obligation of conduct. And here lies the key problem and link to capacity building.

The Czech Republic recognizes that logically, State's capacity to adequately exercise its due diligence obligation is intrinsically linked to that State's cyber resilience capacities. Such factors should be taken into consideration when evaluating the particular measures taken by the acting State.

Mr. Chair, the Czech Republic has its own experience defending from cyberattacks and has accumulated specific legal as well as technical expertise in this regard. We will continue to engage in cyber capacity-building activities and commit to share our practices and lessons learned to bolster cyber resilience globally.

Some of the key types of capacity-building initiatives we engage in involve those that focus on policy, cybercrime, cyber hygiene, incident management/critical infrastructure protection and cybersecurity standards.

We believe that ICT capacity building programs should include cyber-security components and build capacities to prevent and combat cybercrime. At the same time, we recognize that threats in cyberspace affect States differently. Successful capacity-building projects must be demand-driven and must therefore recognize the existence of different capacities, perception and impact of threats between different States.

When designing digital capacity-building tools with real added value, smaller countries like the Czech Republic often lack a detailed and sophisticated understanding of the needs and requirements of potential partner countries in the developing world. In order to design truly meaningful instruments of digital and cyber-security development cooperation, we would like to hear from others - even offline - to identify priority instruments for cyber-capacity building cooperation. Here, we also understand that one-size rarely - if ever - fits all needs. What may be useful in one region or country, can be of little relevance in another context. Regional organisations can play a lead role in formulating context-tailored, demand-driven capacity building programs. However, this does not mean cooperation should stop at the regional level. Maintaining stability of cyberspace is a global concern and requires cross-regional collaboration to design effective multilateral responses and solutions.

A number of delegations suggested that the OEWG could make good progress through the development of concrete recommendations on capacity building. We fully agree and would like to support in particular the following:

A. best-practice guide on capacity-building, which could draw from multi-stakeholder expertise available around the world.

B. UN-administered platform/database for cyber-capacity building partnerships to track requirements and capabilities and facilitate matching as appropriate.

One of our challenges in building cyber-capacities and resilience is correctly matching our capacities and experiences with requirements, needs and priorities of prospective partners in developing countries. Insofar, communication of capacities and requirements in the field of cyber capacity-building remained fragmented across a wide-range of multilateral and bilateral channels. Ideally, a centralized UN database or platform bringing together requests for assistance, on the one hand, and existing cyber capacity-building tools, could be considered. This would be in line with suggestions made by many of our colleagues. Given the UN's core purpose of being the harmonizing centre for international cooperation, this organisation would be the ideal focal point to facilitate cyber-capacity building partnerships.

Thank you Mr. Chair.