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, 7 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

Rules, Norms and Principles

Thank you, Mr. Chair,

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

The Czech Republic considers rules, norms, and principles of Responsible State Behaviour in cyberspace as a means to achieve greater stability and predictability of cyberspace. As recognized in the UN GGE reports in 2010, 2013, 2015 and 2021 and also in the consensual report of the previous OEWG, they reduce risks to international peace, security, and stability.

Our top priority is the implementation of the already established 11 norms of responsible state behaviour unanimously endorsed by the UN General Assembly. In this context I would like to support interventions of Sri Lanka, Canada, Germany, Switzerland and other countries that there is no need to develop new legally binding instrument and we should rather focus on discussion of how the existing international law applies to cyberspace to target potential gaps in common understanding of its applicability. But we will discuss this issue later in the next bloc.

As for 11 norms of responsible state behaviour, they are closely linked to capacity building, because compliance in practice requires a high level of cybersecurity expertise. At the same time, we are convinced that working with the broadest possible range of stakeholder experts will enhance implementation of the norms.

In the past we have been working intensively – in cooperation with the private and non-governmental sector on the area of protection of health sector.

Today the Czech Republic would like to focus on two areas. We are of the opinion that they deserve an attention of the OEWG.

First of all, we would like to focus on **Supply Chain Security.** Some countries mentioned it already yesterday during discussion on existing and potential threats. They argued that Cyber operations attacking supply chains can cause significant damage and pose a threat the OEWG have to deal with. We fully support this argument.

The issue is important also from the perspective of the implementing of the norm of the 2015 GGE Report, which recommends that States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products.

Our lives are increasingly dependent on ICT products and services, as is our critical infrastructure. We must be able to trust the ICTs we integrate into our daily lives.

Highly impactful and sophisticated supply chain attacks such as SolarWinds are detrimental for attaining this trust, and we think there is a need to address these threats appropriately throughout policies and cooperation at national, regional and most importantly global level, with the involvement of all actors including stakeholders.

The Czech Republic is especially concerned with risks and threats posed by Emerging Disruptive Technologies. It is here that we see particularly great potential for further discussion on the implementation of the framework for Responsible State Behaviour in cyberspace.

It is fully consistent with the last consensually agreed Annual Progress Report, that specifies that States should continue to develop guidance and/or checklists on further implementation and elaboration of the framework. The need to ensure Supply Chain Security is one of the pressing challenges that should inform this process.

„We encourage further discussions on developing this norm with a focus on the responsible behaviour of suppliers and their assessment based on their respect for the rule of law, human rights, and democratic values. This in particular applies to the suppliers of critical infrastructure."

Second area I would like to mention is the **misuse of new technologies for human rights abuses** explicitly. I spoke about this in a rather detailed way yesterday also in the context of current and new threats.

Today, I'd like to draw our attention to norm of the 2015 GGE Report, which stipulates that states, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression.

The Czech Republic considers further discussion on implementation of this norm as extremely important in the context of international peace and stability. We should actively promote universal human rights and fundamental freedoms, the rule of law and democratic principles in the digital space and advance a human-centric approach to digital technologies.

Thank you, Mr. Chair