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, 6 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

Current and Emerging Threats

Mr. Chair,

I would like to thank you for all your effort.

First of all, I would like to very briefly, but at the same time very strongly, support Canada's position on multistakeholders participation – both concerning delays and transparency.

As I have already mentioned a couple of times, we need stakeholders in the room, rather than waiting at the door. Otherwise, we risk losing their invaluable insights and technical support.

The Czech Republic has long considered the chapter of current and emerging threats to be one of the most important.

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

As it has been mentioned many times the development of new technologies improves our lives, provides unprecedented opportunities for economic growth and constitutes the backbone of our society. At the same time it is a source of serious risks and threats.

I would like to focus on the four most relevant risks and threats from the perspective of the Czech Republic:

1) If we have to talk about threats in cyber space in general, I cannot start other than to say that the Czech Republic considers as the greatest threat of our time aggressive behaviour of Russia. We strongly condemn the Russia's unprovoked aggression against Ukraine accompanied by cyber-attacks, which represents a flagrant violation of international law, the UN Charter and a disruption of the overall rules-based multilateral order. There are negative impacts throughout the world.

   In this context I would like to particularly emphasise the EU position and positions of others that it is not possible to separate cyberattacks from other aspects of Russian aggression. We are witnessing the enormous reach and impact of cyber operations in warfare with their spill-over effects. It clearly shows the threats that we need to talk about in the OEWG as well.

2) Recently, we have seen a huge increase in ransomware attacks. These can no longer be considered as individual actions with limited impact. On the contrary, they have a significant impact on states. In 2022, we saw ransomware attacks causing significant damage to the critical infrastructure of states. As was already mentioned in the EU statement, we have also noted the case when the state has even been forced to resort to declaring a state of crisis. This phenomenon must therefore be addressed not only in the context of cybercrime, but also from the perspective of international security and peace.

3) The Czech Republic welcomes the development of new technologies such as artificial intelligence or quantum computers. At the same time, we are aware of

the risks and threats posed by the deployment of these technologies. Here I would like especially to appreciate a very complex and comprehensive description of the actual state by our colleague from El Salvador. Elements of automation, acceleration and scalability bring new dynamics and deepen the opacity of current processes and overall uncertainty. The OEWG should develop a more detailed discussion on responsible state behaviour in developing new technologies.

4) However, the Czech Republic is primarily concerned about the misuse of new technologies for human rights abuses. This includes using technology as weapons and for committing crimes, blocking political content, shutting down the internet, massive data collection on its own citizens, partial or total censorship, surveillance of political opponents and all the citizens, etc. Cybersecurity must not be used as a tool to suppress human rights.

   In this context we are concerned about the growing trend whereby the introduction of apparently technical measures concerning new technologies or the adoption of new standards and norms concerning new technologies is in fact a means of suppressing human rights such as freedom of expression, protection of privacy or the right to non-violent association. This is relevant topic for discussion in the OEWG.

   We advocate a human-based approach and a human-centric approach in cyberspace, i.e. that the individual has the same human rights in the online environment as we consensually grant them in the real (offline) world.

   We are fundamentally opposed to the misuse of technology to disrupt the current multilateral rules-based order.

Mr. Chair,

I would like to appreciate your effort and I would like to offer on behalf of the Czech Republic maximum support and cooperation.

Thank you, Chair.