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, 10 February 2020

Thank you Mr. Chair.

The Czech Republic considers norms, rules and principles of responsible behaviour of states as an essential measure to reduce risks to international peace, security and stability.

The Czech Republic fully endorses the norms, rules and principles of state behaviour in cyberspace as articulated in successive UN GGE reports in 2010, 2013 and 2015. We would like to highlight two of them in particular: firstly, that States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs and, secondly, that States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams.

The Czech Republic has no intention to introduce new norms, but it would like to encourage the OEWG to focus our discussions on how to operationalize the GGE norms we already have. Global norms need to be adapted to national contexts and require both policy and technical solutions to be implemented. However, in today's complex and interconnected environment, no government can bear the responsibility for implementing norms alone. The responsibility needs to be shared between States and other stakeholders. Their inclusive participation will lead to a more robust norms internationalisation and compliance in the long run.

In this context we would like to invite all delegations to further consider the issue of **ICT supply chain security**. This topic is listed both in the resolution establishing this Open-Ended Working Group, and in the 2015 GGE Report. Both documents conclude 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.

The Czech Republic is deeply concerned that embedding harmful hidden functions in ICTs affects secure and reliable ICT use and the ICT supply chain for products and services, erodes trust in commerce and threatens national security. Supply chain security should be a shared responsibility of all stakeholders. Operators of critical information infrastructure often depend on technologies from suppliers from the other end of the world. Major security risks arise from cross-border complexities of what is an increasingly global supply chain. Inevitably, a good risk assessment should also involve the assessment of supply chain security.

The Czech Republic considers the risks to ICT infrastructure to be of both technical and non-technical nature. The security of ICTs is, to a considerable extent, a matter of trust. Trust depends not only on the legal and political framework applicable to technology producers and suppliers, but also on the quality of information-sharing arrangements between suppliers, and protection against threats to data security. Trust can be undermined by shortcomings in the rule of law, but also by malicious cyberspace operations conducted by State organs or their proxies.

In conclusion, from our standpoint the importance of the integrity of ICT supply chains and integrity of ICT products and services cannot be overstated. In particular, concerns are increasing regarding backdoors that could be created in ICT products and services even for seemingly legitimate purposes, such as allowing law enforcement officials access to data. Mitigating those concerns will require a multi-stakeholder approach and specific accountability measures. Those measures should be comprehensive and should focus on whole life-cycle process.

The Czech Republic is of the opinion that OEWG should pay high attention to this issue and should discuss more profoundly supply chain risk mitigation strategies.

Thank you.