CZECH REPUBLIC

Statement by

Ms. Tereza Janáková

Legal Advisor, Ministry of Foreign Affairs

at the 2nd substantive session of the
Open-ended Working Group on security of and in the use of information and telecommunications technologies 2021-2025

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

30 March 2022
Statement on Application of International Law

Thank you, Mr. Chair.

The Czech Republic aligns itself with the EU statement and wishes to highlight the following.

Mr. Chair, Distinguished colleagues,

The tragic events of recent months demonstrate that compliance with international law, together with strong enforcement measures, is of the utmost importance if we are to prevent conflict in cyberspace and avoid potentially devastating humanitarian consequences such conflict could have in the physical world.

In this context, we are deeply concerned by the recent wave of cyber-attacks against Ukraine, including those targeting its critical infrastructure, which, as many colleagues mentioned yesterday, already have significant negative spillover effects on other states. Such irresponsible and indiscriminate behavior threatens not only the stability of the European continent, but may as well produce serious repercussions throughout the world.

We are equally appalled that humanitarian organizations are now being deliberately targeted by advanced persistent threat actors in cyberspace, in blatant violation of Geneva Conventions, as described yesterday in chilling statements of our colleagues from the ICRC and Switzerland. We condemn the cyber-attack on the ICRC in the strongest possible terms and call on all states to take practical steps to ensure humanitarian organizations enjoy the same protections online, as they do offline.

Mr. Chair,

In response to your questions, we reiterate our suggestion from last December to hold thematic discussions on different areas of international law. This would help us to structure our discussions and allow us to deepen our shared understanding of how international law applies to state conduct in cyberspace. This systematic approach would also help us to identify potential gaps, if any.

In the light of current events, the Czech Republic believes it is more than ever necessary to advance our work on the applicability of international humanitarian law in cyberspace, especially in the context of increasing cyber-attacks against humanitarian organizations and critical infrastructure, including hospitals.

The events of the past few months sadly show that the non-militarization discussion train has left the station. Wartime cyber operations are no longer an abstract construction, but a grim reality we all must face and respond to together. Now that the 2021 GGE report affirmed the applicability of IHL to cyberspace, the OEWG should build and elaborate upon this work. A failure to do so, especially now, in the context of Russia’s aggression, risks paving the way to a future of impunity for indiscriminate cyber operations and of blatant disregard for existing IHL principles of humanity, distinction and proportionality.
We strongly believe that time is now for the international community to send a clear signal that violations of IHL through cyber means will not be tolerated. In this context, we commend Lichtenstein and number of other partners for producing a Report of the Council of Advisers’ on the Application of the Rome Statute of the International Criminal Court (ICC) to Cyberwarfare, which could be helpful for our future discussions.

In light of escalating cyber-attacks against Ukraine emanating from the territory of the Russian Federation, the Czech Republic also joins France and other previous speakers in highlighting the need to have more in-depth discussions in the OEWG on the duty of due diligence, which calls on states to take practical steps to ensure their territory is not being used for malicious cyber activities.

Mr. Chair,

By a way of concluding, allow me to reiterate Czech Republic’s commitment to comply with all principles of international law in cyberspace, including the principles of sovereignty, due diligence, international humanitarian law, and international law of human rights.

Given Russia’s failure to comply with the existing international law, including in its conduct in cyberspace, we have serious doubts as to its sincerity or intention to comply with any future instrument it is proposing, whether on cybersecurity or cybercrime.

Thank you.