Comments submitted by the Czech Republic in reaction to the initial “pre-draft” report of the Open-Ended Working Group on developments in the field of information and telecommunications in the context of international security

Further to the letter of the Chair of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security (OEWG) dated March 11, 2020 circulating the initial pre-draft of the OEWG final report, the Czech Republic has the honour to submit the following remarks and suggestions:

General remarks:

- The Czech Republic expresses deep appreciation for the Chair’s professional efforts in leading the OEWG process in a highly efficient, fair, and transparent manner.
- The Czech Republic welcomes and commends the Chair’s pre-draft of the OEWG report, which in our view provides a good basis for furthering discussions on practical and concrete recommendations ahead of the upcoming third substantive session of the OEWG.
- In this context, the Czech Republic would like to share the following proposals for inclusion in the draft OEWG report:

I. The Czech Republic proposes to highlight the need to protect health-care infrastructure from malicious ICT activities:

- As highlighted by the current COVID-19 pandemic, medical facilities and their ICT infrastructure represent an indispensable component of critical civilian ICT infrastructure. The rising number of cyberattacks on medical facilities worldwide reinforce the need for coordinated global action to protect public health care sector from malicious ICT activities.
- In this context, the OEWG should emphasize the growing threat of malicious use of ICTs to attack critical civilian infrastructure, including electricity grids, water and sanitation systems, and ICT infrastructure critical for the delivery of health-care services. This threat could be raised in paragraph 19 of the OEWG pre-draft, or elsewhere in section B dedicated to “Existing and Potential Threats”.
- To underscore the need to protect health-care sector from malicious cyber-attacks, the OEWG could also refer to the International Committee of the Red Cross (ICRC) proposal to further elaborate and operationalize norms enshrined in paragraph 13(f) and 13(g) of the 2015 report of the UN Group of Governmental Experts (GGE). This reference could be inserted in placeholder paragraph 39 of the OEWG pre-draft (section C on “Norms, Rules and Principles”) reserved for additional proposals. In this context, we wish to highlight the following proposal advanced by the ICRC:
  - “States should not conduct or knowingly support cyber activity that would harm medical services or medical facilities, and should take measures to protect medical services from harm”.1

II. The Czech Republic proposes to further elaborate why existing international law applies to ICTs in its entirety

- As emphasized by a number of states in prior OEWG sessions, the rapidly evolving nature of ICT technologies makes potential negotiations of new legally binding ICT instruments impractical. The OEWG draft report could further elaborate on why existing framework of international law is not only fully applicable to ICTs, but also sufficient to address the ever-evolving challenges in the digital domain.

- In particular, the OEWG could highlight the following principles, which should guide the applicability of international law in the context of ICTs:
  
  (i) technology-neutral approach to regulating ICTs, which provides a safeguard against rapidly evolving nature of ICT technologies;
  
  (ii) interpretation and application of existing international instruments to ICTs in compliance with Article 31 (3)b of the Vienna Convention on the Law of Treaties (and the so-called dynamic or evolutive interpretation of international law)
  
  (iii) interpretation and application of existing international instruments to ICTs “within the framework of the entire legal system prevailing at the time of such interpretation” (see the 1970 ICJ Advisory Opinion on the Legal Consequences for States of the Continued Presence of South Africa in Namibia);

III. The Czech Republic proposes to enumerate the applicable principles of International Humanitarian Law (IHL) in the context of ICTs

- The Czech Republic attaches particular importance to paragraph 25 of the pre-draft, which underscores the applicability of IHL in the context of ICT use. In this regard, we also welcome paragraph 27 of the pre-draft, which references the need to further study how IHL principles apply to ICT operations.

- One way to further advance this question in the context of ICTs would be to enumerate established IHL principles (i.e. principles of humanity, necessity, proportionality, and distinction) in paragraph 27 or elsewhere in section C of the report. This would also make the pre-draft report more consistent with paragraph 28(d) of the 2015 GGE report, which also enumerates IHL principles.

IV. The Czech Republic proposes to provide further guidance on how to align the need for security of ICTs with existing human rights obligations

- The increasing number of human rights restrictions online, often pursued under the pretext of ensuring greater security of ICTs, is a growing concern. The OEWG should highlight this challenge and propose specific policy guidance on how to align the need for ICT security with respect for existing human rights obligations.

- This could be achieved by adding a reference to the Freedom Online Coalition Statement (FOC) on Human Rights Impact of Cybersecurity Laws, Practices and Policies, which contains specific guidance on implementing norm of responsible state behavior included in paragraph 13(e) of the GGE 2015 report.

- This guidance material could be included in the pre-draft report by inserting a reference to the FOC Statement between paragraphs 35 (reference to GGE norms) and 37 (awareness
raising & norm operationalisation) in section D dedicated to “Norms, Rules, and Principles”.

- To provide practical guidance and further specificity in this regard, the draft report could also highlight the following concrete FOC recommendations:
  
  (i) “the need to comply with existing obligations under international human rights law when considering, developing and applying national cybersecurity policies and legislation”;
  
  (ii) “the need to incorporate perspectives from all relevant and affected stakeholders at the earliest stage of cyber security policy development to ensuring a holistic consideration of the implications of cybersecurity measures for human rights.”

V. The Czech Republic proposes to underscore the importance of due diligence with respect to the use of ICTs

- In order to bolster the ability of states to practice due diligence, the OEWG should identify practical ways to build trust, enhance information sharing, and increase international cooperation in investigating and prosecuting malicious ICT activities.
- Specifically, the OEWG could recall elements contained in paragraph 13(c) and (f) of the UN GGE 2015 consensus report:
  
  (i) “States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs”,
  
  (ii) “States should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public.”
- These ICT-specific norms reflect a general principle of international law obliging States to ensure that territory and objects over which they enjoy sovereignty are not used to harm other States’ rights,2 and should therefore be highlighted in paragraph 23 of the OEWG pre-draft or elsewhere in section C on “International Law”.

- Furthermore, the pre-draft report could also underscore the need to increase international cooperation and assistance in investigating and prosecuting malicious uses of ICTs emphasized in paragraph 13(d) of the UN GGE report. Pending further discussions, practical measures to this effect could be included in placeholder paragraph 39 in section D of the OEWG pre-draft dedicated to “Rules, Norms and Principles of Responsible State Behaviour” or recommended for a follow-up expert discussion.
- Finally, the OEWG report should stress the logical link between a state’s capacity to exercise due diligence and state’s actual cyber resilience capacities. The report could also highlight the importance of practical confidence-building measures and capacity building programs for effective implementation of due diligence globally.

VI. The Czech Republic proposes to include recommendation for a follow-up discussion on specific modalities of a global pairing mechanism for enhancing coherence in capacity-building efforts in the use of ICTs

---

The pairing facilitation mechanism for capacity-building with universal scope, referenced in paragraph 55 of the pre-draft report, has the potential to increase coordination of capacity-building efforts globally. In order to advance discussions on this topic, the Chair could consider adding the following elements in the draft report:

(i) highlight that such mechanism should seek to integrate existing multi-stakeholder efforts and initiatives\(^3\) to achieve coherence and avoid duplication;
(ii) recommendation for convening a follow-up discussion of UN Member States on the purpose, scope, financing and other practical elements of such mechanism.

VII. The Czech Republic notes that the proposals on how to deal with the topic of «developments in the field of information and telecommunication in the context of international security» will require further discussions among UN Member States.

\(^3\) One such initiative is the Global Forum for Cybersecurity Expertise.