31.03.2020

Pre-Draft Report of the OEWG - ICT

Comments by Austria

Austria welcomes the "Pre-Draft" Report of the Open Ended Working Group on developments in the field of Information and Telecommunication in the context of international security (OEWG ICT) presented by the OEWG Chair and would like to offer the following comments:

1. The issue of a new legal instrument governing cyber operations

Paras 27 and 28 of the Pre-Draft read as follows:

> *"27. At the same time, during the discussion, it was also noted that there may be a need to adapt existing international law or develop a new instrument to address the unique characteristics of ICTs. In particular, it was highlighted that certain questions on how international law applies in the use of ICTs have yet to be fully clarified. Such questions include, inter alia, what kind of ICT-related activity might be interpreted by other States as a threat or use of force (Art. 2(4) of the Charter) or might give a State cause to invoke its inherent right to self-defence (Art. 51 of the Charter). They also include questions relevant to how the principles of international humanitarian law, including the protection of civilians and civilian objects, apply to ICT operations in the context of armed conflict. In this regard, it was noted that the issue of the applicability of international humanitarian law to the use of ICTs by States needed to be handled with prudence.*
>
> *28.: In this context, proposals were made for the development of a legally binding instrument on the use of ICTs by States as the quickly evolving nature of the threat environment and the severity of the risk necessitates a stronger, internationally agreed framework. It was noted that such a binding framework may lead to more effective global implementation of commitments and a stronger basis for holding actors accountable for their actions."*

Comments by Austria:

- While para. 27 reflects the spectrum of opinions on the question of whether or not there is need for a new legal instrument "*addressing the unique characteristics of ICTs*", language in para. 28 ("*necessitates a stronger, internationally agreed framework*") seems to refer to an emerging consensus on this issue. It has to be noted that many States highlighted that precisely the "quickly evolving nature of the threat environment" and technical tools meant that a truly universal cyber security framework could only be grounded in existing international law, including the UN Charter in its entirety, international humanitarian law and international human rights law, complemented by norms, rules and principles of responsible State behaviour, as included in UNGGE reports and endorsed by the General Assembly.

- Austria notes that while it is true that existing regimes of international law do not include explicit references to ICTs etc., it needs to be underlined that this does not mean that these rules do not apply in cyber space. Indeed, quite the contrary is the case: As stated by the GGE, **existing international law in its entirety applies to cyber operations**.

- For this reason, **Austria does not see the "need to adapt existing international law" and is not in favour of developing "a new instrument".** As Austria stated on the occasion of the 2nd OEWG substantive session in February, we believe that when talking about "gaps", we are not referring to the set of legally binding rules of international law as such, but rather to the interpretation of these rules in the cyber context and to the issue of *how* to apply these obligations against this background.

- In fact, we believe that stressing the need to adapt existing/develop new legal instruments can be hazardous, as it opens the gate for an *argumentum e contrario* for putting in question the applicability and legally binding character of customary international law, general principles of law and treaty obligations with regard to ICTs. Existing law also provides an answer on how to deal legally with the problem of changing environments. Article 31(3)(b) of the Vienna Convention on the Law of Treaties foresees that when interpreting a treaty, any subsequent practice in the application of that respective treaty which establishes the agreement of the parties regarding its interpretation needs to be taken into account, together with the context.

- Our approach stems from pragmatic reasoning as well. Given the "quickly evolving nature" of "the threat environment" (to quote the Pre-Draft para. 28.), we need to focus on compliance with international law rather than undergoing the procedure of the adoption of new rules, which is time-consuming in multinational fora and involves the risk that factual developments in a particularly fast-paced area may render obsolete the result of cumbersome decision-making processes. **Austria therefore stresses the need to continue discussions on the issues of application and operationalisation of as well as compliance with international law and the need for further guidance,** e.g**.** in the form of **guiding principles**).

2. International Humanitarian Law

- The last sentence of **para. 27** ("*In this regard, it was noted that the issue of the applicability of international humanitarian law to the use of ICTs by States* ***needed to be handled with prudence***.") is unclear and might lead to the false understanding that there was currently a legal vacuum concerning the use of cyber operations besides conventional means of warfare in armed conflicts. Austria strongly proposes to clarify that States are already legally obligated to ensure that lives of innocent civilians are spared –and this is exactly what international humanitarian law obliges all states to do – even with respect to ICT incidents.

- **Austria proposes to include a reference to States' obligations stemming from IHL:** *"IHL obliges States to ensure that lives of innocent civilians are spared, even with respect to ICT incidents"* (as was stated by Austria at the 2nd OEWG substantive session in February 2020).

3. Principle of sovereignty

Paras 23 of the Pre-Draft read as follows:

> *"23. Specific principles of the UN Charter highlighted include sovereign equality; the settlement of international disputes by peaceful means in such a manner that international peace and security and justice are not endangered; refraining in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the purposes of the United Nations; respect for human rights and fundamental freedoms; and non-intervention in the internal affairs of other States."*

- Austria notes that para. 23 of the Pre-Draft includes a general statement on the principle of sovereignty that should be further elaborated. As Austria had highlighted in the 2nd OEWG substantive session, a violation of the principle of State sovereignty constitutes an internationally wrongful act – if attributable to a State – for which a target State may seek reparation under the law of State responsibility. A target State may also react through proportionate countermeasures. It is clear, however, that references to State sovereignty must not be abused to justify human rights violations within a State's borders. In other words, State sovereignty must not serve as a pretext for tightening control over a State's citizens, which undermines their basic human rights such as the right to privacy and the freedom of expression.

- Given the need to increase accountability for malicious cyber activities, Austria would welcome further discussions regarding attribution at the UN level.

4. Human rights

- As Austria stated before, activities in the cyber context (such as e.g. the disconnecting of infrastructure on a State's territory from the internet and/or the blocking of access to cyberspace) may have an impact on the enjoyment of human rights of individuals within a State's borders. Such restrictive activities cannot be justified merely by references to the principle of State sovereignty.

- On the contrary, sovereignty entails rights and obligations for States, in particular with regard to the observance of human rights and fundamental freedoms, including on data protection and privacy, freedom of expression, and freedom of information.

- The Pre-Draft rightly states in para. 10 that "*Developments in ICTs have implications for all three pillars of the United Nations' work: peace and security, human rights and sustainable development"*.

- In this context, **Austria would welcome stronger language on the obligations of States to ensure and respect the human rights enshrined in the UN Covenant on Civil and Political Rights, also reflecting customary international law,** especially those with **particular exposure to cyber activities**, such as **Article 17 ICCPR** (privacy), **Article 19 ICCPR** (right to hold opinions, freedom of expression) and **Article 22 ICCPR** (freedom of association). Furthermore, **Austria would suggest taking up the ICCPR's language governing the (narrow grounds of) justification of interference with Articles 22 and 19 ICCPR ("prescribed by law"; "necessary in a democratic society"; "protection of the rights and freedoms of others").**

- Austria supports the suggestion in para. 61 of the Pre-Draft.

  "61. Noting that many parts of the UN address digital technology issues, including their development, rights and crime dimensions, States recognized the need for a dedicated mechanism under UN auspices focusing on international security issues. It was recalled that there are established forums within the UN system focused on issues relating to ICTs and terrorism, crime, human rights and Internet governance. Greater exchange and exploration of synergies between these bodies, such as through joint meetings of committees of the General Assembly, while respecting the expert nature or specialized mandate of each, was encouraged."

- With regard to the **recommendations in para 68. a)** of the Pre-Draft, in light of the Secretary General's Call for Action, Austria would suggest to also include a recommendation on developing a roadmap for implementing the recommendations of the High-level Panel on Digital Cooperation, embedding human rights considerations in an improved global digital cooperation architecture.

5. Rules, Norms and Principles for Responsible State Behaviour

- Austria welcomes the clear calls for States to be guided in their use of ICTs by the 2015 report of the Group of Governmental Experts (UNGGE), endorsed by the UN General Assembly and to work further on their implementation.

- The protection of critical infrastructure is one of Austria's key concerns. Austria suggests that reference be made in the Report under Section D to the 2015 GGE report, i.e. its Recommendation (f), which notes that *'a State 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'.

- Austria further believes that the discussions at the OEWG on further implementation of the existing UNGGE reports have benefitted greatly from the contributions of other interested stakeholders during the informal sessions. We would therefore welcome if the Chair could find a way to reflect this input in the outcome of the OEWG.

6. Existing and potential threats

- Austria strongly promotes the peaceful use of new technology and strictly opposes the development or use of offensive ICT capabilities that could harm innocent civilian lives.

- Austria hence proposes to include reference to these threats in***, in particular of those deriving from the abuse of new technologies for military gains."***

7. Confidence building measures and capacity building

- Austria supports the concrete proposals contained in the recommendations on confidence building measures (CBMs) and capacity building, such as the consideration of a centralized UN database or platform bringing together requests for assistance, on the one hand, and existing cyber capacity-building tools, on the other as well as a global registry of National Points of Contacts as the first global CBM.

- In this context, Austria considers the continued involvement of regional organisations into the work at UN level very important, in order to foster cross-regional cooperation and exchange of experiences on the development and operationalisation of CBMs and capacity building.

8. Regular institutional dialogue:

- While the purpose, financing and participation of a regular institutional dialogue would have to be discussed further, Austria considers that the following principles need to be observed: consensus and results-oriented basis, expert involvement and openness to stakeholder participation as well as non-duplication of work done in other fora.