The Netherlands – written proposals to OEWG zero draft

February 2021

General

- Overall, we welcome the report positively. It is a comprehensive report covering the discussed elements rather sufficiently.

- We are of the view that, in line with international human rights obligations, the notion of a "free" ICT environment is now missing in paragraph 27. We therefore wish to include the wording "free" in between "open" and "secure". This is in line with what we have previously and consequently highlighted regarding cyber and human rights. Human rights and cybersecurity are complementary, mutually reinforcing and interdependent and consequently, human rights are applicable on- and offline. The same holds for paragraph 7, 13, 37, 86, 96, 103, 110, 117.

- In line with the text on the protection of the public core that was included in the pre-draft, taking into account the convergence on the exact wording, we propose the following. We would like to propose to change the formulation in the last sentence of paragraph 21 on 'integrity, functioning and availability' to the [necessity of protecting] "the technical infrastructure essential to the general availability or integrity of the internet". This holds for para 50 as well. Additionally, we would like to mention the importance of the "protection of the technical infrastructure essential to the general availability or integrity of the internet" under the conclusion/recommendation section of *rules, norms and principles* as well. This may be added as an additional paragraph.
- If the current GGE reaches consensus, a reference in paragraph 7 will be appropriate.

Threats

- We regard positively the mention of the potentially devastating humanitarian consequences of attacks on critical infrastructure (CI) and critical information infrastructure (CII) supporting essential services to the public such as medical facilities, but also attacks undermining trust and confidence in political and electoral processes. (paragraph 21).
- On gender, we would like to see a strengthened text under paragraph 11, recognizing that more gender-related data is needed to drive evidence-based policy making and addressing gender impacts of cyber security policies.

International Law

- We are of the view that existing international law applies in its entirety.

- We welcome the attention that was brought to international humanitarian law in paragraph 29. We also note with appreciation that language endorsed by the ICRC is included.

- We would like to express our concerns about the lack of clarity in paragraph 30 with respect to internationally wrongful acts.

    - As much as we like the reference to internationally wrongful acts, the use of proxies, and the obligation with regards to malicious acts originating from a state's territory, we feel that paragraph 30 has undergone a few changes that are not in accordance with our view, nor with how we feel it would best reflect the discussions among the legal experts.

  - We think it could/should be clarified that the activities of "proxies" are acts of *non-state actors acting on the instructions of, or under the direction and control of a State.*

  - In the second sentence, the notions of due diligence and effective control are combined in a sense that is not in accordance with international law as it stands.

  - In the third and final sentence, it is not clear what "entities" refers to. A State entity is a State organ, which has a different legal meaning than an entity which is under *the effective control* of a state.

  - We share a text proposal for this specific paragraph:
    30. It was also recalled that under customary international law, the responsibilities of States with regard to internationally wrongful acts extend to their use of ICTs. It was recalled that States must not *commit, or* use proxies to commit internationally wrongful acts using ICTs. Proxies are *non-state actors acting on the instructions of, or under the direction and control of a State. States* ~~and~~ should seek to ensure that their territory is not used by non-State actors ~~acting on the instruction or under the control of a State~~ to commit internationally wrongful acts (alternative wording: acts contrary to the rights of other states). ~~The responsibility of States was also noted regarding entities owned by or under the control of the State.~~

- We are happy with the recognition of the progressive development of international law regarding ICTs in the context of international security in paragraph 33. We would like to propose to change the wording of "through opinio juris and State practice" to the terms used in the pre-draft, namely, "through its practical application".

- We would suggest for the wording in par. 34 and 35 to be reflected in the conclusions and recommendations, as we are of the opinion that this would be in line with views expressed during the (informal) sessions. We believe that a recommendation could possibly also include a reference to diverging views on International Law which need further study and in depth discussion in the future. Therefore, in addition to our suggestion to reflect the wording of par. 34 and 35, we would propose to also reflect the language of par. 32 in the conclusions and recommendations, with reference to the notion that, given the importance of continuity, we would like to see a recommendation on the continuance of discussions on how international law applies in cyber space - including on topics we do not necessarily agree on yet.

- We welcome the inclusion of noting that greater focus could be placed on the settlement of disputes by peaceful means in paragraph 36, which is also recognized in paragraph 38. We would propose to expand paragraph 38 (new text in red):
  States also reaffirmed the importance of the settlement of disputes by peaceful means. In accordance with their obligations under article 2(3) and Chapter VI of the UN Charter, States that are party to any international dispute involving the use of ICTs, the continuation of which is likely to endanger the maintenance of international peace and security, shall settle their international disputes by peaceful means. They shall, first of all, seek a solution to settle the dispute through such means as described in Article 33 of the Charter: negotiation, enquiry, mediation, conciliation, arbitration, judicial settlement, resort to regional agencies or arrangements, or other peaceful means of their own choice.

<u>Rules, Norms and Principles</u>

- We are happy with the mention of resolution 70/237 calling upon states to be guided in their use of ICTs by the 2015 GGE report under both the discussions section (paragraph 47) as well as the OEWG recommendation section (paragraph 60). We would like the 2010 and 2013 GGE consensus reports to be added as well.

- Moreover, we would like to add to both paragraph 47 and 60 that resolution 73/27 was not adopted by consensus contrary to resolution 70/237.
- As noted above we would like to mention the importance of the "protection of the technical infrastructure essential to the general availability or integrity of the internet" under the conclusion/recommendation section of *rules, norms and principles* as well. This may be added as an additional paragraph.
- Under paragraph 54, we suggest to add "consensus based norms" as an example after "specific guidance".
- Under paragraph 55, we propose to add the protection of electoral processes as has been acknowledged as a threat under paragraph 21.
- Also, we support that the COVID-19 pandemic has accentuated the importance of protecting healthcare infrastructures as mentioned in paragraph 55.Given that attacks on critical infrastructure that undermine trust and confidence in electoral processes has been regarded as a real concern in para 21, we think that this should also be mentioned under para 55 as part of the norms addressing critical infrastructure.
- Finally, we support the OEWG recommendation that States will survey their national efforts to implement norms (paragraph 58). Additionally, we would like to suggest all survey related recommendations to be combined into one recommendation and request a specific reference to the Survey template.

Confidence building measures

- Under paragraph 63, we welcome the notion on the continuing relevance of the CBMs recommended in the consensus GGE reports, as well as the attention to sharing national views on how international law applies to State use of ICTs.
  - Under the same para 63, we welcome the mention of "issuing national declarations of adherence to the framework for responsible State behaviour". We propose to add the following to this sentence: "..detailing member states' positions", and to add the paragraph under the concluding/recommendation section in order to increase transparency and stability
- Under the conclusions/recommendations section, we welcome the significance of regional and sub-regional organizations in developing CBMs under paragraph 69. As regional organizations have an important role in developing CBMs, we suggest to highlight their role in the section.
  - We would therefore like to add the following: "States may strengthen their shared ability to exercise CBMs by joining regional organizations" in order to encourage trust and confidence." As well as adding: "Regional organizations not yet having CBMs should be encouraged to develop those".
  - Moreover, the last sentence of paragraph 69 is not very clear. We suggest to replace "such measures" with "establishing such avenues".
  - Finally, the importance of multistakeholder initiatives may be addressed in the first sentence.
- Moreover, we welcome strongly as CBM the public re-affirmation of States to be guided in their use of ICTs by the 2015 GGE report. (para 74)
- We welcome the engagement in transparency measures and sharing information and lessons through fora_such as the Cyber Policy Portal of the United Nations Institute for Disarmament Research. (OEWG recommendation para 75).
- Finally, we welcome the notion that States nominate a national Point of Contact at technical, policy and diplomatic levels as well as to consider the modalities of establishing a directory of such Points of Contact at the global level. (OEWG recommendation para 76)
  - We would like to suggest the following addition after "modalities": "which may be drawn upon best practices of existing repositories".

Capacity building

- Under the discussions section, we welcome the mention of the important function of capacity building to empower States and others to fully participate in the international discussions as well as the contribution it can have to the 2030 Sustainable Development Agenda. Under paragraph 80 we would additionally like to underline the mutual reinforcement of cybersecurity capacity building and the SDGs. Providing clear and explicit examples of strong linkage with specific SDGs might help underscore this connection, such as SDG9 on resilient infrastructure, SDG10 on reducing inequalities and SDG5 on gender equality.
- Under paragraph 82, the importance of multistakeholder platforms within and outside the UN may be stressed in the second sentence.
- We welcome the attention that was called to the "gender digital divide" under para 84 .
- Under paragraph 86, we welcome very much the principles to guide capacity building in relation to State use of ICTs in the context of international security, divided into process and purpose; partnerships; and people. We would like to underline especially the Global Forum on Expertise (GFCE) principles on sustainability; trust, transparency and accountability; ownerships; and inclusive partnerships and shared responsibility. which are based on the Busan principles for Effective Development Cooperation.
    - In that light, we would like to add "inclusivity and shared responsibility" to the first principle under partnerships, which are core principles under Busan.
- We welcome the mention of capacity-building is able to help foster an understanding of and address the systemic and other risks arising from a lack of ICT security under para 88. We would like to suggest to add the following to this para: "Capacity building may also help states publish their position on the applicability of international law in cyber."
- We would like to add the following to para 90: "Efforts should enhance and support the work of regional organizations and existing global multistakeholder endeavors such as the Global Forum on Cyber Expertise (GFCE)"

Regular Institutional Dialogue

- In regard to para 98 the Netherlands is of the opinion that whatever form the regular institutional dialogue takes there should be room for implementation and for the elaboration of additional commitments.
- We welcome the mention of the proposal on the establishment of a Programme of Action (PoA) under para 99. We would like to suggest to add "multistakeholder consultations" in the last sentence in order to stress the importance of multistakeholder platforms. Moreover, we suggest to replace "with a view to establishing" with "as", given the PoA is intended as a permanen UN forum to consider the use of ICTs by States in the context of international security.
- Moreover, we would like to add 'open' and 'transparent' to paragraph 109.
- Finally, we would like to add text from para 99 to paragraph 112 (additions in red): States establish a programme to continue to take forward existing agreements and commitments in their use of ICTs as set out in relevant General Assembly resolutions, in particular 70/237, as well as the conclusions and recommendations of this OEWG. Such discussions would take place under the First Committee of the United Nations General Assembly as a Programme of Action for advancing responsible State behaviour in cyberspace as a permanent UN forum to consider the use of ICTs by States in the context of international security. The PoA would constitute a political commitment by States to agreed recommendations, norms and principles, and confidence building measures; convene regular meetings focused on implementation; enhance cooperation and capacity-building among States; and hold regular review conferences. Broad participation and multistakeholder consultations are also foreseen under the PoA proposal.