The Kingdom of the Netherlands’ response to the pre-draft report of the OEWG

1. **The Netherlands would like to commend the work that has been done by the Chair and the support team in the past weeks.** The Netherlands hopes that the Chair, the support team and all other Delegates remain in good health. We welcome the opportunity to comment on the pre-draft report of the Open Ended Working Group on developments in the field of information and telecommunications in the context of international security (OEWG). We believe that this first pre-draft is a good basis to start discussions on the report to be adopted by consensus in the last session of the OEWG. There are areas however, where we believe the pre-draft can be improved and we would like to make use of this opportunity to share our suggestions for further improvement, in addition to the comments made by the EU.

General comments

2. **The Netherlands is appalled** by the abuse of the COVID-19 crisis by States to conduct or effectively control non-state actors in launching cyber operations, including the disruption of the healthcare sector, and cyber enabled information operations to interfere with the crisis response in times of urgent crisis. Not only are these operations highly deplorable examples of irresponsible state behaviour; in many instances, they constitute violations of international law.

3. These examples demonstrate once again the urgent need for the international community to address the use of ICT’s in the context of international peace and security, in particular to ensure implementation of and adherence to international law and the framework established by the consecutive GGE reports.

4. **The Netherlands welcomes** in that light the work done thus far by the OEWG as working group of the First Committee. We would like to reiterate that the OEWG should focus on the use of ICT’s in the context of international peace and security, in particular on responsible State behaviour.

5. **The Netherlands welcomed** the initiative of the drafter and co-sponsors of the resolution creating the OEWG to facilitate multistakeholder participation. The introduction of the pre-draft report rightfully reflects this important step. However, the introduction should also reflect that this promise could not be fulfilled due to the opposition of some states to allow for this greater multistakeholder participation. This point has been raised several times during the substantive discussions that took place in September and February and for some member states vetoing the participation of non-ECOSOC accredited actors was contrary to the aim for this working group to be inclusive and transparent.

6. **The Netherlands underlines** the importance for discussions on responsible state behaviour to take place in the context of the United Nations. However, we believe that there are other important fora outside of the UN that discuss and work on cybersecurity, norms, confidence building measures, capacity building. These include platforms for states, regional fora but also multistakeholder platforms. The Netherlands believes that the OEWG should acknowledge the role played by other fora in this field and its specific place in this ecosystem.

7. **The Netherlands welcomes** the references to the gender perspective in the entire document but would like to see it more incorporated throughout the report. The Netherlands believes that the focus on gender can be improved and recommends seeking to address the gender dimension in all aspects of the report.

8. **A final general comment that the Netherlands would like to make** is related to the reference to states in the current pre-draft. As it currently stands there is no qualifier appearing in front of references to states. We believe this can be misleading and could be perceived as if positions and arguments were shared by all member states. We therefore suggest to add qualifiers such as “for some member states”, “certain member states”; “several states”, etc. in order to better reflect the discussions that took place.

Threats

9. In the COVID-19 crisis, the devastating potential of malicious cyber operations is demonstrated. The fact that some State and non-state actors abuse the crisis to launch cyber operations, including against the health sector, or conduct cyber-enabled information operations to interfere with the crisis response should be an urgent concern for the international community.

10. **The Netherlands would like to once again underline** the fact that those threats against international peace and security through the use of ICTs emanate from States participating in the OEWG. Existing international

law, complemented with the norms and recommendations in the reports from the UN GGE, provides States with a framework for responsible behaviour in cyberspace. It is however up to States to adhere to this framework, fulfil the obligations of this framework, and demonstrate restraint when required.

11. In this light, **the Netherlands supports** a technology-neutral, effects-based approach and a focus on State behaviour, including the use of proxies, for the report of the OEWG. The report of the OEWG should refrain from the use of the term 'militarization of cyberspace' because the meaning and scope of this terminology is unclear and not supported by consensus in the OEWG.

12. **The Netherlands supports** the acknowledgement by the pre-draft report of the OEWG of the new and potential severe threat to international peace and security by autonomous cyber operations initiated by States and non-state actors. These independently operating and developing cyber operations are, once launched, outside the control of the initiators and therefore the adherence to the framework of responsible behaviour including international law cannot be ensured.

13. **The Netherlands fully underlines** the severity of threats against critical infrastructure, including the preparatory activities of carrying cyber operations against critical infrastructure. The threat is amplified because these days, critical infrastructure is no longer confined to the borders of States but is increasingly becoming transnational and interdependent.

14. **The Netherlands would like to suggest** for the report of the OEWG to consider the threat that cyber-operations pose against the general availability or integrity of the public core of the Internet. Over the years, cyber operations against the integrity, functioning and availability of the internet has shown to be a real and credible threat.

15. **The Netherlands would like to advice against** deliberating on issues related to the content of ICT', such as "disinformation" in the work of this working group, as these fall outside of the scope of this working group. The Netherlands asserts that any measure to counter "disinformation" must respect fundamental rights, such as the right to privacy, press freedom and freedom of expression. If the Chair decides otherwise, The Netherlands strongly suggests that the report of the OEWG stresses that all countries should ensure that measures to counter "disinformation" are formulated in a way that respects international human rights law and complies with the principles of legality, legitimacy, proportionality and necessity.

16. **The Netherlands does not agree** with the assertion that encryption is a technological trend comparable to machine learning and quantum computing. Furthermore, **The Netherlands does not agree** with the assertion that encryption amplifies vulnerabilities. Indeed the Netherlands recognizes that strong encryption is important for cybersecurity and for respecting the right to privacy and ensures confidential communication for the government and the private sector.

International law

17. **The Netherlands is of the view that existing international law applies in its entirety**. We do not consider there to be a gap in existing international law. There is however a clear gap in the understanding of how international law applies in cyberspace. Discussions and the recommendations of the OEWG should therefore lead to more clarification on the application of different aspects of international law. A topical example of a type of operation that would require further clarification from states is a cyber-operation against the healthcare sector, and cyber enabled information operations to disrupt the lawful response in times of urgent crisis. If states would clearly state their views on how international law applies in cyberspace, this would enable them to assess these specific cases against a coherent legal framework and make a balanced and informed decision as to any potential response.

18. In light of the above, **the Netherlands would like to provide a number of concrete examples of the application of international law**. Malicious cyber operations targeting healthcare systems or facilities could, depending on the specific circumstances, be qualified as a violation of international law. Equally, cyber enabled information operations that intervene with, for example national crisis response mechanisms during a health crisis, could, depending on the circumstances, be qualified as violation of international law. In addition to this, during an armed conflict, cyber operations targeting healthcare facilities are prohibited when they constitute a violation of International Humanitarian Law.

19. **The Netherlands is of the view** that the report should more clearly distinguish between on the one hand the consensus reached in 2013 and 2015 and on the other hand the discussion at the OEWG meetings on topics beyond this consensus. The 2013 and 2015 GGE consensus reports should be emphasized as the baseline for the discussion, as was universally acknowledged during the meetings. For example, the first part of paragraph 27 of the pre-draft report mentions a new instrument, whereas the second part concerns the question of how international law applies. These two separate discussions belong in separate paragraphs.

20. In addition to this, **the Netherlands would like to see** a more balanced and realistic reflection of the discussion on the applicability of existing international law in relation to the call for a new legal instrument. The latter view was not as broadly supported as could seemingly be inferred from the current pre-draft.

21. Furthermore, during the February meeting of the OEWG a large number of states **emphasized** the applicability of the entirety of international humanitarian law (IHL), not limited to some of its leading principles. Although The Netherlands notes with appreciation that IHL is mentioned in the report, the specific notion that many states referred to its full application should be reflected.

22. **The Netherlands considers** that the pre-draft does not afford sufficient attention to human rights. This aspect was extensively mentioned especially in the February meeting, as it followed the release of the Freedom Online Coalition (FOC) statement on cybersecurity and human rights. Even though many delegations expressed support for the FOC statement and the importance of the application of human rights both offline and online, this is not reflected in the pre-draft. The Netherlands, together with several delegations, emphasized that human rights and cybersecurity are complementary, mutually reinforcing and interdependent. When developing and implementing cybersecurity related laws, policies and practices, states should comply with their international human rights obligations. Further, in addition to the point of human rights and freedom, the Netherlands wishes to include reference to the fundamental importance of an open, **free**, secure, stable, accessible and peaceful ICT environment for the enjoyment of human rights.

23. On the recommendations relating to international law, **the Netherlands has two comments**. **Firstly**, we propose for 68(a) to be more in line with 68(b) by including a clear reference to the GGE consensus reports, for example by recalling that in 2015 the General Assembly agreed by consensus that all States should be guided in their use of ICTs by the 2015 report of the Group of Governmental Experts, which includes a section on international law that serves as the basis for discussions in the OEWG. **Secondly**, on the recommendation to have the International Law Commission be requested to undertake a study of national views and practice on how international law applies in the use of ICTs by States in the context of international security, the Netherlands notes that the proposal to refer these issues to the ILC was supported by a minority of States. While acknowledging the importance of the work of the ILC, it is our belief that it is still premature to engage the ILC at this time, and consider it advisable to wait until such time as there is a broader and deeper understanding amongst States as to how international law applies, including aspects on which we might all in the future agree that they remain unclear. Shifting this important issue to the ILC (or any other body) at this point will not resolve the difficult questions about how international law applies. For the moment, the focus would be better placed on deepening a dialogue on international law amongst States (this could include a UN repository with national positions by states) and at the same time encourage the development of national positions, and expand capacity-building activities so that more State can engage meaningfully in these two key activities.

Rules, norms and principles

24. **The Netherlands agrees** with the vast majority of states that see international law, norms, CBMs and capacity building as integral part of the framework for responsible behaviour in cyberspace. Norms reflect the expectations of the international community and set standards for responsible State behaviour. Norms do not replace or alter existing international legal obligations.

25. **The Netherlands fully supports** the line taken by the OEWG to focus on how to operationalize them. To achieve this the Netherlands made concrete suggestions to address the novel threats as mentioned in the threat section.

26. Firstly, **the Netherlands is appalled** by the abuse of the COVID-19 crisis by States to conduct or effectively control the conduct of malicious cyber operations, including against the health sector, which in these times of global crisis provides critical and essential services to our societies. Without a doubt, this is

irresponsible state behaviour and thus transgressing the standards for responsible behaviour in cyberspace.

27. **The Netherlands therefore suggests** that the OEWG report recommends, as an implementation of UN GGE 2015 recommendation 13(f), that States consider the public healthcare sector as included within the scope of this norm.

28. Secondly, to address the development that critical infrastructure is no longer confined to the borders of States alone the report should acknowledge that critical infrastructure is increasingly becoming transnational and interdependent and that adequate protection of these critical infrastructures would benefit the international community.

29. Of this development, the internet itself is the best example, alongside other critical international information infrastructures. To address these threats, **the Netherlands would like to suggest** that the OEWG considers the recommendation that "State and non-state actors should neither conduct nor knowingly allow activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet, and therefore the stability of cyberspace" as guidance for implementation of UN GGE 2015 recommendation 13(f) and therefore bringing this also under the scope of UN GGE 2015 recommendation 13(g).

30. In addition, the threat against the infrastructure and possibility to disrupt the technical infrastructure essential to elections, referenda or plebiscites have shown to be real and credible. To address these threats **the Netherlands would like to suggest** that the OEWG considers the recommendation that "State and non-state actors must not pursue, support or knowingly allow cyber operations intended to disrupt the technical infrastructure essential to elections, referenda or plebiscites," as guidance for implementation of UN GGE 2015 recommendation 13(f) and therefore bringing this also under the scope of UN GGE 2015 recommendation 13(g).

31. **The Netherlands supports** the recommendation that Member States inform the Secretary General of their views of the developments in the field of ICT's, including the implementation of rules norms and principles. To facilitate this, the Netherlands, together with a group states, would like to suggest that the report of the OEWG endorses the joint proposal on a National Survey of Implementation of United Nations General Assembly Resolution 70/237.

32. **The Netherlands supports** the rationale behind the recommendation that the Secretary-General is requested to establish a repository for national practices. However, the Netherland would like to suggest that this recommendation is seen in conjunction with comparable recommendations regarding international law, CBM's and capacity building and consideration is given to the modalities, including the cooperation with UNIDIR and the financing of these requests.

Confidence-Building Measures

33. **The Netherlands sees** confidence building as one of the most important objectives of the OEWG. The CBMs developed by the previous UN GGEs, complimented and brought forward by regional organizations, e.g. the OSCE, are a key element in achieving this.

34. **The Netherlands highlights** that not all States are members of regional organizations and that not all regional organizations have CBMs in place. In our opinion, the implementation of the CBMs contained in the GGE reports should therefore be considered as international priority. Regional organizations not yet having CBMs should be encouraged to develop those and could benefit from using existing regional CBMs as a template, e.g. from the OSCE. It should be noted that because cyberspace is borderless, CBMs should facilitate cross-regional and international confidence building. The report of the OEWG should encourage states and regional organizations to facilitate cross-regional and international confidence building.

35. **The Netherlands is supportive of further exploring** the establishment of a repository of national Point of Contacts and the establishment of a repository of CBMs on bilateral, (sub) regional, multilateral and multistakeholder level. Further clarification on the role of the Secretary-General and UNIDIR, and related costs, concerning the establishment of the repository of CBMs and the establishment of a global registry of national Point of Contacts, is needed in order to fully support the recommendations.

36. **The Netherlands underlines** that international law, complemented by the norms formulated in the UN GGE reports, provides states with a framework for responsible behaviour in cyberspace. It is up to states to closely stick to this framework and to demonstrate the requested restraint. The Netherlands suggests that the OEWG advices States to make declaratory statements to adhere to this framework, to the positive and negative obligations, and demonstrate restraint.

Capacity building

37. **The Netherlands deems** cyber capacity building as the vehicle that strengthens the overall security and resilience in cyberspace. The report should underline the necessity to have a cross-sectoral, holistic and multidisciplinary approach to capacity building in the context of cybersecurity. The Netherlands would like to underline that capacity should be built in multiple areas, as are listed in paragraph 50. However, we believe that capacity building should be done around the "legal" aspect as well and is missing in the current listing.

38. **The Netherlands supports** a stronger involvement of other stakeholders in the field of capacity building, as expertise and capacities lie in the hands of the private sector, the technical community, academia and civil society.

39. During the substantive meetings of the OEWG, a great number of delegations mentioned the interplay between capacity building and the Sustainable Development Goals (SDGs). The Netherlands thinks that the report should clearly affirm that capacity-building efforts in the field of ICTs are a foundational element of the achievement of the SDGs. We suggest that a recommendation in that sense be added.

40. **The Netherlands would like to suggest** that the report becomes more specific and explains how cybersecurity capacity building and SDGS' mutually reinforce each other. In the written contribution of the Netherlands to the Chair, we specifically point out several SDGs of specific relevance to the discussion, including SDG9 on resilient infrastructure, SDG10 on reducing inequalities and SDG5 on gender equality. The Netherlands thinks these could be useful examples on how the SDGs and cybersecurity capacity building are interlinked.

41. **As raised in the Netherlands submission to the Chair**[1], we believe that the OEWG in its recommendation should call for the endorsement of the principles of capacity building that have been recognized by the Global Forum on Cyber Expertise in the Delhi Communiqué namely:
    i. *Ownership*: nations need to take ownership of capacity building priorities focus on sustainable developments;
    ii. *Sustainability*: obtaining sustainable positive impact should be the driving force for cyber capacity building;
    iii. *Inclusive partnerships and shared responsibility*: effective cyber capacity building requires cooperation among nations, through a multi-stakeholder approach;
    iv. *Trust, transparency and accountability*: transparency and accountability play a key role in establishing trust, which is necessary for effective cooperation.

    In our view, this will support a more effective capacity-building co-operation, based on mutual trust between all parties involved.

42. When referring to a global capacity-building agenda, **the Netherlands would like** this proposal to be further clarified. At the moment, it is unclear what is meant by such an agenda and if it is something that already exists.

43. **The Netherlands sees merit** in the UN playing a more distinct convening role in the area of capacity building as long as it enhances and supports the work of regional organizations and existing global multistakeholder endeavors such as the Global Forum on Cyber Expertise (GFCE)The UN could play a meaningful role in creating a venue where those organizations interact in order to ensure complementarity and mutual reinforcement of initiatives. We would thus like to caution against duplication of the abovementioned existing widely supported regional and multistakeholder initiatives and would welcome more clarification in the text to this end. The Netherlands is ready to share additional information on the

[1] https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/02/letter-to-chair-of-oewg-kingdom-of-the-netherlands.pdf

existing capacity-building programs and invites digitally developing countries and other potential partners to further specify their needs and expectations in this area.

44. Furthermore, **the Netherlands would like to see** a recommendation urging all member states to make capacity-building efforts in the use of ICTs a priority in their national and international capacity building efforts and to urge development organizations to incorporate these programs into their development agendas. In order to ensure sustainability of these capacity-building initiatives, attention should be paid to the cybersecurity aspect of these initiatives.

Regular Institutional Dialogue

45. **The Netherlands supports** an open dialogue, that avoids duplication of existing work, within and outside of the UN, includes interested stakeholders, private sector, academia and civil society, be consensus-driven, but is not endorsing any new legally binding instrument, nor the result of a “politically binding instrument”. The Netherlands will consider any proposal with the aim of reinforcing existing international and multi-stakeholder dialogue on its merits, within the scope of the First Committee, thus limited to responsible State behaviour in cyberspace in the context of international peace and security.

46. **The Netherlands does not recognize** the current recommendations as an outcome of the previous discussions. The pre-draft gives the impression that the discussion on a regular institutional dialogue is finalized and reached a conclusion. Which in our opinion is not the case, the Netherlands, together with a large majority of states have expressed their support for the OEWG. We found the discussions to be constructive, useful and fruitful but there are several questions remaining, which have also been raised by other delegations. In particular, questions on the criteria, modalities, and costs, to be applied if such a dialogue were to be created and endorsed. This is currently not clearly stated in the pre-draft. The Netherlands considers the discussion ongoing. Therefore, the Netherlands is of the view that the recommendation to convene a new OEWG and GGE, both, at the 76th session of the UNGA is premature. Further discussion on the topic of regular institutional dialogue is definitely needed.

47. **The Netherlands reiterates** that any proposal must be designed to include all stakeholders. In our opinion, the pre-draft does not reflect enough the knowledge and the input the multi-stakeholders had during the discussions. The Netherlands would like the final report to not only mention the organization of the inter-sessional consultations, but to also reaffirm the importance of multistakeholderism and recognize the expertise and knowledge that lie outside the hands of governments. The Netherlands would recommend the report of the inter-sessional consultations to be annexed to the final report.

48. **The Netherlands recognizes** that the current COVID-19 pandemic brings us in an unprecedented situation. It raises important practical and substantive questions related to the future work of the OEWG and its upcoming meetings. The Netherlands remains open to discussions on adapting the process to these exceptional circumstances to make sure that all member states can fully participate to further substantive discussions and negotiations.