The Netherlands' Position Paper on the UN Open-ended Working Group "on Developments in the Field of Information and Telecommunications in the Context of International Security" and the UN Group of Governmental Experts "on Advancing responsible State behavior in cyberspace in the context of international security".

Introduction

In our modern world, cyberspace has become a pillar of our society, bringing economic growth and social progress to our citizens. It increases access to information, knowledge and development, facilitates freedom of expression and freedom of assembly to name just a few social benefits. It also boosts trade, entrepreneurship and innovation. These benefits are enhanced by its global and open nature that the international community should uphold and promote. This collective interest should guide our discussions in the OEWG and GGE.

To achieve this we are not starting from scratch and we can build on an already existing framework established by consensus reports of previous GGE's, endorsed by UNGA. We can therefore rely on significant rules, norms and principles of responsible behavior in cyberspace, including the applicability of existing international law and confidence building measures.

The OEWG provides UN Member States with an opportunity to look at practical measures to raise awareness and implement existing agreed norms, confidence building measures and capacity building. We have to ensure that the OEWG helps to provide a better common understanding of cyberspace, how to prevent conflict arising from the use of ICTs and to maintain peace and stability in cyberspace, while preserving its free, open and secure nature. Having the OEWG and GGE is an opportunity to explore the issue in a complimentary fashion, both on a State and expert level, to address the urgent needs of the international community.

The Chairs of the OEWG and GGE, and Member States can be assured of the support of the Netherlands to work constructively in both OEWG and GGE with Member States and other stakeholders throughout these negotiations.

Existing and potential threats

The Netherlands acknowledges that the Chair's take-away reflects the extent of discussion during the first OEWG. The Netherlands supports the technology-neutral approach for both the OEWG and GGE and focuses on State behavior and potential effects. Nevertheless, the Netherlands wishes to make the following two suggestions to be included in the threat section in order to further develop the reports by taking account of new challenges and thus add to the awareness raising function of the OEWG and the GGE.

The Netherlands wishes to raise to the attention of the OEWG and GGE the new and potential severe threat to international peace and security by autonomous cyberoperations initiated by States and non-state actors. These independently operating and developing cyberoperations are, once launched, outside the control of the initiators and therefore the adherence to international law and norms cannot be ensured.

In addition to this, the Netherlands wishes to raise to the attention of the OEWG and GGE the acknowledgement that the lack of resilience, the unequal distribution of resilience or the lagging development of resilience, is in itself now developing into a threat to international peace and security. The Dutch Cyber Security Assessment of 2019 recognized that societies are becoming increasingly dependent on digitalization and the lack of resilience could result in cyberoperations have disrupting impact on societies.

Cyberoperations by both State and non-State actors against critical infrastructure have been recognized by the previous UN GGE reports as a real and credible threat to international peace and security. The Netherlands fully underlines these conclusions and acknowledges that over the past years this has developed into one of the major concerns of international peace and security. Critical infrastructure is no longer confined to the borders of States but is increasingly becoming transnational and interdependent e.g. energy grids, the internet and the international financial systems.

The Netherlands wishes to bring to the attention of the OEWG and GGE two specific examples within the wider threat against (transnational) critical infrastructures, which also have been raised by the Global Commission on the Stability of Cyberspace[1], the Paris Call for Trust and Security in Cyberspace[2] and our Government's response to the 2015 report of the Netherlands Scientific Council for Government Policy[3].

The first being the threat that cyberoperations may substantially damage the general availability or integrity of the public core of the Internet. Over the years, the threat against the integrity, functioning and availability of the internet has shown to be a real and credible threat. It is for this reason and the vital and transnational role the internet plays in today's world that the OEWG and GGE should consider this as a threat for international peace and security.

The second being the threat of malign interference by foreign actors aimed at undermining electoral processes through malicious cyber activities. Over the years, the threat against electoral processes and the possibility to disrupt its infrastructure have been shown to be real and credible. It is for this reason and the far-reaching consequences of interference and disruption that the OEWG and GGE should consider this as a threat for international peace and security.

Lastly, the Netherlands wishes to highlight that the discussions in the context of the OEWG and GGE directly concern the participating States. The application of existing international law, complemented with the reports from the UN GGE's provides States with a framework for responsible behavior in cyberspace. It is however up to States to adhere to this framework, fulfil the positive obligations of this framework, and demonstrate restraint when required.

International law

The Netherlands is of the view that existing international law applies. 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 should therefore focus on clarifying the application of different aspects of international law in the cyber domain. We believe that it would be extremely helpful if states communicate their view on the matter. This could for example be done in a guidance note as suggested by the chair.

The Netherlands has taken an initial position on certain aspects of international law in a letter that was sent to Parliament by the Minister of Foreign Affairs in July 2019, which can be found in the Annex to this letter. To date, a small number of other states have published

[1] https://cyberstability.org/report/
[2] https://pariscall.international/en/
[3] https://www.rijksoverheid.nl/documenten/kamerstukken/2016/05/19/kabinetsreactie-op-aiv-advies-het-internet-een-wereldwijde-vrije-ruimtemet-begrensde-staatsmacht-enwrr-advies-de-publieke-kern-van-het-internet-naar-een-buitenlands-internetbeleid

similar statements. If more states would share their position on the matter this would facilitate a process of identifying common understandings or diverging views that could subsequently form the basis for further discussion among states and experts.

With regard to capacity building on this important matter, we believe that increasing understanding of the application of international law to the cyber domain should be a priority. This complex matter requires both a solid understanding of the full breadth of international law and a thorough grasp of the technical realities of cyberspace. We have been working together with a number of states and regional organizations (Singapore, Australia, OAS and others) on capacity building, supporting courses on international law in cyberspace in a number of countries, and we would welcome an increased international effort in this respect. The Netherlands is willing to share thoughts and ideas with respect to a set of guiding principles on how to best conduct capacity building on this issue.

The Netherlands strongly invites other states to make public their positions as regards the application of international law to cyberspace. States can already deposit papers with UNODA. This might be the right forum to receive such statements on national practice.

Norms, rules and principles for responsible State behavior

The Netherlands acknowledges that the Chair's take-away reflect the extent of the substantive discussion during the first OEWG. The Netherlands underlines that a vast majority of states acknowledged that the OEWG and GGE should not 'start from scratch' and that the consecutive reports of the UN GGE are the solid foundation on which current the OEWG and GGE discussions built.

The Netherland agrees with the majority of states that see international law, norms, CBMs and capacity building as integral part of the framework for responsible behavior in cyberspace. The OEWG could further elaborate on the interplay of the respective elements and how they should reinforce each other.

Norms reflect the expectations of the international community and set standards for responsible State behavior. Norms do not replace or alter existing international legal obligations. Implementation and ensuring adherence is the urgent objective of the OEWG and GGE.

The Netherlands believes that the OEWG and GGE could provide concrete guidance on norm implementation. The OEWG and GGE could explain what each of the General Assembly endorsed norms means in practice, and give concrete advice what steps need to be taken to be implemented by States and regional organizations. States could also provide national best-practices, road maps and conduct peer learning.

In order to support this endeavor to foster implementation, the OEWG and GGE should consider the valuable recommendations made during the multistakeholder consultation of December 2019 and the work done in various multistakeholder fora, such as the Global Commission on the Stability of Cyberspace and the Paris Call for Trust and Security in Cyberspace.

The Netherlands wishes to highlight two specific examples of such multistakeholder input to be used as guidance for implementation. The first being the threat that cyberoperations substantially damage the general availability or integrity of the public core of the Internet and therefore the stability of cyberspace. The Netherlands acknowledges that critical infrastructure is no longer confined to the borders of States but is increasingly becoming transnational and interdependent of which the internet itself is the best example.

Over the years, the threat against the integrity, functioning and availability of the internet has shown to be a real and credible threat. It is also for this reason that the Netherlands has designated the availability of internet as a vital infrastructure. The Netherlands would like to suggest therefore that the OEWG and GGE consider 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).

The second is the proposal from GCSC to counter the threats that aim to disrupt the technical infrastructure essential to elections, referenda or plebiscites. Over the years, the threat against the infrastructure and possibility to disrupt the infrastructure have been shown to be a real and credible.

The Netherlands would like to suggest therefore that the OEWG and GGE consider the recommendation that "State and non-state actors must not pursue, support or allow cyberoperations 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).

Confidence-building measures

The Netherlands acknowledges that the Chair's take-away reflects the extent of the rich discussion during the first OEWG. The Netherlands sees confidence building as one of the most important objectives of the OEWG and the GGE. The CBMs developed by the previous UN GGE's, complimented and brought forward by regional organizations, e.g. the OSCE, are a key element in achieving this.

The Netherlands furthermore acknowledges that not all States are members of regional organizations and that not all regional organization have CBMs in place. In addition to this, as cyberspace is borderless, so should CBMs facilitate cross-regional and international confidence building. The Netherlands therefore suggests that the OEWG endorses the so-called second set of CBMs of the OSCE and further internationalizes them.

The Netherlands would like to reiterate that during the previous meetings of the OEWG the importance of implementation of CBMs was acknowledge by a great number of delegations. Developing guidance for implementation of the CBM's could be considered as low-hanging fruit by the OEWG. To achieve this States could be invited to share their implementation, policies and best practices with other States through inter alia peer learning, and including, if applicable, the established points of contact.

The Netherlands acknowledges that the CBMs in UN and regional organizations have been developed roughly alongside the division of transparency measures and cooperation measures. The Netherlands suggest that that the OEWG and GGE could explore how the next step, the so-called stability measures, for which the UN GGE 2015 report laid the groundwork, could be developed and implemented.

The Netherlands would like to highlight in that respect that with application of existing international law, complimented with the reports from the UN GGE's, States are provided with a framework for responsible behavior in cyberspace. It is however up to States to adhere to this framework and demonstrate the requested restraint. The Netherlands suggests that the OEWG advices States to make declaratory statements in national policy documents to adhere to this framework and the positive and negative obligations. The Netherlands, pursuant to UNGA resolution 70/237 has done this in the annexed letter.

Capacity-building
The Netherlands acknowledges that the Chair's take-away reflect the extent of the rich discussion during the first OEWG. The Netherlands welcomes the increased attention to cyber capacity building. The Netherlands deems cyber capacity building as one of the most important instruments to ensure States are able to adhere to the framework of responsible state behavior.

To support capacity building the Netherlands launched The Global Forum on Cyber Expertise (GFCE) in 2015. The GFCE serves as a global, multi-stakeholder multidisciplinary platform that strives to identify, develop and exchange successful policies, best practices and ideas on cyber capacity building and to multiply these on a global level. The GFCE facilitates and coordinates the exchange of knowledge and expertise for the implementation of the cyber capacity building recommendations of the UN GGE reports.

The UN GGE reports provided recommendations for States when providing assistance and underlined the responsibility to devote proper attention and budget for capacity building. The Netherlands underlines that capacity building should be linked to implementing the consecutive UN GGE reports.

The Netherlands believes that providing guidance on this part could be an important deliverable for the OEWG by identifying which steps need to be taken in order to adequately, implement the norms and CBMs. Furthermore, the OEWG could recognize that the need for capacity building is cross-silos and multidisciplinary – including at technical, policy but also legal level. In addition to this, the OEWG could recognize that all stakeholders, where applicable, have a responsibility to contribute to capacity building to implement the consecutive UN GGE reports.

During the last session of the OEWG, a great number of delegations raised interlinkages between the Sustainable Development Goals and cyber capacity building, and the importance of common principles for capacity building. The Netherlands has developed a non-paper and recommendations on these topics, which is attached and available on the website of UNODA. In the non-paper, the Netherlands recommends the OEWG and GGE to:

1. Recognize the relation between cyber capacity building and achieving the UN Sustainable Development Goals by 2030;
2. Integrate the UN Sustainable Development Goals in cyber capacity building initiatives;
3. Endorse the four principles for cyber capacity building from the Delhi Communiqué:
    i. *Ownership*;
    ii. *Sustainability*;
    iii. *Inclusive partnerships and shared responsibility*;
    iv. *Trust, transparency and accountability*.
4. Use the principles outlined in this non-paper to strengthen cyber capacity building and support the achievement of the Sustainable Development Goals.

Regular institutional dialogue
The Netherlands acknowledges that the Chair's take-away reflect the substantive discussion during the first OEWG. The Netherlands supports an open and regular dialogue, including where appropriate with the private sector, academia and civil society, and through relevant existing regional and international (multistakeholder) fora.

The Netherlands will consider any proposal with the aim of reinforcing existing international and multi-stakeholder dialogues on its merits. Any dialogue would, as a body of the First Committee, limit its scope to responsible State behavior in cyberspace in the context of international security. Furthermore, any UN dialogue should coordinate with the work underway in e.g. UNGA's Third Committee, the UN Security Council's Counter-Terrorism

Committee, the Internet Governance Forum and other international, regional and multistakeholders discussions.

Any proposal should avoid duplicating existing work, should work based on consensus, should provide for expert discussions and the ability to deliver concrete results in addressing the needs of the international community, and where appropriate consult with interested stakeholders.

The Netherlands underlines the need to continue discussions, of which the OEWG and the GGE are already part, with a view to implement and strengthen the framework as established by the consecutive GGE reports, but does not endorse the creation of new unnecessary bodies or institutions.

Attachments:
1. The Netherlands' non-paper on Cybersecurity Capacity Building and the Sustainable Development Goals
2. Letter of 5 July 2019 from the Minister of Foreign Affairs to the President of the House of Representatives on the international legal order in cyberspace
3. The appendix of the letter of 5 July 2019: International law in cyberspace
4. The Report of the Global Commission on the Stability of Cyberspace