Open-Ended Working Group on security of and in the use of information and communications
technologies 2021-2025 (OEWG)

Second substantive session 28 March – 1 April 2022

“National intervention under agenda item 5: Discussions on substantive issues”

Statement by

Kingdom of the Netherlands

NEW YORK, 29 March 2022
OEWG March - Existing and Potential Threats
Tuesday 29 March

Thank you Chair,

1. The Netherlands aligns itself with the statement delivered by the European Union, and I will make some additional remarks.

2. As expressed last December, our National Cyber Security Assessment concluded that disruption and sabotage have the most impact on national security because of their potentially disruptive effects on society and wellbeing of our citizens. We are also deeply concerned with the theft of Intellectual Property via cyber means as well as ransomware. On the latter, we support the points made by Canada.

Chair,

4. There is an ongoing threat of cyberattacks against critical infrastructure, including on electoral processes, the health sector and the technical infrastructure essential to the general availability or integrity of the Internet, which is listed in the reports of the previous Open-ended Working Group and Group of Governmental Experts as well. The Netherlands is concerned that despite our 20 years of work on a normative framework that we all agreed on, these threats continue to persist, including in Ukraine.

5. Initiatives that harm the technical infrastructure essential to the general availability or integrity of the Internet, also referred to as the public core of the Internet, include cyber operations that target the core physical and logical infrastructure of the Internet or the organisations that are central to global routing, naming and numbering, such as Regional Internet Registries, ICANN and large internet exchanges. They also include cyber operations that introduce internet standards and protocols that undermine the open and interoperable character of the Internet. To further deepen our technical understanding of the public core, the Netherlands will initiate activities on the public core to deepen our joint technical understanding among the OEWG community.

6. The Netherlands is also concerned about cyberattacks that target humanitarian organisations and their data. The ICRC hack on 20 January of this year showed that personal data is vulnerable, especially in the context of humanitarian crises. Misuse of personal data can have serious and life threatening implications and should therefore be protected from cyberattacks. Our interpretation of the norm on critical infrastructure and in particular the health care sector also includes the protection of humanitarian organisations.
Chair,

7. As a final point, I would like to express concern over the use of cyber instruments that spread uncontrollably and do not make a clear differentiation between the intended cyber operation and the possible effects. NotPetya has shown that cyber instruments that are not designed to be discriminative can spread uncontrollably and can have even more implications than ones that do discriminate.

8. Furthermore, I support the point made by the United Kingdom regarding hacktivism. We would like to make clear that hacktivism is illegal in the Netherlands.

9. Finally, I very much welcome the points on building resilience made by Malaysia.

Thank you