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, 30 March 2022
Dear Chair, distinguished colleagues,

My delegation aligns itself with the statement of the European Union and we would like to make additional remarks in our national capacity.

1. Before addressing specific topics of international law, I would like to stress how far we have come in our understanding of how international law applies to the cyber domain. The GGEs and first OEWG have paved the way for our future discussion. Together with the national position of many states – and hopefully many more to come – I hope that this OEWG will be able to take a step further. Our work is not done, and much remains to be discussed.

Chair,

2. States must meet their international obligations under international law. In accordance with the law on state responsibility, a state is responsible for an internationally wrongful act when it (1) breaches an international obligations that can be (2) (legally) attributed to the state, unless an internationally recognized justification applies.

3. Allow me to emphasize the importance of legal attribution in the context of international law. This is an absolute requirement for the law of state responsibility and should not be controversial. It simply means that we only hold states accountable for the actions they themselves carry out. And in order to establish whether they can be deemed to have carried out a particular action, international law provides a number of criteria, notably the ‘effective control’ requirement.

4. Legal attribution should be distinguished from 1) technical attribution and 2) political attribution. Clearly maintaining this distinction would be very beneficial for our discussions.

Sometimes, Chair,

5. A legal conflict arises between two or more states. Articles 2(3) and in Chapter VI, article 33 of the UN Charter set out a number of means for the peaceful settlement of disputes between states when a dispute and the continuance thereof is likely to endanger the maintenance of international peace and security.

6. The Netherlands suggest to further develop our understanding on the peaceful settlement of disputes, building on the language that was included in the 2021 OEWG and GGE reports. The previous OEWG adopted a paragraph which states that “States also reaffirmed that States shall seek the settlement of disputes by peaceful means such as negotiation, enquiry, mediation, conciliation, arbitration, judicial settlement, and resort to regional agencies or arrangements, or other peaceful means of their own choice.”
7. With this text, we wanted to underline not only the importance of peaceful settlement, but also the opportunities that this can give states and the different ways in which disputes can be settled peacefully. Further elaboration of how this can be done practically in the cyber context would be a very important confidence building measure.

Chair,

8. Recent events have made it clear once again that despite the prohibition on the use of force contained in article 2(4) of the UN Charter, states still engage in acts of aggression.

9. We are appalled by the horrors of the armed conflict in Ukraine and urge all parties to comply with International Humanitarian Law, the purpose of which is to regulate the conduct of hostilities and to protect those who are not, or no longer, taking part in hostilities. The OEWG should emphasize that IHL reduces risks and potential harm to both civilians and civilian objects as well as combatants in the context of an armed conflict. Like others such as Switzerland, Australia and New Zealand have stressed, the principles of IHL should apply to all military operations, both online and in the physical domain.

Chair,

10. We all agree that fundamental freedoms apply online as well as offline, which means they should be respected, protected and promoted in cyberspace. The OEWG should deepen the understanding of the application of human rights in cyberspace.

11. A good start would be to recognise the interdependence and complementarity of human rights and cybersecurity and the need to fully respect international human rights law when designing, developing and implementing cybersecurity laws and policies.

12. This means that cybersecurity measures should be proportionate and necessary and strike a fair balance between security interests and fundamental rights interests. Too often fundamental freedoms and rights are sacrificed or disproportionately restricted in the name of security. This is a very worrisome development that should be called out and condemned. We feel that this is also an important topic to be addressed in the framework of capacity building.

Chair,

13. In the context of our threats discussion we have recognised that the prevalence, complexity and intensity of crossborder malicious cyber operations are on the increase. This also has very real human rights consequences. Operations against hospitals, energy providers, schools and other institutions affect real people.

14. Now, under human rights law, the states on whose territory those persons find themselves, have an obligation to protect them against violations of their fundamental rights. In addition, we feel it is very important and increasingly urgent to call upon states to respect fundamental
rights and freedoms when conducting cyber operations beyond their own jurisdictions. Here also, we see added value in affording attention to this aspect in the context of capacity building efforts.

Finally, chair,

15. We would highlight the necessity to afford special attention to vulnerable groups that are particularly prone to having their rights violated in cyberspace: women, children, LGBTQI, ethnic minorities and persons with disabilities. States have an obligation to protect persons from these groups against violations of their rights and to reasonably accommodate their special needs and interests.

16. Let me end by saying that the Netherlands looks forward to discussing these and other legal aspects of responsible state behaviour in the use of ICTs with our partners here at the OEWG, with the common goal of advancing a true rule of law in cyberspace.