[check against delivery]

Open Ended Working Group in the Field of Information and Telecommunications in the Context of International Security

Rules, Norms and Principles of Responsible State Behaviour

H.E. Nathalie Jaarsma
Ambassador at-Large for Security Policy and Cyber

NEW YORK, 7 March 2023

Chair, distinguished delegates

The Netherlands aligns itself with the statement delivered by the European Union, and I would like to add some additional remarks in a national capacity.

The eleven norms for responsible State behaviour promote predictability and reduce risks of misperceptions between States. At the same time, and this is of vital importance to the Netherlands, the norms also help to protect citizens, particularly those in vulnerable situations.

In exchanging views on rules, norms and principles of responsible State behaviour in cyberspace, it is important to note that we are building on previous work on this topic, endorsed by the General Assembly by consensus.

The Netherlands considers norms to be complementary to international law. Norms do not replace or alter States' obligations or rights under international law, which are binding, but rather provide **additional specific guidance** on what constitutes responsible State behaviour in the use of ICTs.

The 2021 GGE report provided an additional layer of understanding to the eleven voluntary, non-binding norms of responsible State behaviour. This underscored the value of expected responsible state behaviour and provided practical measures for their implementation.

In this context, let me reiterate the importance of capacity-building to enable all States to implement the norms in their national context. We see this as one of the main purposes of the Programme of Action, and believe the PoA could build on existing work being done to operationalize the normative framework including the 11 norms, making use of the UNIDIR Survey of national Implementation and the Singapore-UNODA norms implementation checklist.

[Norms related to critical infrastructure]

Chair,

The Netherlands has consistently emphasized the importance of norms for the protection of critical infrastructure.

That is why the Netherlands has actively contributed to developing an additional layer of understanding to the norms, including the norms related to critical infrastructure.

While it remains up to states to determine which infrastructure is critical, previous OEWG and GGE consensus reports made reference to **the health care sector**, **the technical infrastructure essential to the general availability or integrity of the internet** and **electoral processes** as examples of critical infrastructure**.** From the Netherlands perspective, it was important to highlight these sectors in response to the evolving threat landscape, and the strong dependency on these infrastructures for States' economies, development, political and social functioning and national security.

[Reference to paper reckless cyber ops]

Chair,

In my intervention under threats I highlighted the growing threat posed by the indiscriminate or reckless use of ICTs that causes harmful spill-over effects on the critical infrastructure and essential services.

To address this threat, The Netherlands would like to put forward proposals for additional guidance on the norm (f), which sets out that States should not conduct or knowingly support ICT activities on critical infrastructure.

Firstly, the OEWG should call on States to actively consider the potential risk of indiscriminate uses of ICTs and the potential harmful spill-over effects that such uses may have on the critical infrastructure and essential services of another State.

Secondly, building on paragraph 46 of the GGE report, the OEWG could also encourage States to take appropriate steps to incorporate such considerations in institutional arrangements and national decision making processes in the development and use of ICTs, as part of their commitment to be guided by the emerging and evolving framework for responsible State behaviour endorsed by all UN Member States.

As I mentioned in my intervention on threats, we will share a working paper on this topic in due course.

[Due diligence norm]

I would also like to draw the attention of the group to the norm stating that States should not knowingly allow their territory to be used for internationally wrongful acts against another state.

The 2021 GGE report set out that this norm raises the expectation that a State will take reasonable steps within its capacity to end ongoing activity in its territory through means that are proportionate, appropriate and effective in a manner consistent with international and domestic law. At the same time – and I would like to stress this point – the GGE agreed that it is not expected that States could or should monitor all activities within their territory.

The 2021 GGE provided further guidance on this norm that is of particular relevance to our work on confidence-building measures: “that an affected State should notify the State from which the activity is emanating. The notified State should acknowledge receipt of the notification to facilitate cooperation and clarification and make every reasonable effort to assist.”

In our view, the APR could recommend the establishment of effective channels, allowing States to communicate requests for assistance or ask for clarification in case of a significant cyber incident. The PoC directory could be an effective tool in this regard.

Also, the exchange of best practices regarding national approaches for responding to such requests for assistance would further contribute to a better implementation of this norm. This all enhances confidence-building, and could therefore be reflected in the APR.

Thank you chair.

+++