[check against delivery]

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

Existing and Potential Threats

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

NEW YORK, 7 March 2023

Chair,

The Netherlands aligns itself with the statement delivered by the European Union. I will make some additional remarks in my national capacity.

I am also aligning myself with others who expressed regret over the objections raised to the participation of a large number of stakeholders.

Their insights are uniquely valuable to the discussions on ICT security.

Let me therefore begin by echoing the many stakeholders that during last Wednesday's multi-stakeholder informal highlighted the growing threat to critical infrastructure, including the technical infrastructure essential to the general availability or integrity of the internet.

[Cyber in armed conflict]

In the 2022 Annual Progress Report we noted that threats have continued to intensify and have evolved significantly in the current challenging geopolitical environment.

It would be an understatement to say that the geopolitical environment has only deteriorated further. And the use of ICTs in the context of an armed conflict is now a reality.

A key pillar of the mandate of this Group is to identify these threats and achieve a common understanding of how they affect international security.

We therefore propose the 2023 APR could reflect several key threats associated to the use of ICTs in the context of armed conflict:

1. The serious risk of ICT activities affecting civilian objects, infrastructure and services, including humanitarian organizations and health care, which may violate the rules of international humanitarian law.
2. The increased risk of ICT activities causing spill-over effects in States not party to the conflict, potentially affecting, among others, food and energy supplies as well as ICT products and services. And this is a **global** risk.
3. The risk of escalation stemming from such spill-over effects.

Chair,

Let me zoom out and address other threats that the Netherlands believes could be reflected in the report:

[Ransomware]

Firstly, many States have raised the risk of ransomware. I would like to thank in particular Costa Rica for sharing their experiences on how they dealt with this threat. We also recognize the increasing risk of ransomware that rises to the level of international security. Let us do more work on thinking through this relationship between ransomware and international security. For example, in many instances we see that the kill chain of a ransomware attack begins with early infiltration in systems, including for

example in critical infrastructures and essential services. Depending on their scale and severity, such activities can pose a significant risks of instability, mistrust and escalation between States.

[New tech and AI]

Secondly, Like El Salvador, Chile, Canada, Malaysia, Singapore, South Africa, India and others the Netherlands draws attention to new technologies. The Netherlands believes that it would be important to further our understanding as OEWG of how new technologies, such as AI and quantum, may affect the risks posed by the use of ICTs to international security.

[Supply chains]

Thirdly, like Germany, Singapore and Israel, we would like to see the risk of cyber activities affecting the supply-chain of ICTs products and services reflected in the report. The EU has been developing regulation to bolster cybersecurity rules to ensure more secure hardware and software products, and many other States are doing the same.

[Reckless cyber ops]

Fourthly, we are also concerned about the risk posed by the indiscriminate or reckless use of ICTs that causes harmful spill-over effects on the critical infrastructure and essential services.

When the use of ICT capabilities that are designed in such a manner that their deployment allows no or limited meaningful control by the initiators, this is likely to diminish the means of a State to ensure adherence to the framework for responsible State behaviour, including international law. As such, the effects of such uses carry with them an additional risk of causing harm to citizens, institutions and economies.

They also increase the likelihood of destabilizing misperceptions and might therefore lead to unintended escalation between States. While a wide range of technical properties have been known to cause such uncontrolled cascading effects in past incidents, the use of automation, as well as new and emerging technologies such as Artificial Intelligence, may exacerbate their probability in the future.

We will soon circulate a working paper on this topic and would welcome feedback from other delegations.

[Support for other delegations]

- Further, I would like to support the points made by Israel and Greece on maritime security.
- I would like to echo the points made by Argentina, Philippines, the United States, Chile, Bangladesh and others on the importance of working with the private sector and other stakeholders in assessing threats and understanding the evolving threat landscape.
- I support the UK on the points they made on the risks of widespread sale and use of high end capabilities in ways that undermine human rights
- I support the points raised by Chile, on threats to women and girls and the points by Costa Rica on threats to all vulnerable groups
- I echo Australia's point about the importance of involving women in the development of technology. And I express the Netherlands' full support to the Women in Cyber Fellowship, enabling the equal involvement of women in our discussions here.

[Conclusion]

I add my voice to those delegations that have condemned the illegal and unwarranted invasion of Ukraine by Russia. The Netherlands stands with Ukraine and the Ukrainian people.

Lastly, I would like to recall the notion captured in previous reports that the use of ICTs by States in a manner inconsistent with their obligations under the framework undermines international peace and security, trust and stability between States. This is the starting point of our discussions. The framework took years of intensive negotiations and the consensus we achieved. It's up to States to live up to those agreements.

Thank you Chair.

+++

-