K I N G D O M O F B E L G I U M

STATEMENT

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

New York, 28 March – 1 April 2022

Agenda item 5: Promoting common understandings on existing and potential threats

---

Mister Chair,

Excellencies,

Distinguished delegates,

Belgium aligns itself with the statement by the European Union and its member states.

In my national capacity I would like to highlight the following points.

First of all, Belgium strongly condemns the acts of aggression committed by Russia in Ukraine, which undermine international security and violate the UN Charter and our common principles as United Nations.

The digital transformation provides the world population and economy with many opportunities for development. However, the growth in our use and dependency of new technologies, which are accelerated by the Covid pandemic, has been accompanied by a significant increase in cyberattacks. Geo-political tensions now further threaten the stability of our digital dependency. Cyber-attacks and spill overs targeting our critical infrastructure, democratic institutions and processes, supply chains and intellectual property are ever increasing.

It is therefore of the utmost importance to make our use of the digital environment as secure as possible, and resilient against all possible threat actors. Also Belgium has been under several cyber-attacks in recent years.

In 2012, Belgium signed off on its first Cybersecurity Strategy, which focused on recognizing cyber threats, improving security, and establishing measures to respond appropriately to incidents.

On May 2021, the National Security Council approved the details of the cyber security strategy 2.0. This strategy is the framework for Belgium's cross-cutting approach to cyber threats and opportunities for our country.

The key values are the following:

- Integration: an integrated and coordinated approach to cybersecurity;
- Empowerment;
- Balance between security and fundamental rights;
- Innovation: the development of new ideas and possibilities which can improve cyber security in Belgium and throughout the world;

- Integrity: honestly and honorable.

The strategy is also based on a strong communication strategy in order to inform citizens, companies, organisations of vital interest and public administration about cyber threats. We believe that they have to play a crucial role in first line cybersecurity.

Belgium also adopted a cyber attribution procedure. This procedure has put in place a mechanism to address the attackers and to take appropriate measures.

Preventing and limiting malicious activities is of crucial importance, reducing the risk of miscalculation and escalation, and we should all strive to respect international law and norms of responsible state behaviour.

The respect for international law, including international humanitarian law and international human rights as well as the norms of responsible state behaviour, is crucial to achieve international security and stability in cyberspace.

Russia's unprovoked aggression against Ukraine, including in cyberspace, is of great concern. We have sadly seen the use of cyber-attacks involving destructive instruments such as wipers for system breakdown, but also service disruptions, intrusion attempts, defacements and DDoS attacks targeting Ukraine, with the potential for spillover into other countries, particularly Ukraine’s neighbours. These activities are violating international law and breach the norms of responsible state behaviour that we have all agreed upon here in the United Nations.

Let me once again thank you Chair for your efforts and commitment to this process, and let me express once again the full solidarity of my country with Ukraine and the Ukrainian people.