Round Table Discussion
"The impact of new and emerging technologies
on international counter-terrorism efforts"
(Monday, February 11, 13.10-14.45 pm, Conference Room 8)

Statement by Andrei Dapkiunas,
Deputy Foreign Minister of Belarus

We live in a quickly changing world that is defined by **globalisation** and **the fourth industrial revolution**.

These trends, as well as efforts of States to prevent and counter terrorism, force individual actors and organised terrorist groups to **migrate to cyberspace** that provides them with almost limitless opportunities.

For major social media platforms, the most effective tool for countering the spread of terrorism-related information along with establishment of significant human moderation divisions are **automated technologies**, including artificial intelligence.

The main challenge is that cyber-space by its nature is not in the national government's domain only: you cannot effectively control and filter terrorism content without due **collaboration** and **self-control by the private sector**.

For Belarus, the main issue is the potential possibility of **cross-border receipt of terrorism-related data** through the Internet by individuals who are exposed to the influence of terrorism. All recently prevented by the Belarusian authorities cases of preparations to commit terrorist acts and engage in terrorist activities abroad were the result of **acquiring the terrorism content from outside Belarus through the web**. This includes detailed instructions on assembling explosive devices at home.

If the situation with major social media companies is more or less clear, the smaller platforms face the challenge of **identification** and immediate **removal of terrorism-related content** due to the significantly lower resources available for such activities.

Another area of concern is the use by terrorists of the **dark web**. Having access limited only to those aware of it existence, the dark web makes **identification and prevention** extremely difficult. Someone with a high level of anonymity may purchase weapons, acquire knowledge on its assembly, receive radicalisation and recruitment materials, raise funds and engage in secret communications with terrorist cells.

From the perspective of governments, ICTs provide opportunities for the gathering of intelligence and other activities to prevent and counter acts of terrorism.

For instance, what is artificial intelligence best at? It is extremely effective in **finding vulnerabilities**, such as **breaches in security**. This is of outmost importance for the protection of critical infrastructure. All we need is to develop necessary software capable to detect such breaches and eventually implement precautionary measures.

But this sword has two edges. Terrorists may obtain one day the AI technology that enables them to detect the same breaches and use this data to commit terrorist acts. This is an example of both challenges and opportunities that ICTs may create in the fight against terrorism.

What can we do to improve the current situation and make proper use of ICTs?

First, neither **universal convention specifically relating to the prevention and suppression of terrorist use of the Internet, nor comprehensive UN treaty on terrorism** have been developed. Belarus is strongly convinced of the need to redouble international efforts aimed at elaborating and adopting of at least the first one.

INTERPOL highlighted the importance of timely joint action in this direction. It warned that terrorist groups might try to acquire the necessary skills to launch major attacks. Compared to their current capabilities that seem to be rather modest and focused mostly on **web-sites defacements** and **DDoS** attacks, capability to commit major attacks will bring their abilities to the new level.

Second**,** we need to be aware of **new technologies** that are developed by the tech companies with potential of being used in terrorist purposes. We are in no way proposing to limit the progress of technologies. We suggest creating a **communication channel between the private sector and UN Member States through UNOCT and CTED**. This could be accomplished on a voluntary basis and provided in a relevant UN resolution, either by the General Assembly or the Security Council.

Third, we are all well aware of the existing time **gap between the elaboration of new terrorist tactics and the counter-actions by the states**. A response-oriented approach is much less effective if compared with the one aimed at **predicting** and **preventing** such evolution. It could be addressed, for instance, by establishing **a group of ICT and CT wise men** that may include representatives of UN Secretariat and major tech companies that will act on an ad-hoc basis. Their conclusions and proposals may be distributed to the Member States by the UN Secretariat.

Finally, Belarus consistently advocates the need **to increase international efforts** to counter the spread of terrorism. We take an active part in the United Nations Global Counter Terrorism Strategy reviews, negotiations on relevant resolution of the Sixth Committee, as well as in negotiations on the Comprehensive Convention on International Terrorism.

As part of our efforts, in October 2018 Belarus hosted the **international high-level conference «Preventing and Countering Terrorism in the Digital Age»**. It was organised in collaboration with the OSCE with the participation of the UN and addressed the issues we are discussing today.

I also would like to announce that this fall Belarus and the United Nations are going to organise in Minsk **an international high-level conference that will specifically address the issue of countering terrorism with new and emerging technologies**.

We believe that such events provide unique opportunities for the frank and in-depth exchange of existing challenges and opportunities, as well as allow us to synchronise and align our approaches and strategies.