

Permanent Mission of Hungary

 to the United Nations

New York

**Security Council Arria-Formula Meeting:
“Cyber Stability, Conflict Prevention and Capacity Building”**

**Organised by the Permanent Mission of Estonia, in cooperation with the Permanent Missions of Belgium, Dominican Republic, Indonesia and Kenya**

**22 May 2020.**

**Intervention by**

**H.E. Ambassador Katalin Annamária Bogyay**

**Permanent Representative**

Mister President,

Excellencies,

Let me start by **congratulating** Estonia for convening this meeting, which during these impossible times is more vital than ever. The clear and present danger of COVID-19 embodieseverything that we needed to focus our attention **on regarding cyber stability, conflict prevention and capacity building.**

In general, Hungary welcomes the continuation of the process to discuss voluntary norms, rules and principles for responsible State behaviour, confidence-building measures and international law on a regular basis under the United Nations First Committee.

In 2018, we supported General Assembly resolutions 73/266 and 73/27 establishing another group of governmental experts on advancing responsible State behaviour in cyberspace and an open-ended working group on developments in the field of information and telecommunications, both in the context of international security to address the threats posed by the use of information and communication technologies. It is the first time that Hungary is taking part in these open-ended negotiations.

Hungary strongly supports an effective multilateral system and the rules-based international order underpinned by strong national competencies and effective multilateral organizations. Our participation in and support for different inter-governmental and multi-stakeholder initiatives clearly demonstrate this approach.

Hungary reiterates the applicability of existing international law to state conduct in cyberspace as recognised by the UN GGE consensus reports from 2010, 2013 and 2015. However, non-compliance with international law obligations by state and non-state actors still constitutes a major threat to international peace and security and to our national sovereignty both in the physical world and in cyberspace. Therefore, we need to be able to deter and prevent both conventional and unconventional attacks.

It is widely expected that the number and sophistication of cyber attacks will keep growing. No single country, or organization, however, may be successful in tackling contemporary security threats alone.As a Member of the European Union, Hungary is actively involved in the development of the EU’s own cyber diplomacy toolbox in order for the EU to able to coordinate its response to malicious cyber activities against its institutions and its Member States originating from outside of the EU. Emphasizing the importance of international cooperation, we support an enhanced dialogue with our strategic partners, allies and other international organizations.

Hungary is one of the few countries with dedicated staff to cyber diplomacy. The Coordinator for Cyber Issues of the Ministry of Foreign Affairs and Trade is responsible for international outreach activities on cyberspace issues both in bilateral and multilateral relations, including the United Nations, the European Union, the OSCE and other relevant multi-stakeholder initiatives like the Global Forum on Cyber Expertise (GFCE). He also coordinates among Hungarian stakeholders, thereby ensuring a consistent approach in all relevant international fora.

On a regional level, we emphasize the role of the OSCE as a platform for holding consultations on a voluntary basis in order to reduce the risk of misperception, and of possible emergence of political or military tensions or conflict that may arise from the use of ICTs. A particular example for this are the regular meetings of the so-called CBM 8 Contact Points. Participating States of the OSCE are getting closer to further operationalize confidence-building measures developed by the OSCE. Hungary is ready to elaborate on the globalization of regional CBMs in the context of UN negotiations.

Considering, however, the challenges of attribution in the ICT environment, in case of a cyber incident, States should act with due diligence and consider all relevant information in order to avoid miscalculations that can escalate the situation into an armed conflict.

Hungary also welcomes the efforts of the good offices of the UN Secretary-General to prevent the escalation of cyber-incidents and the operationalization of voluntary cyber norms as well as further collaboration aimed at closing the cyber knowledge gap amongst Member States.

In our view, the fact that negotiations with the participation of the whole membership of the United Nations are taking place is a confidence-building measure in itself.

As a national contribution, since 2017, the Permanent Representative of Hungary to the OSCE is acting as the Chairperson of the OSCE Informal Working Group on Development of Confidence-Building Measures to reduce the risks of conflict stemming from the Use of ICTs.

Hungary supports the efforts aimed at closer cooperation between UN processes and other relevant regional organizations, like the OSCE. Regionally, we underline the importance of the implementation of the set of CBMs adopted by OSCE. Our focus should be to operationalize each and every regional CBM at the same level of effectiveness.

Competition in cyberspace is expected to further intensify in the years to come and the capacity gap between technologically advanced and developing countries will further expand. Developments in ICTs can have implications for all three pillars of the United Nations’ work: peace and security, human rights and sustainable development. In our view, better coordination between parallel discussions on multiple aspects of digital technologies, including human rights, Internet governance, cybercrime as well as sustainable development would be beneficial.

Other stakeholders could play a key role in raising awareness and disseminating information about these talks.

Within its means, Hungary contributes to capacity-building efforts in third countries. As part of these efforts, cyber security also plays an integral part in Hungary’s international development cooperation policy.

Thank you.