Hungary’s preliminary views on a global points of contact directory pursuant to A/77/275
“Developments in the field of information and telecommunications in the context of international security” containing the progress report on the discussions of the open-ended working group on security of and in the use of information and communications technologies 2021-2025

General appreciation of the issues related to cyberspace in the context of international security

By its resolution 75/240, the UN General Assembly decided to convene a new open-ended working group on security of and in the use of information and communications technologies for the period of 2021–2025, acting on a consensus basis. The first year of the second OEWG was influenced by a challenging geopolitical environment with rising concern over the malicious use of ICTs by State and non-state actors targeting critical infrastructure and essential services.

Hungary welcomes the first Annual Progress Report of the second Open-Ended Working Group and supports the Chair to use this report to establish a clear roadmap for 2023, allowing for further progress in our discussions on 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 and guided by consensus reports of previous UN Groups of Governmental Experts and the first OEWG. For the second consecutive time, Hungary is also taking an active part of these negotiations. Hungary is also ready to exchange views on the scope, structure and content of the proposed United Nations Programme of Action to advance responsible state behaviour in the use of information and communication technologies in the context of international security.

We strongly support an effective multilateral system, underpinned by a rules-based international order, which delivers results in tackling global challenges in cyberspace. Our participation in and support for different inter-governmental and multi-stakeholder initiatives is a good example of this. 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.

International cooperation and other multi-stakeholder initiatives

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 stemming 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.

No single country, or organization, may be successful in tackling contemporary security threats alone. This makes partnerships, in particular EU-NATO cooperation more important today than ever before. There is no alternative but to continue and further deepen this cooperation in the forthcoming years. Countering hybrid threats (including cyber security threats) is certainly one of the main areas where the two organizations should focus their efforts.

It is expected, that conflict in cyberspace will further intensify in the years to come and the capacity gap between technologically advanced and developing countries will further expand.

The commitment of Hungary to cyber security is not new. The first and still only international agreement on countering cybercrime, called the Convention on Cybercrime of the Council of Europe,
also known as the Budapest Convention was agreed in Budapest in 2001 and ever since has served as a guideline to develop comprehensive national legislation against cybercrime and as a framework for international cooperation. The treaty was ratified by the Act LXXIX of 2004. Besides being party to the Budapest Convention, Hungary is actively promoting the accession of third countries to it.

Hungary contributes to capacity-building efforts in third countries. As part of these efforts, cyber security also plays an integral role in Hungary’s international development cooperation policy. In addition to being part different intergovernmental negotiations, Hungary, in addition to a growing number of non-governmental organizations, is a supporter of multi-stakeholder initiatives, like the ‘Paris Call for Trust and Security in Cyberspace’ answering the call for more in-depth cooperation on the development of norms, rules and principles of state behaviour in cyberspace.

Hungary shares the view that that non-governmental organizations (civil society, academia, the private sector and the ICT community) have a range of technical expertise and/or the necessary resources to contribute to the development of a safe and sustainable cyberspace in their own respective roles and responsibilities. States have the leading role in promoting this coordination and collaboration.

**Points of Contact Directory**

Pursuant to the request by the Office for Disarmament Affairs to submit our view on the global points of contact directory as referred to by paragraph 3 of “Recommended next steps” under Section E “Confidence-Building Measures” of the Annex contained in A/77/275 with a view to the preparation of the requested background information paper in advance of the fourth substantive session of the OEWG, Hungary wishes to share the following preliminary views:

Hungary welcomes the recommendation to establish a global points of contact directory among states, allowing to reduce risks stemming from the use of ICTs and making concrete progress on advancing international security and stability.

On the margins of the last substantial OEWG and during our last intersessional meeting, we felt inspired by the contributions made by Member States and organizations like the OSCE, OAS, ASEAN RF on their specific experiences and their ideas on how such a UN Directory would fit into the global discussions on cyber or ICT security.

The OSCE, as the largest regional security policy organization is a front-runner in international efforts with regard to cyber security and it was successful in achieving a breakthrough accomplishment related to cyber with the architecture of 16 confidence-building measures (CBMs) to help facilitate a mechanism by which state to state communication can be established. This underlines the main purpose of the OSCE: defusing conflicts and building confidence, while at the same time also increasing national cyber resilience.

As a national contribution, since 2017, the Permanent Representative of Hungary is acting as the Chairperson of the OSCE Informal Working Group (IWG) established by PC Decision No. 1039 on Development of Confidence-Building Measures (CBMs) to Reduce the Risks of Conflict Stemming from the Use of ICTs. The Chair of the IWG is acting in close cooperation with the OSCE Chairmanship and the OSCE Secretariat. The Hungarian Chair of the informal working group initiated in 2018 the so called “Adopt a CBM” initiative, which invites States or a group of States to champion the elaboration of modalities for implementing a specific CBM. Taking into account the growing number of “adopters” (23 OSCE participating States + the European Union by 2022) and CBM-related projects, this initiative is starting to produce tangible results.
According to CBM No. 8. “Participating States will nominate a contact point to facilitate pertinent communications and dialogue on security of and in the use of ICTs” on a voluntary basis. During the OEWG intersessional meeting, the OSCE Secretariat and many participating States shared their practical experiences on managing or being a member of the OSCE CBM8 Points of Contact (PoC) Network also referring to the importance of such a network even before a crisis hits.

The OSCE Points of Contact Network, together with agreements on a consultation mechanism and available communication channels (CBM No. 3 and No. 13), effectively guide OSCE participating States how to interact with each other in a structured manner and create the backbone of confidence-building measures. In our view, this PoC Network proved to be instrumental in the development of other CBMs and enabled national experts to reach out to each other on different issues.

Moreover, in-person meetings such as workshops, yearly PoC meetings, scenario-based discussions added an additional layer to inter-state communication and formed the “list of experts” into an expert-network throughout the OSCE region. The COVID pandemic and the regular rotation in national experts of the PoC Network showed also the importance of regular awareness-raising about the available tools and frequent updating of the Network and checking the availability of PoC experts.

As a transparency measure, Member States should on a voluntary basis create national PoCs – independent from the type of PoC (technical, national security, military or diplomatic) – in a way that clearly indicates its role in the national cybersecurity system and that does not raise false expectation to other States or PoCs (e.g., in terms of what kind of information a national PoC might be ready or able to share and how this information should be handled).

Hungary supports the efforts aimed at closer cooperation between UN processes and other relevant regional organizations, like the OSCE. We are also in favour of elaborating on the globalization of regional CBMs in the context of OEWG and hope that our experiences could serve as inspiration for other regions and countries. Member States with regional expertise in implementing cyber CBMs should promote cross-regional discussions on best practices and encourage others and be encouraged to “be the first to adopt a global Cyber CBM” (like the adoption of a national PoC).

However, our immediate priority is to operationalize each and every regional CBM at the same level of effectiveness. At the global level, though, we have to continue to discuss the modalities of a UN PoC directory in 2023.