Ministry of Foreign Affairs
of the Czech Republic

Contribution by Czechia, reference: ODA/2023-00042/ ICT-Mapping Exercise

General context of capacity building projects conducted by Czechia:

Cyberspace is a borderless territory. Sharing cybersecurity knowledge and expertise among countries increases the collective ability to defend ourselves against common adversaries and strengthens global cyber resilience.

Therefore, Czechia welcomes and supports the ongoing emphasis on cyber capacity building, including the request to map existing initiatives and efforts.

For Czechia, cyber capacity building is an integral part of international cooperation. We believe that cyber capacity building is a two-way street: we learn from each other, both the provider and receiver. Many times sharing lessons learned on what did and what did not work can be as important, if not more, than the sharing of good practice.

Czechia has a number of skills in the field of cyber security that can share with other countries. Czech cyber capacity building projects focus inter alia on the following topics:

- sharing our approach to cybersecurity framework on the national level (strategies, policies, legislation, etc.);
- establishment and strengthening Computer Emergency Response Teams (CERT);
- approach to cybercrime;
- cooperation in multilateral negotiations on cyber security and the fight against cybercrime;
- exchange of information regarding UN norms of responsible state behaviour in cyberspace, confidence-building measures, and application of international law to cyberspace.

Czechia implements cyber capacity building projects by using instruments of foreign development cooperation and economic diplomacy. It does so in accordance with the National Cyber Security Strategy, the Strategy for Foreign Development Cooperation and the Concept of the Foreign Policy of the Czech Republic.

Czechia has also continuously emphasized that multi-stakeholder approach including public-private partnerships and involvement of civil society have an irreplaceable role in cyber capacity building.

Examples of capacity building projects conducted by Czechia:

Czechia implements its cyber capacity building projects both on bilateral and multilateral basis.

Bilaterally, Czechia has organized a number of seminars focused on cyber security and cybercrime with selected countries of the Indo-Pacific region, Africa, the Western Balkans, and the EU Eastern Partnership. National cyber capacity building platforms (such as CyberVac) were used in case of these projects.

Regarding the multilateral platforms, Czechia regularly carries out cyber capacity building projects in the context of its membership in the EU and NATO. See bellow few examples of such projects.

- Using the resources of "Technical Assistance and Information Exchange instrument of the European Commission" (TAIEX), Czechia organized a study visit of Albania's National Authority for Electronic Certification and Cyber Security (AKCESK) in Czechia. Similarly, also using the resources of TAIEX, the Czech govCERT participated on the expert mission to Bosnia and Herzegovina in order to share our expertise in the field of OSINT, forensics, etc.
- Czechia co-organizes the EU funded project "EU Support to Western Balkans Cybersecurity Capacity Building" that aims at increasing cybersecurity in the region of Western Balkan.
- Czechia supports the EU Cyber Capacity Building Network (EU CyberNet) that has compiled a cyber capacity building mapping, which gives an overview of all initiatives of the EU and Member States, funded by either the EU or the Member State itself.
- Czechia also takes part in the NATO cyber capacity programmes. Project for army CERT in Jordan, for example, will begin next year and focus on providing expertise and sharing skills between technical experts from CERTs.

In addition to the EU and NATO programmes, Czechia also, on ad-hoc basis, considers suitable cyber capacity building platforms associated with:

- United Nations Institute for Disarmament Research (UNIDIR);
- Global Forum on Cyber Expertise (GFCE);
- Freedom Online Coalition (FOC);
- United Nation Development Programme (UNDP);
- United Nations Conference on Trade and Development (UNCTAD);
- International Telecommunication Union (ITU).

Of the above-mentioned platforms, we would like to highlight the GFCE approach. GFCE has been working closely with the Open-ended working group on security of and in the use of information and communication technologies 2021-2025 (OEWG) on cyber capacity building issues. We observe that the quality of GFCE-related projects is continuously increasing. The number of GFCE members is also steadily growing and consist of countries as well as private sector, civil society and academia. We appreciate, in particular, the apoliticalness of the GFCE, functionality of the Cybil Portal and the GFCE effort to avoid duplications by strengthening the collaboration with other cyber capacity building platforms including the UNIDIR Cyber Policy Portal or the EU CyberNet.

16th November 2023