

REFERENCE: ODA/2023-00042/ ICT-Mapping Exercise

Pursuant to the request “ODA/2023-00042/ ICT-Mapping Exercise” the European Union would like to highlight the following on the landscape of information and communications technologies capacity-building programmes and initiatives within and outside the United Nations at the global and regional levels:

As of 1 January 2023, a total of 33 ongoing EU funded cyber capacity-building actions were mapped with an estimated overall funding of almost 179 million EUR¹. The EU’s formal commitment to cyber capacity building can be traced back to the first Cybersecurity Strategy of the European Union, which was adopted in 2013. It outlined the EU’s priorities in the field of cybersecurity, including enhancing global cyber security and resilience, promoting cooperation, and supporting Member States’ efforts to develop and implement robust cybersecurity policies and legislation. This strategy marked the beginning of a more coordinated and comprehensive approach to addressing cyber threats and vulnerabilities and was further strengthened with the 2018 Council Conclusions on the EU External Cyber Capacity Building Guidelines² and the 2020 Cybersecurity Strategy for the Digital Decade, where the EU set further guidance as to the conduct of cyber capacity building and decided to implement two strategic initiatives, namely, developing an EU External Cyber Capacity Building Agenda and an EU Cyber Capacity Building Board. The 2022 Council Conclusions on developing the Union’s cyber posture further highlighted the integration of cyber capacity building in the EU’s role as a security provider. Additionally, it emphasised the need to align the EU’s cyber capacity building strategy with the UN norms of responsible state behaviour in cyberspace.

The EU’s overall external action is defined in the NDICI-Global Europe, guided by the 2018 Council Conclusions on the EU External Cyber Capacity Building Guidelines and supported through other tools dedicated for specific regions, such as Instrument for Pre-accession Assistance (IPA III). With its projects the EU aims to support its partners in addressing their key cyber-related needs by strengthening both their national capabilities (e.g. organisational structures, processes and networks), collective capabilities (through whole-of-society approach) and facilitating international cooperation and partnerships (e.g. through institutional, legislative and policy frameworks), in line with the EU’s core values and principles, the rule of law, human rights, fundamental freedoms and democratic values

In order to mobilise the EU’s collective expertise to support partner countries in building their capacity to defend against cyber threats and promote EU’s good practices and standards in cybersecurity, the EU Cyber Capacity Building Network (EU CyberNet) was launched in 2019. EU CyberNet is implemented by the Estonian Information System Authority (RIA) with the support from the Advisory Board partners – the Federal Foreign Office of Germany and the

¹ Latest figures are depicted at the EU cyber net website www.eucybernet.eu

² <https://data.consilium.europa.eu/doc/document/ST-10496-2018-INIT/en/pdf>

National Cybersecurity Competence Centre of Luxembourg. It is funded by the European Union and managed by the European Commission's Service for Foreign Policy Instruments.

EU CyberNet has compiled a cyber-capacity building mapping, which gives an overview of all EU funded external cyber capacity building projects (actions) around the world, as well as a variety of EU Member States activities.

The main purpose of the mapping is to increase operational awareness, enhance coordination, reduce fragmentation and support various target groups (e.g. European Commission services, EU-funded projects & initiatives, EU Member State's actions etc.). It contributes to the global delivery of the EU's external cyber initiatives through running a 300+ member pan-European Expert Pool, carrying out training activities and providing a forum for exchanges of experiences and mutual learning among the large European Stakeholder Community of capacity building. The majority of the EU's 33 ongoing EU funded cyber capacity-building actions focus on cybersecurity (12), while 11 actions address cybercrime and 2 deal with cyber diplomacy. Geographically, the most funds have been directed to the EU's Neighbourhood (11 actions operate in the East, 7 in the Western Balkans and 4 in the South), followed by Sub-Saharan Africa (9 actions), Asia-Pacific (7 actions) and Latin America & the Caribbean region (5 separate actions). There are also many external cyber projects and activities funded by the EU Member States and the mapping relies on their voluntary contributions. 15 EU Member States have provided information to EU CyberNet so far of about 40 projects with mostly regional and bilateral scopes.

The external cyber capacity building projects mapping has already proven useful for many counterparts of EU CyberNet and continues to be a good source of information. The online mapping with up-to-date information can be found at www.eucybernet.eu/ccb-table.

With the establishment of the EU CyberNet in 2019 and the implementation of the EU Cyber Capacity Building Board in 2022, the EU has also put strong emphasis on mapping various capacity building projects and coordinating them to help reduce fragmentation and duplication of efforts and at the same time identify priorities for new cyber capacity building activities. In this context, roundtables have also been organised among EU Institutions, Member States and partners to ensure a shared understanding of each other's initiatives, engagements and plans on cyber capacity building in different regions but also to make sure that resources invested are put to best use. Additionally, EU Cybernet is a member of the Global Forum on Cyber Expertise (GFCE). GFCE is currently conducting its own mapping exercise and complements the EU CyberNet by expanding the excersition from an EU to a mondial level.

In conclusion, the European Union and its Member States have gained significant experience in working with cyber issues and are one of the leading providers of cyber capacity building

to partner countries. In particular, the EU CyberNet is exemplifying EU's commitment and has become a beacon of knowledge exchange and support for partner countries. Through this approach, EU is contributing to the enhancement of global cyber resilience.