European Commission

Mapping of EU-funded External Cyber Capacity Building Actions 2022

Foreign Policy Instruments

Table of Contents

1. Introduction

Cyber capacity building (CCB) is one of the youngest fields of international cooperation. It is growing fast both in terms of the number of donors, partner countries and organisations involved and the range of issues tackled.[1]

The purpose of this mapping report is to provide a detailed overview of **EU-funded** cyber capacity building actions **outside of the EU** (external cooperation). The accounted actions were all **being implemented on the cut-off date of 1 January 2023**.

The mapping is an initiative of the Service for Foreign Policy Instruments (FPI) of the European Commission. It was undertaken by EU Cyber Capacity Building Network (EU CyberNet) – an action managed by the Unit for global and transregional threats of the FPI – in close collaboration with the European External Action Service (EEAS), the Directorate-Generals for International Partnerships (DG INTPA), for Neighbourhood and Enlargement Negotiations (DG NEAR), for Communications Networks, Content and Technology (DG CNECT), and for Migration and Home Affairs (DG HOME).

The mapped actions are funded through the financial instruments managed by the European Commission, including Global Europe: Neighbourhood, Development and International Cooperation Instrument (NDICI), as well as the various instruments of the previous financial framework such as for example the Instrument contributing to Stability and Peace (IcSP), the European Neighbourhood Initiative (ENI) or the European Development Fund (EDF).

The mapping includes all CCB areas with the exception of cyber defence, where the European Commission does not have competences in external relations due to the defence / military dimension of this field.

The data were collected by EU CyberNet through an online questionnaire sent to the implementers of other EU actions. The collected data were then checked with the relevant Commission services. EU CyberNet wishes to thank all who contributed to the exercise for their collaboration.

Most actions listed have CCB as their main focus. A growing number of actions may however have a different overall objective, while CCB is pursued only by one of their components or in a separate work strand. This is typically the case of digitalisation programmes. This poses some challenges as regards how to include them in the mapping. For the purposes of quantitative analysis, only a relevant share of their budget was listed and counted. In some cases, this budgetary share was defined by the approved budget of the action, in many other cases, however the share is an indicative estimate of the action's cyber dimension.

Actions working in areas closely related to cyberspace – such as internet governance, artificial intelligence, data protection – were also included in the mapping due the nature of their scope and in order to provide more comprehensive overview.

In case there were several clearly distinctive components within a wider programme, with different focuses and implementers, they were counted as separate actions.

In addition to this overview of EU-funded actions, another layer of the mapping focuses on the actions of the EU Member States. This aims to achieve better programming and operational awareness, strengthen coordination, and reduce risks of duplication. In this regard, on 24 May 2022, the EEAS Director for Security and Defence Policy and the Acting Director – Head of Service of FPI invited the EU Member States in a joint letter to provide voluntary contributions to the mapping about nationally funded actions. A number of Member States have subsequently provided input. **The data on Member States actions have not been included in this report. However, a full overview of all EU and Member States' actions is available on EU CyberNet's web www.eucybernet.eu/ccb-table/.**

[1] More information in an ISS report International Cyber Capacity Building: Global Trends and Scenarios, 2021, by N. Barmpaliou, R. Collett, coordinated by P. Pawlak, O. Vosatka.

While this report provides a static overview of the situation on 1 January and will be updated on a yearly basis, EU CyberNet aims to keep the online mapping on its website more up-to-date. This applies especially to EU-funded actions. In this regard, all who would wish to send an update to the mapping may do so through an online questionnaire. Please reach out to EU CyberNet to get the appropriate link.

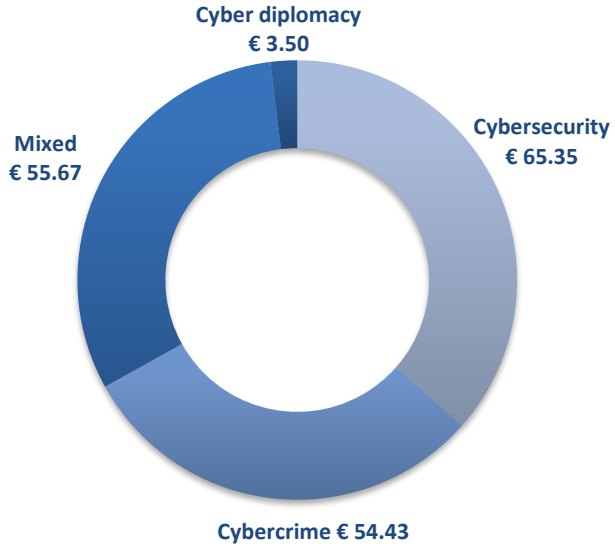
2. Thematic focus

Altogether, 33 cyber capacity building actions were mapped. Their overall funding is estimated to be 178,95 million euros. This figure is only indicative as in many cases it is impossible to extract cyber-related activities and relevant budget from cyber components of larger programmes.

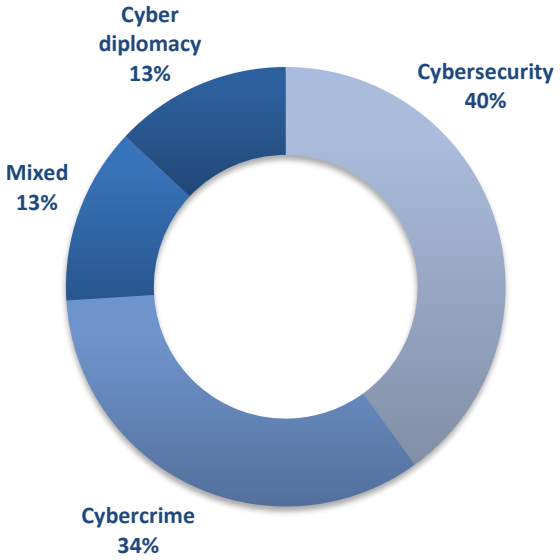
25 actions have a thematic focus on one single area: The majority of these focuses on cybersecurity (12), while 11 actions address cybercrime and 2 deal with cyber diplomacy.

Additionally, 8 actions have a wider mandate and more than one focus (referred to as mixed actions in the graph below).

The estimated division of the funds according to focus areas is as follows (million euros):



Overall, based on the mandate, the highest number of actions are dealing with **cybersecurity** issues (18 actions, 40%), followed by **cybercrime** (15 actions, 34%), while **cyber diplomacy** is part of the mandate in 6 occasions (13%). Additionally, 13% are working also on other areas with a strong cyber dimension (governance, artificial intelligence, and data protection).



3. Geographic focus

6 actions operate globally, 18 actions have a defined regional scope (55%), while 9 actions are focused on a specific country. The mapping differentiates between geographical scope, where the action has mandate to operate (that can be wider in case of global or regional scope) and concrete beneficiary countries, where it is or has operated.

The most funds have been directed to the EU's Neighbourhood (11 actions operate in Eastern Neighbourhood and 7 in Western Balkans, 4 actions in Southern Neighbourhood), followed by Sub-Saharan Africa (9 actions), Asia-Pacific (7 actions) and Latin America & the Caribbean region (5 separate actions). The number of actions operating in each region includes also global ones that are usually present in several regions (and thus cannot be summed up).

Region	Number of actions operating in the region
Eastern Neighbourhood	11
Western Balkans	7
Southern Neighbourhood	4
Africa	9
Asia-Pacific	7
Latin America & Caribbean	5

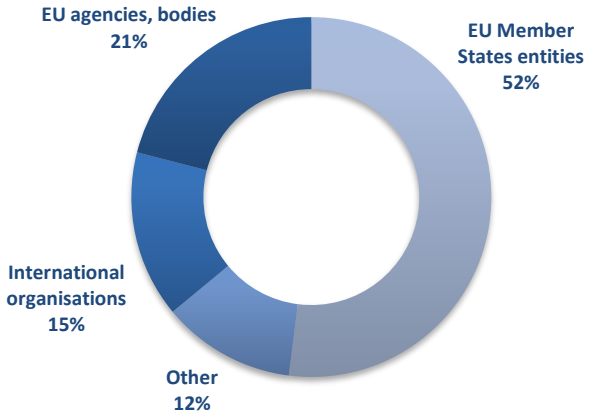
Wherever possible, the budget of global and trans-regional actions was divided to parts corresponding to specific regions according to the implementation. However, this separation was not possible in all cases. These actions are therefore listed as the "Other" in the graph below.

Region	Budgetary Commitments
EU Neighbourhood	**88,64 million €**
Eastern Neighbourhood	66,1 million €
Western Balkans	10,35 million €
Southern Neighbourhood	12,19 million €
Africa (Sub-Sahara)	**43,35 million €**
Latin America & Caribbean	**16,35 million €**
Asia-Pacific	**16,11 million €**
Other	**14,5 million €**

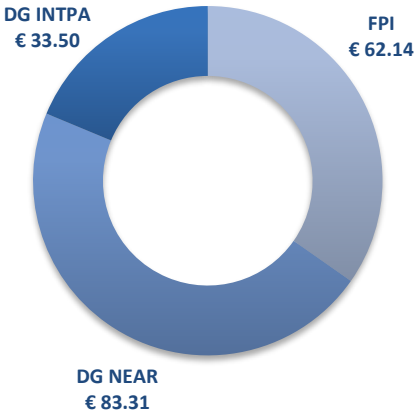
4. Implementing partners

58% of actions have more than one implementer where partners are working in a consortium; while 42% of actions have a single implementer.

Most actions are being implemented by Member State entities (52%), followed by EU agencies and bodies (21%) and international organisations (15%). 12% of actions are implemented by other type of partners (private profit/non-profit organisations).

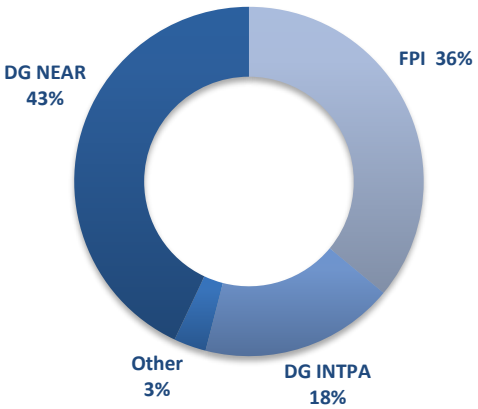


In terms of budget (million €), the division between the Commission services is as follows:



5. Institutional responsibility

DG NEAR has the most actions under their responsibility, 14 actions (43%), FPI manages 12 actions (36%), while DG INTPA manages directly 6 (18%) actions and one is managed by another body (Eurojust) (3%).



The mapping of EU-funded external cyber capacity building actions and the report have been conducted by EU Cyber Capacity Building Network (EU CyberNet) under supervision of FPI.1 – Stability and Peace – Global and Transregional Threats, and in cooperation with EEAS and DG INTPA, DG NEAR, DG CNECT and DG HOME.

EU CyberNet is funded by the European Union. The project is implemented by the Estonian Information System Authority in cooperation with German Federal Foreign Office and Luxembourg House of Cybersecurity.

The purpose of EU CyberNet is to strengthen the global delivery, coordination and coherence of the European Union's external cyber capacity building actions and to reinforce European Union's own capacity to provide technical assistance to third countries in the field of cybersecurity and cybercrime. EU CyberNet maintains and operates a Pool of Expert who are ready to contribute to capacity building initiatives and provide expertise to EU's efforts in partner countries. The Expert Pool can be used by Commission services, Member States and all members of the EU CyberNet Stakeholder Community, including implementing partners of ongoing and future cyber capacity building actions at EU CyberNet's technical platform CynAct.

More about EU CyberNet and its activities can be found at website www.eucybernet.eu.