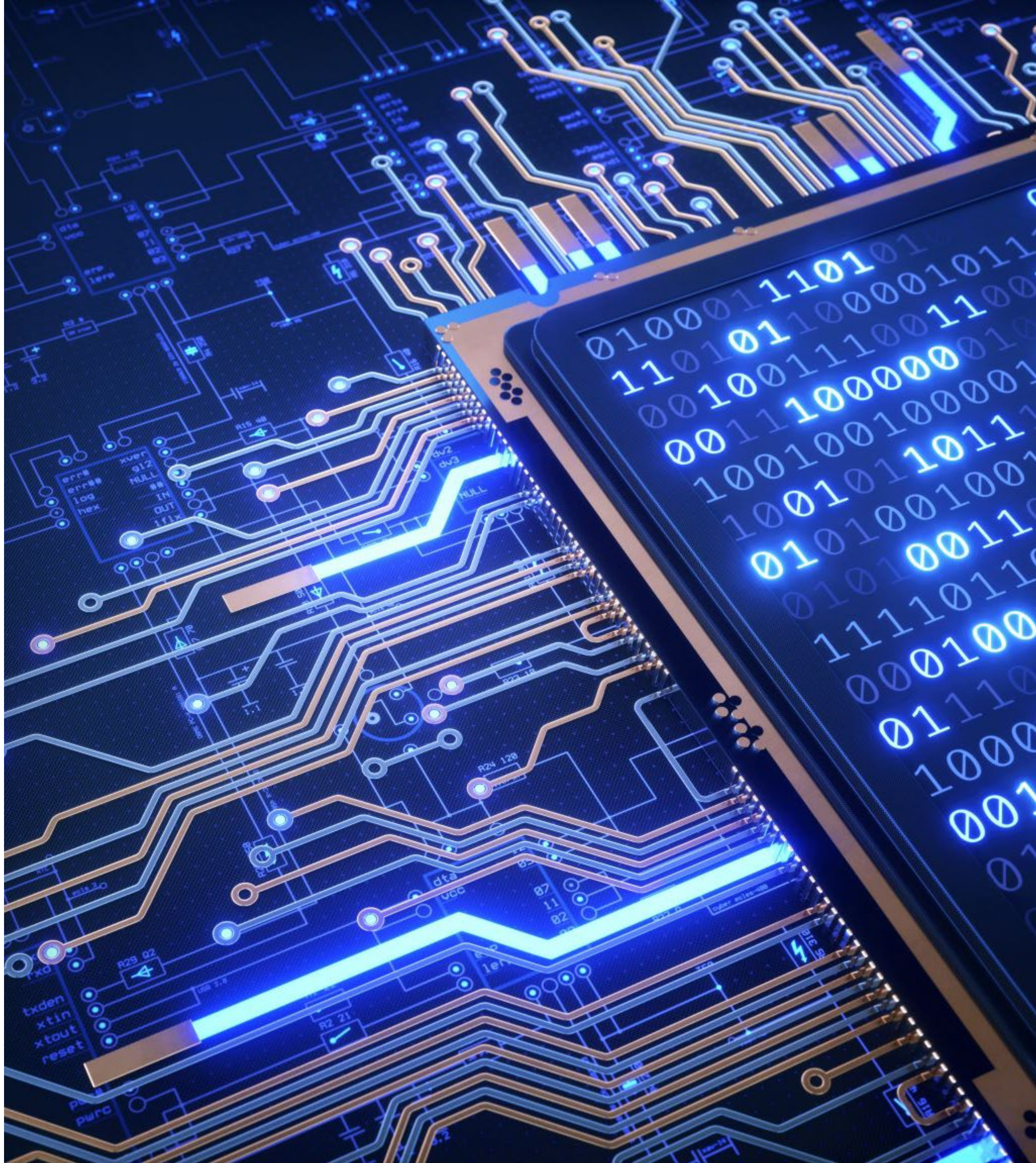
International Digital Security Forum

Vienna

19 – 21.09.2023

- Building Cyber Resilience: National Strategies for Capacity Development in Cybersecurity



National Cybersecurity Strategy 2020 -2025

HELLENIC REPUBLIC
MINISTRY OF DIGITAL GOVERNANCE
NATIONAL CYBERSECURITY AUTHORITY

National Cyber Security Authority
HELLENIC REPUBLIC

NATIONAL
CYBERSECURITY
STRATEGY
2020 - 2025

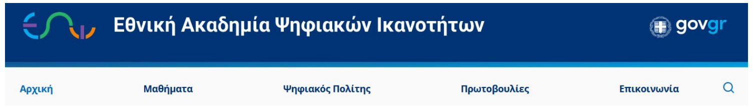
National Cybersecurity Strategy 2020 -2025

Capacity building, promoting information and awareness raising

Objectives	Activities
Building capacity by organizing cybersecurity exercising activities	Elaboration of the National Program for Cyber Security Exercises
	Capacity building and “lessons learned” procedures
	Utilization of a “cyber range” type platform for the training of managers (security, networks, systems, applications, databases, etc.) of the authorities and the entities
Apply state - of - the - art educational and training methods and tools	Information and educational material compilation (general and by entities category)
	Elaboration of an Education and Awareness Action Plan
	Framework for upgrading expertise and skills of professionals
Promote open - ended cybersecurity information and awareness raising for entities and citizens	Elaborating a National Program for Cybersecurity Awareness Developing a framework for communicating incident management

Flagship initiative at a Greek national level

National Academy of Digital Skills 1/2



- Source: https://nationaldigitalacademy.gov.gr/

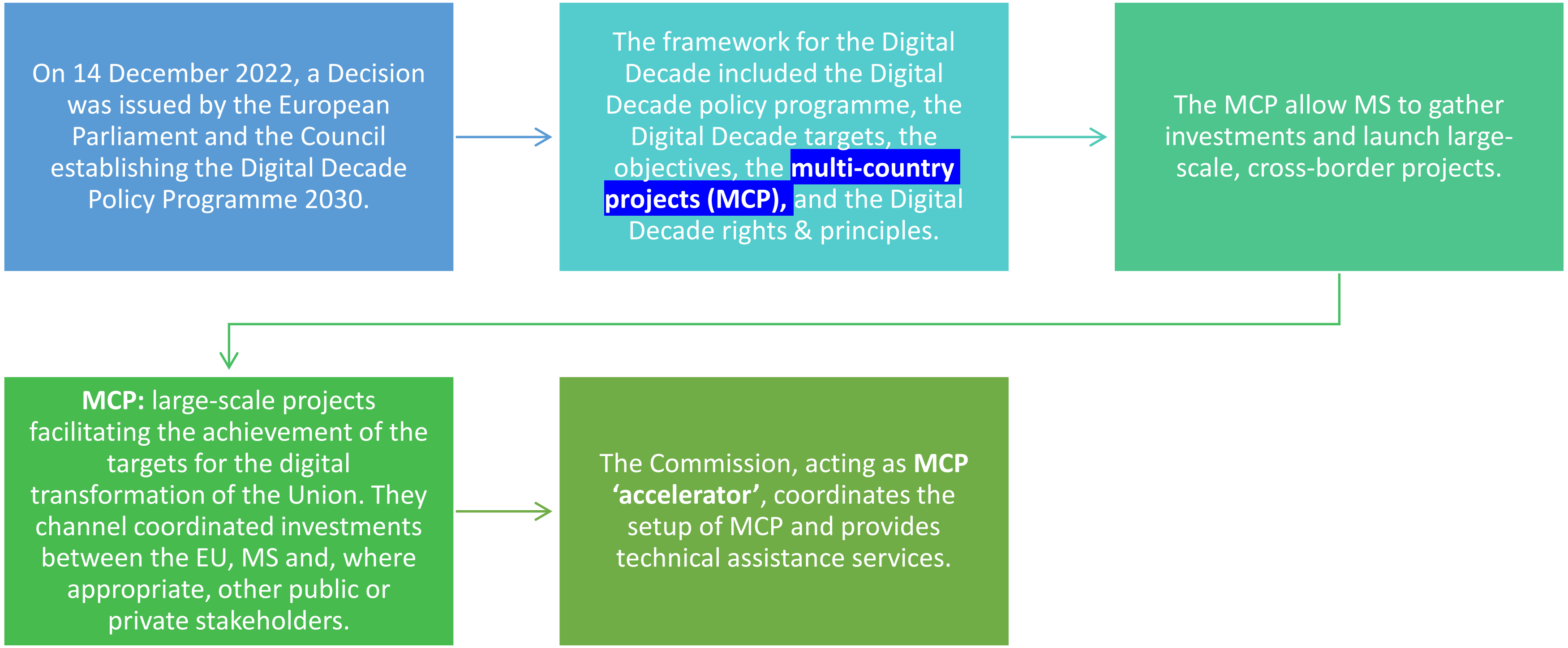
National Academy of Digital Skills 2/2

- An initiative of the Hellenic Ministry of Digital Governance to develop and aggregate educational content at a single-entry point, aiming to develop digital skills for all levels of citizens and professionals,
- Interested parties can find courses for free that will meet their personal needs and help shape their professional profile to meet the demands of the digital era.
- 323 courses
- 34 subject areas (e.g., cybersecurity, artificial intelligence, machine learning, data analysis, big data)
- 1800+ training hours for different skills categories
- 40 providers

EDIC - European Cybersecurity Skills Academy

(A joint initiative of European MS)

EDIC background 1/2



On 14 December 2022, a Decision was issued by the European Parliament and the Council establishing the Digital Decade Policy Programme 2030.

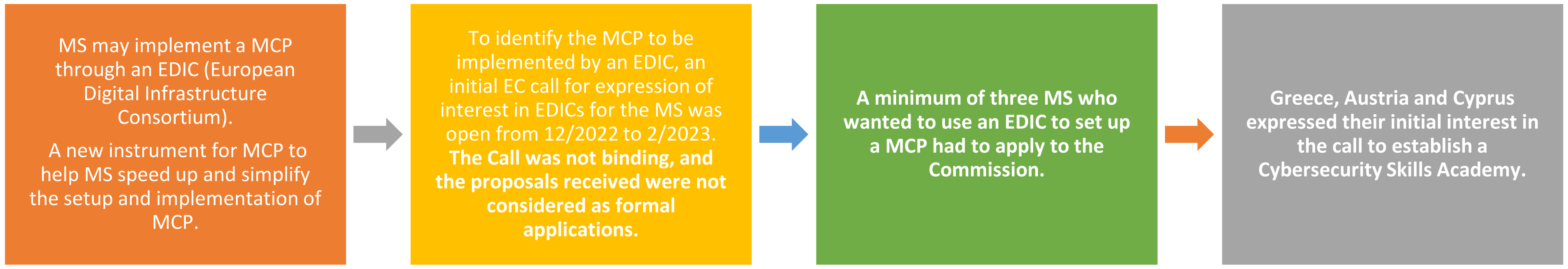
The framework for the Digital Decade included the Digital Decade policy programme, the Digital Decade targets, the objectives, the **multi-country projects (MCP),** and the Digital Decade rights & principles.

The MCP allow MS to gather investments and launch large-scale, cross-border projects.

MCP: large-scale projects facilitating the achievement of the targets for the digital transformation of the Union. They channel coordinated investments between the EU, MS and, where appropriate, other public or private stakeholders.

The Commission, acting as **MCP 'accelerator'**, coordinates the setup of MCP and provides technical assistance services.

EDIC background 2/2



MS may implement a MCP through an EDIC (European Digital Infrastructure Consortium).

A new instrument for MCP to help MS speed up and simplify the setup and implementation of MCP.

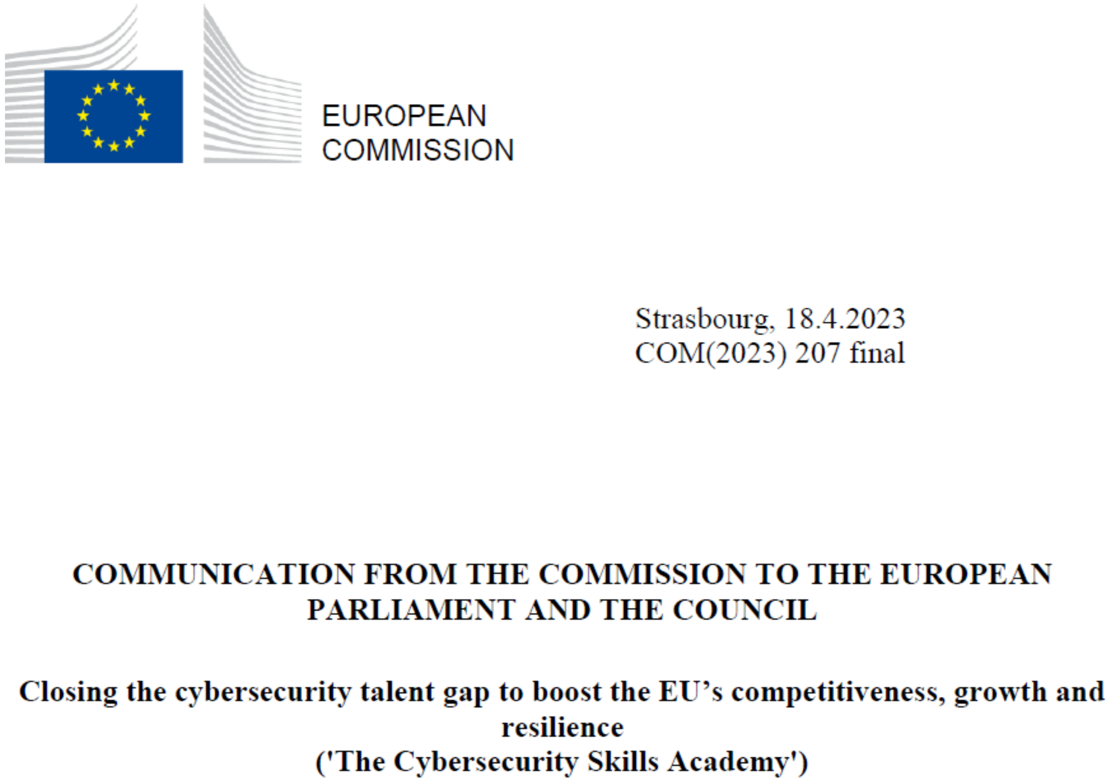
To identify the MCP to be implemented by an EDIC, an initial EC call for expression of interest in EDICs for the MS was open from 12/2022 to 2/2023. **The Call was not binding, and the proposals received were not considered as formal applications.**

A minimum of three MS who wanted to use an EDIC to set up a MCP had to apply to the Commission.

Greece, Austria and Cyprus expressed their initial interest in the call to establish a Cybersecurity Skills Academy.

Prenotification preparation phase

- Started in late April 2023 following the initial call for expression of interest.
- Based on the EC COM as the basis for further analysis and development



EUROPEAN
COMMISSION

Strasbourg, 18.4.2023
COM(2023) 207 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

Closing the cybersecurity talent gap to boost the EU's competitiveness, growth and resilience
('The Cybersecurity Skills Academy')

Participating countries so far (in alphabetical order)

- Austria
- Cyprus
- Greece (Chair of the WG)
- Italy
- Portugal
- Slovenia
- Other countries expressed interest to join this initiative

Discussions with participating MS - Addressed topics 1/3

- EDIC participants and their role in the EDIC (members or observers)
  - For the establishment of an EDIC, at least 3 MS required as members
- Implementation strategy
  - Main objectives, (e.g., mission, scope, collaboration with key stakeholders, risks and how to mitigate them, timeline, indicative budget)
  - How these to be reached
- Name of the EDIC – European Cybersecurity Skills Academy
- Statutory seat – Athens, Greece

Discussions with participating MS - Addressed topics
2/3

- MS wishing to sign the application
- Financial contributions
  - Indicative budgetary figures from at least 3 MS. No financial threshold to join this initiative.
  - Disclaimer added: Commitments subject to formal national confirmation.
  - This budget forecast should be able to demonstrate the viability of the EDIC for the first 2-3 years.
- In-kind contributions
  - (e.g., expertise, premises…)

Discussions with participating MS - Addressed topics 3/3

- Rationale and objectives of the MCP to be implemented by the EDIC
  - Why an EDIC has been chosen as implementation mechanism for the MCP
  - MS should also indicate any encountered legal / policy issues
- Timeline for the work ahead
  - Expected submission date and expected date of the start of EDICs activities

Implementation Strategy

Implementation Strategy

(EC COM as the basis for further analysis and development of the Strategy)

1/2

- Mission
- Scope
- Deliverables
- Actions to ensure setting up and successful operation
- Indicative budget figures and in-kind contribution
- Time framework for the work ahead
- Assess whether additional Member States wish to join the EDIC

Implementation Strategy (EC COM as the basis for further analysis and development of the Strategy) 2/2

- Risks and how to mitigate them:
  - Legal
  - Financial
  - Operational
  - Strategic
  - Policy
  - Technological
  - Cybersecurity
  - Compliance
  - Supply chain
  - Human factor
  - Reputational

Shortly on the Mission 1/2

Address the shortage of cybersecurity specialists in Europe and meet the increasing demand for cybersecurity skills

- **Goal:** Protect businesses and public services by enhancing cybersecurity capabilities.
- **Role**: Serve as a European umbrella organization for cybersecurity education and training.
- **Objectives**:
  - Increase visibility, accessibility, and overall impact of cybersecurity education and training activities,
  - Coordinate training programs to bridge the cybersecurity skills gap,
  - Promote the use of up-to-date curricula in cybersecurity education,
  - Facilitate standardization of procedures for cybersecurity competence recognition and professional certification,

Shortly on the Mission 2/2

Address the shortage of cybersecurity specialists in Europe and meet the increasing demand for cybersecurity skills

- European Cybersecurity Ecosystem: a reference place in Europe for cyber security stakeholders,
- Serve as an information exchange, knowledge sharing and coordination platform,
- Keep track of the various funding and subsidy programs available in Europe supporting the development of cyber security skills,
- Encourage collaboration and knowledge sharing among researchers and practitioners from the participating MS.

Target audience

- Government entities, policy makers
- Academia
- Students
- Research institutes
- IT Professionals
- Women in ICT
- Businesses, Industry
- Certification bodies
- International organisations

Overall scope and impact

- Protect citizens, businesses, and public services from cybersecurity threats in Europe
- Promote the growth of the cybersecurity workforce, support cybersecurity education and training initiatives.
- Engage in cross-border partnerships and collaborations
- Support students, professional to pursue cybersecurity-related educational programs and careers
- Skill, upskill, reskill
- Shield Europe as a unified entity

Entities that may become members of the EDIC – Cybersecurity Skills Academy

- MS of the Union
- Regions of the Member States
- Other public entities established in MS
- Third countries if associated to a directly managed Union programme that supports digital transformation of the Union
- International organisations of European interest
- Private entities
- Other categories may be added if relevant for the EDIC

Last but not least…1/2

The EDIC will be a legal entity set up by a decision of the Commission to implement a specific MCP.

The EDIC remains open to all MS, including those that were not ready at the time of the initial launch

MS that provide a financial and/or non-financial contribution shall be members of the EDIC with voting rights. Otherwise, they will be assigned the role of the observer (no voting rights)

Exact timing for submission of the final application to be determined among all the participating countries in the upcoming period

Last but not least…2/2

- The implementation of the Academy will be supported by a EUR 10 million funding from the Digital Europe Programme (DEP)*

* *Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240*

Thank you for attention!

Annex

Supporting material – further ideas for discussion

Cybersecurity challenges ahead… (not only as regards the ‘Academy’)

- Shortage of cybersecurity professionals,
- Difficulty of attracting and retaining talents and cybersecurity experts,
- Budget constraints for training and development,
- Rapidly evolving cyber threats (sophisticated cyber attacks),
- Critical infrastructure vulnerabilities,
- New attack surfaces,
- Cross – border collaboration.

Suggestions…?

Invest in cybersecurity training,

Promote a cybersecurity culture,

Clear career pathways,

Active engagement with educational institutions regarding future cybersecurity professionals,

Continuous collaboration between all relevant stakeholders,

Organizations to match their strategic plans based on their unique needs and challenges,

Offer competitive salaries and benefits,

Assess and update cybersecurity policies.

Ioannis Panolias

Hellenic National Cybersecurity Authority

Directorate for Cybersecurity Strategic Planning

Department of Strategic Planning

i.panolias@mindigital.gr

National Cyber Security Authority

HELLENIC REPUBLIC