THE EUROPEAN CYBERSECURITY INDUSTRIAL, TECHNOLOGY AND RESEARCH COMPETENCE CENTRE & NETWORK

KATARZYNA PRUSAK – GÓRNIAK,

VICE-CHAIR OF THE ECCC GOVERNING BOARD

The Centre (ECCC)

The European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) - REGULATION (EU) 2021/887 of 20 May 2021

National Coordination Centres (NCC)

The Network of NCCs

The Cybersecurity Community

ECCC

Strategic Tasks

- Agenda-monitoring and priority-setting
- Technical and strategic support to industry and SMEs
- Expert advice to the Member States upon request
- Support cooperation between relevant Union institutions
- Coordination of national centres through the Network

Implementation Tasks

- DEP cyber, possibly HE
- Administration of the Network and the Community
- Deployment of ICT Infrastructure
- Annual work programme, expert advice to the EC
- Cooperation with the European Digital Innovation Hub
- Synergies of civilian and defence spheres
- Promotion of the ECCC, NCC and the Community

ECCC

EUROPEAN CYBERSECURITY
COMPETENCE CENTRE

National Coordination Centres (NCCs)

- Nominated by Member States as the national contact point
- Objective: national capacity building, link with existing initiatives, support ECCC and Network
- May receive funding and may pass on financial support
- One NCC per Member State
- Alignment with EDIHs to reach synergies and avoid duplication of efforts.

Community

- Cybersecurity stakeholders (industry, research, private and public sectors)
- Entities established in MS with cybersecurity expertise in:
  - (a) academia, research or innovation;
  - (b) industrial or product development;
  - (c) training and education;
  - (d) information security or incident response operations;
  - (e) ethics;
  - (f) formal and technical standardisation and specifications.
- Application through the NCC/ registration by ECCC
- Advisory Group

The Strategic Agenda

- Adopted by the GB in March 2023
- A comprehensive and sustainable cybersecurity industrial, technology and research strategy
- Sets out strategic recommendations for the development and growth of the European cybersecurity industrial, technological and research sector
- Sets out strategic priorities for the Competence Centre's activities
- Goals to achieve by investing in projects that will *"strengthen the EU leadership and strategic autonomy, support Union technological capacities and increase the global competitiveness of the Union's cybersecurity industry"*

First Impact statement (2023-2027)

By 2027, the ECCC and the Network will have funded European SMEs in developing and using strategic cybersecurity technologies, services and processes through a coordinated cascade funding mechanism via NCCs and national co-financing that lowers the application threshold for SMEs.

Actions

Processes and tools for managing cybersecurity information and risk management

- Technologies, services and processes supporting information sharing, prevention, detection and response/recovery and investigation of cybersecurity incidents.
- Awareness raising and vulnerability management, development of CVD
- Innovative modelling and simulation solutions
- Accessible and user-friendly cybersecurity tools for SMEs

Secure and resilient hardware and software systems

- Increase the resilience of essential and important entities defined in NIS2
- Automation tools for cybersecurity processes/ AI-based cybersecurity solutions
- Security and privacy ‘by design’
- Post-quantum cryptography in secure products and services

Second impact statement

By 2027, the ECCC and the Network will have supported and grown the cybersecurity professional workforce in both quantity and quality through the standardisation and certification of cybersecurity skills and investments in education and training of cybersecurity professionals.

Actions

- ***Development of cybersecurity skills: education and professional training***
  - educational curricula aligned with the needs of the market, the public sector,
  - common tools and platforms for hands-on technical education, training and testing opportunities
  - campaigns for cybersecurity career path development
  - security and privacy ‘by design’ approach in training and education
  - awareness of cybersecurity threats
- ***Cybersecurity skills framework and competence assessment***
  - Adoption and implementation of cybersecurity skills frameworks, including the European Cybersecurity Skills Framework (ECSF).
  - Competence assessment and certification schemes

Third impact statement

By 2027, the ECCC and the Network will have strengthened the research, development and innovation expertise and competitiveness of the EU cybersecurity community through the development and implementation of an efficient and coherent action plan.

Actions

- *Promoting post-quantum cryptography standardisation and adoption*
- *Support for European Cybersecurity Certification*
- *Strengthening market competitiveness*
- *Promoting collaboration and information sharing*

Solidarity Act - draft

- Pan European infrastructure of national and cross border SOC
- **Cyber Emergency Mechanism**:
  - Strengthen preparedness by testing entities in highly critical sectors (healthcare, transport, energy, etc.) for potential vulnerabilities.
  - EU Cybersecurity Reserve - incident response services from trusted providers ready to intervene, at the request of a Member State, in case of significant and large-scale cybersecurity incidents.
  - Financial support for mutual assistance between Member States
- **Cybersecurity Incident Review Mechanism**

Cybersecurity Skills Academy

A single point of entry for cybersecurity education& training offers and funding opportunities (virtual platform)

4 pillars

- Stimulating **stakeholders to take action**
- Better channelling & visibility for **funding opportunities**
- Fostering **knowledge generation** through education & training
- Defining indicators to **monitor market evolution** and assessing effectiveness for the skilling of cybersecurity professionals

First a virtual single entry point via the Commission’s Digital Skills and Jobs Platform…

… then, possibly as a European digital infrastructure consortium (EDIC)

Skills Academy – role of NCC

- Contribute to the **European Cybersecurity Skills Framework** reviews
- Explore setting up national **Cyber Campuses/Academies**
- Support ENISA in **mapping** of education institutions providing cyber programmes and development of **repositories** on trainings and certifications
- Gather information on **how EU funds are used** to finance cybersecurity skills, assess the effectiveness of funding

Skills Academy – role of NCC

- Provide guidance on **actions to be financed** to better address the cyber skills gap
- Provide feedback on **draft indicators** to be designed by ENISA with the NIS CG and the EC
- Support the **collection of data** following the definition of indicators
- Support **ENISA in defining KPIs** for cybersecurity professionals
- Contribute to the Digital Skills and Jobs Platform, relay messages to industry(pledges) and national actors

Thank you for attention