EU Cybersecurity

24 January 2019
Brussels

Jakub Boratynski
Head of Unit
DG CONNECT – H2 Cybersecurity & Digital Privacy Policy
European Commission

NIS Directive
The First EU Cybersecurity Law

Boosting the overall cybersecurity in the EU

- Increased national cybersecurity capabilities
- EU level cooperation (NIS Cooperation Group)
- Security & Notification requirements
- National Cybersecurity Strategies
- National Computer Security Incident Response Teams (CSIRT Network)

State of play :

24 Member States notified full transposition.

2 Member states notified partial transposition.

Ongoing identification of Operators of Essential Services

Next? Monitoring of implementation process followed by in-depth checks.

Cybersecurity Act
EU Cybersecurity Agency (ENISA)

What's new?

- Permanent Status
- Adequate Resources
- Focused Mandate

Mandate & Objectives - Contribute to high Cybersecurity

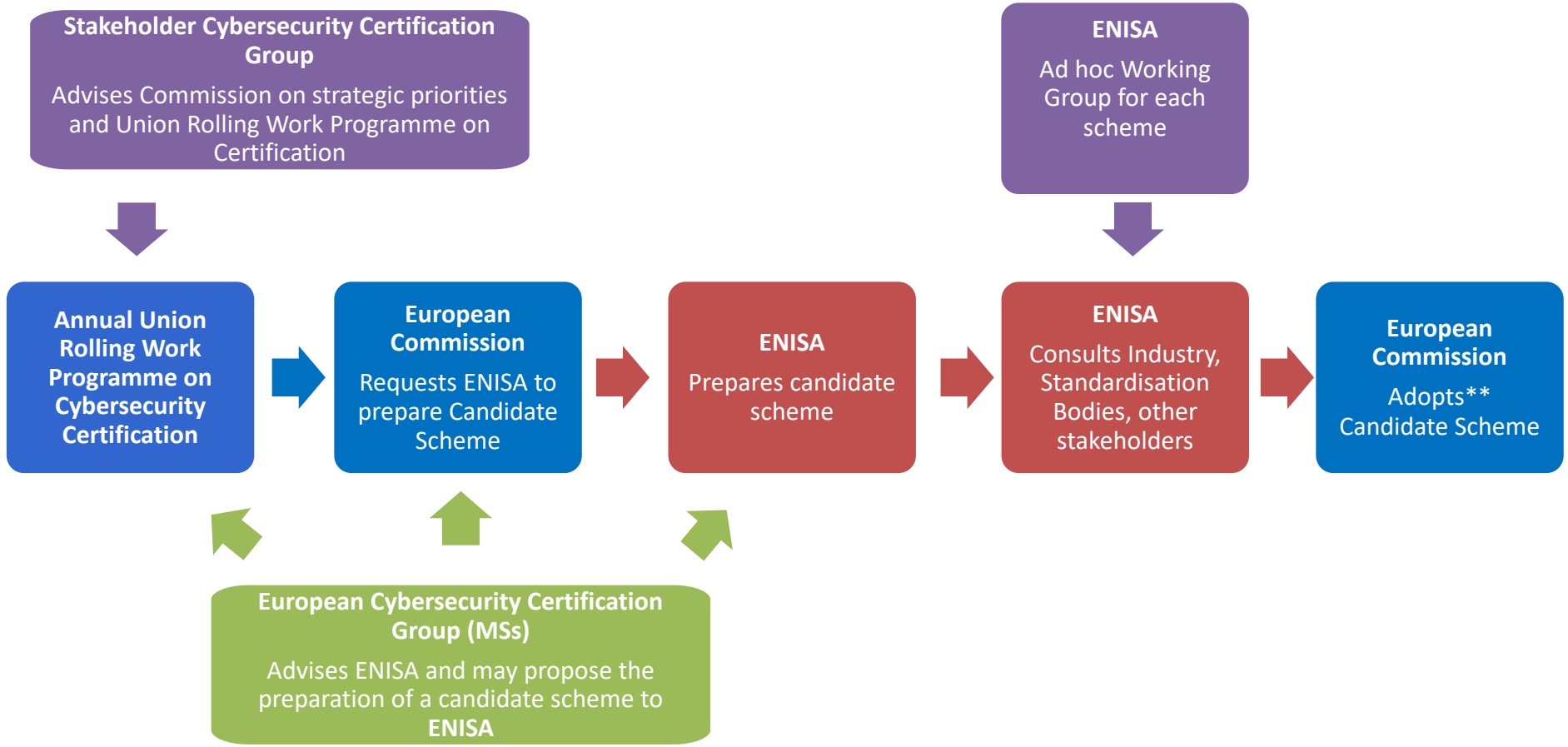
- Promote the use of certification & contribute to the cybersecurity certification framework
- Be an independent center of expertise
- Assist EU Institutions and MSs in policy Development & implementation
- Support capacity building & preparedness
- Promote high level of awareness of citizens & businesses
- Promote cooperation & coordination at Union level
- Increase cybersecurity capabilities at Union level to complement MSs action

Cybersecurity Act
EU Cybersecurity Certification Framework

Some key elements

- EU Cybersecurity Agency (ENISA)
- Member State involvement - European Cybersecurity Certification Group (ECCG)
- Stakeholders' involvement – Stakeholder Cybersecurity Certification Group (SCCG)
- Union rolling work programme for European Cybersecurity Certification
- Voluntary certification schemes throughout the EU.
- Independent assessment of the schemes.

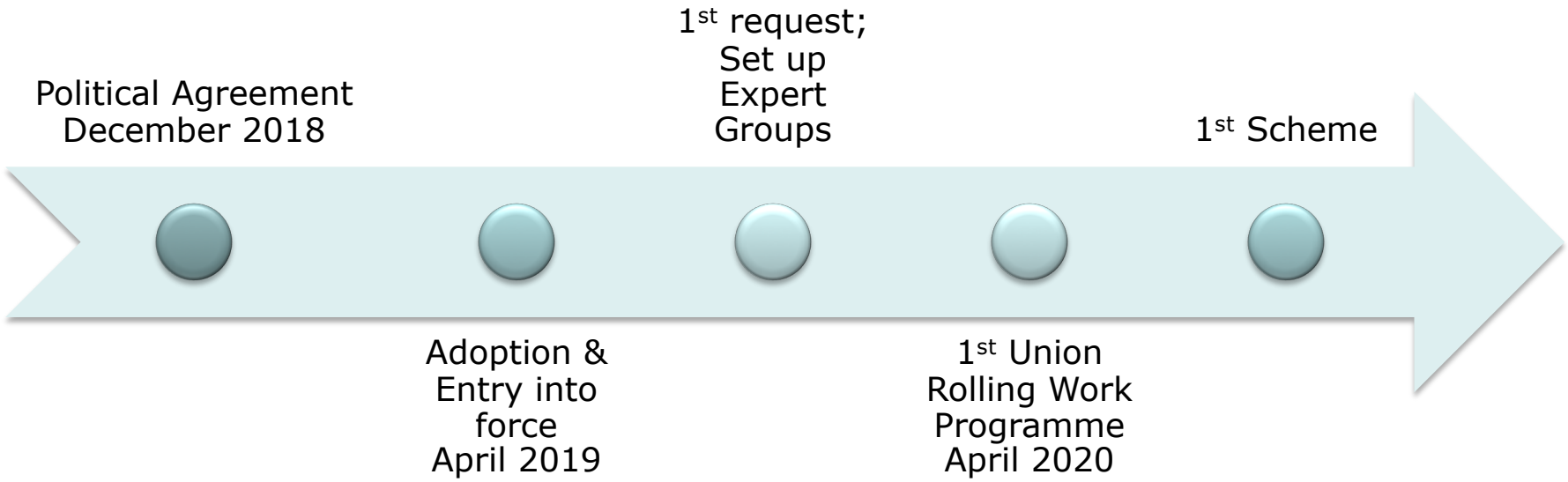
How: Establishment of an EU Cybersecurity Certification Scheme*



* subject to final political agreement

** "better regulation" + Commitology

State of Play and Timeline



European Cybersecurity Industrial, Technology & Research Competence Centre
&
Network of National Coordination Centres

Cybersecurity Package Commitment

EUROPEAN COMMISSION

Brussels, 13.9.2017

JOIN(2017) 450 final

JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

Resilience, Deterrence and Defence: Building strong cybersecurity for the EU

The EU has added value to provide, given the sophistication of cybersecurity technology, the large-scale investment required, and the need for solutions that work across the EU.

Building on the work of Member States and the Public-Private Partnership reinforce EU cybersecurity capability through a network of cybersecurity competence centres with a European Cybersecurity Research and Competence Centre at its heart.

This network and its Centre would stimulate development and deployment of technology in cybersecurity and complement the capacity building efforts in this area at EU and national level.

The proposal in a nutshell

European Cybersecurity Technology & Innovation Ecosystem

European Competence Centre:

- manage the funds foreseen for cybersecurity under Digital Europe and Horizon Europe 2021-2027
- facilitate and help coordinate the Network and Community to drive the cybersecurity technology agenda
- support joint investment by the EU, Member States and industry and support deployment of products and solutions.

Network of National Coordination Centres:

- Nominated by Member States as the national contact point
- Objective: national capacity building and link with existing initiatives
- National Coordination Centres may receive funding
- National Coordination Centres may pass on financial support

Competence Community:

- A large, open, and diverse group of cybersecurity stakeholders from research and the private and public sectors, including both civilian and defence sectors

The Competence Centre – what will it do?

Facilitate and help coordinate the work of the Network

Implement cybersecurity parts of Digital Europe and Horizon Europe Programmes

Enhance cybersecurity capabilities, knowledge and infrastructures

Contribute to the wide deployment of state-of-the-art products and solutions; support SMEs

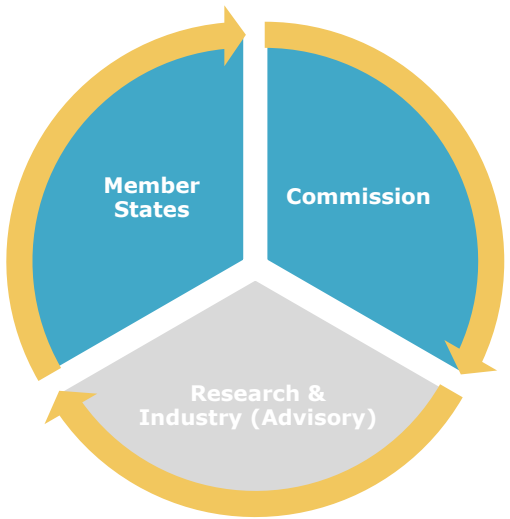
Contribute to reducing cybersecurity skills gaps

Support cybersecurity research and development

Enhance cooperation between the civilian and defence spheres with regard to dual use technologies

Enhance synergies in relation to the European Defence Fund

The Competence Centre – governance



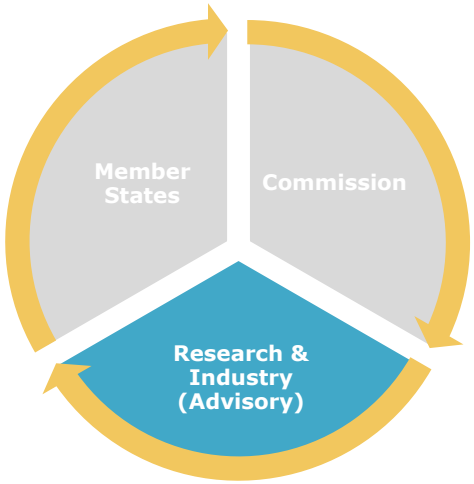
Governing Board:

- **1 representative of each Member State** (+alternate) with cybersecurity knowledge and managerial skills
- **5 representatives of the Commission**
- **Renewable term of 4 years**
- **Observers admitted** (ENISA as a permanent observer)
- **Executive Director** chosen for 4 years (renewable once)

Voting Rules:

- **Union** holds **50% of voting rights**
- **Every participating Member State = 1 vote**
- Decisions taken by a **majority of at least 75% of all votes,** representing **at least 75% of the total financial contributions** to the Competence Centre.
- **The Chairperson takes part in the voting**.

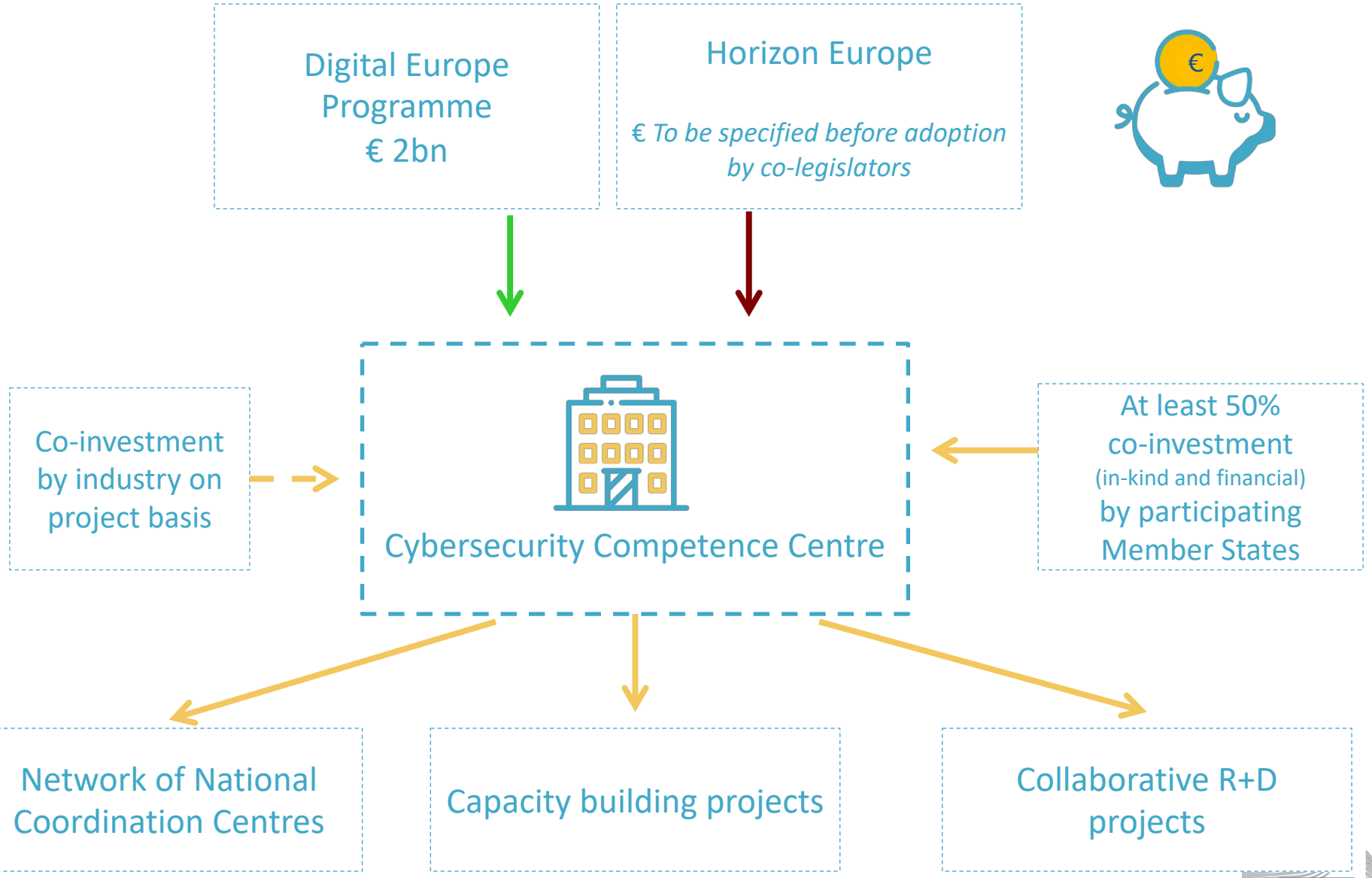
Industrial & Scientific Advisory Board



- **16 members** appointed by the Governing Board from among the representatives of the entities of the Competence Community
- **Expertise** in cybersecurity research, industrial development, professional services or deployment
- **Investment of cPPP experience**
- **3 years' renewable** term
- **Commission** and **ENISA** participates in the works of the Advisory Board
- Meets at least 2 x year
- **Tasks:**
  - Advises on establishing working groups
  - Organises public consultations and provides input for drafting the work plan & multi-annual strategic plan
  - promotes and collects feedback on the work plan and multi-annual strategic plan of the Competence Centre.

Financing of the initiative

2021-2027 proposed EU cybersecurity funding sources



Next Steps

By Q2/2019

Finalise negotiations

2019-2020

Preparatory Phase

2020

Prepare to launch 2021 actions

Thank you for your attention!