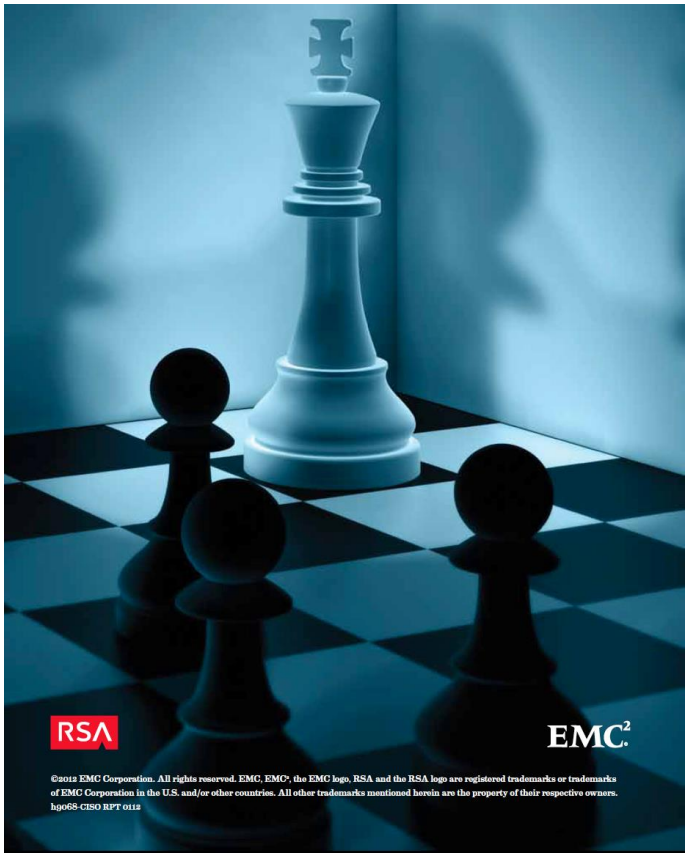
Cyber Threat Intelligence: a key enabler for building strong cybersecurity for the EU

5 November 2018
Brussels

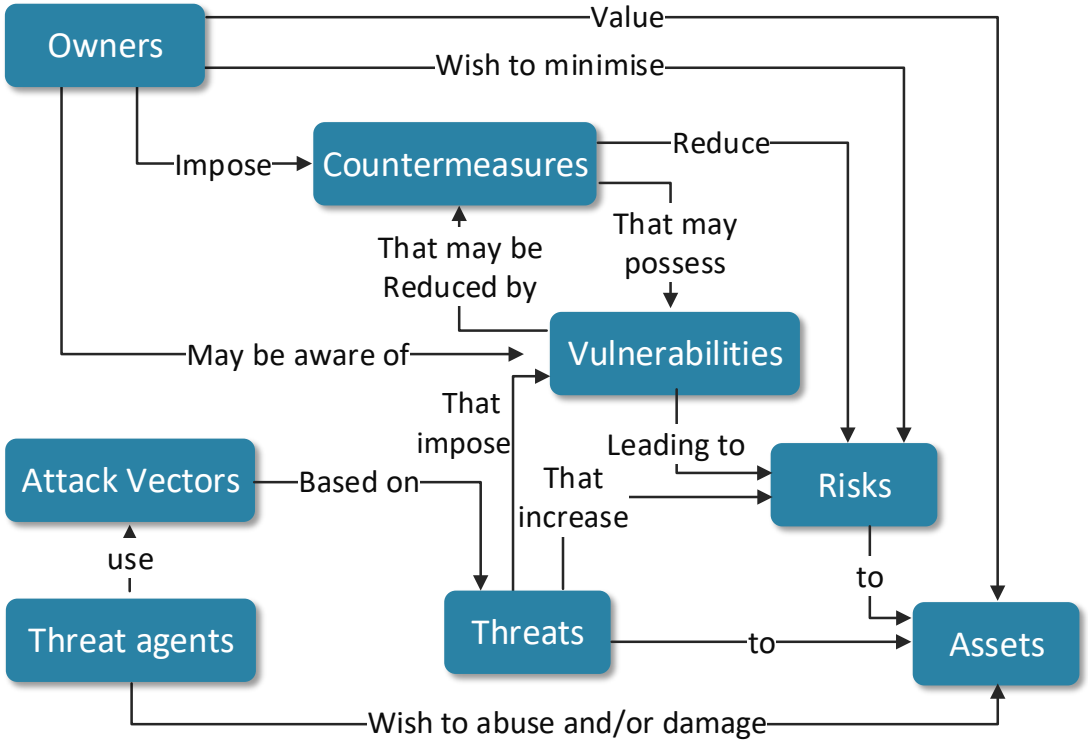
Ioannis Askoxylakis
Cybersecurity Policy Officer
Unit H1: Cybersecurity Technology & Capacity Building
Directorate H: Digital Society, Trust and Cybersecurity
Directorate General for Communication Networks, Content & Technology
DG CONNECT
European Commission

Emerging threat landscape

- **Open hyperconnected world**
  - **IoT**
  - **Cloud computing**
  - **Social networking**
  - **Fast adoption of ICT by consumers**
- **Adversaries are:**
  - **taking advantage at Gaps in Security**
  - **moving faster**
  - **better coordinated**
  - **easily penetrating traditional perimeter defenses**
  - **developing intelligence**



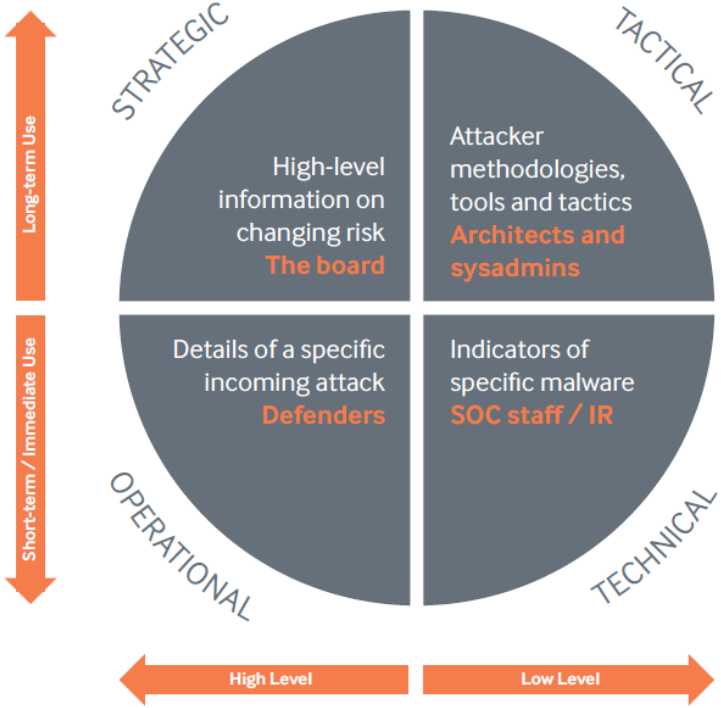
Cybersecurity landscape



European Commission

Emerging threat landscape

Emerging threat landscape



https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/MWR_Threat_Intelligence_whitepaper-2015.pdf

Cyber Threat intelligence at a glance

Developing real-time knowledge on threats and the organization's posture against those threats in order to prevent, detect and/or predict attacks, make informed risk decisions, optimize defensive strategies and enable action.

Roadmap to Cyber Threat Intelligence

1. **START WITH THE BASICS**
   - Inventory of strategic assets
   - Incident response process
   - Risk assessment

2. **MAKE THE CASE**
   - The value proposition
   - Key stakeholders
   - Opportunities for “quick wins”

3. **FIND THE RIGHT PEOPLE**
   - Train existing
   - Hire skilled

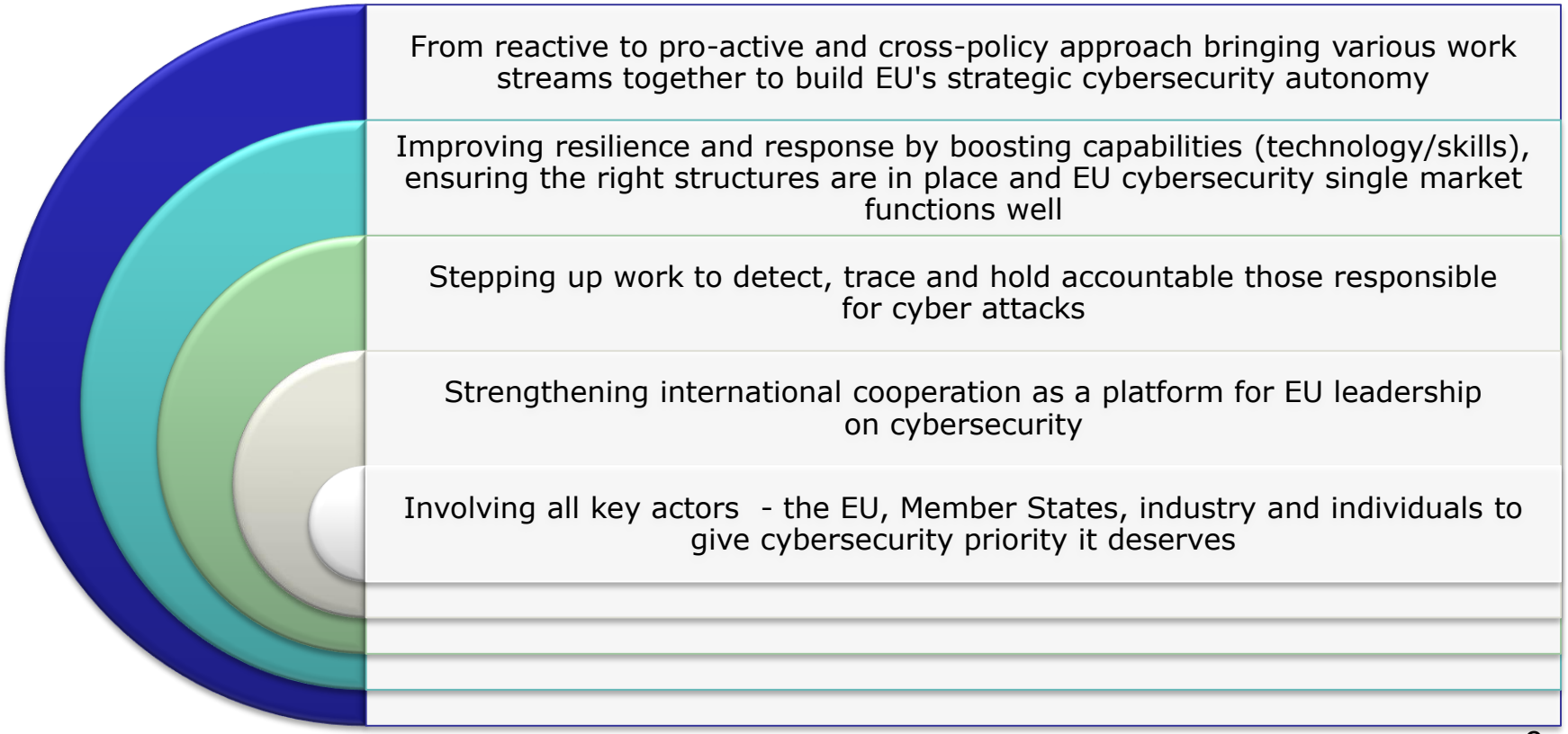
4. **BUILD SOURCES**
   - Evaluation
   - Cost
   - Relationships

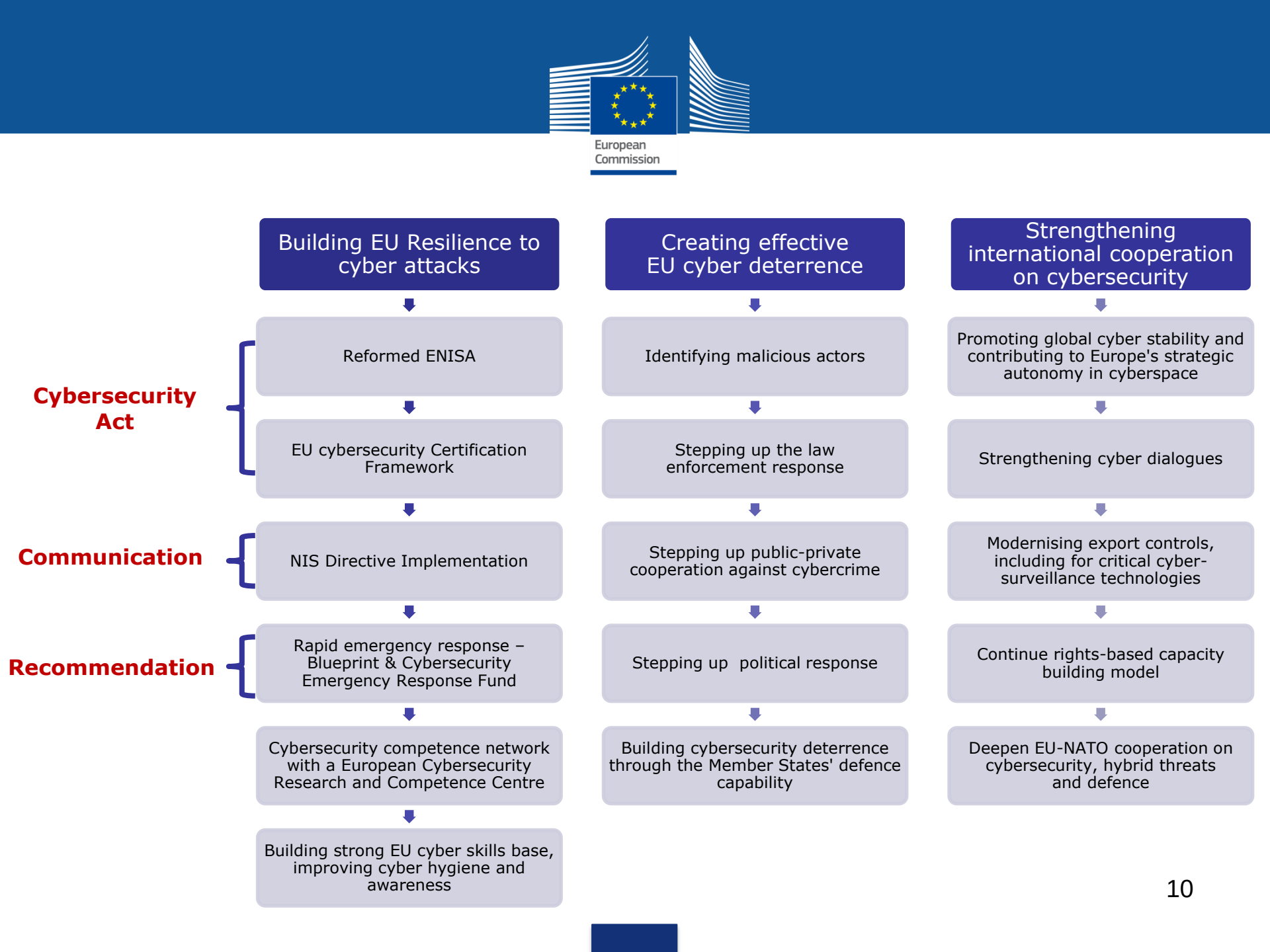
5. **DEFINE A PROCESS**

6. **IMPLEMENT AUTOMATION**
   - Consumption of threat feeds
   - Collections of employees observations
   - Log analysis and full packet capture
   - Fusion of data from multiple sources

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

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




European Commission
Building EU Resilience to cyber attacks
Creating effective EU cyber deterrence
Strengthening international cooperation on cybersecurity
Cybersecurity Act
Reformed ENISA
EU cybersecurity Certification Framework
Communication
NIS Directive Implementation
Recommendation
Rapid emergency response – Blueprint & Cybersecurity Emergency Response Fund
Cybersecurity competence network with a European Cybersecurity Research and Competence Centre
Building strong EU cyber skills base, improving cyber hygiene and awareness
Identifying malicious actors
Stepping up the law enforcement response
Stepping up public-private cooperation against cybercrime
Stepping up political response
Building cybersecurity deterrence through the Member States' defence capability
Promoting global cyber stability and contributing to Europe's strategic autonomy in cyberspace
Strengthening cyber dialogues
Modernising export controls, including for critical cyber-surveillance technologies
Continue rights-based capacity building model
Deepen EU-NATO cooperation on cybersecurity, hybrid threats and defence

European Commission

STATE OF THE UNION 2018

Building strong cybersecurity in Europe

#SOTEU

'Cyber-attacks know no borders, but our response capacity differs very much from one country to the other, creating loopholes where vulnerabilities attract even more the attacks. The EU needs more robust and effective structures to ensure strong cyber resilience and respond to cyber-attacks. We do not want to be the weakest links in this global threat.'

Jean-Claude Juncker, Tallinn Digital Summit, 29 September 2017

European Commission

Blueprint

Resilience through crisis management and rapid emergency response

Improving resilience through crisis management and rapid emergency response – with a focus on Response

Improving resilience through crisis management and rapid emergency response - 2 lines of actions

1. **Blueprint** - Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises (COM(2017) 6100).

2. **ENISA** (COM(4776/2)) - Tasks relating to operational cooperation at Union level
   - The Agency shall contribute to develop a cooperative response, at Union and Member States level, to large-scale cross-border incidents or crises related to cybersecurity

Blueprint – Core objectives

Blueprint – Cooperation at all levels

Technical

- Incident handling during a cybersecurity crisis.
- Monitoring and surveillance of incident including continuous analysis of threats and risk.

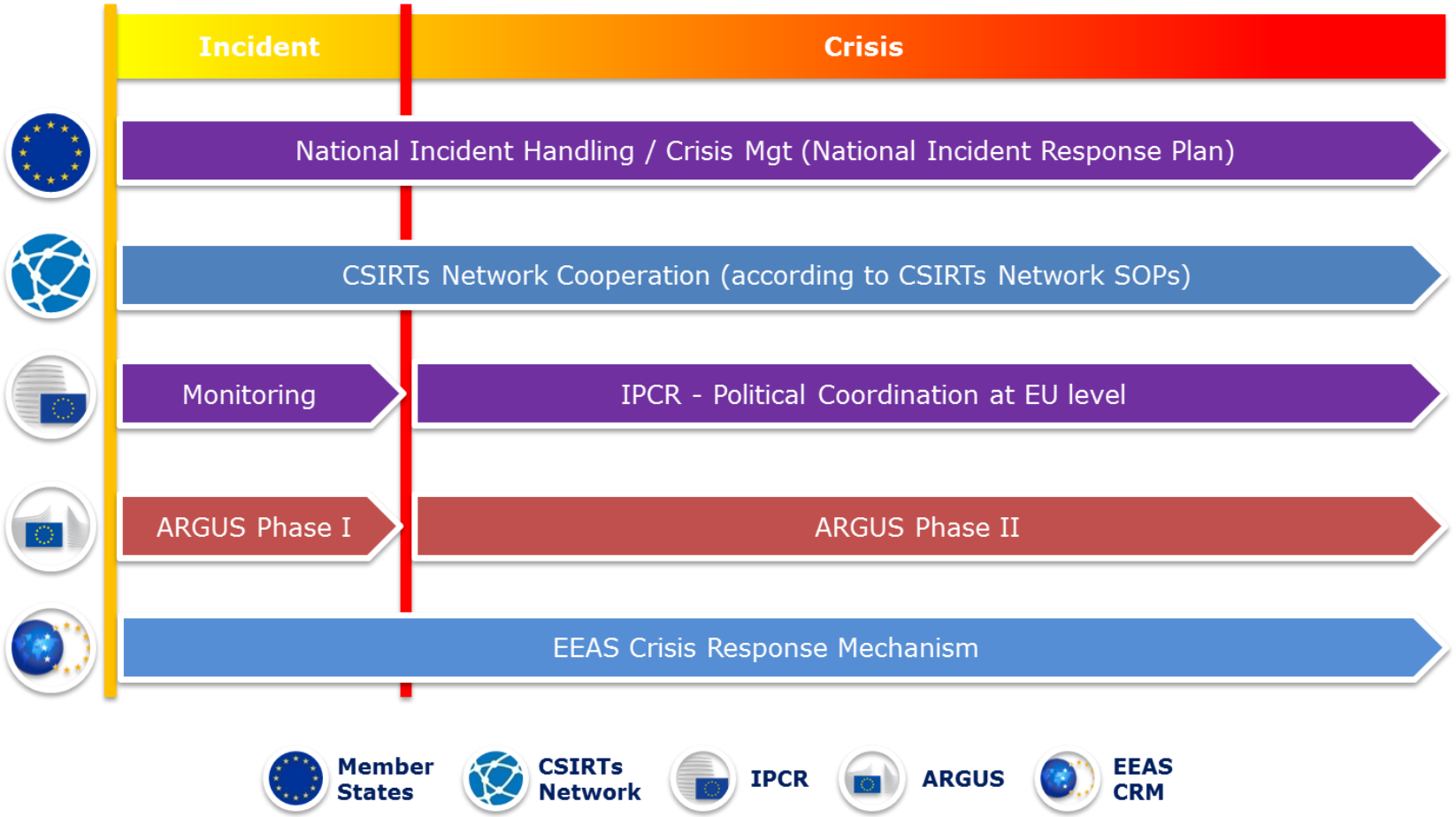
Operational

- Preparing decision-making at the political level.
- Coordinate the management of the cybersecurity crisis (as appropriate).
- Assess the consequences and impact at EU level and propose possible mitigating actions.

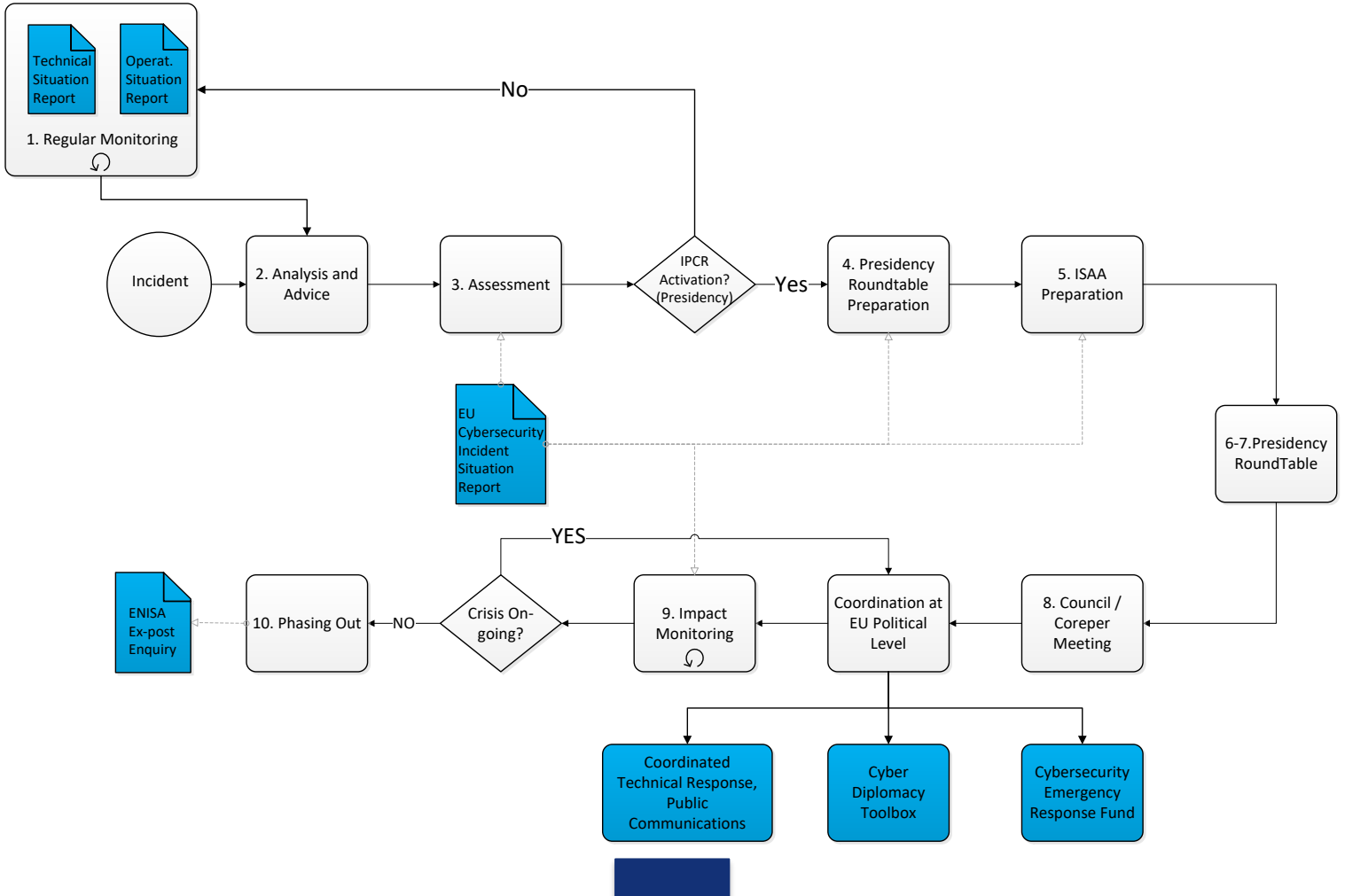
Political / Strategic

- Strategic and political management of both cyber and non-cyber aspects of the crisis including measures under the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities

Blueprint – key mechanisms



Blueprint – cybersecurity integration in IPCR arrangements



Blueprint – The way forward

- Establish an EU Cybersecurity Crisis Response Framework
  - standard operating procedures
  - information sharing and cooperation protocols

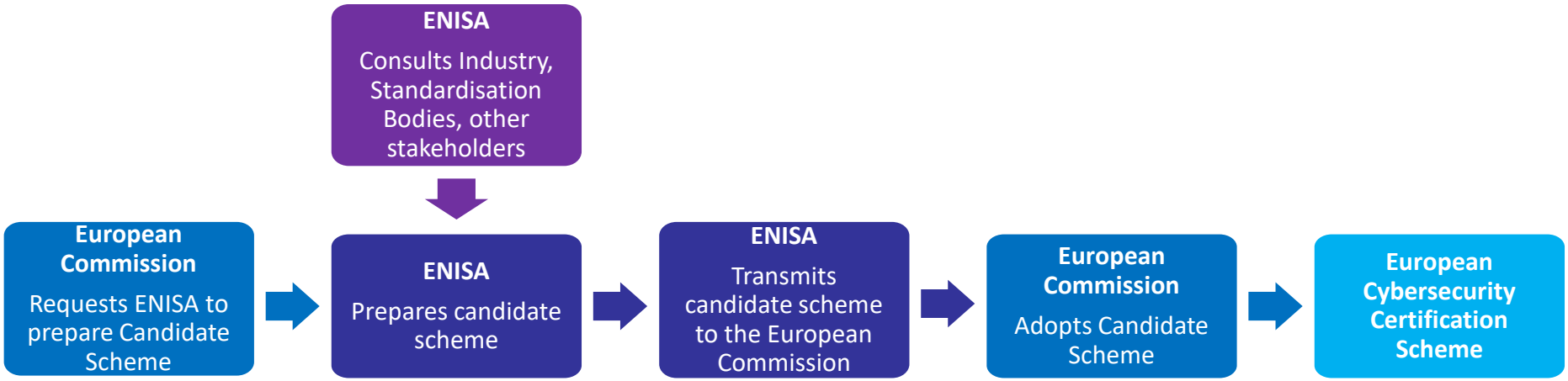
- Ensure that National Crisis Management mechanisms adequately address cybersecurity incident response as well as provide necessary procedures for cooperation at EU level within the context of the EU Framework.

- Develop and adopt a common taxonomy and template for situational reports describing the technical causes and impacts of cybersecurity incidents.

- Test in the context of the *E-Pace* exercise.

ICT cybersecurity certification

Towards a true cybersecurity single market in the EU



Establishment of an EU Cybersecurity Certification Scheme (COMM proposal)

Priority areas identified in the Communication

Internet of Things

Use of "security by design" methods in low-cost, digital, interconnected mass consumer

Security in critical or high-risk applications

From our cars to the machinery in factories, from the largest of systems such as airplanes or power plants to the smallest such as medical devices

Widely-deployed digital products, networks, systems and services

Used by private and public sector alike to defend against attacks– such as email encryption, firewalls and Virtual Private Networks

Horizon Scanning Capability

ET² (Emerging Technologies-Emerging Threats)

Sectoral approach & analysis (thematic ETLs)

Post-incident analysis (NIS) for CTI

Scenario building for complex intersectoral emerging threats

Exercises

European Commission

Thank you for your attention!