CYBER CRISIS MANAGEMENT IN THE EUROPEAN UNION

Module DI.CYBER.1

Rosaria Talarico
Cosimo Melella

MODULE OUTLINE

Topic 1: Relevant Legislation

- Network and Information Systems 2 (NIS2), Cyber Resilience Act (CRA), Cyber Solidarity Act (CSOA)

Topic 2: What Constitutes a Crisis?

- Incident vs. Large-scale Incident vs. Crisis; impact – entities and services affected

Topic 3: The New European Cyber Blueprint

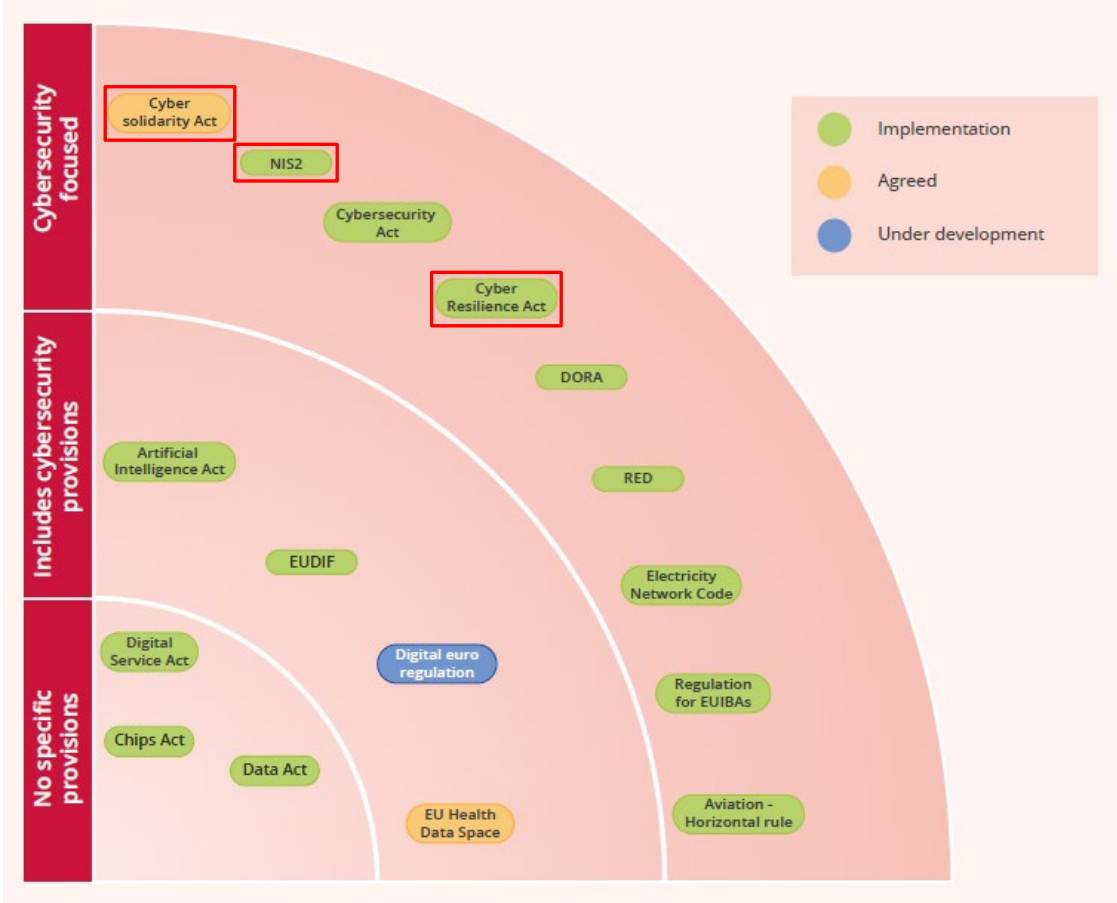
- Technical (CSIRTs), Operational (ENISA/EU-CyCLONe/Cyber Hubs), Strategic (IPCR)

RELEVANT LEGISLATION

Network and Information Systems 2 (NIS2)

Cyber Resilience Act (CRA)

Cyber Solidarity Act (CSOA)



NIS2 (2022)

Formalises CyCLONe and strengthens CSIRTs Network

Mandates national authorities and crisis response plans

Imposes incident notification and reporting obligations on MS and 18 sectors

CYBER RESILIENCE ACT (2024)

Common cybersecurity requirements for products with digital elements

Obligations to report severe cybersecurity incidents

Instructs ENISA to set up a Single Reporting Platform

CYBER SOLIDARITY ACT (2025)

AI-enabled cross-border SOCs or Cyber Hubs

Cybersecurity Emergency Mechanism

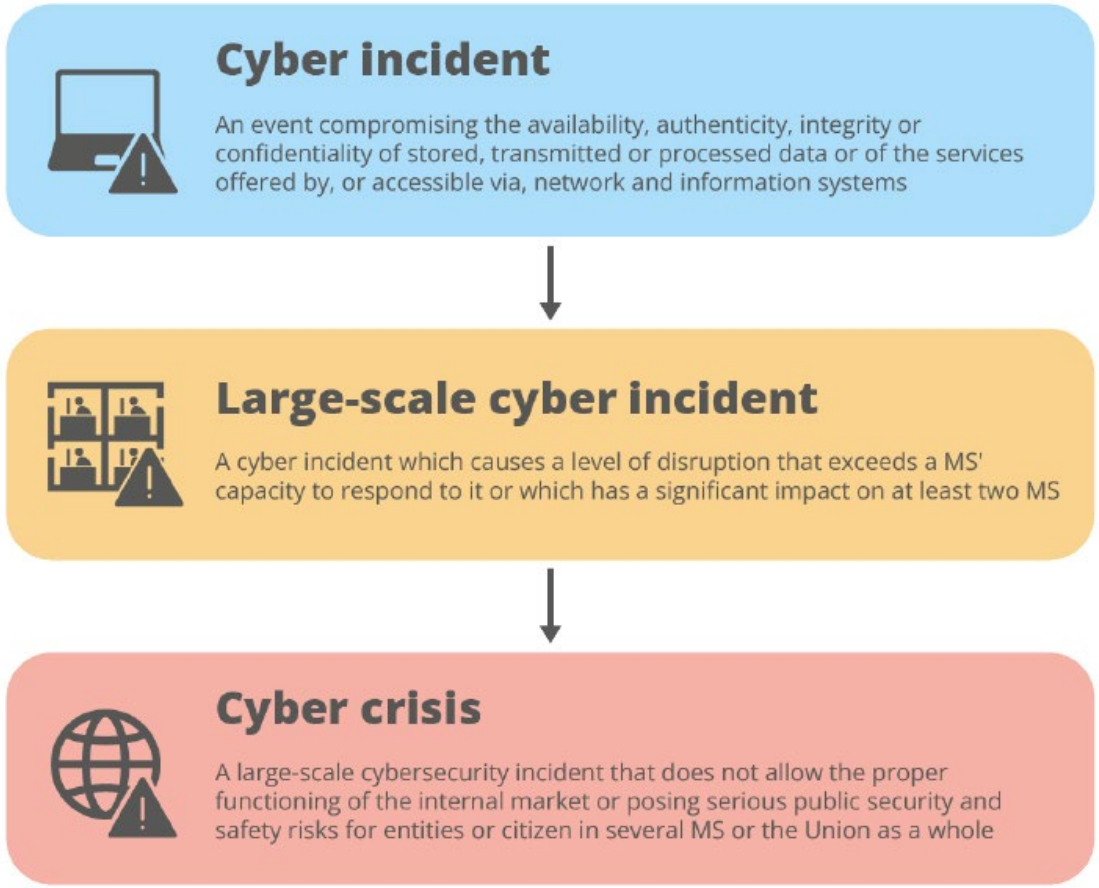
Cybersecurity Incident Review Mechanism to capture lessons learned

WHAT CONSTITUTES A CRISIS?

Transition to crisis status is a political decision

A cyber crisis is a level 4 systemic event with union-wide consequences.

Severity levels are based upon impact, determined by #entities and criticality of services (essential, important) affected.



EXAMPLE: WANNACRY

EU CyberNet

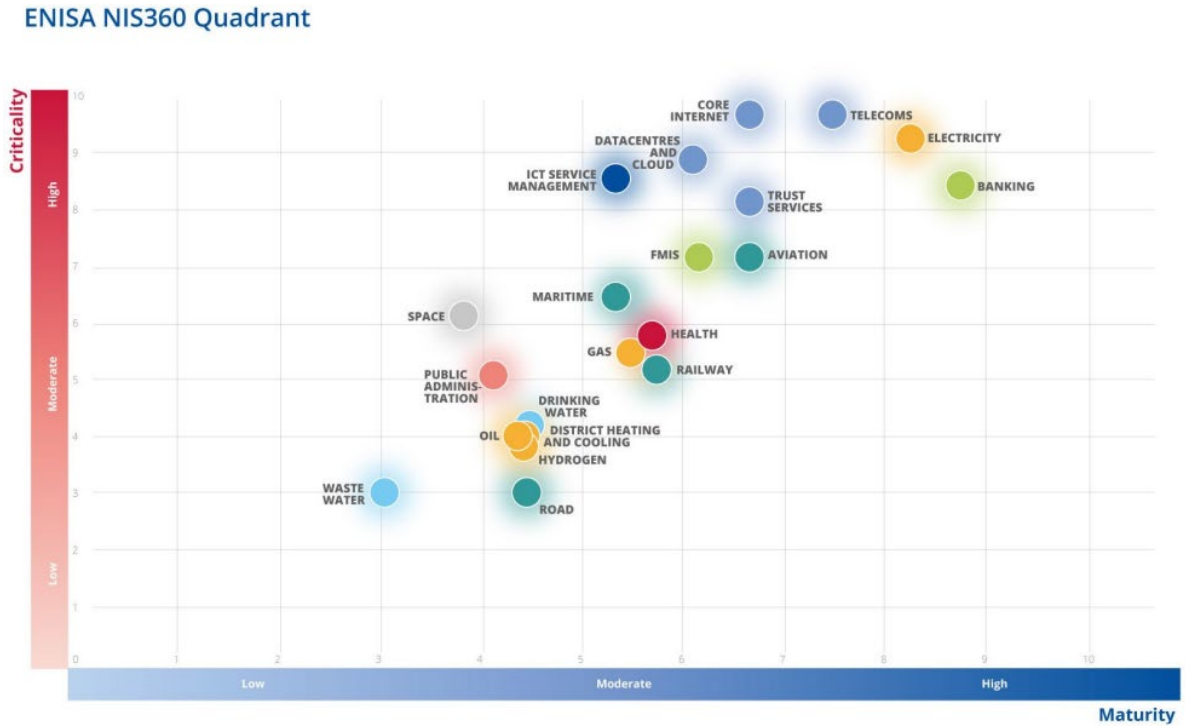
May 2017 first case of cooperation at EU level

Considered a large-scale creeping cybersecurity incident

Not elevated to the status of crisis

SEVERITY LEVELS

Level 0 – Normal: No incident; standard monitoring.
Level 1 – Low: Minor localised incident, no cross-border effects.
Level 2 – Moderate: Limited cross-border or cross-sector impact; information-sharing initiated.
Level 3 – High: Major incident affecting multiple Member States or critical functions; operational coordination triggered via EU-CyCLONe.
Level 4 – Crisis: Systemic event with Union-wide consequences; strategic coordination via IPCR mechanism.



THE EUROPEAN RESPONSE STRUCTURE

EU CyberNet

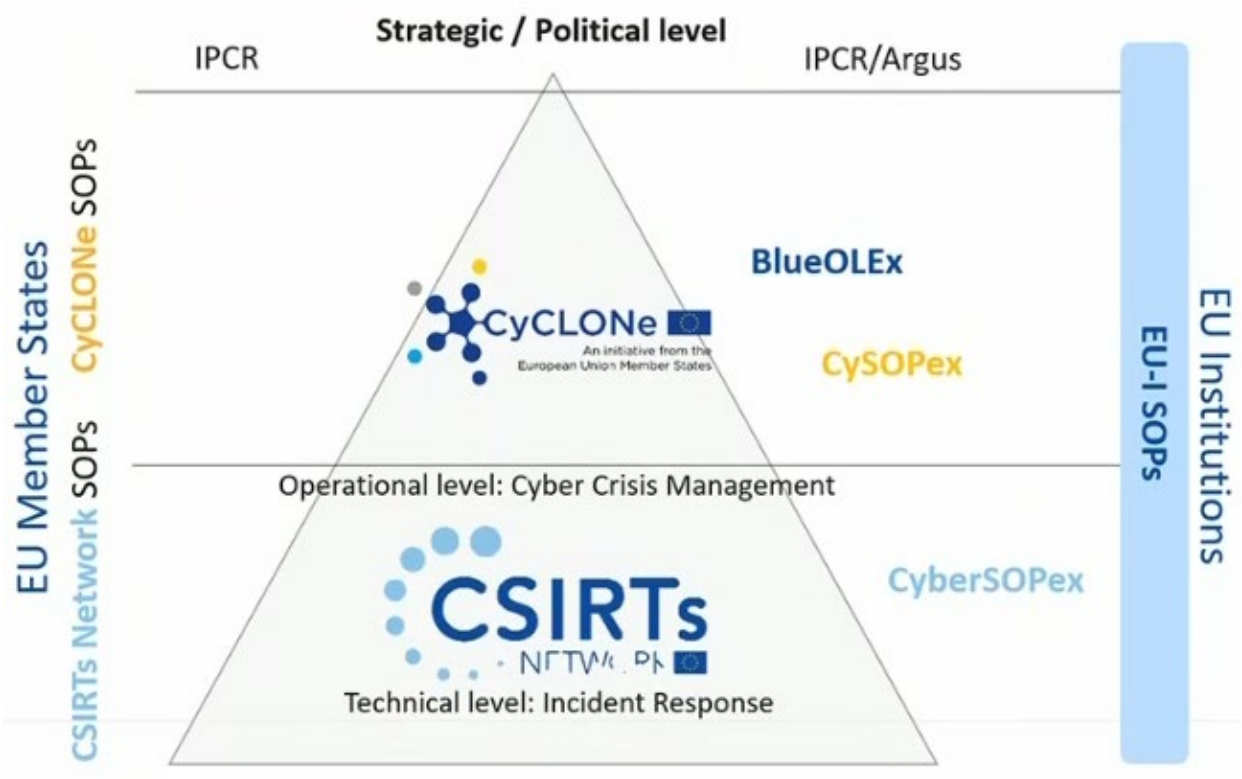
IPCR: Integrated Political Crisis

ARGUS: EU Commission's general rapid alert system

CyCLONe: EU Cyber Crises Liaison Organisation Network

CSIRTs : Computer Security incident Response Teams

SOP: Standard Operating Procedure



Courtesy of Rossella Mattioli

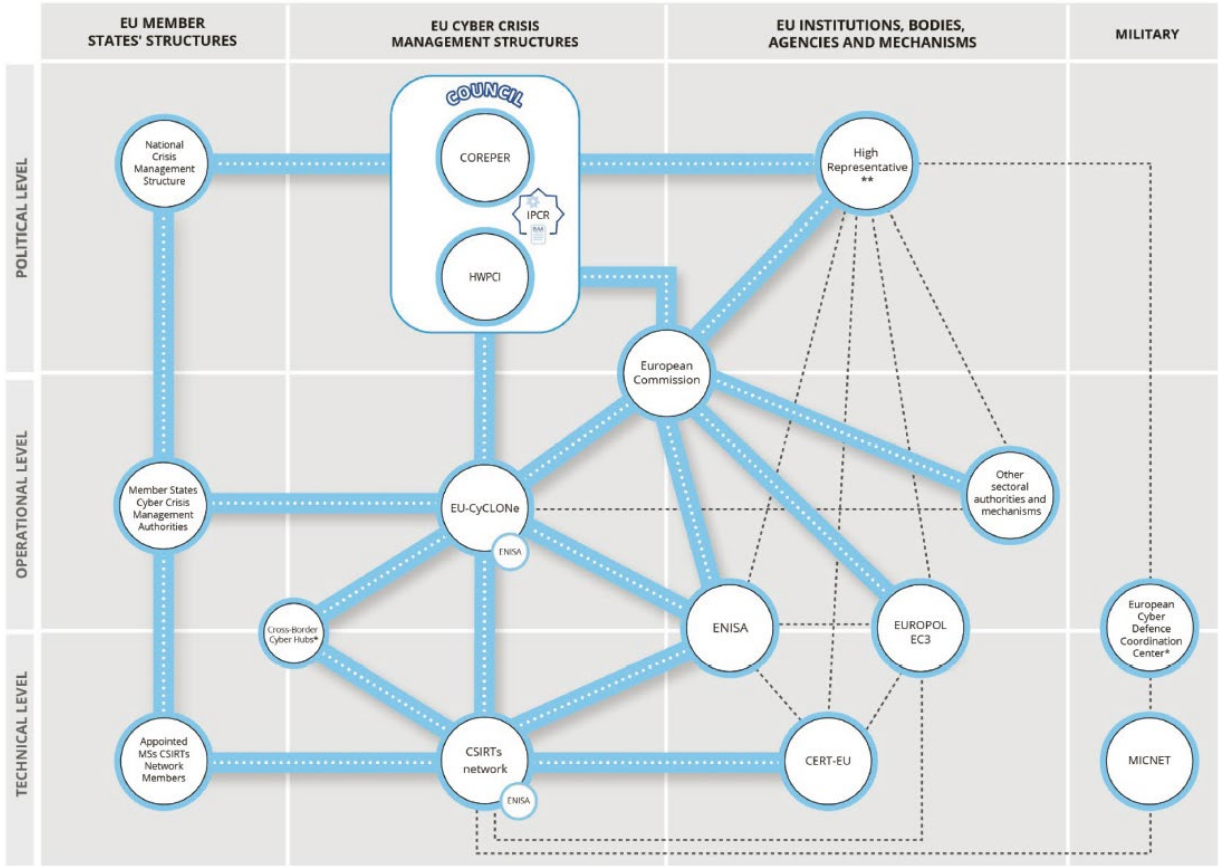
NEW EUROPEAN CYBER BLUEPRINT (2025)

EU CyberNet

Harmonises operational architecture for cyber crisis management

EU-CyCLONe manages the interface between the technical and political levels

The Rolling Annex evolves as new incident types and tools emerge



INTEGRATED CRISIS RESPONSE

Cyber Diplomacy Toolbox

FIMI Toolbox

Hybrid Toolbox

EEAS Crisis Response Mechanism

Emergency Response Coordination Centre

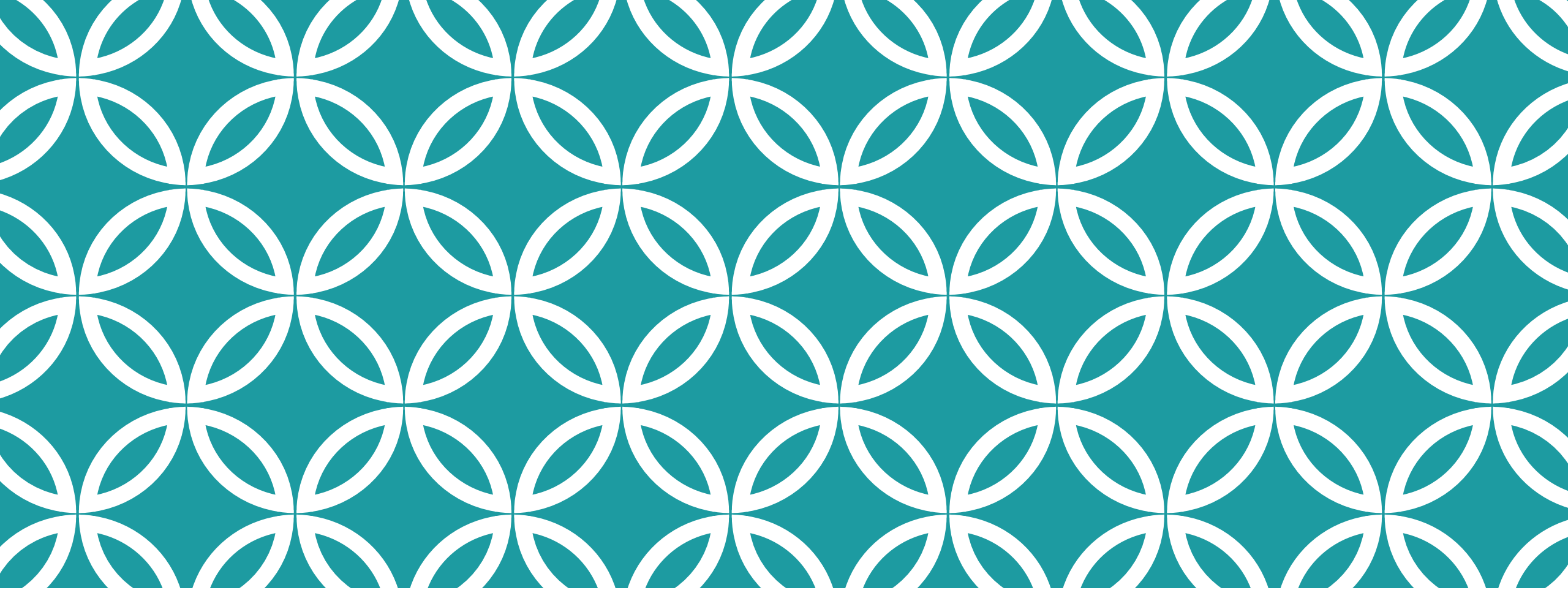
MODULE: QUIZ

1. That are the most important EU laws pertaining to cyber crisis management?

2. What is the difference between a large-scale incident and a crisis?

3. Which crisis management network is the interface between the political and technical levels?

4. Which European instrument brings all the important elements of cyber crisis management together?



BACKUP

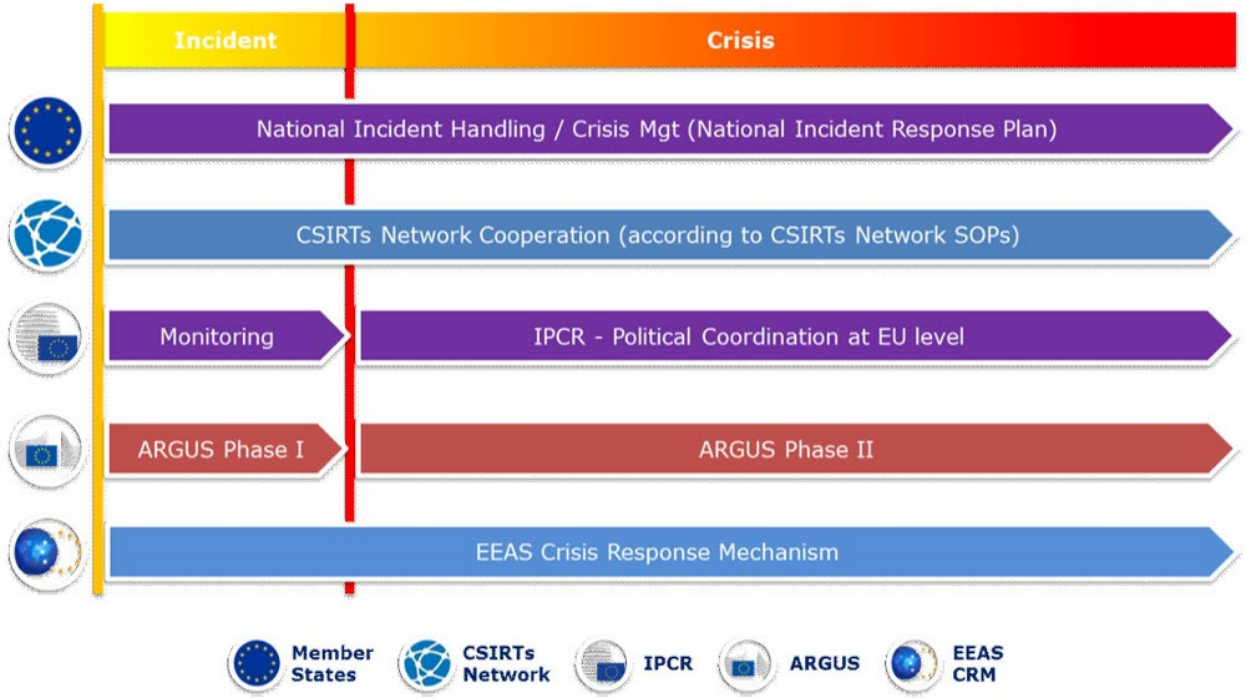
Just in case

EU BLUEPRINT 2017

Political coordination via IPCR

Coordination within the Commission uses ARGUS rapid alert system.

If crisis entails important external or Common Security and Defence Policy dimension the EEAS CRM is activated.



2017 IPCR CYBER PROCESS

Monitor, analyse, advise

Activate IPCR

Screate stuation reports, exchange information

Prepare Presidency and CoReper/Council

CoReper/Council decisions

Monitor impact

Phase out