

Slide 1



## MODULE OUTLINE



### Topic 1: Relevant Legislation

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

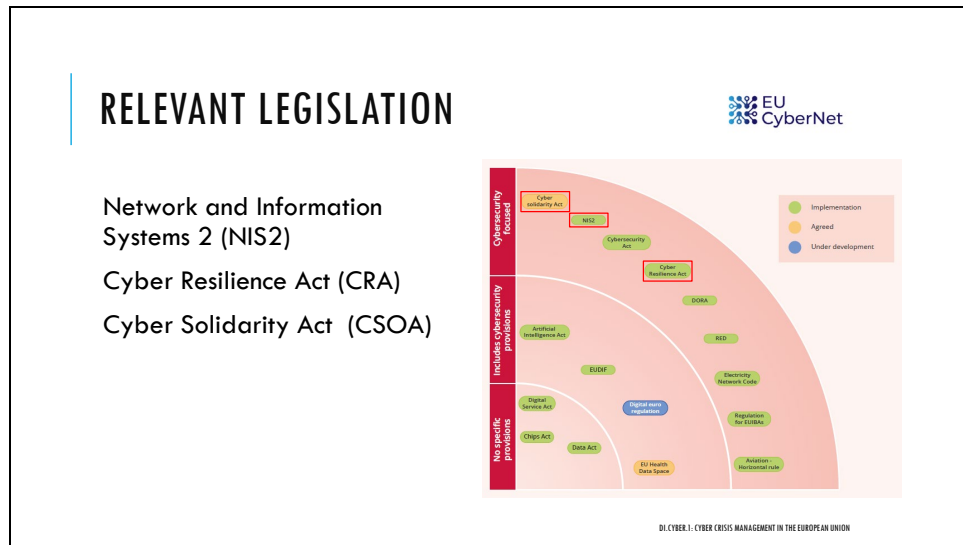
### Topic 2: What Constitutes a Crisis?

- 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)

## Slide 3




There are a plethora of regulations relevant to cybersecurity incidents and crises. The slide highlights the most important three.  
The new EU Cyber Blueprint takes account of the latest legislation and weaves the requirements from the different regulations together.

### References

<https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union>

## 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



EU CyberNet

DL CYBER.1: CYBER CRISIS MANAGEMENT IN THE EUROPEAN UNION

In 2022 NIS2 was adopted, including provisions covering cyber crisis management at the levels of the EU and MSs, and involving specific organisations such as important and essential entities. In particular, NIS2:

- Formalises the establishment of a European cyber crisis liaison organisation network (EU-CyCLONe) to support the coordinated management of large-scale cybersecurity incidents and crises at operational level, and strengthens the role of the CSIRTs Network, composed of CSIRTs appointed by EU MSs and tasked, among other things, to promote swift and effective operational cooperation among them;
- Mandates the designation of national authorities responsible for the management of large-scale cybersecurity incidents and crises and the adoption of national large-scale cybersecurity incident and crisis response plans;
- Mandates MSs to entities take appropriate and proportionate technical, operational and organisational measures, including on crisis management that is essential and important.

NIS2 imposes legal obligations on entities across 18 sectors of the economy, including in terms of security requirements and the notification of incidents. It requires Member States to increase preparedness with, for instance, extended prerogatives and missions for Computer Security Incident Response Teams (CSIRTs) and competent authorities. The NIS2 Directive also promotes cooperation among all Member States by continuing and strengthening the Cooperation Group set up originally under the NIS Directive to support and facilitate strategic cooperation and the exchange of information among Member States.

The NIS2 Directive outlines obligations for national-level cooperation, applying to competent authorities, single point of contacts (SPOCs), and CSIRTs (hereby referred to as 'NIS2 entities'). They are expected to cooperate among themselves and also, to various degrees, with the authorities responsible for specific domains, e.g. those competent for the financial sector under DORA.

One of the most prominent areas of information sharing concerns cybersecurity incidents. The implementation of reporting provisions relies on the establishment of dedicated processes and tools, as well of a common understanding of what constitutes an incident and how it shall be communicated. NIS2 (formerly NIS1), European Digital Identity Framework (EUDIF formerly eIDAS) and EECC are the main pieces of EU legislation mandating the reporting of incidents with a significant impact. They apply respectively to essential and important entities, trust services providers and telecommunication services providers.

NIS2 Article 23 sets the obligation for Member States to ensure that essential and important entities notify any incident that has a significant impact on the provision of their services. ENISA recommends that the NIS Cooperation Group, with the support of ENISA and the EC, establish a single common EU framework (including templates and data fields) to report incidents under NIS2

#### References

<https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union>

<https://www.enisa.europa.eu/publications/enisa-single-programming-document-2025-2027> (Activity 4)

[https://www.europarl.europa.eu/thinktank/en/document/EPRS\\_BRI\(2021\)689333](https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333)

<https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene/raising-awareness-campaigns/network-and-information-systems-directive-2-nis2>


<https://nis2directive.eu/>

## 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



The graphic features a blue background with a red banner at the top that reads 'EU Cyber Resilience Act'. Below the banner is a shield icon with a checkmark inside, surrounded by a circular pattern of dots. Underneath the shield, the text 'For safer & more secure digital products' is written. At the bottom of the graphic, the hashtags '#DigitalEU' and '#CyberSecEU' are displayed.

DI CYBER-1: CYBER CRISIS MANAGEMENT IN THE EUROPEAN UNION

The Cyber Resilience Act (CRA) was adopted on 23 October 2024. The CRA introduces common cybersecurity requirements for products with digital elements, hardware and software, with the aim of minimising product vulnerabilities and ensuring that cybersecurity is taken seriously both at the design and production phases and that vulnerability management is guaranteed across the support period for such products. Manufacturers will have to apply the rules 36 months after their entry into force. Reporting obligations regarding actively exploited vulnerabilities and severe cybersecurity incidents are also introduced, applicable 21 months after the entry into force of the Act.

### References

<https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union>

<https://www.enisa.europa.eu/publications/enisa-single-programming-document-2025-2027> (Activity 5)


<https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act>

## CYBER SOLIDARITY ACT (2025)

AI-enabled cross-border SOC  
or Cyber Hubs

Cybersecurity Emergency  
Mechanism

Cybersecurity Incident Review  
Mechanism to capture lessons  
learned



EU CyberNet

DI CYBER.1: CYBER CRISIS MANAGEMENT IN THE EUROPEAN UNION

The Cyber Solidarity Act (CSOA) entered into force in February 2025. The CSOA lays down measures to strengthen capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents. It introduces three main pillars to strengthen solidarity at Union level to better detect, prepare for and respond to significant or large-scale cybersecurity incidents, comprising the European Cybersecurity Alert System (pan-European Network of Cyber Hubs), the Cybersecurity Emergency Mechanism and the European Cybersecurity Incident Review Mechanism.

The European Cybersecurity Alert System aims to improve the detection, analysis and response to cyber threats. The system will be composed of national and cross-border Security Operations Centres (SOCs) across the EU, so-called “Cyber Hubs” which will constitute the so-called “European Cyber Shield”. These SOC will use advanced technology such as Artificial Intelligence (AI) and data analytics to detect and share warnings on threats with authorities across borders.

The EU Cybersecurity Emergency Mechanism will consist of the EU Cybersecurity Reserve, entrusted to ENISA . This will be a pool of trusted private sector incident response service providers.

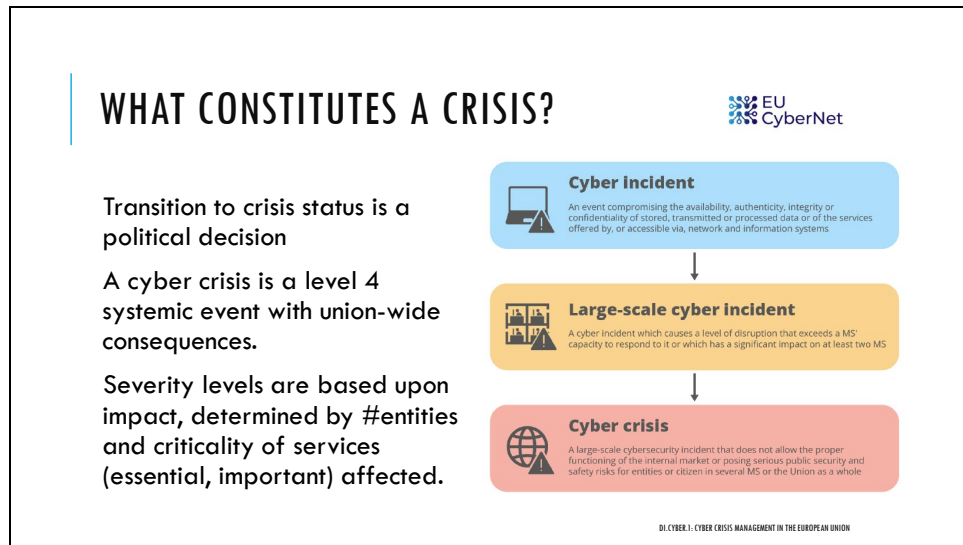
### References

<https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union>

<https://www.enisa.europa.eu/publications/enisa-single-programming-document-2025-2027> (Activity 6)

<https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity>





A cyber crisis transcends political, functional, and sectoral boundaries.

The new blueprint recognizes that Member States define critical infrastructure differently. So it defines severity levels based upon impact. Typically critical infrastructures includes essential services such as energy, transport, banking, financial market infrastructure, health, drinking water, waste water, digital infrastructure, ICT service management, public administration, and space, and important services such as postal and courier services, waste management, manufacturing, chemicals, production, food, manufacturing, digital suppliers, and research. If these services are affected, the incident is likely to reach crisis level, given the potential to disrupt vital services.

#### References

<https://industrialcyber.co/expert/the-eus-cybersecurity-blueprint-and-the-future-of-cyber-crisis-management/>

[https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AC\\_202503445](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AC_202503445)

## EXAMPLE: WANNACRY

May 2017 first case of cooperation at EU level

Considered a large-scale creeping cybersecurity incident

Not elevated to the status of crisis



DI CYBER-1: CYBER CRISIS MANAGEMENT IN THE EUROPEAN UNION

WannaCry was the first ever case of cyber cooperation at the EU level.

In May 2017, the WannaCry ransomware rapidly spread to more than 230 000 computers in 150 countries, encrypting files on the hard drives of Windows systems, preventing users from accessing them and demanding a ransom to decrypt the files. It was a cross-sector propagation that affected several users in several countries, impacting thousands of operating systems (35).

It was propagated using EternalBlue, an exploit developed by the United States National Security Agency (NSA) for Microsoft Windows systems. EternalBlue was stolen and leaked by a group called The Shadow Brokers (TSB) a month prior to the attack.

The attack began at 07:44 UTC on 12 May 2017 and was halted a few hours later at 15:03 UTC by the registration of a kill switch discovered by Marcus Hutchins. The kill switch prevented already infected computers from being encrypted or further spreading WannaCry.

WannaCry was considered a large-scale cyber security incident and was not elevated to the status of a crisis. At the time, only the technical level of cyber crisis management was in place.

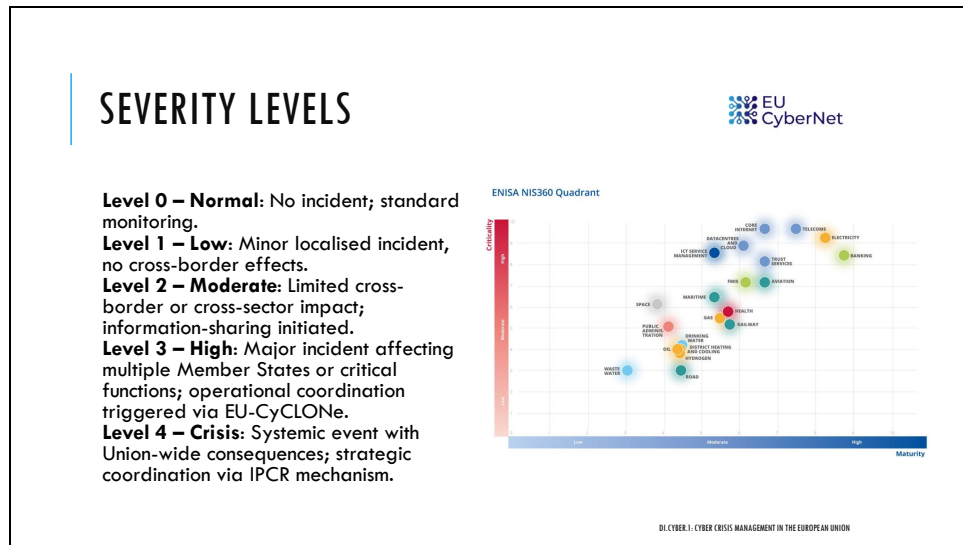
WannaCry could be considered a large-scale creeping cybersecurity incident because the cyberthreat was hidden in plain sight, evolving gradually over time on computers around the world in a non-linear pattern.

## References

<https://www.enisa.europa.eu/publications/best-practices-for-cyber-crisis-management>, p15.

[https://en.wikipedia.org/wiki/WannaCry\\_ransomware\\_attack](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack)

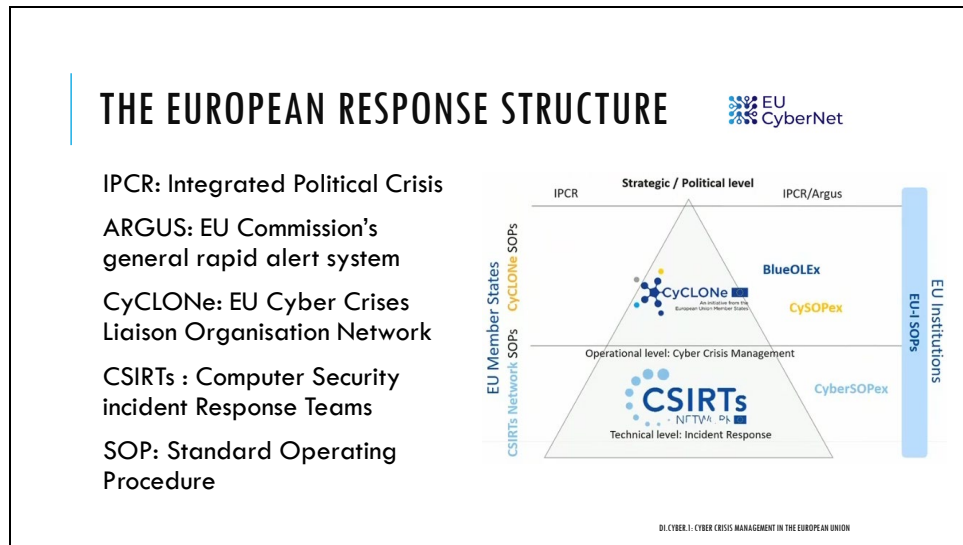
[https://link.springer.com/chapter/10.1007/978-3-030-70692-0\\_3](https://link.springer.com/chapter/10.1007/978-3-030-70692-0_3)



IPCR = Integrated Political Crisis Response

### References

[https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AC\\_202503445](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AC_202503445)  
<https://www.enisa.europa.eu/publications/enisa-nis360-2024>



The ENISA CSIRTs inventory lists 675 CSIRTs in the Member States of which 39 are members of the CSIRTs Network.

77% of the Members of the CSIRTs Network are also members of FIRST, the Forum for Incident Response and Security Teams.

31% are certified or are candidates for (re)certification under Trusteer Introducer, meaning their incident response plans adhere to internationally recognized standards.

Cyber SOPEX is a cooperation exercise managed by the CSIRTs Network

CySOPex is a cooperation exercise managed by CyCLONE to test member states' procedures for fast cyber crisis management when the EU is facing large-scale, cross border cyber-attacks.

The Blue OLEx exercise tests the Standard Operating Procedures (SOP) of the EU CyCLONE at the executive level

### References

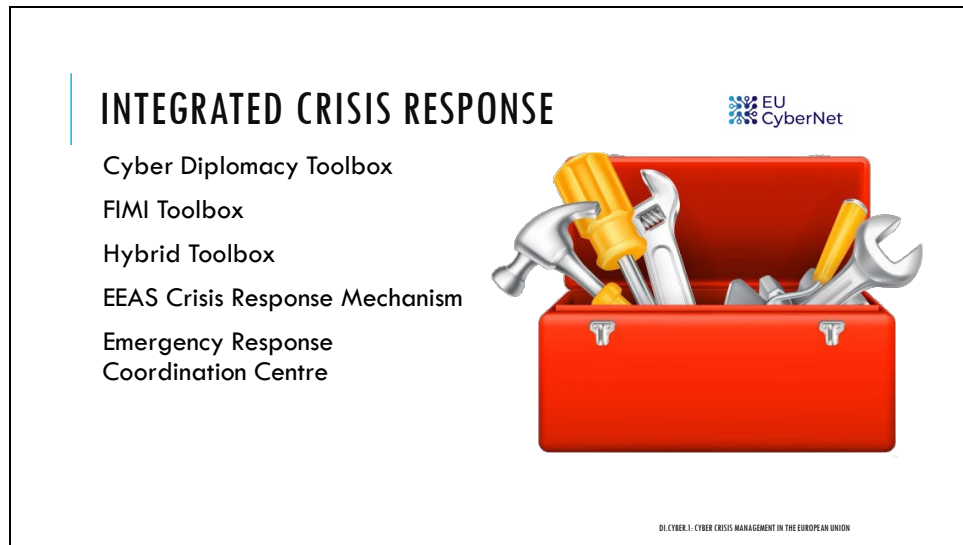
<https://one->

[conference.nl/video/2023/40\\_Johannes\\_Clos\\_Rossella\\_Mattioli\\_2023\\_11\\_17T15\\_34\\_24.mp4](https://one-conference.nl/video/2023/40_Johannes_Clos_Rossella_Mattioli_2023_11_17T15_34_24.mp4)

<https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union>

<https://industrialcyber.co/expert/the-eus-cybersecurity-blueprint-and-the-future-of-cyber-crisis-management/>

[https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AC\\_202503445](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AC_202503445)



A Europoc analysis in February 2024 concluded:

First, preventive measures by far dominated other tool applications quantitatively, with stabilising and cooperative measures following suit. In turn, the EU uses restrictive measures, such as sanctions, rarely. Overall, the use of CDT measures over time has clearly increased, with measures taken in the context of Russia's aggression against Ukraine being a strong driving factor.

Second, capacity-building initiatives were most frequently applied as preventive measures. These capacity-building measures mostly addressed states that were candidates for EU accession, thus the entry barriers for such measures were rather low. Cooperative measures, such as strategic dialogues, were directed towards powerful cyber-allies and powerful cyber-adversaries alike.

Third, focusing on the discursive dimension of the CDT's instruments, we find substantial evidence that the EU's stabilising measures still use open and often vague diplomatic language, thus allowing for ambiguous interpretations by various actors (Byers 2020).

Lastly, most of the observed CDT measures were not directly linked to specific cyberattacks. Five years into the application of the CDT, the question remains as to why some cyber operations trigger a response while others do not, and if they do, why not all available tools are used.

A more recent Europoc analysis in May 2025 concluded:

For the 2019 elections, we identified 18 measures (see Graph 4a), most of them focussing on the risks of election-related cyberattacks, such as: hacking of voting machines; theft of personal information from voter rolls (#13 EU); cyberattacks on electoral servers (#22 EU); or manipulation of voter numbers or vote counts (#26 EU). 14 RP Nr. 3 | MAY 2025 In contrast, significantly fewer measures addressed the risk of cyber-based disinformation campaigns influencing the elections. For the 2024 EU elections, we observed a significant decrease in mentions of cyber threats targeting electoral processes, with only six measures recorded in the 18 months leading up to the elections (see Graph 4a). Notably, none of these measures referenced potential hacking of electoral systems, vote counting, or similar attacks. Instead, this time the primary concern shifted toward disinformation campaigns, particularly those linked to Russia's hybrid threat operations since the war against Ukraine started.

To counter these hybrid threats, the EU relied on multiple tools, including:

- The EU Hybrid Toolbox and the Foreign Information Manipulation and Interference Toolbox (mentioned in #232 EU)
- The Digital Services Act (DSA), i.a., allows for combating disinformation through content moderation and algorithmic amplification by very large online platforms (mentioned in #254 EU)

This increased cross-referencing and implementation of other EU toolboxes aligns with the explicit objectives of the CDT revision. The revised framework aims for closer integration with other toolboxes (Council of the European Union 2023, p. 4), marking a qualitative shift in the EU's cyber diplomacy approach and demonstrating the growing aspiration to counter cross-domain threats effectively, which requires de-siloed empirical threat information as its basis.

#### References

[https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AC\\_202503445](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AC_202503445) (Article 9)

<https://www.cyber-diplomacy-toolbox.com/>

<https://eurepoc.eu/wp-content/uploads/2024/02/Right-Thoughts-Right-Words-Right-Actions-February-2024.pdf>

<https://eurepoc.eu/wp-content/uploads/2025/05/More-Thoughts-More-Words-Different-Actions.pdf>



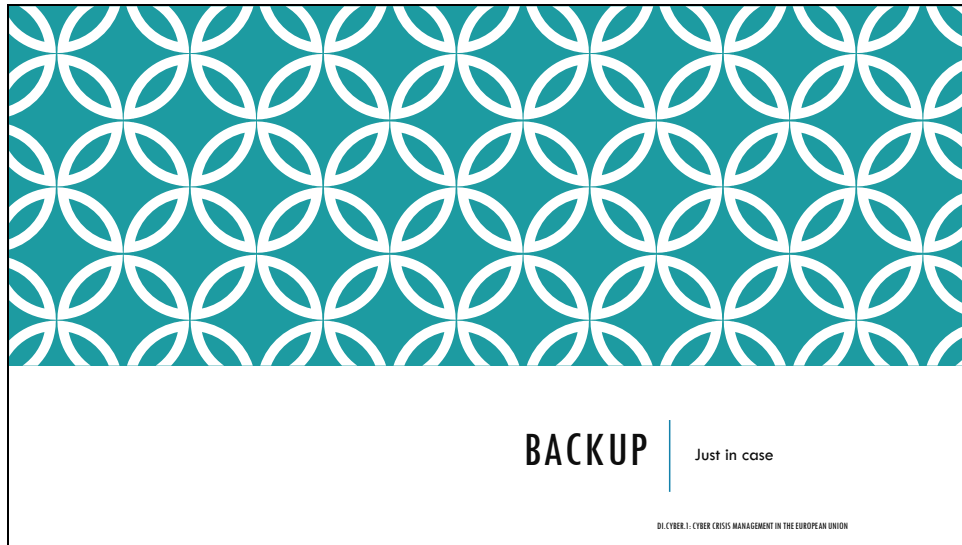
## MODULE: QUIZ

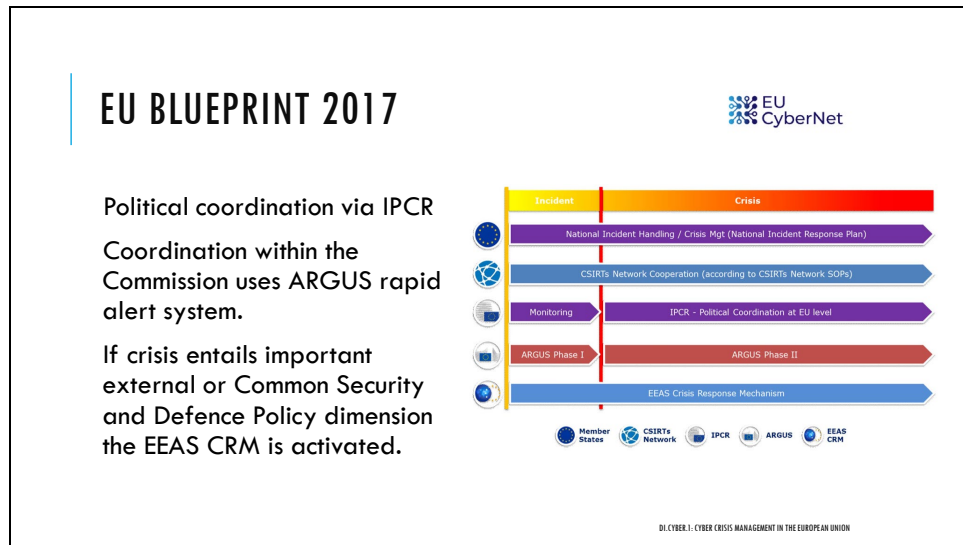


1. That are the most important EU laws pertaining to cyber crisis management?
2. What is the difference between a large-scale incident and a crisis?
3. Which crisis management network is the interface between the political and technical levels?
4. Which European instrument brings all the important elements of cyber crisis management together?

DI CYBER.1: CYBER CRISIS MANAGEMENT IN THE EUROPEAN UNION

- NIS2, CRA, CSOA
- Crisis impedes functioning of internal market or poses serious public safety or security risks for citizens of several MS or the Union as a whole
- EU-CyCLONe
- The EU Cyber Blueprint





This Blueprint applies to cybersecurity incidents which cause disruption too extensive for a concerned Member State to handle on its own or which affect two or more Member States or EU institutions with such a wide-ranging and significant impact of technical or political significance that they require timely policy coordination and response at Union political level.

Such large-scale cybersecurity incidents are considered a cybersecurity 'crisis'.

In case of an EU-wide crisis with cyber elements, coordination at Union political level of the response shall be carried out by the Council, using the Integrated Political Crisis Response (IPCR) arrangements.

Within the Commission, coordination will take place in accordance with the ARGUS rapid alert system.

If the crisis entails an important external or Common Security and Defence Policy (CSDP) dimension, the EEAS Crisis Response Mechanism is activated.

The Blueprint describes how these well-established Crisis Management mechanisms should make full use of existing cybersecurity entities at EU level as well as of cooperation mechanisms between the Member States.

In doing so, the Blueprint takes into account a set of guiding principles (proportionality, subsidiarity, complementarity and confidentiality of information), presents the core objectives

of cooperation (effective response, shared situational awareness, public communication messages) at three levels (strategic/political, operational and technical), the mechanisms and the actors involved as well as the activities to meet said core objectives.

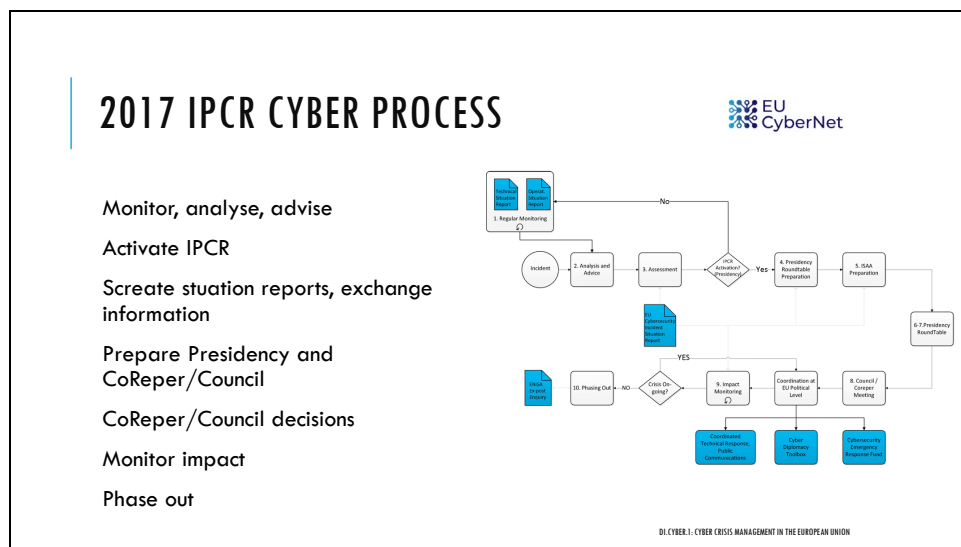
The Blueprint does not cover the full crisis management lifecycle (prevention/mitigation, preparedness, response, recovery) but focuses on response. Nevertheless, certain activities, in particular those related to achieving a shared situational awareness, are addressed.

It is also important to note that cybersecurity incidents can be at the origin or part of a broader crisis, impacting other sectors. Given that most cybersecurity crises are expected to have effects on the physical world, any appropriate response must rely upon both cyber and non-cyber mitigation activities. Cyber crisis response activities should be coordinated with other crisis management mechanisms at EU, national or sectoral levels.

Finally, the Blueprint does not replace and should be without prejudice to existing sector-specific or policy-specific mechanisms, arrangements or instruments such as the one set up for the European Global Navigation Satellite System (GNSS) programme.

#### References

COMMISSION RECOMMENDATION (EU) 2017/ 1584 - of 13 September 2017 - on coordinated response to large-scale cybersecurity incidents and crises



— Step 1 — Regular sectoral monitoring and alerting: the existing, regular sectoral situation reports and alerts provide indications to the Council Presidency on a developing crisis and its possible evolution.

— Identified gap: There are currently no regular and coordinated cybersecurity situation reports and alerts as regards cybersecurity incidents (and threats) at EU level.

— Blueprint: EU Cybersecurity situation monitoring/reporting

— A regular EU Cybersecurity Technical Situation Report on cybersecurity incidents and threats will be prepared by ENISA on incidents and threats, based on publicly available information, its own analysis and reports shared with it by Member States' CSIRTs (on a voluntary basis) or NIS Directive single points of contact, European Cybercrime Centre (EC3) at Europol, CERT-EU and European Union Intelligence Centre (INTCEN) at the European External Action Service (EEAS). The report should be made available to the relevant instances of the Council, the Commission and the CSIRTs Network.

— On behalf of SIAC, the EU Hybrid Fusion Cell should compile an EU Cybersecurity Operational Situation Report. The report also supports the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities.

— Both reports are disseminated to EU and national stakeholders to contribute to their own situational awareness and inform decision-making and facilitate cross-border regional cooperation. 19.9.2017 L 239/50 EN Official Journal of the European Union After an incident has been detected

— Step 2 — Analysis and advice: based on available monitoring and alerting, the Commission services, the EEAS, and the GSC keep each other informed on possible developments, in order to be ready to advise the Presidency for a possible activation (in full or in information-sharing mode) of the IPCR.

— Blueprint:

— For the Commission, DG CNECT, DG HOME, DG HR.DS and DG DIGIT, supported by ENISA, EC3 and CERT-EU.

— EEAS. Drawing on the work of the Sitroom, and intelligence sources, the EU Hybrid Fusion Cell provides situational awareness on actual and potential hybrid threats affecting the EU and its partners including cyber threats. Therefore, when the analysis and assessment of the EU Hybrid Fusion Cell indicates the existence of possible threats directed against a Member State, partner countries or organisation, INTCEN will inform (in the first instance) on the operational level, according to established procedures. The operational level will then prepare recommendations for the political strategic level, including the possible activation of crisis management arrangements in monitoring mode (e.g. EEAS Crisis Response Mechanism or the IPCR monitoring page).

— The CSIRTs Network Chair assisted by ENISA prepares an EU Cybersecurity Incident Situation Report ( ) which is presented to the Presidency, the Commission and the HRVP via the CSIRT of the rotating Presidency. 1

— Step 3 — Assessment/decision on IPCR activation: the Presidency evaluates the need for political coordination, information exchange or decision-making at EU level. To this end, the Presidency may convene an informal round table meeting. The Presidency carries out an initial identification of the areas requiring Coreper or Council involvement. This will form the basis of the guidance for the production of Integrated Situational Awareness and Analysis (ISAA) reports. The Presidency will decide, in light of the characteristics of the crisis, its possible consequences, and the related political needs, on the appropriateness of convening meetings of the relevant Council Working Parties and/or Coreper and or PSC.

— Blueprint:

— Round table participants:

— The Commission services and the EEAS will advise the Presidency on their respective areas of competence.

— Member States' representatives in the Horizontal Working Party on Cyber Issues supported by experts from the capitals (CSIRTs, Cybersecurity Competent Authorities, others).

— Political/Strategic Guidance for ISAA reports based on the latest EU Cybersecurity Incident Situation Report and additional information provided by the round table participants.

— Relevant Working Parties and Committees:

— Horizontal Working Party on Cyber Issues. The Commission, EEAS and GSC, in full agreement and associating the Presidency, can also decide to activate the IPCR in information-sharing mode by generating a crisis page, in order to prepare the ground for a possible full activation.

— Step 4 — IPCR Activation/Information gathering and exchange: upon activation (whether in information-sharing mode or in full), a crisis page is generated on the IPCR web platform, allowing specific exchanges of information focusing on aspects that will contribute to feed ISAA and to prepare the discussion at political level. The ISAA lead service (one of the Commission services or EEAS) will depend on the circumstances of the case.

— Step 5 — ISAA production: the production of ISAA reports will be initiated. The Commission/EEAS will issue ISAA reports as outlined in the ISAA SOPs and may further foster information-exchange on the IPCR web platform, ( 1 ) The EU Cybersecurity Incident Situation Report is an aggregation of national reports provided by national CSIRTs. The format of the report should be described in the CSIRTs Network SOPs. 19.9.2017 EN Official Journal of the European Union L 239/51 or issue specific requests for information. The ISAA reports will be tailored to the needs of the political level (i.e. Coreper or the Council) as defined by the Presidency and laid out in its guidance, thus allowing a strategic overview of the situation and an informed debate on the agenda items defined by the Presidency. In accordance with the ISAA SOPs, the nature of the cybersecurity crisis will determine whether the ISAA report is prepared by one of the Commission Services (DG CNECT, DG HOME) or the EEAS.

Following the activation of the IPCR, the Presidency will outline the specific areas of focus for ISAA in order for it to support the political coordination and/or decision-making process in the Council. The Presidency will also specify the timing of the report, following consultations with the Commission services/EEAS.

— Blueprint:

— The ISAA report includes contributions from relevant services including:

— The CSIRTs Network in the form of the EU Cybersecurity Incident Situation Report.

— EC3, Sitroom, the EU Hybrid Fusion Cell, CERT-EU. The EU Hybrid Fusion Cell will support and provide contributions to the ISAA lead service and the IPCR round table, as appropriate.

— EU sectoral agencies and bodies depending on the impacted sectors

— Member States authorities (other than the CSIRTs).

— Gathering ISAA inputs ( 1 ):

— Commission and EU Agencies. The ARGUS IT system will provide the internal backbone network for ISAA. EU Agencies shall send their contributions to their respective responsible DGs, which in turn will feed the relevant information into ARGUS. Commission services and Agencies will gather information from existing sectorial networks with Member States and international organisations and from other relevant sources.

— For the EEAS. The EU Situation Room supported by the other relevant EEAS departments, will provide the internal backbone network and single point of contact for ISAA. The EEAS will gather information from third countries and relevant international organisations.

— Step 6 — Preparation of the informal Presidency round table: the Presidency, assisted by the General Secretariat of the Council, will define the timing, agenda, participants, and expected outcome (possible deliverables) of the informal Presidency round table meeting. The GSC will

relay relevant information on the IPCR web platform on behalf of the Presidency, and will issue in particular the meeting's notice.

— Step 7 — Presidency round table/preparatory measures for EU political coordination/decision-making: the Presidency will gather an informal round table to review the situation, and to prepare and review the items to be brought to the Coreper or Council's attention. The informal Presidency round table will also be the forum to develop, review and discuss all proposals for action to be submitted to Coreper/Council.

— Blueprint:

— The Council Horizontal Working Party on Cyber Issues should prepare PSC or Coreper.

— Step 8 — Political coordination and decision-making at Coreper/Council: The results of the Coreper/Council meetings concern the coordination of response activities at all levels, decisions on exceptional measures, political declarations, etc. These decisions also constitute an updated political/strategic guidance for the further production of ISAA reports.

— Blueprint:

— The political decision to coordinate the response to the cybersecurity crisis is implemented through the activities (performed by the corresponding actors) described above in Section 1 'Cooperation at Strategic/political, operational and technical levels' as regards Response and Public Communication.

— ISAA production continues based on cooperation at technical, operational and political/strategic levels as regards Situational awareness also described above in Section 1. ( ) ISAA SOPs. 1 19.9.2017 L 239/52 EN Official Journal of the European Union

— Step 9 — Impact monitoring: the ISAA lead service will provide, with the support of ISAA contributors, information on the evolution of the crisis and on the impact of the political decisions taken. This feedback loop will support an evolving process and support the Presidency's decision in continuing the involvement of the EU political level or in phasing down the IPCR.

— Step 10 — Phasing out: following the same process as for the activation, the Presidency may convene an informal round table meeting to assess the opportunity to maintain the IPCR active or not. The Presidency can decide to close or downgrade the activation.

— Blueprint:

— ENISA may be invited to contribute to or carry out an ex post technical inquiry of the incident in accordance with the provisions in its mandate.

## References

COMMISSION RECOMMENDATION (EU) 2017/ 1584 - of 13 September 2017 - on coordinated response to large-scale cybersecurity incidents and crises



