Council of the European Union
General Secretariat

Brussels, 24 April 2025

WK 5108/2025 ADD 1

LIMITE

CYBER	**JAIEX**
IPCR	**POLMIL**
RELEX	**HYBRID**
JAI	**TELECOM**
	COSI

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

WORKING DOCUMENT

From: To:	Presidency Horizontal Working Party on Cyber Issues
N° prev. doc.:	WK 4493/2025
Subject:	Proposal for a Council Recommendation for an EU Blueprint on cybersecurity crisis management - Annexes of the third Presidency compromise

Delegations will find attached the three annexes of the third Presidency compromise text of the abovementioned proposal for a Council Recommendation.

EUROPEAN
COMMISSION

Brussels, XXX
[…](2025) XXX draft

ANNEXES 1 to 3

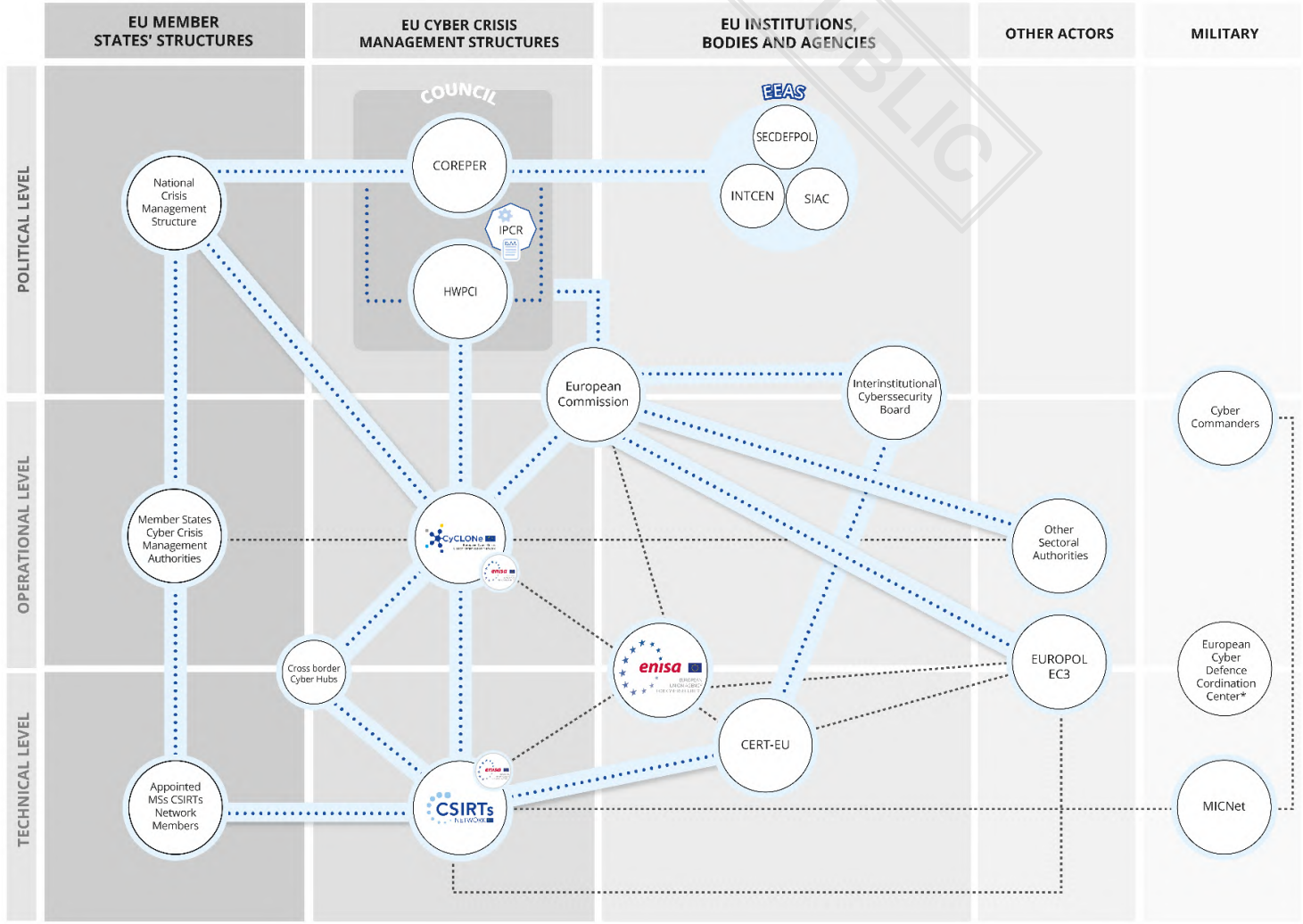
ANNEXES

to the

Proposal for a COUNCIL RECOMMENDATION

for an EU Blueprint on cybersecurity crisis management

ANNEX I – The Union Blueprint for responding to a cybersecurity crisis



ANNEX II – RELEVANT UNION-LEVEL ACTORS (ENTITIES AND NETWORKS) AND CRISIS MANAGEMENT MECHANISMS

(1) Main actors across the cyber crisis management life cycle (only large-scale incidents and cyber crises)

	Preparedness – threat landscape	Preparedness – exercises	Detection	Response – technical level	Response – operational level	Response – political level	Response to a crisis	Public communica-tion	Recovery
Member States	X		X	X	X	X	X	X	X
The Commission		X			X	X	X	X	
The High Representative	X	X			X	X	X		
The Council		X				X	X	X	X
ENISA	X	X		X			X		
CERT-EU	X		X	X				X	
CSIRTs network	X	X	X	X	X		X		X
EU-CyCLONe	X	X	X		X	X	X	X	X

(2) Roles and competences of the relevant Union-level actors (in alphabetical order) in relation to cyber crisis management

Actor	Level	Role and competence	Reference
CERT-EU	Technical / Operational	Coordinates the response and the management of major incidents affecting Union entities. Member of the CSIRTs Network. Supports the Commission in EU-CyCLONe. Acts as the cybersecurity information exchange and incident response coordination hub, facilitating the exchange of information regarding incidents, cyber threats, vulnerabilities and near misses among Union entities and counterparts. Requests the deployment of the EU Cybersecurity Reserve on behalf of Union entities. Cooperates with the NATO Cybersecurity Centre on the basis of their Technical Agreement.	Regulation (EU, Euratom) 2023/2841
Council	Political	Carries out policy-making and coordinating functions	Article 16 of the Treaty on European Union
Presidency of the Council of the EU	Political	Decides (except where the solidarity clause is activated under TFEU Article 222 of the Treaty on the Functioning of the European Union) whether to activate or deactivate the IPCR, at the invitation of a Member State, in consultation affected Member States as appropriate, as well as the Commission and the HR, and when to escalate or deescalate from one mode of activation to the other.	Article 16 of the Treaty on European Union Council Implementing Decision (EU) 2018/1993

Actor	Level	Role and competence	Reference
Cross-border cyber hubs	Technical	Formed of three or more national cyber hubs, they ensure exchange of relevant information related to cyber threats, near misses, indicators of compromise, cyber alerts within the cross-border hub. Cooperate closely with the CSIRTs Network to share information. Provide information relating to a potential or ongoing large-scale cybersecurity incident to Member States' authorities and the Commission through EU-CyCLONe and the CSIRTs Network.	Regulation (EU) 2025/38
CSIRTs Network	Technical	Contributes to the development of confidence and trust and promotes swift operational cooperation among Member States. Is the main network to ~~E~~exchange~~s~~ relevant information about incidents, near misses, cyber threats, risks, and vulnerabilities. At the request of a member potentially affected by an incident, the Network exchanges and discusses information in relation to that incident and associated cyber threats. The Network can also implement a coordinated response to an incident that has been identified within the jurisdiction of a requesting member. Receives information from Member States regarding their requests to the EU Cybersecurity Reserve.	Article 15 of Directive (EU) 2022/2555
Cyber Commanders conference		A forum for cyber commanders at the national level within Member States to collaborate and exchange vital information regarding	Cyber Defence Joint Communication

Actor	Level	Role and competence	Reference
		ongoing cyberspace operations and strategies for mitigating large-scale cyber incidents. It is organised by the rotating presidency of the Council of the European Union with the support of European Defence Agency (EDA), European External Action Service (EEAS), and the EU Military Staff (EUMS).	
Commission	Operational / Political	Executive body of the European Union. Ensuring the smooth functioning of the Internal market. Facilitates coherence and coordination between related Union-level crisis response actions. Provides~~ing~~ analytical reports (ISAA) for the IPCR mechanism General preparedness actions, including managing the Emergency Response Coordination Centre and the Common Emergency Communications and Information system. Observer in EU-CyCLONe and Member in case of potential or ongoing large-scale incident. Observer in the CSIRTS Network. Overall responsibility for the implementation of the EU Cybersecurity Reserve. Point of contact of the Inter-institutional Cybersecurity Board for sharing relevant information in relation to major incidents with EU-CyCLONe. Strategic oversight of the Galileo Security Monitoring Centre. (GSMC) Consulted by Presidency of the Council on decisions to activate or deactivate the IPCR. Commission	Article 17 of the Treaty on European Union Implementing Decision (EU) 2018/1993 Decision No 1313/2013/EU of the European Parliament and of the Council Directive (EU) 2022/2555 Regulation (EU) 2025/38Regulation (EU, Euratom) 2023/2841

Actor	Level	Role and competence	Reference
		services develop, with the EEAS, the ISAA report.	
European Cybersecurity Agency (ENISA)	Technical / operational	Carries out tasks for the purpose of achieving a high level of cybersecurity across the Union, including actively supporting Member States. Provides the secretariat for the CSIRTs Network and EU-CyCLONe. Helps develop a common response to large-scale cross border incidents or crises by: Aggregating and analysing reports from national sources Ensuring flow of information between technical, operational and political levels Facilitating handling of incidents Supporting Union entities with regards to public communication. Testing incident response capabilities and regularly organising cybersecurity exercises. Operates and administrates the EU Cybersecurity Reserve, partly or fully, as provided in the Cyber Solidarity Act. Reviews and assesses threats, known vulnerabilities and mitigation actions for a specific significant or large-scale cyber incident. Prepares an incident review report	NIS 2 Directive (EU) 2022/2555 Regulation (EU) 2019/881 Regulation (EU) 2025/38 Regulation (EU) 2024/2847
European cyber crisis liaison organisation network (EU-CyCLONe)	Operational	Supports the coordinated management of large-scale cybersecurity incidents and crises at operational level Ensures the regular exchange of relevant information among	Directive (EU) 2022/2555 Regulation (EU) 2025/38

Actor	Level	Role and competence	Reference
		Member States and Union institutions, bodies, offices, and agencies. Coordinates the management of large-scale cybersecurity incidents and crises and supports decision-making at political level in relations to such incidents and crises. Assesses the consequences and impact of relevant large-scale cybersecurity incidents and crises and proposes possible mitigation measures. Develops, together with ENISA, the template to facilitate submission of requests for support from the EU Cybersecurity Reserve. Receives information from Member States regarding their requests to the EU Cybersecurity Reserve. Receives information relating to a potential or ongoing large-scale cybersecurity incident from the cross border cyber hubs or the CSIRTs Network.	
High Representative of the Union for Foreign Affairs and Security Policy supported by the European External Action Service	Political	Leads on and coordinates the Union's efforts to address external security threats in the fields of hybrid and cyber Responsible for the Union cyber diplomacy and cyber defence instruments to deter and respond to external threats by using the Union's Hybrid and Cyber Diplomacy Toolboxes. Engages with external partners also including through CSDP engagement. Provides preparedness Union and Member States' situational	Council Decision 2010/427/EU

Actor	Level	Role and competence	Reference
		awareness of and capacity to react to hybrid and cyber threats, for example through practical exercises, training and networks. Handles security and defence implications of Union space assets, especially under the Union's Common Security and Defence Policy (CSDP). Consulted by Presidency of the Council on decisions to activate or deactivate the IPCR. EEAS develop, with the Commission services, the ISAA report.	
Europol	Operational	Provides operational and technical support to the Member States' competent authorities for the prevention and deterrence of cybercrime.	Regulation (EU) 2016/794, including all amendments
Interinstitutional Cybersecurity Board		Approves the interinstitutional cyber crisis management plan for Union entities. Adopts, based on a CERT-EU proposal, guidelines or recommendations on incident response cooperation for significant incidents concerning Union entities. .	Regulation (EU, Euratom) 2023/2841
Military Computer Emergency Response Team Operational Network (MICNET)	Technical	Foster a more robust and coordinated response to cyber threats affecting defence systems in the Union, including those used in military CSDP missions and operations; established and supported by the European Defence Agency.	Cyber Defence Joint Communication 2022
Single Intelligence Analysis		Composed of (1) EU Intelligence and Situation Centre (EU INTCEN) which handles civilian intelligence and open-source intelligence and provides strategic	Articles 38 and 42 to 46 of the Treaty on European Union

Actor	Level	Role and competence	Reference
Capacity (SIAC)		intelligence on foreign policy, terrorism, and hybrid threats, and (2) EU Military Staff Intelligence Directorate (EUMS INT) which handles military intelligence for CSDP missions and supports Union defence and crisis management operations. Under the authority of the High Representative.	Council Joint Action 2001/555/CFSP Council Decision 2010/461/CFSP

(3) Relevant Union-level crisis mechanisms

Mechanism	Horizontal/ sector/ cyber-specific	Description	Reference
ARGUS	Horizontal	Allows the Commission to exchange relevant information on emerging multisectoral crises or foreseeable or imminent threats that require Union-level action.	Commission Communication (2005)662
EEAS Crisis Response Centre (CRC)	Horizontal	The single-entry point for all crisis-related issues in the EEAS and the 24/7 permanent crisis response capability for emergencies threatening the safety of the staff in EU Delegations, and/or in reaction to crises affecting Union citizens abroad. It brings together security, consular and situational awareness experts, while relying on committed professionals on the ground in Union delegations.	A Strategic Compass for Security and Defence - For a European Union that Protects Its Citizens, Values and Interests and Contributes to International Peace and Security (21 Mach 2022)
Critical Infrastructure Blueprint	Horizontal	Coordinates a response at Union-level to disruptions to critical infrastructure with significant cross-border relevance.	Council Recommendation C/2024/4371
Cybersecurity Alert System	Cyber-specific	Ensures advanced Union capabilities to enhance detection, analysis and data processing capabilities in	Regulation (EU) 2025/38 (Cyber

Mechanism	Horizontal/ sector/ cyber-specific	Description	Reference
		relation to cyber threats and the prevention of incidents in the Union.	Solidarity Act) OJ L series, 15.1.2025
Cyber Diplomacy Toolbox (Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities)	Cyber-specific	The joint Union diplomatic response to malicious cyber activities, contributing to conflict prevention, the mitigation of cybersecurity threats, and greater stability in international relations.	Council Conclusions of 19 June 2017 Revised implementing guidelines 10289/23, 08.06.2023
European Cyber Reserve	Cyber-specific	Mobilises cybersecurity experts and resources during crises to support response efforts in Member States, Union institutions, bodies or agencies	Regulation (EU) 2025/38
Network code on sector-specific rules for cybersecurity aspects of cross-border electricity flows	Sectoral	Establishes a recurrent process of cybersecurity risk assessments in the electricity sector, contains provisions specific to crisis management and links to the CSIRTs Network and EU-CyCLONe.	Commission Delegated Regulation (EU) 2024/1366
EU Cyber Defence Coordination Centre	Horizontal	Its initial objective is to primarily enhance the Union's and its Member States' shared situational awareness on malicious activities in cyberspace, particularly concerning military CSDP missions and operations.	Cyber Defence Joint Communication 2022
Hybrid Toolbox	Horizontal	Includes a set of provisions to ensure an overview of what is available at EU level in response to all kind of hybrid threats, their coordinated use, ensuring coherence of our actions across domains. The Hybrid Toolbox helps ensure that decision making based on a comprehensive situational awareness and the lessons learned	Council conclusions on a Framework for a coordinated EU response to hybrid campaigns, 22 June 2022
Hybrid Rapid Response Teams (EU HRRTs)	Horizontal	As part of the EU-Hybrid Toolbox, the EU Hybrid Rapid Response Teams draw on relevant sectoral national and EU civilian and military	Guiding framework for the practical establishment of the EU Hybrid Rapid

Mechanism	Horizontal/ sector/ cyber-specific	Description	Reference
		expertise to provide tailored and targeted short-term assistance to member states, Common Security and Defence Policy missions and operations, and partner countries in countering hybrid threats and campaigns.	Response Teams (21 May 2024)
IPCR	Horizontal	Supports rapid and coordinated decision-making at Union political level for major and complex crises, including acts of terrorism. Decision to activate and deactivate is taken by the Presidency of the Council which consults (except where in the solidarity clause has been invoked) the affected Member States, the Commission and the HR. GSC, Commission services and EEAS may also agree, in consultation with the Presidency, to activate IPCR in information sharing mode. Discussions are informed by the ISAA report developed by Commission services and the EEAS. The report is based on relevant information and analysis provided by the Member States (e.g. from relevant national crisis centres) particularly through the web platform, and by Union Agencies	Council Implementing Decision (EU) 2018/1993
EU Law Enforcement Emergency Response Protocol	Horizontal	A tool to support the Union law enforcement authorities in providing immediate response to major cross-border cyber-attacks through rapid assessment, the secure and timely sharing of critical information and effective coordination of the international aspects of their investigations.	Council conclusions (26 June 2018) on EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises.

Mechanism	Horizontal/ sector/ cyber-specific	Description	Reference
PESCO Cyber Rapid Response Teams (CRRT)	Cyber-specific	Deploy specialized teams to respond swiftly to significant cyber incidents as well as perform preventative actions, such as vulnerability assessments and election monitoring. Member State initiative, partly funded by Connecting Europe Facility.	Article 42 (6), Article 46 and Protocol 10 of the Treaty on European Union.
Space Threat Response Architecture (STRA)	Sectoral (Space Threats including cyber related)	Space Threat Response Architecture (STRA) on responsibilities to be exercised by the Council and the High Representative to avert a threat arising from the deployment, operation or use of the systems set up and services provided under the Union Space Programme	Council Decision (CFSP) 2021/698
Systemic Cyber Incident Coordination Framework (EU-SCICF)	Sectoral	A framework which is under development for communication and coordination that addresses and manages potential systemic cyber events in the financial sector. It will build on one of the envisaged roles of the European Supervisory Authorities (ESAs) under the Regulation (EU) 2022/2554 of gradually enabling an effective Union-level coordinated response in the event of a major cross-border information and communication technologies (ICT) related incident or related threat having a systemic impact on the Union's financial sector as a whole.	Recommendation of the European Systemic Risk Board of 2 December 2021 on a pan-European systemic cyber incident coordination framework for relevant authorities (ESRB/2021/17)
Union Civil Protection Mechanism (UCPM)	Horizontal	Ensures civil protection cooperation to improve prevention, preparedness, and response to disasters.	Decision 1313/2013.
CISE - Common Information	Maritime specific	CISE - is a network that connects systems of EU/EEA authorities with responsibility in maritime surveillance. CISE enables the	A Strategic Compass for Security and Defence - For a European Union that

Mechanism	Horizontal/ sector/ cyber-specific	Description	Reference
Sharing Environment	covering seven sectors.	exchange of relevant information across borders and different sectors in a seamless and automated way.	Protects Its Citizens, Values and Interests and Contributes to International Peace and Security (21 March 2022).

(4) Sectors of high criticality and other critical sectors under Directive (EU) 2022/2555 and Union level sectoral crisis mechanisms (where applicable)

Sectors	Subsector	Applicable sectoral crisis mechanisms
Energy	Electricity	Electricity Coordination Group
	District heating and cooling	n/a
	Oil	Oil Coordination Group The European Union Offshore Authorities Group (EUOAG)
	Gas	Gas Coordination Group
	Hydrogen	n/a
Transport	Air	European Aviation Crisis Coordination Cell (EACCC)
	Rail	n/a
	Water	European Fisheries Control Agency (EFCA) SafeSeaNet (SSN) Integrated Maritime Services (IMS) Long Range Identification and Tracking data centre (LRIT) EMSA Maritime Support Services
	Road	n/a
	Horizontal	The Network of Transport Contact Points, established by the Contingency Plan for Transport (COM(2022) 211)
Banking		EU-SCICF
Financial market infrastructures		EU-SCICF European Financial Stabilisation Mechanism

Health		Early Warning and Response System (EWRS) Health Emergency Operations Facility (HEOF) Rapid alert system for tissue and cell and blood Components (RATC/RAB) Public Health Emergency Framework Rapid Alerting System for Chemical incidents (RASCHEM) The European surveillance portal for infectious diseases Health Emergency Preparedness and Response (HERA) Medical health intelligence System (MediSys) Executive Steering Group on Shortages of Medical Devices (MDSSG) Pharmacovigilance Rapid Alert EU Health Task Force (EUHTF)
Drinking water		n/a
Waste water		n/a
Digital infrastructure		n/a
ICT service management		n/a
Public administration		n/a
Space		Space Threat Response Architecture (STRA)
Postal and courier services		n/a
Waste management		n/a

Manufacture, production and distribution of chemicals		Rapid Alerting System for Chemical incidents (RASCHEM)
Production, processing and distribution of food		European crop monitoring System Global agricultural production anomaly hotspot detection (ASAP) European Network of Plant Health Information Systems (EUROPHYT) EU Veterinary Emergency Team (EUVET) Rapid Alert System for Food and Feed (RASFF) European Food Security Crisis preparedness and response Mechanism (EFSCM) Internal Market Emergency and Resilience Act (IMERA)
Manufacturing	Medical devices	n/a
	Computer, electronic and optical products	n/a
	Machinery and equipment	n/a
	Manufacturing of motor vehicles, trailers and semi trailers	n/a
	Manufacturing of other transport equipment	n/a
Digital providers		n/a
Research		n/a

ANNEX III – EU Cybersecurity Crisis Management Framework and Related Instruments

Since 2017, the Union has developed its cybersecurity framework through several instruments that contain provisions relevant for cybersecurity crisis management:

- Regulation (EU) 2019/881 of the European Parliament and of the Council[1],
- Directive (EU) 2022/2555 of the European Parliament and of the Council[2],
- Commission Implementing Regulation 2024/2690[3], Regulation (EU, Euratom) 2023/2841 of the European Parliament and of the Council[4],
- Regulation (EU) 2021/887 of the European Parliament and of the Council[5],
- Regulation (EU) 2024/2847 of the European Parliament and of the Council[6], and
- Regulation (EU) 2025/38 of the European Parliament and of the Council ('Cyber Solidarity Act')[7].

Specific sectoral cybersecurity crisis measures include Commission Delegated Regulation (EU) 2024/1366[8] and the forthcoming systemic cyber incident coordination framework (EU-SCICF) in the context of Regulation (EU) 2022/2554 of the European Parliament and of the Council[9].

Directive 2013/40[10] provides the reference for the definition of criminal activities related to cyberattacks and Union rules on cross-border access to electronic evidence, in particular Regulation (EU) 2023/1543 of the European Parliament and of the Council[11], once implemented, will significantly facilitate law enforcement action in this domain.

The EU Policy on Cyber Defence[12] outlines the roles of an EU network of Military Computer Emergency Response Teams Operational Network (MICNET) and the EU Cyber Commanders Conference and envisages the establishment of an EU Cyber Defence Coordination Centre (EUCDCC).

Other, non-cyber related situational awareness and crisis response mechanisms exist in some of the critical sectors listed in the Annexes I and II to Directive (EU) 2022/2555.

The 'Council Recommendation on a Blueprint to coordinate a response at Union level to disruptions of critical infrastructure with significant cross-border relevance'[13] provides for cooperation between relevant actors where an incident affects both physical aspects and the cybersecurity of critical infrastructure.

[1] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15, , ELI: http://data.europa.eu/eli/reg/2019/881/oj).

[2] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), (OJ L 333, 27.12.2022, p. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

[3] Commission implementing Regulation (EU) 2024/2690 of 17.10.2024 laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service

providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers, (OJ L, 2024/2690, 18.10.2024).

[4] Regulation (EU, Euratom) 2023/2841 of the European Parliament and of the Council of 13 December 2023 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union, (OJ L, 2023/2841, 18.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2841/oj).

[5] Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres, (OJ L 202, 8./6./2021, p. 1, ELI: http://data.europa.eu/eli/reg/2021/887/oj).

[6] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (OJ L, 2024/2847, 20.11. 2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

[7] Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act) (OJ L, 2025/28, 15.12025, ELI: http://data.europa.eu/eli/reg/2025/38/oj).

[8] Commission Delegated Regulation (EU) 2024/1366 of 11 March 2024 supplementing Regulation (EU) 2019/943 of the European Parliament and of the Council by establishing a network code on sector-specific rules for cybersecurity aspects of cross-border electricity flows (OJ L, 2024/1366, 24.5.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1366/oj).

[9] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011, (OJ L 333, 27.12.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

[10] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (OJ L 218, 14.8.2013, p. 8, ELI: http://data.europa.eu/eli/dir/2013/40/oj).

[11] Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings and Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings (OJ L 191, 28.7.2023, p. 118, ELI: http://data.europa.eu/eli/reg/2023/1543/oj).

[12] JOIN(2022) 49 final.

[13] *OJ C, C/2024/4371, 5.7.2024.*