Council of the European Union

Brussels, 6 June 2025
(OR. en)

9794/25

Interinstitutional File:
2025/0036 (NLE)

CYBER 157
IPCR 42
RELEX 706
JAI 738
JAIEX 54
POLMIL 138
HYBRID 63
TELECOM 178
COSI 108

OUTCOME OF PROCEEDINGS

From:	General Secretariat of the Council
On:	6 June 2025
To:	Delegations
Subject:	Council Recommendation on an EU blueprint for cyber crisis management - Council Recommendation approved by the Council at its meeting on 6 June 2025

Delegations will find attached the Council Recommendation approved by the Council at its meeting on 6 June 2025.

ANNEX

COUNCIL RECOMMENDATION

on an EU blueprint for cyber crisis management

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 and 292 thereof,

Having regard to the proposal from the European Commission,

Whereas:

(1) Digital technology and global connectivity are the backbone of the Union's economic growth, competitiveness and the transformation of critical infrastructure. However, an interconnected and increasingly digital economy also increases the risk of cybersecurity incidents and cyberattacks. Moreover, increasing geopolitical tensions, conflicts and strategic rivalry are reflected in the impact, volume and sophistication of malicious cyber activities. Such activities may form part of hybrid campaigns or military operations. They can also directly affect the Union's security, economy and society. In addition, they have spillover potential, particularly when these activities are targeted at international strategic partner countries such as candidate or neighbouring countries.

(2) A large-scale cybersecurity incident can cause a level of disruption that exceeds a Member State's capacity to respond to it or has a significant impact on more than one Member State. Such an incident, depending on its cause and impact, could escalate and turn into a fully-fledged crisis, affecting the proper functioning of the internal market or posing serious public security and safety risks for entities or citizens in several Member States or the Union as a whole. Effective crisis management is essential for maintaining economic stability and protecting European governments, critical infrastructure, businesses and citizens, as well contributing to international security and stability in cyberspace. Cyber crisis management is accordingly an integral part of the overarching EU crisis management framework.

(3) Given the interdependencies and interconnections between Union entities' and Member States' ICT environments, an incident in a Union entity might pose a cybersecurity risk to Member States and vice versa. The sharing of relevant information and coordination in respect with both large-scale cybersecurity incidents and major incidents, as defined in Article 3(8) of Regulation (EU, Euratom) 2023/2841[1], is crucial in the context of the EU blueprint for cyber crisis management ('Cyber Blueprint').

[1] 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, p. 1-27.

(4) In case of a crisis for which the EU Integrated Political Crisis Response ('IPCR') under Council Implementing Decision (EU) 2018/1993[2] ('IPCR arrangements') have been activated, the Cyber Blueprint should fully respect the IPCR arrangements for the coordination and response. The political and strategic coordination would take place in the IPCR. The IPCR arrangements are the tool for horizontal coordination and response at Union political level. Pursuant to the IPCR arrangements, the decision to activate or deactivate the IPCR is taken by the Presidency of the Council of the European Union. Integrated Situational Awareness and Analysis ('ISAA') reports prepared by the Commission services and the European External Action Service ('EEAS') support the work of the IPCR in both its information-sharing mode and its full activation modes.

(5) Member States have the primary responsibility in the management of cybersecurity incidents and cyber crises. The potential cross-border and cross-sectoral nature of cybersecurity incidents, however, requires Member States and the relevant Union entities to cooperate at technical, operational and political level to coordinate effectively across the Union. Full-lifecycle cyber crisis management includes preparedness and shared situational awareness to anticipate large scale cybersecurity incidents, the necessary detection capabilities to identify the needed response and recovery tools to mitigate and contain large scale cybersecurity incidents, as well as reaction capabilities to deter and prevent further incidents.

[2] Council Implementing Decision (EU) 2018/1993 of 11 December 2018 on the EU Integrated Political Crisis Response Arrangements, OJ L 320, 17.12.2018, p. 28–34.

(6) Commission Recommendation (EU) 2017/1584[3] on coordinated response to large-scale cybersecurity incidents and crises sets out the objectives and modes of cooperation between Member States and Union entities in responding to large-scale cybersecurity incidents and cyber crises. It mapped the relevant actors at technical, operational and political level, and explained how they were integrated into the existing Union crisis management mechanisms, such as the IPCR arrangements. The core principles set out in Recommendation (EU) 2017/1584 remain valid, namely, subsidiarity, complementarity and confidentiality of information as well as the three-level approach (technical, operational and political). The present Recommendation builds on those core principles and is intended to replace Recommendation (EU) 2017/1584, setting out a new Union framework for cybersecurity crisis management.

(7) Some definitions used in this Recommendation are based on definitions and terms used in Directive (EU) 2022/2555[4]. However, the scope of this Recommendation is different than the scope of Directive (EU) 2022/2555. This Recommendation sets out the Union framework for cyber crisis management within the context of the EU's overall preparedness for large-scale cybersecurity incidents and cyber crises arising from such incidents – irrespective of whether what sector or entity is affected. To the extent feasible, definitions are based on those contained in Directive (EU) 2022/2555.

---

3 Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises, OJ L 239, 19.9.2017, p. 36-58.

4 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. 80–152.

(8) An updated Cyber Blueprint is necessary to provide clear and accessible guidance explaining what a large-scale cybersecurity incident or Union-level cyber crisis is, how the crisis management framework is triggered and what the roles of relevant Union level networks, actors and mechanisms are, and what the interaction between these actors and mechanisms throughout the entire cyber crisis lifecycle is. Cyber Blueprint aims to support the broader framework of EU civilian-military relations in the context of cyber crisis management, including against the background of deepening EU-NATO relations, where possible including through inclusive, reciprocal and non-discriminatory enhanced information-sharing mechanisms in cyber crisis management.

(9) Cross-sectoral crisis management at Union level should be reinforced to enable an integrated crisis response, particularly in cases where large-scale cybersecurity incidents and crises cause physical consequences. This Recommendation complements the IPCR arrangements and other Union crisis management mechanisms, including the Commission's general rapid alert system ARGUS, the Union Civil Protection Mechanism ('UCPM') supported by the Emergency Response Coordination Centre ('ERCC') established under the UCPM by Decision No 1313/2013/EU of the European Parliament and of the Council on a Union Civil Protection Mechanism[5] ('UCPM decision'), the EEAS's Crisis Response Mechanism ('CRM'), as well as other processes, such as those described in the EU Cyber Diplomacy Toolbox[6], the Hybrid Toolbox[7] and in the revised EU Protocol for countering hybrid threats[8]. It also complements and should be coherent with the Council Recommendation (EU) 2024/4371 on a blueprint to coordinate a response at Union level to disruptions of critical infrastructure with significant cross-border relevance[9] ('EU Critical Infrastructure Blueprint'), which covers non-cyber physical resilience, and which aims at improving coordination of response at Union level in this area.

---

5 Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism, OJ L 347, 20.12.2013, p. 924–947.

6 Council conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (9916/17)

7 Council conclusions on a Framework for a coordinated EU response to hybrid campaigns, 22 June 2022

8 Joint Staff Working Document – EU Protocol for countering hybrid threats (SWD(2023) 116 final).

9 OJ C, C/2024/4371, 5.7.2024

(10) The European cyber crisis liaison organisation network ('EU-CyCLONe') is the network for coordination of management of large-scale cybersecurity incidents and crises at the operational level also in case of cross-sectoral large-scale cybersecurity incident and cyber crisis. In order not to further complicate the existing frameworks the creation of sectoral structures that would duplicate the tasks of EU-CyCLONe should be avoided. EU-CyCLONe should receive operational cybersecurity related information also from the sectors and feed into the political level.

(11) Member States are encouraged to make full use of the financial resources available for cybersecurity provided by relevant Union programmes. It should be ensured that these programmes impose minimal administrative burdens on applicants for the funding and the participation of Member States in these programmes is facilitated by providing relevant guidance on viable financial support options.

(12) This Recommendation contributes to wider preparedness actions required for the Union in the face of cross-sectoral crises in line with the principles embedded in the EU Preparedness Union Strategy, namely an integrated all-hazards, whole-of-government and whole-of-society approach, in particular with regard to improving awareness of risks and threats and cross-sectoral crisis response.

HAS ADOPTED THIS RECOMMENDATION:

I: Aim, scope, and guiding principles of the EU cyber crisis management framework

Aim and scope

(1) This Recommendation on an EU blueprint for cyber crisis management ('Cyber Blueprint') sets out the Union framework for cyber crisis management within the context of the EU's overall preparedness for large-scale cybersecurity incidents and cyber crises. The framework reflects the roles of both Member States and the Union institutions, bodies, offices and agencies ('Union entities') within their respective competences, with full respect for national laws and internal rules, to ensure comprehensive and coordinated action at Union level.

(2) The Cyber Blueprint should be applied in coherence with the EU Critical Infrastructure Blueprint, in particular in the case of incidents affecting both the physical resilience and the cybersecurity of critical infrastructure[10].

(3) The Cyber Blueprint provides guidance for the response to large-scale cybersecurity incidents or cyber crises, and it should be used complementarily with any relevant sectoral response mechanisms, such as those listed in the Annex II. Relevant cybersecurity stakeholders should help and assist in reaching the goals of those sectoral mechanisms, both on national and Union level.

(4) In case of an EU-wide cross-sectoral crisis with cyber aspects for which the IPCR is activated, coordination of the response at Union political level should be carried out by the Council, using the IPCR arrangements. When the IPCR has been activated, measures under Cyber Blueprint should support the EU response at political level, providing specific support on cybersecurity.

10 The EU Critical Infrastructure Blueprint further details coordination in such cases in its Section 4 of Part I of its Annex.

Guiding principles

(5) The following guiding principles apply to cyber crisis management at Union level:

(a) *Proportionality*: most cybersecurity incidents affecting Member States fall below what could be considered a national or Union large-scale cybersecurity incident or cyber crisis. In case of cybersecurity incidents and threats, Member States cooperate and exchange information, voluntarily, on a regular basis within the network of computer security incident response teams ('CSIRTs network') and EU-CyCLONe, in line with the networks' Standard Operating Procedures ('SOPs').

(b) *Subsidiarity*: Member States have the primary responsibility for the response and remediation in case of a cybersecurity incident, a large-scale cybersecurity incident, or a cyber crisis affecting them. With a view to potential cross-border effects, the Council, the Commission, the High Representative, the European Union Agency for Cybersecurity ('ENISA'), the Cybersecurity Service for the Union Institutions, Bodies, Offices and Agencies ('CERT-EU'), Europol and all other relevant Union entities should cooperate throughout the entire crisis life cycle. This role stems from Union law and reflects how large-scale cybersecurity incidents and cyber crises impact one or more sectors of economic activity within the single market, the security and international relations of the Union, as well as the Union entities themselves.

(c) *Complementarity*: this Recommendation takes fully into account existing crisis management mechanisms at Union level listed in the Annex II, in particular the IPCR arrangements, ARGUS, and the EEAS CRM. This Recommendation takes into account the mandates of the CSIRTs network and EU-CyCLONe, as well as Regulation (EU, Euratom) 2023/2841. Where the IPCR is activated, the work of relevant networks, entities and activated sectoral mechanisms should continue and should feed into and support the political and strategic coordination taking place in the IPCR.

(d) *Confidentiality of information*: all information exchanges in the context of this Recommendation should comply with applicable rules on security and on the protection of personal data. Informal non-disclosure agreements, such as the Traffic Light Protocol for labelling sensitive information, should be taken into account when appropriate. For the exchange of classified information, regardless of the classification scheme applied, existing binding rules and agreements on processing of classified information should be used alongside available accredited tools.

(6) In accordance with the abovementioned guiding principles, Member States and Union entities should deepen their cooperation on cyber crisis management, fostering mutual trust and building on existing networks and mechanisms. This cooperation, within the framework of Cyber Blueprint, benefits from the implementation of Articles 22 and 23 of Regulation (EU, Euratom) 2023/2841. In particular the cyber crisis management plan established on the basis of Article 23 of Regulation (EU, Euratom) 2023/2841, among other things, contributes to the regular exchange of relevant information among Union entities and with Member States, and defines arrangements concerning coordination and information flow among Union entities.

II: Definitions

(7) For the purpose of this Cyber Blueprint the following definitions apply:

(a) ‘incident’ means an event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems;

(b) ‘significant incident’ means an incident that:

a. has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned;

b. has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage;

(c) ‘large-scale cybersecurity incident’ means an incident which causes a level of disruption that exceeds a Member State’s capacity to respond to it or which has a significant impact on at least two Member States;

(d) ‘cyber crisis’ means a large-scale cybersecurity incident that escalated into a fully-fledged crisis not allowing the proper functioning of the internal market or posing serious public security and safety risks for entities or citizens in several Member States or the Union as a whole.

III: National Cyber Crises Management Structures and Responsibilities

(8) Member States have the primary responsibility for the response in case of large-scale cybersecurity incidents or cyber crises affecting them. Each Member State, in line with Directive (EU) 2022/2555, has one or more cyber crisis management authorities, as well as one or more CSIRTs.

(9) Through the adoption of Directive (EU) 2022/2555 and other cybersecurity legislative and non-legislative instruments, Member States have been aligning their cybersecurity frameworks by setting out minimum rules regarding the functioning of the coordinated regulatory framework, laying down mechanisms for effective cooperation among the responsible authorities in each Member State, and providing effective remedies and enforcement measures, which are key to the effective enforcement of those obligations.

(10) In accordance with Article 9(4) of Directive (EU) 2022/2555, Member States should adopt national large-scale cybersecurity incident and crisis response plans. These plans include, among others, national preparedness measures, cyber crisis management procedures and national procedures and arrangements between national authorities and bodies to ensure their effective participation in and support of the coordinated management of large-scale cybersecurity incidents and cyber crises at Union level. The cyber crises management procedures include as well provisions on their integration into the general national crisis management framework and information exchange channels.

(11) In accordance with Article 9(1) of Directive (EU) 2022/2555, Member States should ensure coherence with the existing frameworks for general national crisis management. In case of activation of the IPCR, national crisis management authorities should, for the purpose of informing the IPCR, collect inputs from the cyber crisis management authorities and national sectoral crisis mechanisms.

(12) In accordance with Article 9(5) of Directive (EU) 2022/2555, EU-CyCLONe, upon the request of a Member State concerned, should exchange information on the relevant parts of national large-scale cybersecurity incident and crisis response plans, in particular on the provisions to ensure effective participation in and support of the coordinated management of large-scale cybersecurity incidents and cyber crises at Union level, in order to exchange best practices and reflect if the overall framework would work in practice.

(13) EU-CyCLONe and the Interinstitutional Cybersecurity Board (‘IICB’) are invited to exchange, where appropriate, on coherence of crisis management plan established by the IICB in accordance with Article 23 of the Regulation (EU, Euratom) 2023/2841 with national large-scale cybersecurity incident and crisis response plans.

(14) EU-CyCLONe, with the support of ENISA as its secretariat, should maintain an up-to-date list of national cyber crisis management authorities with contact details of EU-CyCLONe officers and executives, and make it available to EU-CyCLONe members.

IV: Main networks and actors in the EU Cyber Crisis Management Ecosystem

(15) The CSIRTs network is the main technical network to exchange relevant information about incidents, in particular in the scope of this Recommendation, in accordance with the relevant tasks described in Article 15(3) of Directive (EU) 2022/2555. It contributes to the development of confidence and trust and promotes swift and effective operational cooperation among Member States. The Chair of the CSIRTs network may participate as an observer in the IICB.

(16) CERT-EU is the cybersecurity service for all Union entities. CERT-EU acts as the cybersecurity information exchange and incident response coordination hub for Union entities in accordance with Article 13 of Regulation (EU) 2023/2841. CERT-EU is a member of the CSIRTs network and supports the Commission in EU-CyCLONe. CERT-EU operates at the technical level and is responsible for coordinating the management of major incidents affecting Union entities.

(17) EU-CyCLONe works as an intermediary between the technical and political level, in particular during large-scale cybersecurity incidents and cyber crisis. It supports the coordinated management of large-scale cybersecurity incidents and cyber crises at operational level and ensures the regular exchange of relevant information among Member States and Union institutions, bodies, offices and agencies in accordance with Article 16 of Directive (EU) 2022/2555. The Chair of EU-CyCLONe may participate as an observer in the IICB.

(18) ENISA is the Union agency carrying out the tasks assigned under Regulation (EU) 2019/881[11] for the purposes of achieving a high common level of cybersecurity across the Union, including by actively supporting Member States and Union institutions, bodies and agencies. ENISA provides, among others, the secretariat for the CSIRTs network and EU-CyCLONe, situational awareness services, and assists Member States by regularly organising cybersecurity exercises at Union level. In accordance with Directive (EU) 2022/2555 and Regulation (EU) 2024/2847[12], ENISA receives information about significant cross-border incidents and actively exploited vulnerabilities and incidents affecting digital products.

(19) The Council of the European Union ('the Council') is the institution with policy-making and coordinating functions pursuant to Article 16 of the Treaty on the European Union ('TEU') and is entrusted with the IPCR which concerns coordination and response at Union political level. The Council operates through Council configurations, Committee of Permanent Representatives, and relevant Council preparatory bodies, especially the Horizontal Working Party for Cyber Issues ('HWPCI'), as well as, where relevant, the IPCR arrangements.

---

[11] 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. 15–69.

[12] 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) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act), OJ L, 2024/2847, 20.11.2024, p.1-81.

(20) The Commission, as the institution promoting the general interest of the Union and taking appropriate initiatives to that end as well as ensuring the application of the Treaties and of measures adopted by the institutions under Article 17 TEU, is responsible for certain general Union-level preparedness and certain situational awareness actions, including the management of the ERCC and the Common Emergency Communications and Information System ('CECIS'), in line with the UCPM Decision. It facilitates coherence and coordination between related Union-level crisis response actions at operational level. It is consulted on decisions to activate or deactivate the IPCR. Commission services together with the EEAS prepare the ISAA reports. It is a member of EU-CyCLONe in cases where a potential or ongoing large-scale cybersecurity incident has or is likely to have a significant impact on services and activities falling within the scope of Directive (EU) 2022/2555, and an observer in other cases. It is the point of contact in the IICB to EU-CyCLONe. It is an observer in the CSIRTs network.

(21) The High Representative for Foreign Affairs and Security Policy (High Representative), assisted by the EEAS, conducts the Union's Common Foreign and Security Policy ('CFSP'), and contributes by their proposals to the development of that policy, including the Common Security and Defence Policy ('CSDP'). This includes diplomatic, intelligence and military structures and mechanisms, notably the Single Intelligence Analysis Capacity ('SIAC') as the single point of entry for Member States' intelligence, the EU Military Staff ('EUMS') as the source of military expertise, the EU Cyber Diplomacy Toolbox, as well as the network of EU Delegations, that may contribute to crises management from an external dimension. The EEAS also prepares with the Commission the ISAA reports.

(22) The Annex II describes the roles and competences of the relevant Union level actors in relation to cyber crises management, including the main networks and actors.

V: Preparing for large-scale cybersecurity incidents and a cyber crisis

Threat landscape

(23) Member States and relevant Union entities should take the necessary measures to enhance situational awareness, recognising that the threat landscape and incident-specific situational awareness require distinct modes of operation. Member States and relevant Union entities should work together on the basis of verified, reliable data, including trends in incidents, tactics, techniques and procedures, and actively exploited vulnerabilities.

(24) When sharing information at EU level, Member States should make full use of the existing platforms for technical and operational cooperation, such as those used by the CSIRTs network and EU-CyCLONe.

(25) In order to enhance shared situational awareness and to facilitate assessment of the EU impact, EU-CyCLONe and the CSIRTs network with support of ENISA should use internally agreed reporting mechanism to produce an EU overview of technical and operational activities based on the information gathered at the national level.

(26) EU-CyCLONe and the CSIRTs network should:

(a) cooperate to improve information sharing between the technical and operational level and situational awareness as a whole;

(b) continue to build a climate of trust between their members and between the networks;

(c) make full use of the available tools for information sharing, with support of ENISA, reflect on how to improve these tools and ensure interoperability between the networks.

(27) EU-CyCLONe, the CSIRTs network and the IICB should cooperate to ensure effective exchange of relevant information.

(28) ENISA, as the secretariat for the CSIRTs network and EU-CyCLONe, has a central role in supporting Member States and Union institutions, bodies and agencies to achieve a common EU situational awareness on the technical and operational level to support preparing for large-scale cybersecurity incidents and crises.

(29) In accordance with Directive (EU) 2022/2555 and Regulation (EU) 2019/881, Member States and relevant Union entities should coordinate with the private sector, including open-source communities and manufacturers, to improve information sharing. In particular ENISA should utilise its partnership programme in this regard. Additionally, Member States and relevant Union entities could also build on existing Information Sharing and Analysis Centres ('ISACs') at EU and national levels, to enhance cybersecurity capacity and to respond to cybersecurity incidents, including through joint meetings of the private sector with EU-CyCLONe or the CSIRTs network.

(30) To enhance information sharing within and between the networks, and to clarify mutual expectations for such sharing, EU-CyCLONe should, with the support of ENISA as secretariat and after consulting the CSIRTs network and the NIS Cooperation Group, within 24 months from adoption of this Recommendation, agree on a common aligned taxonomy of incident severity levels. This taxonomy should enable a comparison of the severity of incidents across Member States by considering the impact on service delivery, the number of affected entities and their respective relevance, the impact on other services and infrastructure, as well as the monetary, reputational and political damage inflicted. It should build on relevant existing scales or taxonomies, such as Reference Incident Classification Taxonomy.

Technical level

(31) The CSIRTs network is the platform for technical cooperation and information sharing between all Member States and through CERT-EU with the Union entities.

(32) In accordance with Directive (EU) 2022/2555, each CSIRT has a task of monitoring and analysing cyber threats, vulnerabilities and incidents at the national level. CSIRTs should exchange, both within the CSIRTs network and bilaterally, relevant information about incidents, near misses, cyber threats, risks and vulnerabilities to achieve a shared situational awareness.

(33) In order to enhance operational cooperation at Union level, the CSIRTs network should consider inviting Union bodies and agencies involved in cybersecurity policy, such as Europol, to participate in its work.

(34) In accordance with Regulation 2023/2841, CERT-EU should collect, manage, analyse and share information with the Union institutions, bodies, offices and agencies on cyber threats, vulnerabilities and incidents in unclassified ICT infrastructure and, when necessary, issue specific proposals to the IICB for guidelines and recommendations towards Union institutions, bodies, offices and agencies. CERT-EU should cooperate and exchange information with Member States counterparts, including by means of the CSIRTs network.

Operational level

(35) In accordance with the Directive (EU) 2022/2555, EU-CyCLONe should serve as a platform for cooperation between Member States cyber crisis management authorities and through the Commission with the relevant Union entities, with the objective of increasing the level of preparedness of the management of large-scale cybersecurity incidents and cyber crises and developing a shared situational awareness for large-scale cybersecurity incidents and cyber crises.

(36) In accordance with Directive (EU) 2022/2555 and Regulation (EU) 2024/2847, ENISA receives information about significant cross-border incidents and actively exploited vulnerabilities and incidents affecting digital products. ENISA acting as the secretariat should advise the CSIRTs network and EU-CyCLONe with the objective of supporting the networks in determining whether further actions should be taken and to contribute to the shared situational awareness.

Political level

(37) Member States and relevant Union entities should monitor international developments which affect cybersecurity (including cyber threats, hybrid threats and foreign information manipulation and interference ('FIMI') including disinformation where relevant). Initiatives like the Joint Cyber Assessment Reports ('JCAR'), analyses provided by SIAC and other relevant products providing specialised insights should be taken into account.

(38) The High Representative should continue to inform and involve Member States in the Union diplomatic efforts related to cyber threats, especially those that involve state actors, its engagement with third countries and international organisations, including NATO and the implementation of diplomatic measures, including restrictive measures.

(39) The Presidency of the Council of the European Union may initiate a monitoring page on the IPCR web platform where Member States and EU institutions and bodies can exchange information on a possibly developing crisis.

Common exercises

(40) The Commission, in coordination with the High Representative, supported by ENISA, after consulting EU-CyCLONe and the CSIRTs network, should compile an efficient annual rolling programme of cyber exercises to prepare for cyber crises and to enhance organisational efficiency. The rolling programme of cyber exercises should take account of exercises of the UCPM and other Union-level crisis response mechanisms exercises, including the exercise outlined in the EU Critical Infrastructure Blueprint. The first rolling programme should be developed within 12 months after the adoption of the Cyber Blueprint, with subsequent programmes to be completed by 31 March of each year. The rolling programme should be submitted to the Council for information.

(41) The rolling programme should also cover exercises developed using the EU coordinated risks assessments scenarios. It should cover exercises involving all relevant actors, in particular the private sector and NATO.

(42) ENISA, in its role of secretariat of the CSIRTs network and EU-CyCLONe, should ensure the systematic collection of lessons learnt from exercises, as well as the identification and proposing ways of implementation of resulting actions, to guarantee their effective execution and positive impact on the EU common resilience, including respective SOPs.

(43) All actors and networks should improve the coordination in case of a large-scale cybersecurity incident or cyber crisis on the basis of the lessons learnt from the exercises. In particular EU-CyCLONe and the CSIRTs network should address the challenges identified during the exercises to improve the coordination, especially those concerning the cooperation among the networks and, if needed, swiftly adapt SOPs.

(44) The NIS Cooperation Group should invite the CSIRTs network, EU-CyCLONe and ENISA to present lessons learnt from the exercises, as well as the identification and proposed way of implementation of resulting actions.

(45) The Council may invite the chairs of the CSIRTs network, EU-CyCLONe, the NIS Cooperation Group and ENISA, to present how lessons learnt from the exercises were implemented.

(46) ENISA, in cooperation with the Commission and the High Representative, is invited to organise an exercise to test Cyber Blueprint during the next Cyber Europe exercise. The exercise should involve all relevant actors, including the political level. ENISA is invited to coordinate with the Presidency of the Council of the European Union the involvement of the political level. The exercise may also include the private sector and NATO.

VI: Detecting an incident that could escalate to a large-scale cybersecurity incident or cyber crisis

(47) In accordance with their respective mandates and based on the all-hazards approach, all actors should contribute information indicating a potential large-scale cybersecurity incident or cyber crisis to relevant networks.

(48) In accordance with Regulation (EU) 2025/38[13], where the Cross-Border Cyber Hubs obtain information relating to a potential or ongoing large-scale cybersecurity incident, they should ensure, for the purposes of common situational awareness, that relevant information is provided to Member States' authorities and the Commission through EU-CyCLONe and the CSIRTs network without undue delay.

[13] 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, 2025/38, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj.

(49) When a significant incident is observed, in particular causing immediate impact, it might be notified to or detected by a CSIRT, as well as by Member States' cyber crisis management authorities or other sectoral authorities. Member States are encouraged to share information related to such incident within the networks, which should consider taking appropriate actions. The activation of the CSIRTs network and EU-CyCLONe can be independent from each other depending on the nature of the incident and the response required. However, both networks are encouraged to continue cooperation with each other on the basis of agreed procedural arrangements. The decision to activate rests solely and independently with each respective network.

(50) The CSIRTs network should advise EU-CyCLONe on whether an observed cybersecurity incident may be deemed a potential or ongoing large-scale cybersecurity incident.

(51) As indicated in Directive (EU) 2022/2555, the CSIRTs network and EU-CyCLONe should without delay agree on procedural arrangements in the case of a potential or ongoing large-scale cybersecurity incident, to ensure technical-operational coordination and timely and relevant information to the political level.

VII: Responding to a large-scale cybersecurity incident or cyber crisis at Union level

Response to a large-scale cybersecurity incident or cyber crisis for which IPCR is not activated in full mode

(52) Effective response to large-scale cybersecurity incidents or cyber crises at EU level depends on effective technical, operational and political cooperation in a whole-of-government approach, including where possible law enforcement.

(53) At each level, the actors involved should perform specific activities to achieve shared situational awareness and coordinated response. Such measures shall ensure the orderly and effective dissemination of information.

(54) Response should be appropriate to the impact of the large-scale cybersecurity incident or cyber crisis. In accordance with the Directive (EU) 2022/2555, Member States' cyber crisis management authorities should ensure national coherence and coordination between the sectoral responses to the cyber crisis.

(55) In the event of a large-scale cybersecurity incident or a cyber crisis, all actors and networks should respond in close coordination as follows:

(a) at the technical level:

i. The affected Member States and their CSIRTs should cooperate with the affected entities to respond to incidents and provide assistance, where applicable;

ii. The CSIRTs should cooperate through the CSIRTs network to share relevant technical information about the incident; the CSIRTs cooperate in their efforts to analyse the available technical artefacts and other technical information related to the incident with a view of determining the cause and possible technical mitigation measures;

iii. When a CSIRT or a Member State's cyber crisis management authority becomes aware of a significant incident, they are encouraged to share within the CSIRTs network or EU-CyCLONe.

iv. The CSIRTs network, with the support of ENISA, should prepare an aggregation of national reports provided by CSIRTs, which should be presented to EU-CyCLONe;

v. When a cybersecurity incident has the potential to escalate to a large-scale cybersecurity incident or a cyber crisis, the CSIRTs network should share appropriate information with EU-CyCLONe. EU-CyCLONe should use this information to brief the Council;

vi. The CSIRTs network should be in close contact with Europol to ensure exchange of relevant technical information. The CSIRTs network and Europol should establish points of contact to enhance information sharing when relevant in case of a large-scale cybersecurity incident;

(b) at the operational level:

i. Member States should mitigate the impact of the incident on the national level using appropriate measures;

ii. The CSIRTs network should provide EU-CyCLONe with technical assessments of the ongoing incidents, that can be used by EU-CyCLONe;

iii. EU-CyCLONe should assess the consequences and impact of relevant large-scale cybersecurity incidents and cyber crises and propose possible mitigation measures, and support the coordinated management of large scale cybersecurity incidents and cyber crises, as well as support the decision-making at the political level;

iv. Should a large scale cybersecurity incident with cross-sectoral impact, require the activation of Union-level response actions, in particular relevant Union-level horizontal and sectoral crisis management mechanisms listed in Annex II,

(a) the appropriate actors may, depending on the type of Union-level sectoral crisis management mechanisms, call for activation of the said mechanism;

(b) in the case of the activation of such a sectoral mechanism, the relevant entities support the sectoral entities in mitigating the impact of the incident;

(c) the Commission should facilitate the flow of necessary information between points of contact for the relevant horizontal and sectoral Union level crisis mechanisms listed in Annex II and EU-CyCLONe, and should pursue an integrated cross-sectoral analysis and propose options for appropriate integrated response plan;

(d) the Commission, through EU-CyCLONe, where relevant, in cooperation with the High Representative, should ensure coherence and coordination of the EU level operational measures in the cyber domain with related Union-level response actions, in particular in relation to requests of assistance through UCPM;

(e) if a monitoring IPCR page has been initiated information about the incident, its impacts and measures taken should also be shared among Member States and Union entities via the IPCR web platform;

v. Member States may request services from the EU Cybersecurity Reserve in accordance with Article 15 of Regulation (EU) 2025/38. Without prejudice to any future implementing acts under that Regulation, services of the EU Cybersecurity Reserve should be deployed within 24 hours of the request.

(c) at the political level:

i. The Council may request briefings from the key stakeholders in particular the Commission, the High Representative and EU-CyCLONe in order to conduct appropriate political and strategic response;

ii. The Council supported by the Commission and the High Representative, could decide on the appropriate measures to respond to the large-scale cybersecurity incident, including the possible diplomatic responses in line with Chapter IX;

iii. Member States may activate additional cyber crisis management mechanisms or instruments depending on the nature and impact of the incident;

iv. When the IPCR is activated in information sharing mode, the ISAA support capability is triggered, increasing information exchanges via the IPCR web platform and ensuring a shared situational overview. The situational reports from EU-CyCLONe and the CSIRTs network should remain the main instruments presenting the common situational awareness on the operational and technical levels respectively. These reports may inform the ISAA reports;

v. In case of an incident that requires activation of Union-level response actions, in particular relevant Union-level horizontal and sectoral crisis management mechanisms listed in the Annex II, the Council, in cooperation with the Commission and the High Representative, should ensure coherence and coordination between the responses to the cyber crisis and related Union-level response actions;

vi. Where relevant mechanisms, in particular the services of the Cybersecurity Reserve, are requested, the Commission services and, when appropriate, the EEAS, as well as relevant Council bodies, notably the HWPCI and the Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats ('HWP-ERCHT'), as appropriate, should coordinate as regards the design and implementation of measures, as well as the appropriate decision-making process with additional measures, in line with the Hybrid Toolbox[14] in the case of malicious cyber activities that are part of a wider hybrid campaign.

Response to a large-scale cybersecurity incident or cyber crisis for which IPCR is activated in full activation mode

(56) The steps listed in the section '*Response to a large-scale cybersecurity incident or cyber crisis for which IPCR is not activated in full activation mode'* above should be implemented.

(57) When the IPCR is activated in full activation mode, the ISAA reports serve to ensure common situational awareness on the political level. The situational reports from EU-CyCLONe and the CSIRTs network should remain the main instruments presenting the common situational awareness on the operational and technical level respectively. These reports may inform the ISAA reports.

(58) In the event of a large-scale cybersecurity incident or cyber crisis that results in the activation of the IPCR in full activation mode, all actors should respond in close coordination in a whole-of-government approach as follows:

(a) coordination of the response at Union political level is carried out by the Council, using the IPCR arrangements;

14 The Hybrid Toolbox is a framework for a coordinated response to hybrid campaigns affecting the EU and its Member States, comprising for instance preventive, cooperative, stability, restrictive and recovery measures and support solidarity and mutual assistance.

(b) EU-CyCLONe, in cooperation with the CSIRTs network, should provide clear information to the political level on impact, possible consequences and response and remediation measures of the incident, including by contributing to the ISAA reports;

(c) in addition to the ISAA capability, the Presidency of the Council of the European Union would convene IPCR roundtables to enable political and strategic coordination of EU response, with actions under Cyber Blueprint and the work of relevant sectoral mechanisms feeding into the work of the IPCR. The roundtables can moreover identify some specific gaps in the response and invite specific EU actors to address them and report back at future roundtables, to support the political and strategic coordination in IPCR;

(d) the Presidency of the Council of the European Union should consider inviting EU-CyCLONe to relevant meetings, including roundtables under the IPCR arrangements and other relevant Council meetings;

(e) Member States' crisis management authorities should ensure coherence and coordination between the sectoral responses to the cyber crisis supported by cyber crisis management authorities;

(f) the possible diplomatic responses should be considered and conducted in line with Chapter IX.

VIII: Public communication efforts

(59) While communicating to the population of an individual Member State on an ongoing large-scale cybersecurity incident or cyber crisis, including as a part of awareness raising is a national competence, Member States, the Commission and the High Representative should aim to coordinate their public communication to the extent possible. The IPCR informal network of crisis communicators may be involved, as appropriate.

(60) For the purposes of preparing for large-scale cybersecurity incidents and cyber crises, Member States and, as appropriate, the Commission and CERT-EU, are invited to exchange on their communication efforts within EU-CyCLONe and the CSIRTs network, including best practices, such as advisories or awareness raising campaigns. ENISA should provide tools supporting such an exchange and ensuring an easy access.

(61) In case of a large-scale cybersecurity incident or cyber crisis, Member States are invited to share within EU-CyCLONe information on their public communication efforts to build a common awareness and coordinate the actions. EU-CyCLONe on its own initiative or requested by the Council can share with the Council an overview of such approaches.

IX: Diplomatic response and cooperation with strategic partners

(62) The High Representative, in close cooperation with the Commission and other relevant Union entities, should:

(a) support the decision-making in the Council, including through analyses, reports and proposals, on the use of possible measures as part of the EU Cyber Diplomacy Toolbox. This will enable the use of the full spectrum of Union tools available to prevent, deter and respond to malicious cyber activities, reinforcing its cyber posture and promoting international peace, security and stability in cyberspace;

(b) where a relevant incident is identified, facilitate the flow of necessary information with strategic partners, including with NATO when relevant;

(c) enhance coordination with strategic partners, including NATO when relevant, on response to malicious cyber activities by persistent threat actors, notably when using the EU Cyber Diplomacy Toolbox, in line with implementing guidelines.

(63) Member States, the High Representative, the Commission and other relevant Union entities should cooperate with strategic partners and international organisations to promote good practices and responsible state behaviour in cyberspace and ensure rapid and coordinated response in case of potential or large-scale cybersecurity incidents.

(64) European Union and NATO cooperation should be conducted in accordance with the agreed guiding principles of inclusiveness, reciprocity and transparency, and in full respect of the Union autonomous decision-making.

(65) The Commission and the High Representative, taking into account existing agreements such as the CERT-EU/NATO technical agreement of 2016, should establish points of contact for coordination with NATO in the event of a cyber crisis to exchange necessary information on the situation and the use of crisis response mechanisms to increase cooperation on and the effectiveness of response. To this end, the Union should explore ways to improve information sharing with NATO, in an inclusive, reciprocal and non-discriminatory manner, in particular through ensuring tools for secure communication while taking into account the information sharing standards of different Member States.

(66) As part of the Union cyber exercise rolling programme referred to in Chapter V above, the Commission services and the EEAS should consider organising an exercise at staff level with NATO, in order to test cooperation between civilian and military entities in the event of a large-scale cybersecurity incident or cyber crisis where Member States or NATO Allies seek responses to a cyber attack affecting their security. The exercise should be conducted in an inclusive and non-discriminatory manner, and in full respect of the agreed principles of the parameters of EU-NATO cooperation. The exercise should be conducted within the framework of the EU Integrated Resolve exercise (Parallel and Coordinated Exercise, 'PACE'). All necessary measures should be taken to ensure the participation of all actors referred to in the Cyber Blueprint.

(67) Joint Union level cyber exercises with the Western Balkan countries, the Republic of Moldova, Ukraine, as well as other strategic partners and like-minded third countries should also be considered, in consultation with the Council, the Commission and the High Representative.

X. Coordination of cyber crisis management with military actors at the EU level

(68) Member States should continue to strengthen cooperation between civilian and military cyber actors at the national level.

(69) EU-CyCLONe and the CSIRTs network should identify possible ways and procedures to cooperate with the relevant EU military actors, such as the EU Cyber Commanders Conference and the Military Computer Emergency Response Team Operational Network ('MICNET') in order to benefit from a joint military and civilian perspective, in particular through joint meetings. EU-CyCLONe and the CSIRT network should inform the Council on the progress made in regards to such a cooperation.

(70) The affected Member State is invited to inform EU-CyCLONe, as well as the EEAS, if relevant national or multinational military response capabilities are used in the context of a large-scale cybersecurity incident or cyber crisis, and the provision of this information is mutually agreed between the user and the provider of such response capability.

(71) As part of the Union cyber exercise rolling programme referred to in Chapter V above, the Commission and the High Representative should consider organising a joint exercise in order to test cooperation between both civilian and military cyber actors in the event of a large-scale cybersecurity incident affecting Member States.

XI: Recovery and lessons learnt from a cyber crisis

(72) Member States, relevant Union entities and networks should collaborate during the recovery phase after a cyber crisis to ensure the swift restoration of core functionalities. The law enforcement communities should also, where relevant, be involved in such a cooperation. In this phase, cooperation with the private sector is crucial, particularly in facilitating the recovery of data and the reinstatement of systems. Effective coordination among stakeholders should prioritise minimising disruption and ensuring business continuity.

(73) Member States, relevant Union entities and networks should work together in the recovery phase building on lessons learnt from cyber crises or managed cybersecurity incidents in the past, as well as incident reports, in particular in the context of the European Cybersecurity Incident Review Mechanism established by Regulation (EU) 2025/38.

(74) A comprehensive list of lessons learnt from cyber crises or managed cybersecurity incidents in the past and best practices should be provided by EU-CyCLONe to the CSIRTs network, the NIS Cooperation Group, and the Council. ENISA should ensure that these lessons learnt are properly reflected in future preparedness activities and when considering the planning of future exercises.

XII: Secure communication

(75) Based on the mapping of existing secure communications tools[15], the Commission should propose by the end of the 2026 an interoperable set of secure communication solutions. The Council, the Commission, the High Representative, EU-CyCLONe and the CSIRTs network should agree on this set by the end of 2027. These solutions should benefit from the actions in the area of secure communications that EU institutions could take under the EU Preparedness Union Strategy and should cover the full range of communication modes required (voice, data, video-teleconferencing, messaging, collaboration and document sharing and consultation). The solutions should meet commonly defined requirements for the protection of sensitive non-classified information. Solutions based on open protocol with open-source implementations suitable for real-time communication, managed by an EU-resident entity should be used.

(76) EU-CyCLONe and the CSIRTs network, for the purpose of exchanging information classified as RESTREINT UE/EU RESTRICTED, if needed, should be able to use secure communication channels ensured for the EU institutions, bodies and agencies for exchanging classified information between themselves and with Member States.

15 WK 862/2023.

(77) The European Cybersecurity Industrial, Technology and Research Competence Centre ('ECCC'), established under Regulation (EU) 2021/887[16], without prejudice to the future multiannual financial framework, should consider funding through the Digital Europe Programme to assist Member States in deploying secure communication tools. Any duplication of investments in interoperable secure systems should be avoided

(78) In particular, EU entities and Member States should develop contingencies for severe crises where normal communication channels relying on Internet or telecommunications networks are disrupted or unavailable.

(79) Communication and information sharing mechanisms between law enforcement and cybersecurity networks, particularly at the technical level, should be established for effective cyber crisis response. These mechanisms should respect the role of each party and avoid interfering with ongoing operations and guarantee redundancy of communications. The EU Critical Communication System ('EUCCS') currently under development can benefit the joint response with relevant cyber communities.

XIII: Final provisions

(80) EU-CyCLONe, in cooperation with the CSIRT network and other main actors in the EU Cyber Crisis Management Ecosystem, supported by ENISA, should develop, within one year following the publication of the Recommendation, detailed process flow diagrams outlining the information flows between relevant actors, decision-making processes and reports developed during the management of large-scale cybersecurity incident or cyber crisis as described in this Recommendation. The flow diagrams should cover different cooperation modes and layers. They should be updated when necessary.

[16] 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. 1–31.

(81) To support the effective application of the revised Cyber Blueprint, and building on the experience gained through the joint cyber exercises conducted under it, the Council may develop, if needed, a set of implementing guidelines. These guidelines could address the practical challenges identified in the course of exercises and close identified gaps and missing links in coordination, communication, and operational interaction.

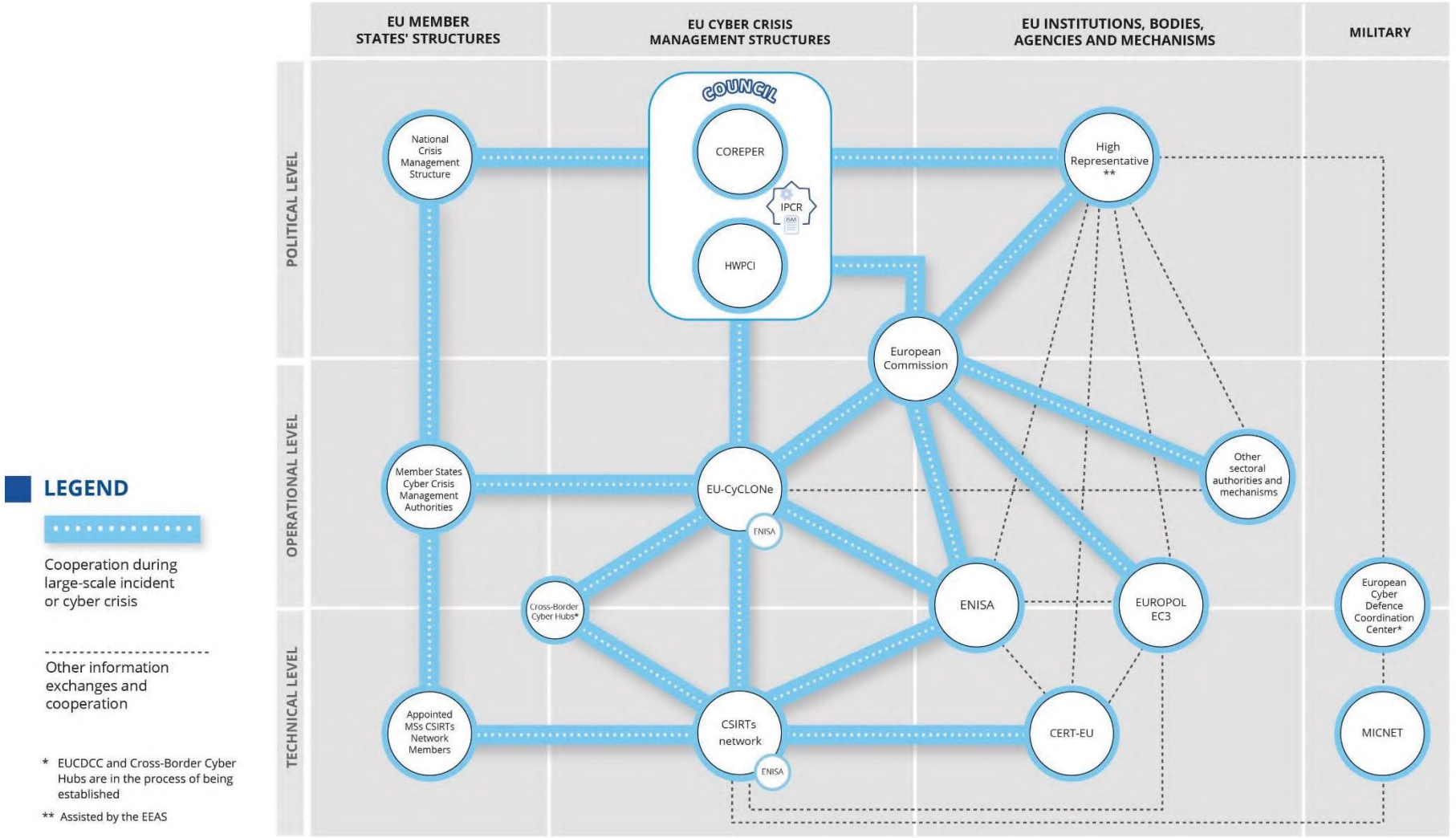
(82) This Recommendation should be reviewed by the Commission in cooperation with the Member States, at least every four years following its publication. Following each review, the Commission should publish a report and present it to the Council. The Commission and Member States should take into account, in particular, the impact of the changing threat landscape, the results of joint exercises and legislative changes – in particular any possible changes stemming from the revision of Regulation (EU) 2019/881.

Done at Brussels,

For the Council

The President

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) Involvement of the main actors across the cyber crisis management life cycle (large-scale cybersecurity incidents and cyber crises)

	Preparedness	Detection	Response to a large scale cybersecurity incident or a cyber crisis			Public communication	Recovery and lessons learnt
			on technical level	on operational level	on political level		
Member States	X	X	X	X	X	X	X
Commission	X			X	X	X	
High Representative assisted by EEAS	X			X	X	X	
Council	X				X	X	X
ENISA	X		X	X			
CERT-EU	X	X	X	X		X	X
CSIRTs network	X	X	X				X
EU-CyCLONe	X			X	X		X

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

Actor	Level	Role and competence	Reference
CERT-EU	Technical / Operational	Coordinates the crisis response at technical level and the management of major incidents affecting Union entities. Maintains an inventory of the available technical expertise that would be needed for incident response in the event of major incidents and assists the IICB in coordinating Union entities' cyber crisis management plans for major incidents. Member of the CSIRTs Network. Supports the Commission in EU-CyCLONe on the coordinated management of large-scale cybersecurity incidents and crises. Acts as the cybersecurity information exchange and incident response coordination hub, facilitating the exchange of information regarding incidents, cyber threats, vulnerabilities and	Regulation (EU, Euratom) 2023/2841 Regulation (EU) 2025/38

Actor	Level	Role and competence	Reference
		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.	
Council of the European Union	Political	Policy-making and coordinating functions. Is entrusted with the IPCR which concerns coordination and response at Union political level.	Article 16 of the Treaty on European Union
Presidency of the Council of the European Union	Political	Decides (except where the solidarity clause is invoked under TFEU Article 222 of the Treaty on the Functioning of the European Union) whether to activate the IPCR, in consultation affected with Member States as appropriate, as well as the Commission and the HR.	Article 16 of the Treaty on European Union Council Implementing Decision (EU) 2018/1993
Cross-Border Cyber Hubs	Technical	Cross-Border Cyber Hub is a multi-country platform, established by a written consortium agreement that brings	Regulation (EU) 2025/38

Actor	Level	Role and competence	Reference
		together in a coordinated network structure National Cyber Hubs from at least three Member States, and that is designed to enhance the monitoring, detection and analysis of cyber threats to prevent incidents and to support the production of cyber threat intelligence, in particular through the exchange of relevant data and information, anonymised where appropriate, as well as through the sharing of state-of-the-art tools and the joint development of cyber detection, analysis, and prevention and protection capabilities in a trusted environment; 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.	

Actor	Level	Role and competence	Reference
CSIRTs Network	Technical	Contributes to the development of confidence and trust and promotes swift operational cooperation among Member States. Is the main network to exchange 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 related to that incident and associated cyber threats. The Network may also facilitate a coordinated response to an incident that has been identified within the jurisdiction of a requesting member. Provides assistance to Member States in managing cross-border incidents and explores further forms of cooperation, including mutual assistance. Receives information from Member States regarding their	Directive (EU) 2022/2555 Regulation (EU) 2025/38

Actor	Level	Role and competence	Reference
		requests to the EU Cybersecurity Reserve.	
Cyber Commanders conference		A forum for cyber commanders at the national level within Member States to collaborate and exchange vital information regarding 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), including the EU Military Staff (EUMS).	Joint Communication on the EU Policy on Cyber Defence (2022)
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. Certain general Union level preparedness actions under the	Article 17 of the Treaty on European Union Implementing Decision (EU) 2018/1993 Decision No 1313/2013/EU Directive (EU) 2022/2555

Actor	Level	Role and competence	Reference
		UCPM decision, 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 that has or is likely to have a significant impact on services and activities falling within the scope of Directive (EU) 2022/2555. Observer in the CSIRTs network. Overall responsibility for the implementation of the EU Cybersecurity Reserve. Point of contact in the Inter-institutional Cybersecurity Board for sharing relevant information in relation to major incidents to EU-CyCLONe. Consulted by the Presidency of the Council on decisions to activate or deactivate the IPCR (except where the solidarity clause	Regulation (EU) 2025/38 Regulation (EU, Euratom) 2023/2841

Actor	Level	Role and competence	Reference
		is invoked under Article 222 TFEU). Commission services prepare, with the EEAS, the ISAA reports.	
European Union Agency for Cybersecurity (ENISA)	Technical / operational	Carries out tasks for the purpose of achieving a high level of cybersecurity across the Union, including by actively supporting Member States and Union institutions Provides the secretariat for the CSIRTs network and EU-CyCLONe. Prepares a regularEU Cybersecurity Technical Situation Report on incidents and cyber threats (with the EC3 and CERT-EU and in close cooperation with the Member States). Contributes to developing a common response to large-scale cross border incidents or crises mainly by: - aggregating and analysing reports from national sources;	Directive (EU) 2022/2555 Regulation (EU) 2019/881 Regulation (EU) 2025/38 Regulation (EU) 2024/2847

Actor	Level	Role and competence	Reference
		- ensuring flow of information between technical, operational and political levels; - upon request facilitating handling of incidents; - supporting Union entities with regards to public communication; - supporting the Member States with regards to public communication, upon request; - testing incident response capabilities and regularly organising cybersecurity exercises. Acts as a contracting authority where it has been entrusted to operate and administrate the EU Cybersecurity Reserve, partly or fully. Organises biennially large-scale comprehensive cybersecurity exercise at Union level with technical, operational or strategic elements. Prepares an incident review report in collaboration with the Member State concerned and other relevant stakeholders, to assess the causes, impact and mitigation of an incident (at the request of the	

Actor	Level	Role and competence	Reference
		Commission or EU-CyCLONe and with the approval of the concerned Member State). Informs EU-CyCLONe if information provided under the reporting obligations of the Cyber Resilience Act are relevant for the coordinated management of large-scale cybersecurity incidents and crises at an operational level.	
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 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.	Directive (EU) 2022/2555 Regulation (EU) 2025/38

Actor	Level	Role and competence	Reference
		Assesses the consequences and impact of relevant large-scale cybersecurity incidents and crises and proposes possible mitigation measures. Discusses, upon the request of a Member State concerned, national large-scale cybersecurity incident and crisis response plans. Develops, together with ENISA and the Commission 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	Political	Leads on and coordinates the Union's efforts to address external	Council Decision 2010/427/EU

Actor	Level	Role and competence	Reference
Foreign Affairs and Security Policy assisted by the European External Action Service		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, including 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 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). Supports the EU Cyber Commanders Conference. Supports the EU Military Computer Emergency Response	

Actor	Level	Role and competence	Reference
		Team Operational Network (MICNET). Consulted by Presidency of the Council on decisions to activate or deactivate the IPCR (except where the solidarity clause is invoked under Article 222 TFEU). EEAS prepares, with the Commission services, the ISAA reports.	
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.	Joint Communication on the EU Policy on Cyber Defence (2022)
Europol	Operational	Provides operational and technical support to the Member States' competent authorities for the prevention and deterrence of cybercrime. Assists the competent authorities of the Member States, upon their request, in responding to cyberattacks of suspected criminal origin.	Regulation (EU) 2016/794, including all amendments

Actor	Level	Role and competence	Reference
Interinstitutional Cybersecurity Board		Establishes a cyber crisis management plan with a view to supporting, at an operational level, the coordinated management of major incidents affecting Union entities and to contributing to the regular exchange of relevant information. Coordinates the adoption of individual Union entities' cyber crisis management plans 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; supported by the European Defence Agency.	Cyber Defence Joint Communication 2022

Actor	Level	Role and competence	Reference
Single Intelligence Analysis Capacity (SIAC)		Composed of (1) EU Intelligence and Situation Centre (EU INTCEN) and (2) the EU Military Staff Intelligence Directorate (EUMS INT) SIAC. Provides strategic intelligence on foreign policy, terrorism, and cyber and hybrid threats, and Handles military intelligence for CSDP missions and supports Union defence and crisis management operations. Under the authority of the High Representative.	Articles 38 and 42 to 46 of the Treaty on European Union

(3) Relevant Union-level crisis management mechanisms and platforms

Mechanism	Horizontal/ sector/ cyber-specific	Description	Reference
ARGUS	Horizontal	The Commission's coordination process and general alert system for a coherent response in the event of a major transboundary crisis requiring action at the EU level. It brings together all the relevant services and Cabinets to decide on and coordinate measures. 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	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 March 2022)

Mechanism	Horizontal/ sector/ cyber-specific	Description	Reference
		professionals on the ground in Union delegations.	
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 relation to cyber threats and the prevention of incidents in the Union.	Regulation (EU) 2025/38
Cyber Diplomacy Toolbox (Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities)	Cyber-specific	Allows for a 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, 8 June 2023
EU Cybersecurity 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

Mechanism	Horizontal/ sector/ cyber-specific	Description	Reference
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, on the Union, Member State, regional and entity level. Contains provisions specific to crisis management and cooperation with the CSIRTs and EU-CyCLONe in cases when a large-scale cybersecurity incident has an impact on other sectors depended on the security of electricity supply.	Commission Delegated Regulation (EU) 2024/1366
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 Implementing guidelines for the Framework for a coordinated EU response to hybrid campaigns, 14 December 2022

Mechanism	Horizontal/ sector/ cyber-specific	Description	Reference
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 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.	Guiding framework for the practical establishment of the EU Hybrid Rapid Response Teams (21 May 2024) Operational Guidance for the Deployment of Hybrid Rapid Response Teams, approved by Coreper 4 December 2024
IPCR	Horizontal	Supports rapid and coordinated decision-making at Union political level for major and complex crises. 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	Council Implementing Decision (EU) 2018/1993

Mechanism	Horizontal/ sector/ cyber-specific	Description	Reference
		activate IPCR in information sharing mode. The work of IPCR is informed by the ISAA reports prepared by the Commission services and the EEAS. Such reports are based on relevant information and analyses provided by the Member States (e.g. from relevant national crisis centres), and by the relevant Union Agencies and bodies.	
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.
PESCO Cyber Rapid Response Teams (CRRT)	Cyber-specific	PESCO CRRTs is a commonly developed EU Member States' civilian-military cyber defence capability to respond swiftly to cyber	Article 42 (6), Article 46 and Protocol 10 of the Treaty on European Union.

Mechanism	Horizontal/ sector/ cyber-specific	Description	Reference
		incidents and cyber crises as well as perform preventative actions, such as vulnerability assessments and election monitoring. PESCO CRRTs mission is to provide cyber support, upon request, to the EU Member States, EU institutions, bodies and agencies, military EU CSDP missions and operations, as well as partner countries.	

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	Horizontal	Ensures civil protection cooperation to improve prevention, preparedness, and response to disasters.	Decision 1313/2013.

Mechanism (UCPM)			
CISE - Common Information Sharing Environment	Maritime specific covering seven sectors.	CISE - is a network that connects systems of EU/EEA authorities with responsibility in maritime surveillance. CISE enables the exchange of relevant information across borders and different sectors in a seamless and automated way.	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 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) Health Security Commitee
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). ELI: https://data.europa.eu/eli/reg/2024/2690/oj).

[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, 2025/38, 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. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022JC0049

[13] *OJ C, C/2024/4371, 5.7.2024.* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C_202404371