Council of the European Union
General Secretariat

Brussels, 24 April 2025

WK 5108/2025 INIT

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:	Presidency
To:	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 - Third Presidency compromise

Delegations will find attached the third Presidency compromise text of the abovementioned proposal for a Council Recommendation. The text in annex indicates the amendments compared to the second Presidency compromise text as set out in WK 4493/2025.

EUROPEAN
COMMISSION

Brussels, XXX
[…](2025) XXX draft

Proposal for a

COUNCIL RECOMMENDATION

for an EU Blueprint on cybersecurity crisis management

Proposal for a

COUNCIL RECOMMENDATION

for an EU Blueprint on 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 threats 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.

(2a) Given the interdependencies and interconnections between Union entities' and Member States' ICT environments, 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 to 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 Cyber Blueprint.

(3) In the interest of efficiency and effectiveness, in case of a crisis for which the EU Integrated Political Crisis Response ('IPCR') arrangements have been activated, the EU Cyber Blueprint should fully respect the IPCR arrangements for the coordination of the

[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

response, and political and strategic coordination would take place in the IPCR. The IPCR arrangements remain the main tool for horizontal coordination of response at Union political level. The decision to activate or deactivate the IPCR is taken by the ~~Council~~ Presidency of the Council of the European Union, in accordance with the Council Implementing Decision (EU) 2018/1993[1]. Integrated Situational Awareness and Analysis ('ISAA') reports prepared by Commission services and the EEAS support the work of IPCR in both its full and information-sharing activation modes.

(4) Member States have the primary responsibility in the management of cybersecurity incidents and cyber crises ~~as defined in Chapter II of this Recommendation.~~ 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.

(5) Commission Recommendation (EU) 2017/1584[2] on coordinated response to large-scale cybersecurity incidents and ~~cyber~~ 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 broader Union crisis management, 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.

~~(8~~(5a) Some definitions used in this Recommendation are based on definitions and terms used in Directive (EU) 2022/2555. 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.

(6) An updated Recommendation setting out a blueprint on cybersecurity ('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. The Cyber Blueprint aims~~is~~ to support the broader framework of EU civilian-military relations in the context of cyber crisis management against the background of deepening EU-NATO relations,

[2] 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, ELI: http://data.europa.eu/eli/reco/2017/1584/oj).

where possible including through inclusive, reciprocal and non-discriminatory enhanced information-sharing mechanisms in cyber crisis management.

(~~9~~7) 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 ~~real-life~~physical consequences. This Recommendation complements the IPCR arrangements and wider Union crisis mechanisms, including the Commission's general rapid alert system ARGUS, the Union Civil Protection Mechanism (UCPM) supported by the Emergency Response Coordination Centre (ERCC), the European External Action Service's Crisis Response Mechanism (CRM), as well as other processes, such as those described in the EU Cyber Diplomacy Toolbox, the Hybrid Toolbox[3] and in the revised EU Protocol for countering hybrid threats. ~~It also complements the Cyber Diplomacy Toolbox (CDT).~~ It also complements and should be coherent with the Council Recommendation on a blueprint to coordinate a response at Union level to disruptions of critical infrastructure with significant cross-border relevance ('Critical Infrastructure Blueprint') which covers non-cyber physical resilience, and which aims at improving coordination of response at Union level in this area.

(~~10~~8) EU-CyCLONe ~~should remain~~is the ~~main horizontal supporting~~ network for coordination of ~~response~~management of large scale cybersecurity ~~relevant stakeholders~~ incidents and crises at the operational level also in case of cross~~multi~~-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 the EU-CyCLONe should be avoided. EU-CyCLONe should ~~serve as an EU level central hub to~~ gather operational information also from the sectors and feed into the political level.

(~~11~~9) Member States should make full use of the financial resources available for cybersecurity provided by relevant Union programmes. ~~The Commission~~It should ~~ensure~~be ensured that these programmes impose minimal administrative burdens on ~~Member State~~applicants for the funding and ~~facilitate~~ the participation of Member States in these programmes is facilitated by providing relevant guidance on viable financial support options.

(10) The 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 coordination and capability through the EU crisis coordination hub within the Emergency response Coordination Centre.

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

HAS ADOPTED THIS RECOMMENDATION:

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

Aim and scope

(1) This Recommendation (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 ~~arising from such incidents.~~. The framework reflects the roles of both Member States and Union entities within their respective ~~mandates and~~competences, with full respect of ~~their~~national laws and internal rules to ensure comprehensive and coordinated action at ~~the~~ Union level.

(3) The Cyber Blueprint should be applied in coherence with the Critical Infrastructure Blueprint, in particular in the case of incidents affecting both the physical resilience and the cybersecurity of critical infrastructure[4].

(4) 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 Annex II. Relevant cybersecurity stakeholders should help and assist in ~~meeting~~reaching the goals of those sectoral mechanisms, both on national and Union level.

(5) In case of an EU-wide cross~~multi-dimensional~~sectoral crisis with cyber ~~elements~~aspects, coordination of the response at Union political level ~~of the response shall~~ should be carried out by the Council, using the EU Integrated Political Crisis Response (IPCR) set out in Council Implementing Decision (EU) 2018/1993. ~~In case of~~When the IPCR has been activated~~,~~ measures under the Cyber Blueprint should ~~be part of~~complement the EU response at political level, providing specific support on cybersecurity. ~~The political and strategic coordination should take place in the IPCR.~~

Guiding principles

(6) 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 CSIRTs network and EU-CyCLONe, in line with the networks' Standard Operating Procedures (SOPs). ~~In case of a large-scale cybersecurity incident or cyber crisis, cooperation and information exchange can be increased within the CSIRTs network and EU-CyCLONe on the basis of their 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 cyber crisis affecting them. With a view to potential cross-border effects, the Council, the Commission, the High Representative, ENISA, 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 ~~EU entities~~

[4] The Critical Infrastructure Blueprint further details coordination in such cases in its Section 4 of Part I of its Annex

themselves. Where the IPCR is activated to respond to a crisis, the work of relevant entities and activated sectoral mechanisms should continue and should feed into and support the political and strategic coordination taking place in the IPCR.Union entities themselves.

(c) *Complementarity*: this Recommendation takes fully into account existing crisis management mechanisms at Union level listed in Annex II, in particular the IPCR arrangements, ARGUS, and the EEAS Crisis Response Mechanism. This Recommendation takes into account the modified mandates of the CSIRTs network and EU-CyCLONe, as well as Regulation (EU, Euratom) 2023/2841. Where the IPCR is activated to respond to a crisis, 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 and . Informal non-disclosure agreements such as the Traffic Light Protocol system 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.

(7) 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. The This cooperation, within the framework of the Cyber Blueprint, benefits in this context from the implementation arrangements of articlesArticles 22 and 23 of Regulation (EU, Euratom) 2023/2841, as mandatedin particular the cyber crisis management plan is established, among other things, to the IICB in Article 11, point (q) of the same Regulation.contribute to the regular exchange of relevant information among Union entities and with Member States. While the Cyber Blueprint does not interfere with how Union entities define their internal procedures, each entity should clearly define the procedural arrangements used for working with other entities. These procedural arrangements should be jointly agreed between the entities concerned and clearly documented.

II: Definitions

(8) 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 (as defined in Article 6, point (6) of Directive (EU) 2022/2555);;

(b) Significant incident is 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 (as reffered to in Article 23(3) of Directive (EU) 2022/2555);;

(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 ~~(as defined in Article 6, point (7) of Directive (EU) 2022/2555), for the purposes of this Recommendation, this definition also extends to the sectors outside of the scope of Directive (EU) 2022/2555;~~;

(d) ‘cyber crisis’ means a large-scale cybersecurity incident that escalated into fully-fledged crises 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~~.~~ (e) ‘crisis’ means a situation of such a wide-ranging impact or political significance, that it requires timely policy coordination and response at Union political level;

III: National Cyber Crises Management Structures and Responsibilities

(9) 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 the Directive (EU) 2022/2555 has one or more cyber crisis management authorities, as well as one or more CSIRTs.

(10) 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 a 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.

(11) In accordance with Article 9(4) of Directive (EU) 2022/2555, Member States should adopt national large-scale cybersecurity incident and ~~cyber~~ crisis response plans~~, in accordance with Article 9(4) Directive (EU) 2022/2555.~~,. These plans include amongst 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.

(12) In accordance with Article 9(1) of Directive (EU) 2022/2555, Member States should ensure coherence with the existing frameworks for generic national crisis management~~, in accordance with Article 9(1) Directive (EU) 2022/2555. Member States should provide input to inform the IPCR.~~,. In case of activation of the IPCR, ~~input~~national crisis management authorities should, for the purpose of informing the IPCR, collect the inputs from the cyber crisis management authorities ~~should feed into national crisis management structures which also include input from~~and national sectoral crisis mechanisms ~~for the purpose of informing the IPCR.~~

(13) ~~Member States within~~In accordance with Article 9 para 5 of the Directive (EU) 2022/2555, EU-CyCLONe, upon the request of a Member State concerned, should exchange on ~~their~~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 practises and reflect if the overall framework would work in practise.

(14) EU- CyCLONe ~~is~~and the IICB are invited to exchange ~~with the IICB Chair, via the point of contact under Article 23(2) of Regulation 2023/2841~~ on coherence of crises management plan adopted by IICB in accordance with Article 23 of the Regulation (EU, Euratom) 2023/2841 with national large-scale cybersecurity incident and crisis response plans.

(15) 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

(16) The CSIRTs network ~~is established in order to contribute~~contributes to the development of confidence and trust and ~~to promote~~promotes swift and effective operational cooperation among Member States. It is the main 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, point (3) of Directive (EU) 2022/2555. The Chair of the CSIRTs network participates as an observer in the IICB. The CSIRTs network operates at the technical level.

(16a) CERT-EU is the Cybersecurity Service for all Union institutions, bodies, offices and agencies (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 the EU-CyCLONe. CERT-EU operates at the technical level~~.~~ and is responsible for coordinating the management of major incidents affecting Union entities.

(16b) EU-CyCLONe supports the coordinated management of large-scale cybersecurity incidents and cyber crises at operational level and ~~to ensure~~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 the EU-CyCLONe ~~participates~~may participate as an observer in the IICB. EU-CyCLONe works as an intermediary between the technical and political level, in particular during large-scale cybersecurity incidents and cyber crisis.

(17) ENISA is ~~a~~ the Union agency carrying out the tasks assigned under Regulation (EU) 2019/881 for the ~~purposed~~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 ~~ENISA~~ assists Member States by regularly organising cybersecurity exercises at Union level. 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.

(18) The Council of the European Union ~~plays a key role in shapping strategic priorities at Union level~~carries out policy-making and ~~fostering coordination between Member States, the Commission, the High Representative and relevant EU agencies. It ensures harmonised implementation of cybersecurity measures across the EU.~~coordinating functions. The Council operates through Council configurations, COREPER, and relevant Council preparatory bodies, especially the Horizontal Working Party for Cyber Issues, as well as, where relevant, the IPCR arrangements.

(19) The Commission ~~is the~~ exercises coordinating, executive ~~body of the European Union.~~and management functions. It is responsible for general Union-level preparedness and the coordination of situational awareness actions, including the management of the ERCC and the Common Emergency Communications and Information system. It facilitates coherence and coordination between related Union-level crisis response actions. It is consulted on decisions to activate or deactivate the IPCR~~, and its~~. Commission services and the EEAS develop the ISAA report. 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 the observer in other cases. It is the point of contact of the IICB in EU-CyCLONe. It is an observer in the CSIRTs network.

(20) The High Representative for Foreign Affairs and Security Policy (HR), assisted ~~supported~~ by the European External Action Service (EEAS), conducts the Union's ~~is responsible for steering the EU'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 ~~is~~ also develops with the Commission~~co-responsible for developing~~ the IPCR ~~Integrated Situational Awareness and Analysis (~~ISAA report~~)~~.

(21) 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

(22) Member States~~,~~ and relevant Union entities ~~and essential and important entities under Directive (EU) 2022/2555,~~ 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.

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

(24) In order to enhance shared situational ~~awarness~~awareness and to facilitate ~~assessment~~assessment of the EU impact, EU-CyCLONe and the CSIRTs network

with support of ENISA should use internally agreed reporting mechanism to ~~have~~produce an EU overview of technical and operational activities based on the information gathered at the national level.

(25) 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;

~~(d) cooperate with the IICB to ensure effective exchange of information gathered by the Union entities.~~

(25a) EU-CyCLONe, the CSIRTs network and the IICB should cooperate to ensure effective exchange of relevant information.

(26) ENISA as the secretariat for the CSIRTs network and EU-CyCLONe has a central role to support 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. In accordance with Directive (EU) 2022/2555 and Regulation (EU) 2019/881, Member States and relevant Union ~~entities, in particular ENISA, and via its cyber partnership programme should~~entities should coordinate with the private sector, including open-source communities and manufacturers, to improve information sharing~~, building~~. 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.

~~(27) The Chairs of the CSIRTs network and EU-CyCLONe, with the support of ENISA, should continue to strengthen and promote swift and effective operational cooperation among Members of both networks.~~

~~(28) ENISA within its role as secretariat, should closely involve with both Networks and support them to achieve a common situational awareness for preparedness during large-scale cybersecurity and cyber crises to support Member States in their response and decision making.~~

(29) 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 ~~12~~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~~.~~

~~In support of this common taxonomy and situational awareness, 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~~.

Technical level

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

(31) 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.

(32) 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.

(33) 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 guidelines and recommendations towards Union institutions, bodies, offices and agencies. CERT-EU should ensure sharing the relevant information through the CSIRTs network.

Operational level

~~(34) In accordance with Directive (EU) 2022/2555, Member States' cyber crisis management authorities should cooperate within EU-CyCLONe.~~

(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 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 ~~gather intelligence about shifts in the global political environment and new technological~~monitor international developments, ~~in particular in the context of critical sectors and current threats~~ which affect cybersecurity (including cyber threats, hybrid threats, foreign information manipulation and interference (FIMI) ~~and~~including disinformation where relevant). Initiatives like the Joint Cyber Assessment Reports (JCAR), analyses provided by the

European Union Single Intelligence and Analysis Capability Centre (SIAC) and other relevant products providing specialised insights should be taken into account.

(38) The High Representative should continue ~~informing~~to inform and involve Member States ~~about EU's~~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 ~~and~~, including cyber sanctions.

~~(39) A monitoring page on the IPCR web platform could be initiated by the Presidency to monitor a possibly developing crisis and allow Member States and EU institutions and bodies to share information even without the activation of IPCR.~~

Common exercises

(40) The Commission ~~and~~in coordination with the High Representative, supported by ENISA, after consulting the EU-CyCLONe and the CSIRTs network should develop 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 EU Civil Protection Mechanism (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 cover exercises ~~that involve~~developed using the EU coordinated risks assessments scenarios. It should cover exercises involving all relevant actors, ~~including~~in particular the private sector and NATO ~~and are developed using the scenarios based on the EU coordinated risk assessments.~~.

(42) ENISA, in its role of secretariat of the CSIRTs network and EU-CyCLONe, should ensure the systematic collection of lessons ~~learned~~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) ~~The lessons learnt from the exercises should be taken into account by the respective~~All actors and networks ~~to~~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~~networks and, if needed, swiftly adapt SOPs.

(44) The ~~Chairs of EU-CyCLONe and~~ NIS Cooperation Group should invite the CSIRTs network ~~should reflect if~~, EU-CyCLONe, and ENISA, to present lessons learnt from the exercises, as well as the identification and proposed way of implementation of ~~the lessons learnt requires the involvement of the NIS Cooperation Group. On the basis of the input given by the EU-CyCLONe and CSIRTs network the NIS Cooperation Group should undertake necessary policy steps to address relevant challenges~~resulting actions.

(45) The Council may invite Chairs of the CSIRTs network, EU-CyCLONe and the NIS Cooperation Group, as well as 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 the Cyber Blueprint ~~within the framework of~~during the next Cyber Europe exercise. The exercise should involve all relevant actors, including the political level. ENISA is invited to coordinate with the ~~Council~~ Presidency of the Council of the EU 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) To address the complexity of cybersecurity incidents and the growing challenges in their detection, both public and private entities should implement threat-informed detection strategies across their digital infrastructures, to identify possible pre-positioning that may be leveraged subsequently for disruption purposes. According to Directive (EU) 2022/2555, when covert operations are identified, entities should proactively share relevant information with their partners well before situations escalate into crises.~~

(47) As noted in the Directive (EU) 2022/2555, information sharing contributes to an increased awareness of cyber threats, which, in turn, enhances entities' capacity to prevent such threats from materialising into incidents and enables entities to better contain the effects of incidents and recover more efficiently.

(48) 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.

(49) In accordance with Regulation (EU) 2025/38, the Cross-Border Cyber Hubs~~, already established~~ should ensure situational awareness and strengthen solidarity. In situations where Cross-Border Cyber Hubs obtain information related to a potential or ~~to be established under the Regulation (EU) 2025/38,~~ongoing large-scale cybersecurity incident, they should provide ~~all~~ relevant information ~~about identified threats, including methods to detect them,~~ to the CSIRTs network and inform, as an early warning, EU-CyCLONe.

(50) ~~A~~When a significant incident is observed, in particular causing immediate impact ~~can also~~, it might be ~~observed~~notified to or detected by CSIRTs, as well as by Member States' cyber crisis management authorities or other sectoral authorities. ~~In that~~ Member States are encouraged to share information related to such incident within the networks, which should consider taking appropriate actions. In case of a large-scale cybersecurity incident, it may require coordination by EU-CyCLONe ~~in the event of a large-scale cybersecurity incident.~~. The ~~escalation of cooperation modes~~activation of the CSIRTs network and EU-CyCLONe is independent from each other, however both networks are encouraged to continue cooperation with each other on the basis of agreed procedural arrangements. The decision to activate ~~the network is always a sole and independent decision of CSIRTs network or EU-CyCLONe, respectively.~~ rests solely and independently with each respective network.

(51) The CSIRTs network should advise EU-CyCLONe on whether an observed cybersecurity incident may be deemed a potential or ongoing large-scale cybersecurity incident. ~~ENISA should advice in line with paragraph (…).~~

(52) As indicated in Directive (EU) 2022/2555, the CSIRTs network and EU-CyCLONe should without delay ~~finalise~~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 where IPCR is not activated~~

(53) Effective response to large-scale cybersecurity ~~incidents or cyber crisis at~~incidents at the EU level depends on effective technical, operational and political cooperation in a whole-of-government approach.

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

(55) Response should be appropriate to the impact of the large-scale cybersecurity incident. 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.

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

(a) at the technical level:

- the affected Member States and their CSIRTs should cooperate with the affected entities to respond to incidents and provide assistance, where applicable;
- the CSIRTs should cooperate through the CSIRTs network to share relevant technical information about the incident; 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;
- ~~In accordance with Regulation (EU) 2025/38, the Cross-Border Cyber Hubs, already established or to be established under that Regulation, should provide all relevant information about identified threats, including methods to detect them, to the CSIRTs network and inform, as an early warning, EU-CyCLONe;~~
- When a CSIRT or Member States' cyber crisis management authority becomes aware of a significant incident, they are encouraged to share within the CSIRTs network or EU-CyCLONe ~~through their national single point of contacts in accordance with Directive (EU) 2022/2555;~~.
- The CSIRTs network ~~Chair~~, with the support of ENISA, should prepare an aggregation of national reports provided by ~~national CSIRTs (EU~~

~~Cybersecurity Incident Situation Report),~~CSIRTs, , which ~~is~~should be presented to EU-CyCLONe;

– 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 ~~prepare high-level strategic political messages and present them to~~brief the Council;

– 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 ~~or cyber crisis~~;

(b) at the operational level:

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

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

– EU-CyCLONe should assess the consequences and impact of relevant large-scale cybersecurity incidents and cyber crises and propose possible mitigation measures, and coordinate the management of the crisis;

– In case of a large cybersecurity incident with cross-~~multi-~~sectoral impact, that requires activation of Union-level response actions, in particular relevant Union-level horizontal and sectoral crisis management mechanisms listed in Annex 2, (a) depending on the type of Union-level sectoral crisis management mechanisms, appropriate actors may call for its activation;

(b) in case of activation of such sectoral mechanism, 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 relevant horizontal and sectoral Union level crisis mechanisms listed in Annex II and EU-CyCLONe and pursue an integrated cross~~multi-~~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 the requesting of assistance through UCPM

– If a monitoring IPCR page has been initiated, complementary, comprehensive information about the incident, its impacts and the measures taken should be shared among Member States and Union entities via the IPCR web platform.;

– In accordance with Directive (EU) 2022/2555, EU-CyCLONe should provide clear information to the political level on impact, possible consequences and response and remediation measures of the incident

– 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.

~~(b) at the operational level:~~

~~– Member States should mitigate the impact of the incident on the national level using appropriate measures;~~

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

~~– EU-CyCLONe should assess the consequences and impact of relevant large-scale cybersecurity incidents and cyber crises and propose possible mitigation measures, and coordinate the management of the crisis;~~

~~– The Commission, in cooperation with the High Representative where relevant, through EU-CyCLONe, should ensure coherence and coordination of the EU level operational measures in the cyber domain with related Union-level response actions, in particular relevant Union-level sectoral crises management mechanisms listed in Annex 2, and in relation to the requesting of assistance through UCPM;~~

~~– Where a potential or large-scale cybersecurity incident is detected including where there is multi-sectoral impact:~~

~~(a) the Commission should facilitate the flow of necessary information between points of contact for relevant horizontal and sectoral Union level crisis mechanisms listed in Annex II and EU-CyCLONe;~~

~~(b) relevant Union entities should support EU-CyCLONe in assessing consequences for sectors and the population;~~

~~– Comprehensive information about the incident, its impacts and the measures taken should be shared among Member States and EU institutions and bodies via the IPCR web platform, if a monitoring page has been initiated. In case the IPCR is activated in information sharing mode, this information will be complemented by ISAA reports;~~

~~– In accordance with Directive (EU) 2022/2555, EU-CyCLONe, based on technical information received from the CSIRTs network, should provide clear information to the political level on impact, possible consequences and response and remediation measures of the incident.~~

(c) at the political level:

– the Council ~~should~~may request briefings from the key stakeholders in particular the Commission, the EEAS and EU-CyCLONe in order to conduct appropriate political and strategic response;

– the Council supported by the Commission and the High Representative, could decide on the appropriate measures to respond to the large-scale cybersecurity incident;

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

– the Presidency of the Council may~~, without activating the IPCR,~~ 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. ~~If the monitoring page is activated comprehensive information about the incident, its impacts and the measures taken should be shared among Member States and EU entities;~~

~~– The Presidency of the Council may also decide to activate IPCR in information sharing mode, which would entail the production of ISAA reports to inform discussions in the Council on the response. The ISAA report will be complemented by the information shared through the monitoring page;~~

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 Annex 2, the Council, in cooperation with the Commission and where relevant the High Representative, should ensure coherence and coordination between the responses to the cyber crisis and related Union-level response actions.

– Where relevant mechanisms, in particular the services of the Cybersecurity Reserve ~~were~~, are requested, the ~~EEAS and appropriate~~ Commission services, and if appropriate the EEAS, as well as relevant Council bodies, notably the Horizontal Working Party on Cyber Issues (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[5] in the case of malicious cyber activities that are part of a wider hybrid campaign.

~~(57) In case of an incident that requires activation of Union-level response actions, in particular relevant Union-level sectoral crisis management mechanisms listed in Annex 2, and in relation to the requesting of assistance through the UCPM:~~

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

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

[5] 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.

~~(c) 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.~~

~~Large~~Response to cyber crisis

(58) The steps listed in the chapter r*esponse to a large-scale cybersecurity incident ~~or cyber crisis that results in the activation of the IPCR~~*

~~(58) The steps listed~~ above should be implemented.

(59) When the IPCR is activated to respond to a cyber crisis, whether in information-sharing or in full activation mode, the IPCR's ISAA reports serve to ensure common situational awareness~~. Information sharing between the Member States and EU institutions and bodies can also take place via the IPCR web platform when IPCR is activated~~ on the political level. The situational reports from EU-CyCLONe and the CSIRT should remain the main instruments presenting the common situational awareness on the technical and operational level respectively.

(60) In the event of a ~~large-scale cybersecurity incident or~~ cyber crisis that results in the activation of the IPCR in full 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;

(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 Integrated Situational Awareness and Analysis (ISAA) report under the IPCR arrangements;

(c) In addition to the ISAA capability, the Presidency would convene IPCR ~~crisis~~ roundtables to enable political and strategic coordination of EU response, with actions under the 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 Council Presidency should consider inviting ~~the Chair of~~ EU-CyCLONe to relevant meetings, including ~~crises roundtable meetings~~roundtables under the IPCR arrangements and other relevant Council meetings under the IPCR arrangements;

(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

(61) While communication to the population of an individual Member State on an ongoing large-scale cybersecurity incident or cyber crisis, as well as a part of awareness raising is a national competence, Member States ~~should~~may coordinate/ should aim for coordination of their public communication to the extent possible. The IPCR informal network of crisis communicators may be involved, as appropriate.

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

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

~~(64) In case of a large-scale cybersecurity incident or cyber crisis, based on the shared situational awareness developed in EU-CyCLONe, the HWPCI may organise an exchange of views on the public communication approaches of the Member States, the Commission and the High Representative, including to ensure that the crisis situation is not used to spread inaccurate information. If needed, the HWPCI should try to identify common ground, to facilitate coordination among Member States.~~

IX: Diplomatic response and cooperation with strategic partners

(65) 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 and reports, on the use of possible measures as part of the 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 Cyber Diplomacy Toolbox, in line with implementing guidelines.

(66) Member States, the High Representative, the Commission and other relevant Union entities should ~~collaborate~~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.

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

(68) The ~~Union~~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~~. Information sharing could be enhanced~~, in particular through ~~complementarity between the Union and NATO respective~~ensuring tools for secure communication ~~and information systems,~~ while taking into account the information sharing standards of different Member States ~~into account~~.

(69) As part of the Union cyber exercise rolling programme referred to in section II above, the Commission services and the EEAS should consider organising a joint exercise at staff level with NATO, in order to test cooperation between both civilian and military components in the event of a large-scale cybersecurity incident affecting Member States and NATO ~~Allies , including where Article 4 or 5 of the North Atlantic Treaty applied or likely to be applied. The~~Allies. The exercise may be conducted within the framework of the next 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.

(70) Given the exposure of the Western Balkans candidate countries and the potential of cybersecurity incidents taking place in the Union's neighbourhood, and in line with the Brussels Declaration of 18 December 2024, joint exercises involving candidate countries from the region should be considered. Reconfirming also the EU's solidarity with Ukraine and Moldova in countering hybrid and cyber threats, relevant joint exercises should be considered.

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

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

(72) ~~MICNET~~EU-CyCLONe and the CSIRTs network should ~~establish~~ identify possible ways and procedures ~~for collaboration between~~to cooperate with the ~~civilian and~~relevant EU military ~~cyber actors. Both networks should appoint liaison officers to establish contact between networks and promote collaboration.~~

~~(73) EU-CyCLONe and~~organisations, such as the EU Cyber Commanders Conference ~~should identify possible ways to cooperate~~and 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 ~~regard~~regards to such a cooperation~~. EU-CyCLONe and the EU Cyber Commanders Conference should appoint liaison officers to establish bilateral contact and promote collaboration~~.

(~~74) EU-CyCLONe should identify possible ways to cooperate with the future EU Cyber Defence Coordination Centre to benefit from a joint military and civilian perspective. EU-CyCLONe should inform the Council on the progress made in regard to such a cooperation.~~

(~~75~~73) The affected Member State is invited to inform EU-CyCLONe, as well as the EEAS, ~~and in the future the EU CDCC,~~ if the relevant military response capabilities, such as the PESCO CRRTs ~~or the Hybrid Rapid Response Teams~~ 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.

(~~76~~74) As part of the Union cyber exercise rolling programme referred to in section II above, the Commission and the High Representative should consider organising a joint exercise in order to test cooperation between both civilian and military ~~components~~cyber actors in the event of a large-scale cybersecurity incident affecting Member States.

XI: Recovery from a cyber crisis

(77) Member States, relevant Union entities, and networks ~~shall~~should collaborate during the recovery phase after a cyber crisis to ensure the swift restoration of core functionalities. 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. ~~Additionally, the involvement of law enforcement authorities is essential for the tracking and management of data throughout the recovery process.~~

(78) Member States, relevant Union entities and networks should work together in the recovery phase building on lessons ~~learned~~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. ENISA ~~shall~~should ensure that the lessons learnt and incident reports are then properly reflected in future preparedness activities and when considering the planning of future exercises. EU-CyCLONe should ~~be responsible for providing~~provide to the NIS Cooperation Group and the Council a comprehensive list of lessons learnt from cyber crises or managed cybersecurity incidents in the past and best practices ~~to the Council.~~ .

XII: Secure communication

(79) Based on the mapping of existing secure communications tools[6], the Commission should propose by the end of the 2026 an interoperable set of secure communication solutions. The Council, the Commission, the High Representative, ~~Member States,~~ EU-CyCLONe~~;~~ and the CSIRTs network~~, and relevant Union entities~~ should agree ~~by the end of 2026 on an interoperable set of secure communication solutions for relevant Union actors.~~on this set by the end of 2027. These solutions should benefit from the actions in the area of secure communications that EU institutions will take under the EU Preparedness Union Strategy and should cover the full range of communication

6

modes required (voice, data, video-teleconferencing (VTC), messaging, collaboration and document sharing and consultation). ~~The solutions should reflect key principles such as Union security interests, technological sovereignty, and confidentiality, as well as features such as usability, security-by-design, certification by European information security bodies, end-to-end encryption, authentication, availability, and post-quantum cryptography.~~ 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.

(80) EU-CyCLONe and the CSIRTs network for the purpose of exchanging the RESTREINT UE/EU RESTRICTED information, if needed, should be able to use secure communication channels ensured ~~by~~for the EU institutions, bodies and agencies for exchanging classified information between themselves and with Member States. ~~Any duplication of investments in interoperable secure systems should be avoided.~~

~~(81) On this basis, Union-level actors should use solutions based on a PQC compliant, open protocol with open-source implementations (such as Matrix) suite for real-time communication, managed by an EU-resident entity.~~

(80a) The European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) established under Regulation (EU) 2021/887, without prejudice to the future multiannual financial framework, should consider funding through the Digital Europe Programme to assist Member States in deploying ~~these tools.~~secure communication tools. Any duplication of investments in interoperable secure systems should be avoided

(~~82~~81) 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.

~~(83) In the medium term, communication~~(82) 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 ~~Commission works with Member States on establishing the~~ European Critical Communication System (EUCCS~~), which should connect by 2030 the communication networks of law enforcement and civil protection across the Schengen area, so that critical communication equipment can be used in the territory of other Member States. EUCCS can therefore also~~) currently under development can benefit the joint response with relevant cyber communities~~. This system should include back up communications through for example satellite communications~~.

XIII: Final provisions

(83) 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. The graphical representations should cover different cooperation modes and layers.

(84) To support the effective application of the revised EU Cyber Blueprint, and building on the experience gained through the joint cyber exercises conducted under it, the Council could develop 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.

(85) This Recommendation should be reviewed by the Commission in cooperation with the Member States, every four years, following its publication. Following the 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