EUROPEAN
COMMISSION

Brussels, 24.2.2025
COM(2025) 66 final

2025/0036 (NLE)

Proposal for a

COUNCIL RECOMMENDATION

for an EU Blueprint on cybersecurity crisis management

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

• Reasons for and objectives of the proposal

The Council, in its Conclusions on the Future of Cybersecurity of 22 May 2024,

> *"call[ed] upon the Commission to swiftly evaluate the current cybersecurity Blueprint and, on this basis, propose a revised Cybersecurity Blueprint in the form of a Council recommendation that will address the current challenges and complex cyber threat landscape, strengthen existing networks, enhance cooperation, and break silos between organisations, utilising to this end first and foremost existing structures. Furthermore, the revised Blueprint should rely on time-tested guiding principles of cooperation (proportionality, subsidiarity, complementarity and confidentiality of information) and expand them to the full crisis management lifecycle and should contribute to aligning and enhancing secure communication in the cybersecurity field. The revised Blueprint should ensure its compatibility with existing frameworks such as the IPCR, the EU Cyber Diplomacy Toolbox, the EU Hybrid Toolbox, the Law Enforcement Emergency Response Protocol (LERP), emerging frameworks such as the Critical Infrastructure Blueprint, sectoral procedures, and overall crisis management structures within Union entities, involving also the High Representative and Europol. In this revised Blueprint, the role of the Commission, the High Representative and ENISA, in line with their competences, should focus in particular on supporting horizontal coordination."*

The objective of this draft Council Recommendation on the Union Blueprint for cybersecurity crisis management (Cyber Blueprint) is to present, in a clear, simple and accessible manner, the European Union (EU) framework for cyber crisis management. This should enable relevant Union-actors (meaning Union-level individual entities and networks of entities) to understand how to interact and make the best use of available mechanisms across the full crisis management lifecycle. It aims to explain what a cyber crisis is and what triggers a cyber crisis mechanism at Union level. It explains the use of available mechanisms like the Cybersecurity Emergency Mechanism, including the EU Cybersecurity Reserve, in preparing how to manage, respond to and recover from a crisis arising from a large-scale cybersecurity incident. It furthermore aims to foster a more structured cooperation between civilian and military actors, including cooperation with North Atlantic Treaty Organisation (NATO), given that a large-scale cyber incident affecting Union civilian infrastructure on which the military rely may also activate NATO response mechanisms.

The Cyber Blueprint is a non-binding instrument which identifies specific actions for relevant actors in a cyber crisis and which can enhance the overall effectiveness of the cyber crisis management framework. It updates the blueprint set out in Commission Recommendation (EU) 2017/1584 on coordinated response to large-scale cybersecurity incidents and crises, and it is informed by the outcomes and lessons learned from Union-level exercises since that recommendation was adopted. It is part of wider political priorities in the areas of preparedness and security.

As defined in Directive (EU) 2022/2555 (NIS 2 Directive), a large-scale cybersecurity incident is an incident which causes a level of disruption that exceeds a Member State's capacity to respond to it or has a significant impact on at least two Member States. Such an incident, depending on its cause and impact, may escalate and turn into fully-fledged crises 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.

- **Consistency with existing policy provisions in the policy area**

The proposal is consistent with relevant Union instruments in the cybersecurity domain, notably the NIS 2 Directive and Regulation (EU) 2023/2841 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union. It is also consistent with the framework of the Union Civil Protection Mechanism (UCPM), established by Decision No 1313/2013/EU of the European Parliament and of the Council, the Implementing Decision (EU) 2018/1993 on the EU Integrated Political Crisis Response (IPCR) Arrangements, and sectoral instruments for situational awareness and crisis management including in the electricity sector.

- **Consistency with other Union policies**

The Cyber Blueprint complements and is consistent with the recently adopted Council Recommendation on a Blueprint to coordinate a response at Union level to address disruptions of critical infrastructure with significant cross-border relevance since the latter covers disruptions related to non-cyber physical resilience. It closely interacts with the Common Foreign and Security Policy (CFSP) and Common Security and Defence Policy (CSDP) crisis management mechanisms and tools, as set out in the Council's Strategic Compass for Security and Defence. Moreover, Union initiatives to fight cybercrime can support the objectives pursued by the present Recommendation.

2. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY

- **Legal basis**

The proposal is based on Article 292 TFEU, which lays down the relevant rules regarding the adoption of Recommendations.

The proposal would complement the whole cybersecurity legislative framework established at Union level. The proposal does not address the management of major incidents affecting Union entities within the meaning of Regulation 2023/2841, adopted on the basis of Article 298 TFEU. It does however address information exchange between Union entities and Member States, including the provisions in Regulation 2023/2841 for the Commission representative in the Institutional Cybersecurity Board (IICB) to be the point of contact to facilitate the IICB's sharing of relevant information in relation to major incidents with the European cyber crisis liaison organisation network EU-CyCLONe, as a contribution to the shared situational awareness.

- **Subsidiarity (for non-exclusive competence)**

Whereas responding to disruptions of critical infrastructure or of the services provided by essential and important entities is first and foremost the responsibility of Member States, certain malicious cyber activities of a cross-border nature can disrupt and damage critical information infrastructures on which the smooth functioning of the internal market depends. Therefore, the Union plays an important role in the event of a significant incident or crisis. Such disruption can impact several or even all sections of economic activity within the single market, and it could affect the security and international relations of the Union. With the aim of securing the functioning of the internal market, coordinating at Union level in case of disruptions of critical infrastructure with significant cross-border effect is not only appropriate but also necessary. Coordinated responses at Union level will support Member States' responses to the disruption through shared situational awareness, coordinated public communication and mitigating the consequences of the disruption on the internal market.

- **Proportionality**

The present proposal is in conformity with the principle of proportionality as provided for in Article 5(4) of the Treaty on the European Union. Neither the content nor the form of this proposed Council Recommendation exceeds what is necessary to achieve its objectives. The actions proposed are proportional to the pursued objectives, which focus on ensuring a coordinated Union management of cyber crises.

- **Choice of the instrument**

To achieve the objectives referred to above, the TFEU provides for the adoption, by the Council, of Recommendations, notably in its Article 292, based on a proposal from the Commission. In accordance with Article 288 TFEU, Recommendations do not have binding force. A Council Recommendation is an appropriate instrument in this case since it signals the commitment of Member States to the measures included therein and provides a strong basis for cooperation in coordinating the management of large-scale cybersecurity incidents and crises. In this manner, the proposed Recommendation would complement the binding legal framework (in particular, the NIS 2 Directive).

3. RESULTS OF EX-POST EVALUATIONS, STAKEHOLDER CONSULTATIONS AND IMPACT ASSESSMENTS

- **Stakeholder consultations**

In developing this proposal, the Commission consulted on the review of the Cyber Blueprint and invited input from Member States and relevant Union entities. It considered the views of the Member States experts, as well as ENISA, expressed at the workshop co-organised in Karpacz on 5 September 2024 by the Commission and Poland.

The Commission consulted Member States representatives in the CSIRTs Network, EU-CyCLONe and the NIS Cooperation Group in meetings in September 2024 and invited written contributions.

The Commission presented and gathered feedback from the Council during two dedicated discussions at the Horizontal Working Party on Cyber Issues held in October and November 2024.

The Commission consulted representatives of the private sector, as well as Member States, the European External Action Service (EEAS) and ENISA, at a workshop hosted by the Polish Permanent Representation to the EU in Brussels in November 2024.

The Commission consulted relevant Union entities, namely the EEAS, ENISA, Europol and CERT-EU, including through high-level discussions at the Cyber Crisis Task Force[1] meetings held in July and November 2024.

Consensus emerged on the need for an up-to-date clear, simple and operational document which enables relevant actors to understand the framework for cyber crisis management and use available mechanisms effectively. There was also consensus on the need to avoid duplication of instruments and make good use of existing Union-level mechanisms for coordination, information-sharing and response, without creating new structures, or

[1] An informal group composed of Commission services and other EU services

interfering with the internal standard operating procedures of existing networks and of existing sectoral mechanisms.

2025/0036 (NLE)

Proposal for a

COUNCIL RECOMMENDATION

for an EU Blueprint on cybersecurity crisis management

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 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 cyber 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 multidimensional 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, citizens and businesses, 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) In accordance with the procedures set out in Council Implementing Decision (EU) 2018/1993[2], a decision to activate and deactivate the EU Integrated Political Crisis Response (IPCR) 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 High Representative (HR). In addition, according to the IPCR procedures, the General Secretariat of the Council, Commission services and EEAS may also agree, in consultation with the Presidency, to activate IPCR in information-

[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, ELI: http://data.europa.eu/eli/dec_impl/2018/1993/oj).

sharing mode. Discussions under the IPCR are informed by Integrated Situational Awareness and Analysis reports developed by Commission services and the European External Action Service ('EEAS').

(4) While Member States have a primary responsibility in the management of national cyber crises, the potential cross-border and cross-sectoral nature of cybersecurity incidents requires Member States and the relevant Union entities to cooperate at technical, operational and political level to coordinate effectively across the Union. At the same time, crisis response and recovery are costly for the affected entities and sectors. Full-lifecycle crisis management, therefore, includes preparedness and shared situational awareness to anticipate cybersecurity incidents, the necessary detection capabilities to identify and the needed response and recovery tools to mitigate, deter and contain cybersecurity incidents.

(5) Commission Recommendation (EU) 2017/1584[3] on coordinated response to large-scale cybersecurity incidents and crises set out the objectives and modes of cooperation between Member States and Union entities in responding to large-scale cybersecurity incidents and 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).

(6) 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[4], Directive (EU) 2022/2555 of the European Parliament and of the Council[5], Commission Implementing Regulation 2024/2690[6], Regulation (EU, Euratom) 2023/2841 of the European Parliament and of the Council[7], Regulation (EU) 2021/887 of the European

---

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

4 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).

5 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).

6 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).

7 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).

Parliament and of the Council[8], Regulation (EU) 2024/2847 of the European Parliament and of the Council[9], and Regulation (EU) 2025/38 of the European Parliament and of the Council ('Cyber Solidarity Act')[10]. Specific sectoral cybersecurity crisis measures include Commission Delegated Regulation (EU) 2024/1366[11] 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[12]. Directive 2013/40[13] 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[14], once implemented, will significantly facilitate law enforcement action in this domain. The EU Policy on Cyber Defence[15] 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'[16] provides for cooperation between relevant actors where an incident affects both physical aspects and the cybersecurity of critical infrastructure.

---

8 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).

9 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).

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

11 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).

12 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).

13 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).

14 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).

15 JOIN(2022) 49 final.

16 OJ C, C/2024/4371, 5.7.2024.

(7) At Union level, the relevant actors that have cyber crisis management responsibilities include the Commission, the EEAS including the Single Intelligence and Analysis Capacity (SIAC), the European Union Agency for Cybersecurity (ENISA), the Cybersecurity Service for the Union institutions, bodies, offices and agencies (CERT-EU), Europol through its European Cybercrime Centre (EC3), the European Cyber Liaison Officers Network (EU-CyCLONe), the Computer Security Incident Response Teams (CSIRTs) Network, the EU Satellite Centre (SATCEN), the Galileo Security Monitoring Centre, and the Union's network of delegations. These Union actors should together determine areas for cooperation and contributing to the implementation the Union cyber crisis management framework, in accordance with their competences under applicable laws.

(8) An updated Recommendation setting out a blueprint on cybersecurity ('Cyber Blueprint') is necessary to provide clear and accessible guidance explaining what a Union-level cyber crisis is, how the crisis management framework is triggered and what the roles of relevant Union level actors and mechanisms, and the interaction between these actors and mechanisms throughout the entire cyber crisis lifecycle. The Cyber Blueprint is to be seen within the wider context of civilian-military and EU-NATO relations.

(9) This Recommendation complements the arrangements on an Integrated Political Crisis Response (IPCR) 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 Hybrid Toolbox[17] and in the revised EU Protocol for countering hybrid threats. 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) A comprehensive and integrated approach to crisis management should be fostered across all sectors and levels of governance. Cross-sectoral crisis management at Union level should be reinforced to enable an integrated crisis response, particularly in cases where cyber incidents cause real-life consequences. Where cybersecurity incidents are part of a wider hybrid campaign or crisis, the relevant actors should support efforts to develop a unified situational picture across several sectors and domains. The Recommendation contributes to wider preparedness actions required for the Union in the face of multi-dimensional hybrid threats [in line with the principles embedded in the Preparedness Union Strategy].

(11) The security of critical digital infrastructure is fundamental for the resilience of the Union's economy, society and defence. Entities falling into the scope of Directive (EU) 2022/2555, including those providing undersea communications cables, need to take measures to protect the physical and environmental security of network and information systems based on an all-hazards approach, such as system failures, human error, malicious acts or natural phenomena. In addition, those entities should report incidents, including those related to the submarine communication cables to the CSIRTs or, where applicable, to the competent authority. Although the fundamental

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

principles underpinning the Cyber Blueprint are relevant to the security of submarine cables, the mechanisms it lays out are not sufficiently comprehensive to cover the full crisis resilience cycle. Its specific nature warrants a concerted and tailormade effort to address the needs for integrated threat surveillance and situational awareness for the sea basins around the EU, strategic investments to create redundancies and a common European approach to step up repair and recovery capabilities. The EU Maritime Security Strategy comprises actions to enhance cyber security in the maritime domain, and to enhance surveillance and protection of critical maritime infrastructure, including submarine cables. For Union level crisis management, a specific network of national points of contacts and close civilian-military interactions, including with NATO would be an avenue to consider.

(12) Preparedness for a crisis requires a comprehensive all-hazards and all-threats risk assessment, given the convergence of the EU's economic and security interests. A shared Union situational awareness among Member States and Union entities, facilitated by agreeing on a common taxonomy and secure communications channels, should enable a coordinated and informed response to potential and large-scale cybersecurity incidents, as well as deterrence of persistent threat actors. Based on the need-to-know principle and considering the importance of trust in information sharing, groups of Member States in various configurations, and, where appropriate, relevant Union entities, might wish to cooperate and share information relevant for cyber incident management. Member States and Union entities sharing on threats, risks and maturity gaps should enable the identification of the right priorities for sound investment and tangible actions that would lead to better cyber resilience.

(13) In accordance with Article 6 of Regulation (EU) 2019/881, ENISA, in close cooperation with the Member States, prepares a regular in-depth EU Cybersecurity Technical Situation Report on incidents and cyber threats. That report is referred to as the EU Joint Cyber Assessment Report (EU-JCAR) and is prepared with Europol/EC3 and CERT-EU, with the aim of strengthening Union preparedness, as it provides situational awareness based on an analysis of incidents and cyber threats.

(14) Key critical infrastructure, such as energy, transport, digital infrastructure, health or financial services, as well as the security solutions deployed to protect it, are usually operated by private companies. Safeguarding this infrastructure against large-scale cyber incidents requires close cooperation between public and private entities, including manufacturers and open-source developers, built on trust and clear and dedicated procedures for information sharing, dissemination and coordination of response.

(15) Union-level cyber exercises are a highly effective tool for testing procedures and cooperation mechanisms and thereby enhancing preparedness. As exercises are resource-intensive, the exercise agenda needs to be as streamlined and consolidated as possible and needs to consider the scenarios developed in Union coordinated risk assessments and other relevant initiatives.

(16) European digital infrastructures have many deeply embedded technical dependencies. These should be addressed to ensure business continuity of operations in a crisis. This concerns for instance, the Domain Name System (DNS), which is a crucial component that underpins the Internet's operations. DNS resolvers are essential for accessing the Internet, including during a major cyber crisis, as they translate Internet domain names into IP addresses. Directive (EU) 2022/2555 encourages relevant stakeholders to adopt a DNS resolution diversification strategy. It also encourages Member States to foster

the development and use of a public and secure European DNS resolver service as a key measure to ensure crisis preparedness and resilience.

(17) Furthermore, to enhance the resilience of other critical components, such as the routing system, and ensure their functionality during major cyber crises, it is essential to implement corresponding best practices and latest available standards in a timely manner. Consequently, Implementing Regulation (EU) 2024/2690 mandates establishing a multistakeholder forum to identify the best available standards and deployment techniques for essential cybersecurity elements and encourages participation from relevant entities.

(18) To effectively detect malicious activity in the increasingly complex global supply chains that can have a Union-wide impact, a coordinated approach is necessary. This is especially relevant for areas where the Union relies on technology from high-risk suppliers subject to the jurisdiction of a third country that requires reporting information on software or hardware vulnerabilities to its authorities prior to their being known to be exploited. States-sponsored actors may also preposition themselves in critical infrastructure with the intention of causing disruption at a later time, for example during a conflict. This is difficult to detect using traditional methods, since threat actors disguise their activities by blending in with legitimate traffic and fusing "living off the land" techniques which rely on legitimate tools and processes to hide malicious activities. The same is true for third countries where, according to public statements of the Union or its Member States, threat actors operating out of the territories of those countries have carried out malicious cyber activities against the Union. Supply chains should become more resilient and diversified, while maintaining a common baseline of preparedness.

(19) At the technical level, CSIRTs, law enforcement authorities, as well as the National and Cross-Border Cyber Hubs (cyber hubs) to be established under the Regulation (EU) 2025/38, play an essential role in detecting incidents, cyber threats and vulnerabilities, supporting technical attributions, and recovering from cyberattacks. Effective procedural arrangements for cooperation between the CSIRTs Network and EU-CyCLONe, as required by Directive (EU) 2022/2555 are essential. The European Cyber Security Alert Mechanism aims to support the development of advanced capabilities for the Union to enhance detection, analysis and data processing capabilities in relation to cyber threats and the prevention of incidents in the Union.

(20) In terms of immediate response, mechanisms at the disposal of Member States include the EU Cybersecurity Reserve and actions supporting mutual assistance established under the Regulation (EU) 2025/38, Hybrid Rapid Response Teams and Permanent Structured Cooperation (PESCO) Cyber Rapid Response Teams (CRRTs), as well as mechanisms provided for NATO allies. In addition, the EU Law Enforcement Emergency Response Protocol (LEERP) supports the EU 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, including deconfliction at law enforcement level and coordination with non-law enforcement partners. Achieving a clear picture of which response options are available in cases of cyber incidents and hybrid activities and how they are used can ensure an efficient allocation of resources and avoid their duplication. Accordingly, under the Regulation (EU) 2025/38, Member States are required to inform the CSIRTs Network and EU-CyCLONe when requesting services of the EU Cybersecurity Reserve.

(21) Effectively combating cybercrime is essential for cybersecurity. Deterrence cannot be achieved solely through resilience, but also requires identification, prosecution of and response to offenders. Cooperation through adapted technical systems and platforms and exchange of relevant information among cybersecurity actors, cyber diplomacy entities, and law enforcement are therefore essential to ensure a comprehensive understanding of the threat landscape and be able to respond in a coherent and coordinated manner.

(22) Crises generate uncertainty which adversaries can easily exploit to spread disinformation and sow distrust. To counter this, clear and coherent public communication about the situation, and what steps are being taken to remedy it, is essential. A coordinated strategic communication can also support diplomatic actions towards persistent threat actors and the development of a narrative on threats to the Union, its deterrence actions and the need to promote responsible State behaviour in cyberspace.

(23) For effective crisis management, it is necessary to identify common secure communication solutions for the cyber domain and implement them across the Union, including where necessary for the exchange of EU classified information. Following the request of the Council, the Commission and other relevant Union entities mapped existing secure communication tools and presented the results in December 2022. There are several existing separate efforts by Union entities to build up secure communications capacities in a crisis that require better coordination and leveraging. This includes the establishment of an EU Critical Communication System (EUCCS) to enhance resilience of public communication infrastructure against malign interference and improve daily operational cooperation, including across borders.

(24) The Union's security environment demands an all-hazards, whole-of-government and whole-of-society approach to civilian and military preparedness and readiness. Military bodies rely on civilian critical infrastructure, such as communications, energy, health, transport and logistics. Accordingly, and as emphasised in the EU Policy on Cyber Defence[18], the EU's cybersecurity requires greater cooperation and synergies between civilian and military networks' capacities for preparedness and response, including in the case of an armed attack. Cybersecurity actors should work together across institutional and operational silos to anticipate and to address the threat of multisectoral, multidimensional disruption, in line with the principles that [to be embedded] in the Preparedness Union Strategy. Furthermore, malicious cyber activity is playing an increasing role in wider hybrid campaigns against the Union, its Member States and strategic partners. Stronger cooperation between the Union and NATO is therefore required.

(25) In the military community, the future EU Cyber Defence Coordination Centre and the Single Intelligence Analysis Capacity (SIAC) within the European External Action Service, the Military Computer Emergency Response Team Operational Network (MICNET) and the EU Cyber Commanders Conference facilitated by the European Defence Agency (EDA), as well as relevant projects under the Permanent Structured Cooperation (PESCO), represent important actors and initiatives for coordination and cooperation on preparedness for detection, deterrence and defence against, and recovery from, cyber threats affecting the Union and Member States. Therefore, cooperation between civilian and military actors should be encouraged, such as the

[18] EU Policy on Cyber Defence; JOIN/2022/49 final

cooperation between EU-CyCLONe and the EU Cyber Commanders Conference, as well as the potential collaboration between MICNET and the CSIRTs Network.

(26) Cooperation with strategic international partner countries and organisations outside of the Union enhances the Union's cybersecurity capabilities. By fostering international cooperation, the Union and its partners can ensure shared situational awareness and coherence in cyber crisis management and a robust cyber posture, contributing to a global, open, stable, secure and resilient cyberspace. This collaboration should be based on trust and the shared goal of protecting critical infrastructure and essential services from cyber threats, including by promoting responsible state behaviour in cyberspace grounded in the United Nations (UN) framework and by holding threat actors accountable for their irresponsible and illegal behaviour in cyberspace. Cyber diplomacy measures contribute to the deterrence and response to malicious cyber activities and provide for coordination and cooperation with strategic international partner countries.

HAS ADOPTED THIS RECOMMENDATION:

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

(1) This Recommendation sets out the Union framework for cybersecurity crisis management within the context of the EU's overall preparedness for multi-dimensional hybrid threats. How an incident may escalate into a large-scale incident and in turn into EU-level crisis is illustrated and summarised in Annex 1, including where such an incident coincides with other hybrid threats requiring interaction between the necessary responses. The cyber crisis management framework should enable relevant Union-level actors, including entities and networks, to understand how to interact and make the best use of the existing mechanisms listed in Annex II across the full crisis management lifecycle. In addition, it recommends to these Union-level actors how the effectiveness of existing mechanisms may be improved.

(2) The Union and its Member States should follow the Cyber Blueprint in the management of a crisis arising from a large-scale cybersecurity incident, as defined in Article 6, point (7) of Directive (EU) 2022/2555, which affects the proper functioning of the internal market or poses serious public security and safety risks for entities or citizens in several Member States or the Union as a whole ('cyber crisis').

(3) When a cybersecurity incident, detected at the technical level by a CSIRT or a cyber hub, results in escalation under the internal procedures of the CSIRTs Network, appropriate information should be shared with EU-CyCLONe according to relevant procedural arrangements, who in turn should consider whether it represents a potential or ongoing large-scale incident as defined in Article 6 point (7) of Directive (EU) 2022/2555. The determination of whether a cyber crisis exists or ceases to exist as a result of this large-scale incident should be carried out in accordance with Implementing Decision (EU) 2018/1993 and in particular Articles 4 and 5 thereof.

(4) In accordance with the principles of proportionality, subsidiarity, complementarity, and confidentiality of information set out in Annex III, Member States and Union entities should deepen their cooperation on cyber crisis management, fostering mutual trust and building on existing networks and mechanisms. While the Cyber Blueprint does not interfere with how entities define their internal procedures, each entity should clearly define the interfaces used for working with other entities. These interfaces should be jointly agreed between the entities concerned and clearly documented.

(5) 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[19]. Where there are sector-specific crisis management measures that cover cybersecurity incidents, those measures should be implemented coherently with this Recommendation.

II: Preparing for a Union level cyber crisis

(a) Situational awareness and information sharing

(6) Verified, reliable data, including trends in incidents, tactics, techniques and procedures, and actively exploited vulnerabilities should be the basis for a common situational awareness among Member States and Union entities of the cyber threat landscape. This shared knowledge should be used by Member States and Union entities to anticipate, prepare for and detect cyberattacks, in line with their respective areas of responsibility. This common situational awareness should:

(a) apply to all critical sectors listed under Directive (EU) 2022/2555, especially communications, digital infrastructure, energy, transport, finance, space and health and should also apply, through CERT-EU, to the networks and systems of Union entities in accordance with Regulation (EU, Euratom) 2023/2841;

(b) be based on high-quality diversified and integrated datasets that are collected, processed and shared in real-time;

(c) be taken into account in the Joint Cyber Assessment Report (JCAR) and other relevant products;

(d) take into account related hybrid threats, including foreign information manipulation and interference (FIMI) and disinformation;

(e) support short-term actions and response measures, as well as feeding into long-term policy planning in the context of preparedness and deterrence;

(f) [link to other risk and threat assessments produced regularly and reinforced by the Preparedness Union Strategy in order to ensure synergies and simplification for reporting obligations for Member States.]

(7) 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 members;

(c) make full use of the available tools for information sharing.

(8) Member States and relevant Union entities should improve ways to coordinate and partner with the private sector, including open-source communities and manufacturers, to improve information sharing, building on existing Information Sharing and Analysis Centres at EU and national levels, to enhance cybersecurity capacity and to respond to cybersecurity incidents, including through roundtable discussions with EU-CyCLONe and the CSIRTs Network.

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

(9) Member States, and relevant Union entities could choose, for the purpose of advancing cooperation and strengthening trust, and building on the cybersecurity information-sharing arrangements of the Directive (EU) 2022/2555 and the provisions of Regulation (EU) 2025/38 regarding cyber hubs, to create voluntary collaborative clusters on a need-to-know basis where there are common concerns, such as deterrence of, detection of, or response to a particular type of threat that they uniquely face. Any such clusters should respect the mandate of relevant actors, as well as already established structures. Those collaborative clusters could call on Union entities to facilitate their collaboration, including via appropriate infrastructure.

(10) Member States through the NIS Cooperation Group established by Directive (EU) 2022/2555 should, within 12 months of adoption of the Cyber Blueprint, develop a common taxonomy with respect to cyber crisis management and provide a guide on the secure handling and exchange of information related to cybersecurity incidents and crises, including a section dedicated to determining the confidentiality level of this information (categorisation).

(11) When determining the confidentiality level for the information available, Member States and relevant Union entities should consider the potential impact that over-classification can have on voluntary information exchange and achieving a common situational awareness. When sharing non-classified information, 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.

(b) Common exercises

(12) Member States and relevant Union entities should develop an efficient rolling cycle of cyber exercises to prepare for cyber crises and to enhance organisational efficiency. These exercises should be based on the scenarios developed based on EU coordinated risk assessments including those concerning multi-sectoral crisis. The rolling cycle of cyber exercises should take account of the UCPM and other Union-level crisis response mechanisms. It should ensure that lessons learned from exercises are effectively implemented.

(13) Relevant Union actors could conduct smaller exercises to test their interactions and interfaces in case of escalating cyber incidents.

(14) Commission services, EEAS and ENISA are invited to organise an exercise to test the cyber blueprint within 18 months of the adoption of the Cyber Blueprint, involving all relevant actors, including the private sector.

(c) DNS resolution capabilities

(15) Member States, relevant Union entities, as well as private entities such as critical infrastructure operators, should enhance their Domain Name Systems (DNS) resolution diversification strategy, including the use of at least one Union-based DNS infrastructure such as DNS4EU to ensure reliable DNS resolution during major crisis. ENISA and EU-CyCLONe should develop and make available emergency failover guidelines that outline the steps for switching to Union-based DNS infrastructure in case other DNS services fail, ensuring continuity of critical services during a crisis.

(16) In addition, national cyber hubs and cross-border cyber hubs should share relevant information on threats with such Union-based DNS infrastructures to support them in

providing a high-level of protection against Union-specific threats and thereby further increasing capabilities to detect and mitigate Union-specific threats.

(17) To generally strengthen the security and availability of critical Internet infrastructure, also during crises, Member States should actively promote the participation of all relevant stakeholders—including those not directly addressed by the NIS2 implementing act—in the mandated multistakeholder forum tasked with identifying best available standards and deployment techniques for crucial network security measures. Moreover, Member States should consider engaging in the forum and adopt the recommended guidelines themselves.

(d) Resources

(18) Member States should make full use of the financial resources available for cybersecurity provided by relevant Union programmes.

III: Detecting an incident that could escalate to a cyber crisis

(19) To address the escalating complexity of cyber 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. When covert operations are identified, entities should proactively share relevant information with their partners well before situations escalate into crises.

(20) All actors should contribute, in accordance with their respective mandates and based on the all-hazards approach, information indicating a potential cyber crisis to relevant networks.

(21) The CSIRTs Network and EU-CyCLONe should establish 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.

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

(23) The Cross-Border Cyber Hubs, already established or to be established under the Regulation (EU) 2025/38, should contribute with relevant information to the Union-level mechanisms in cases of a potential or ongoing large-scale cybersecurity incident based on the all-hazards approach, including physical damage to critical infrastructure which compromises 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.

(24) Where a potential or large-scale cybersecurity incident with multi-sectoral impact is detected:

(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.

IV: Responding to a cyber crisis at Union level

(25) In the event of a cyber crisis established under the IPCR, all actors should respond in close coordination with other entities responding to wider hybrid threats in an all-of-of-government approach as follows:

(a) the affected Member State(s) and the CSIRTs Network should cooperate to rapidly restore compromised systems, ensuring minimal operational disruption;

(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) the Commission, in cooperation with the High Representative where relevant, should ensure coherence and coordination between the responses to the crisis and related 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;

(d) the Council Presidency should consider inviting the Chair of EU-CyCLONe to informal roundtable meetings and other relevant Council meetings under the IPCR arrangements;

(e) the Council, supported by EU-CyCLONe and relevant Union entities, should coordinate public communication efforts, including to ensure that the crisis situation is not used to spread inaccurate information;

(f) the High Representative, in close cooperation with the Commission and other relevant Union entities, should 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;

(g) the Commission, the High Representative, and Member States should also leverage economic tools like trade bans more effectively to better prevent, deter and respond to persistent malicious cyber activities by state actors.

(26) Where a user of the services provided by the EU Cybersecurity Reserve[20] requests services from the EU Cybersecurity Reserve in accordance with Article 15 of Regulation (EU) 2025/38, and without prejudice to any future implementing acts under that regulation:

(a) services should be deployed within 24 hours of the request;

[20] The EU Cybersecurity Reserve is a mechanism consisting of services from trusted managed security service providers to, upon request, support response and initiate recovery actions in the case of significant cybersecurity incidents, large-scale cybersecurity incidents or large-scale-equivalent cybersecurity incidents affecting Member States, Union institutions, bodies, offices or agencies, or DEP-associated third countries.

(b) the Commission and the High Representative should ensure coordination with additional measures, in line with the Hybrid Toolbox[21] in the case of malicious cyber activities that are part of a wider hybrid campaign;

(c) in the case of malicious cyber activity with a military dimension, the requesting Member State should inform the Union Cyber Commanders Conference of its request.

(27) In the event of a large-scale cybersecurity incident which affects the proper functioning of space services essential for the security of the Union or its Member States, EU-CyCLONe should inform the High Representative with a view to coordinate possible response with the Space Threat Response Architecture established in accordance with Council Decision (CFSP) 2021/698.

V: Recovery from a cyber crisis

(28) Member States, relevant Union entities and networks should work together in the recovery phase building on lessons learned from conducted exercises, as well as incident reports, in particular in the context of the European Cybersecurity Incident Review Mechanism established by Regulation (EU) 2025/38.

VI: Secure communication

(29) Based on the mapping of existing secure communications tools[22], the Commission, the High Representative, EU-CyCLONe, the CSIRTs Network, and relevant Union entities should agree by end 2026 on an interoperable set of secure communication solutions for relevant Union actors. These solutions should cover the full range of communication 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 and include tools for the exchange of RESTREINT UE/EU RESTRICTED information.

(30) On this basis, Union-level actors should use solutions based on the Matrix protocol for real-time communication. 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.

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

(32) In the medium term, communication and information sharing mechanisms between law enforcement and cybersecurity networks, particularly at the technical level,

---

21 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.

22 HWPCI WK 862/23

should be established for effective crisis response. These mechanisms should respect the role of each party and avoid interfering with ongoing operations. 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 benefit the joint response with relevant cyber communities. This system should include back up communications through for example satellite communications.

VII: Coordination of cyber crises with military actors

(33) EU-CyCLONe and the EU Cyber Commanders Conference, MICNET and the CSIRTs Network, as well as a future EU Cyber Defence Coordination Centre, and its civilian Union counterparts, should cooperate to develop common situational awareness between civilian and military actors.

(34) The Union, taking into account existing agreements such as the CERT-EU/NATO technical agreement of 2016, should endeavour to 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 this end, the Union should explore ways to improve information sharing capabilities with NATO, including through possible interconnections between their respective communication and information systems.

(35) Where a Member State, in the context of a cybersecurity incident, uses relevant defence initiatives, such as the PESCO CRRTs or other relevant initiatives, such as the Union Hybrid Rapid Response Teams (HRRTs), it should inform EU-CyCLONe as well as the EU Cyber Commanders Conference.

VIII: Cooperation with strategic partners

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

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

(b) enhance coordination with strategic partners on response to sustained malicious cyber activities by persistent threat actors, notably when using the Cyber Diplomacy Toolbox, in line with its implementing guidelines.

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

(38) As part of the rolling cycle of exercises referred to in section II above, Commission services and the EEAS should consider organising a joint staff exercise to test cooperation between both civilian and military components in the event of a large-scale cyber incident affecting Union Member States and NATO Allies, including where Articles 4 or 5 of the NATO Treaty are triggered or likely to be triggered.

(39) Given the exposure of candidate countries and the potential of cyber incidents taking place in the Union's neighbourhood, joint exercises involving candidate countries should be considered.

Done at Brussels,

For the Council

The President