Council of the European Union

Brussels, 7 September 2023
(OR. en)

12485/23

Interinstitutional File: 2023/0318(NLE)

PROCIV 57	ATO 48
ENV 925	CSC 408
JAI 1084	ECOFIN 839
SAN 494	CSCI 149
COSI 140	DATAPROTECT 216
CHIMIE 85	MI 698
ENFOPOL 356	CODEC 1500
RECH 380	COPS 418
CT 133	JAIEX 46
DENLEG 38	COPEN 292
COTER 153	IND 441
RELEX 987	POLMIL 221
ENER 467	IPCR 55
HYBRID 53	DIGIT 160
TRANS 329	DISINFO 62
CYBER 203	CSDP/PSDC 608
TELECOM 251	MARE 18
ESPACE 45	POLMAR 47

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	6 September 2023
To:	Ms Thérèse BLANCHET, Secretary-General of the Council of the European Union
No. Cion doc.:	COM(2023) 526 final
Subject:	Proposal for a COUNCIL RECOMMENDATION on a Blueprint to coordinate a Union-level response to disruptions of critical infrastructure with significant cross-border relevance

Delegations will find attached document COM(2023) 526 final.

Encl.: COM(2023) 526 final

EUROPEAN
COMMISSION

Brussels, 6.9.2023
COM(2023) 526 final

2023/0318 (NLE)

Proposal for a

COUNCIL RECOMMENDATION

on a Blueprint to coordinate a Union-level response to disruptions of critical infrastructure with significant cross-border relevance

(Text with EEA relevance)

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

• Reasons for and objectives of the proposal

In the current geopolitical context, characterised by growing instability, notably due to Russia's war of aggression against Ukraine and increasing complexity of security threats, as well as by climate change effects such as an increase in unusual climate events or water scarcity, the Union must remain vigilant and adapt constantly. Citizens, companies and authorities in the Union rely on critical infrastructure[1] because of the essential services that the entities operating such infrastructure provide. Such services are crucial for the maintenance of vital societal functions, economic activities, public health and safety or the environment and must be provided in an unobstructed manner in the internal market. Therefore, due to the importance of these essential services for the internal market and, consequently, the need to make critical infrastructure more resilient and, more broadly, to ensure the resilience of critical entities providing these services, the Union must take measures to enhance such resilience and mitigate any disruptions in the provision of such essential services. Such disruptions may otherwise have serious consequences for citizens in the Union, our economies and trust in our democratic systems and may affect the smooth functioning of the internal market, in particular in a context of growing interdependencies between sectors and across borders.

The Union has already taken a number of measures to enhance the protection of critical infrastructure, notably as regards cross-border infrastructure, and the resilience of critical entities, in order to avoid or mitigate the effects of disruptions in the essential services that they provide in the internal market.

Directive 2008/114/EC on the identification and designation of European critical infrastructures[2] (''ECI Directive'') was the first legal instrument to establish an EU-wide procedure for identifying and designating European critical infrastructures and a common Union approach to assess the need to improve the protection of such infrastructure against man-made threats – both intentional and accidental – as well as natural disasters. However, it only focused on the energy and transport sectors and the protection of critical infrastructure and did not provide for wider measures to enhance the resilience of the entities operating such infrastructure.

Due to the increasingly inter-connected and cross-border nature of operations in the internal market, there was a need to cover more than two sectors and go beyond protective measures of individual assets. That is why Directive (EU) 2022/2557 on the resilience of critical entities[3] (''CER Directive'') was adopted in 2022, together with Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union[4] (''NIS 2 Directive''). The aim is to ensure a comprehensive level of physical and digital resilience of critical

---

[1] Critical infrastructure means an asset, a facility, equipment, a network or a system, or a part of an asset, a facility, equipment, a network or a system, which is necessary for the provision of an essential service (Article 2(4) of Directive (EU) 2022/2557 on the resilience of critical entities).

[2] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (OJ L 345, 23.12.2008, p. 75).

[3] Directive (EU) 2022/2557 of the European Parliament and of the Council on the resilience of critical entities and repealing Council Directive 2008/114/EC (OJ L 333, 27.12.2022, p. 164).

[4] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (OJ L 333, 27.12.2022, p. 80).

entities. The CER Directive entered into force on 16 January 2023 and aims at helping Member States to enhance the overall resilience of critical entities, while reinforcing coordination at Union level. It will replace the ECI Directive as of 18 October 2024, by which date Member States will have to take the necessary measures to comply with the CER Directive. The CER Directive applies to 11 sectors[5]. It shifts the focus from the protection of critical infrastructure to the wider concept of resilience of critical entities operating such critical infrastructure, covering the before-during-after of an incident. The NIS 2 Directive also entered into force on 16 January 2023 and modernises the existing legal framework to adapt to the increased digitisation and an evolving cybersecurity threat landscape. The NIS2 Directive also expands the scope of the cybersecurity rules to new sectors and entities and improves the resilience and incident response capacities of public and private entities, competent authorities and Union as a whole.

The CER Directive comprises provisions regarding incident notification by the critical entity to the national competent authority, notification of other (potentially) affected Member States by the national competent authority and notification of the Commission if the incident affects six Member States or more. The CER Directive stipulates certain incident notification obligations where the incident has or might have a significant impact on critical entities and the continuity of the provision of essential services to or in one or more other Member States[6].

As illustrated by the sabotage of the Nord Stream gas pipelines in September 2022, the security context in which critical infrastructure operates has changed significantly and additional urgent action is needed at Union level in order to enhance the resilience of critical infrastructure, not only as regards preparedness but also as regards a coordinated response.

In this context, a Council Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure[7] ("the Critical Infrastructure Resilience Recommendation") was adopted on 8 December 2022 following a Commission proposal. That Recommendation highlights, among others, the need to ensure at Union level a coordinated and effective response to current and future risks to the provision of essential services. More specifically, the Council invited the Commission "to draft a Blueprint on a coordinated response to disruptions of critical infrastructure with significant cross-border relevance". The Recommendation mentions that the Blueprint should be coherent with the EU Protocol for countering hybrid threats[8], take into account the Commission Recommendation 2017/1584 on coordinated response to large scale cybersecurity incidents and crises[9] (''Cyber Blueprint'') and respect the Integrated Political Crisis Response[10] (''IPCR'') arrangements.

Against this background, the current proposal for an additional Council Recommendation contains such a Blueprint. The proposal aims at complementing the current legal framework by describing the coordinated response at Union level when it comes to disruptions of critical infrastructure with significant cross-border relevance while making use of existing Union-level arrangements. Concretely, the proposal describes the scope and the objectives of the

---

5 Energy, transport, banking, financial market infrastructure, digital infrastructure, public administration, space, health, drinking water, waste water, production, processing and distribution of food.

6 In conformity with Art 15 (1) and (3) of the CER Directive.

7 Council Recommendation of 8 December 2022 on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure 2023/C 20/01 (OJ C 20, 20.1.2023, p. 1).

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

9 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).

10 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).

Blueprint and the actors, the processes and existing tools that could be used in order to respond, in a coordinated way at Union level, to a disruptive critical infrastructure incident with significant cross-border effect and describes the modes of cooperation between the Member States, Union institutions, bodies, offices and agencies in such situations.

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

This proposal for a Council Recommendation is in line with and complements the current legal framework on the protection of critical infrastructure and the resilience of critical entities - the ECI Directive and the CER Directive respectively, as well as the Critical Infrastructure Resilience Recommendation - since it aims at ensuring, in a complementary way, the coordination between Member States, and between them and the Union institutions, bodies, offices and agencies when it comes to responding to incidents that cause disruptions of critical infrastructure with significant cross-border relevance and the provision of essential services. The proposal makes use of existing structures and mechanisms at Union level, including those established by the CER Directive, namely the cooperation between competent authorities and the Critical Entities Resilience Group, which is a group established by the CER Directive to support the Commission and facilitate cooperation among Member States and the exchange of information on issues relating to the CER Directive.

This proposal for a Council Recommendation is also in line with and complementary to the Union framework on cybersecurity as laid down by NIS 2 Directive.

The current proposal aims at putting forward, in the area of resilience of critical entities and protection of critical infrastructure, a Critical Infrastructure Blueprint similar to the Cyber Blueprint.

Point 4(b) of Part I of the Annex also explains the interlinkages with the Cyber Blueprint, which applies to large-scale cybersecurity incidents that cause disruption too extensive for a concerned Member State to handle on its own or which affect two or more Member States or Union institutions with such a wide-ranging and significant impact of technical or political significance that they require timely policy coordination and response at Union political level. An incident is defined in NIS 2 Directive as ‘’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” (‘’cyber incident’’).

Competent authorities under the CER Directive and under the NIS 2 Directive have the obligation to cooperate and exchange information on cybersecurity incidents and incidents affecting critical entities, including with regard to relevant measures taken. In a situation where a significant critical infrastructure incident and a large-scale cybersecurity incident affect the same entity, there should be coordination on possible responses between the relevant actors.

The proposal is consistent with the EU Protocol for countering hybrid threats the latter being applicable in the case of hybrid incidents. Point 4(a) of Part I of the Annex explains the interlinkages with the EU Protocol, including which instrument applies in case of a significant critical infrastructure incident with a hybrid dimension.

The proposal is also coherent with other existing crisis management mechanisms at Union level, such as the Council’s IPCR arrangements, the Commission’s internal crisis coordination

process, ARGUS[11] and the Union Civil Protection Mechanism[12] (''UCPM'') supported by its Emergency Response Coordination Centre (''ERCC''), and the European External Action Service Crisis Response Mechanism.

The proposal is also consistent with other relevant sectoral legislation, and notably with specific measures therein that regulate certain aspects of response to disruptions by entities operating in concerned sectors.

2. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY

• Legal basis

The proposal is based on Article 114 of the Treaty on the Functioning of the European Union (''TFEU''), which involves the approximation of laws for the improvement of the internal market, together with Article 292 TFEU, which lays down the relevant rules regarding the adoption of Recommendations.

The choice of Article 114 TFEU as the substantive legal basis is justified by the fact that the proposed Council Recommendation aims at ensuring a coordinated response in case of disruptions of critical infrastructure with significant cross-border relevance. Such disruptions affect several Member States and risk impacting the functioning of the internal market because of the growing interdependencies between infrastructure and sectors in an increasingly interdependent Union economy. Improved response to disruptions will avoid, in turn, disruptions in the functioning of the internal market since those critical infrastructure and the essential services they provide are crucial for the maintenance of vital societal functions, economic activities, public health and safety, or the environment.

The proposal would complement the ECI and CER Directives, which are also based on Article 114 TFEU. The Critical Infrastructure Resilience Recommendation is, like the Recommendation now proposed, also based on Articles 114 and 292 TFEU.

• Subsidiarity (for non-exclusive competence)

Whereas responding to disruptions of critical infrastructure or of the services provided by the critical entities operating that critical infrastructure is first and foremost the responsibility of Member States, the Union has an important role in case of a disruption of critical infrastructure with significant cross-border relevance, since such disruption may impact several or even all sections of economic activity within the single market, the security and international relations of the Union. With the aim of securing the functioning of the internal market, the coordination, at Union level, in case of disruptions of critical infrastructure with significant cross-border effect is not only appropriate but also necessary since such coordinated response at Union level will support Member States' response to the disruption by way of shared situational awareness, coordinated public communication and mitigating the consequences of the disruption on the internal market.

---

[11] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Commission provisions on "ARGUS" general rapid alert system, COM(2005) 662 final.

[12] Regulation (EU) 2021/836 of the European Parliament and of the Council of 20 May 2021 amending Decision No 1313/2013/EU on a Union Civil Protection Mechanism (OJ L 185, 26.5.2021, p. 1).

- **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 response at the Union level in case of disruptions of critical infrastructure or of the services provided by the critical entities operating that critical infrastructure and which have a significant cross border relevance. This proposed coordinated response is proportionate with Member States' prerogatives and obligations under national law. Incidents that disrupt critical infrastructure or the provision of essential services by critical entities often fall below the threshold of a significant critical infrastructure incident and may be addressed effectively at national level. Therefore, the use of the mechanism provided by in this proposal is limited to major disruptions that have a significant cross-border relevance affecting several Member States.

- **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 the area of coordinated response in case of significant disruptions of critical infrastructure. In this manner, the proposed Recommendation would complement the binding legal framework (in particular, the CER Directive) and also the earlier adopted Critical Infrastructure Resilience Recommendation, which calls for such complementary measures, while fully respecting Member States' responsibilities in the area at issue.

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

- **Stakeholder consultations**

In developing this proposal, Member States, Union institutions and agencies were consulted. Also, the views of the Member State experts expressed both at the workshop of 24 April 2023 and sent in writing after that workshop were taken into consideration.

There was overall consensus on the usefulness of more coordination in the response at Union level to disruptions of critical infrastructure with significant cross-border relevance in the current threat context, while respecting the competence of Member States in this area and confidentiality of sensitive information. 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.

While certain Member States had a positive view as regards the wider scope of the Critical Infrastructure Blueprint, others considered that the threshold of six or more Member States provided in the CER Directive when it comes to the identification of critical entities of particular European significance was sufficient and it was not necessary to have a second type of incident included in the scope. A few Member States remarked on the importance of involving, where appropriate, operators of critical infrastructure providing essential services, due to their expertise and the importance of taking into account the cyber dimension.

- **Detailed explanation of the specific provisions of the proposal**

The proposal for a Council Recommendation consists of a main part and an annex.

The main part consists of 11 points as follows:

Point (1) sets out the need for enhanced cooperation as regards response to significant critical infrastructure incidents in accordance with the Critical Infrastructure Blueprint contained in the present proposed Recommendation, including the relevant parts of its Annex.

Point (2) specifies the scope of the Critical Infrastructure Blueprint, which refers to two types of situations of disruptive incidents that would trigger the application of the Critical Infrastructure Blueprint: the incident has either a significant disruptive effect on the provision of essential services to or in six or more Member States; or has a significant disruptive effect in two or more Member States and there is agreement among the relevant actors mentioned therein of the need for Union level coordination due to the significant impact of the incident.

Point (3) refers to the identification of the relevant actors to be involved in the Critical Infrastructure Blueprint and the levels at which the Critical Infrastructure Blueprint will operate (operational, strategic/political). This is further explained in the Annex to the Recommendation.

Point (4) recommends the application of the Critical Infrastructure Blueprint in coherence with other relevant instruments, as described in the Annex.

Point (5) recommends to Member States to effectively respond, at national level, to significant disruptions of critical infrastructure.

Point (6) recommends establishing or designating points of contact by the relevant actors that should support the use of the Critical Infrastructure Blueprint. Where possible, these points of contact should be the same as the single points of contact under the CER Directive.

Point (7) refers to the flow of information in case of a significant critical infrastructure incident.

Point (8) expands on how the exchange of information should take place.

Point (9) recommends testing the functioning of the Critical Infrastructure Blueprint through exercises.

Point (10) recommends that lessons identified should be discussed in the Critical Entities Resilience Group, which should prepare a report, including recommendations. The report should be adopted by the Commission.

Point (11) recommends to Member States to discuss the report in the Council.

The Annex describes the objectives, principles, main actors, the interplay with existing crisis response mechanisms and the functioning of the Critical Infrastructure Blueprint with its two modes of cooperation: the information exchange and the response.

2023/0318 (NLE)

Proposal for a

COUNCIL RECOMMENDATION

on a Blueprint to coordinate a Union-level response to disruptions of critical infrastructure with significant cross-border relevance

(Text with EEA relevance)

THE COUNCIL OF THE EUROPEAN UNION,

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

Having regard to the proposal from the European Commission,

Whereas:

(1) The reliance on resilient critical infrastructure and resilient critical entities providing services that are crucial for the maintenance of vital societal functions, economic activities, public health and safety, or the environment, is fundamental for the smooth functioning of the internal market and the society as a whole.

(2) In the current evolving risk landscape and in light of growing interdependencies between infrastructure and sectors and, more broadly, interconnections across sectors and borders, there is a need to address and enhance, in a comprehensive and coordinated manner, the protection of critical infrastructure and the resilience of critical entities operating such infrastructure.

(3) An incident which disrupts critical infrastructure and thereby disables or severely hampers the provision of essential services may have significant cross-border effects and negatively impact the internal market. In order to ensure a targeted, proportionate and effective approach, measures should be taken to address, in particular, significant critical infrastructure incidents, as specified in this Recommendation, covering for instance situations where the disruption caused by the incident is of long duration or may have considerable cascading effects in the same or other sectors or Member States.

(4) A coordinated response to significant critical infrastructure incidents is essential in order to avoid major disruptions in the internal market and to ensure the restoration of the provision of those essential services as soon as possible, since such incidents may have serious consequences on the economy and citizens in the Union. A timely and effective Union-level response to such incidents requires swift and effective cooperation amongst all relevant actors and coordinated action supported by at Union-level. Such response relies, therefore, on the existence of previously established and, to the extent possible, well-rehearsed cooperation procedures and mechanisms with specified roles and responsibilities of the key actors at national and Union level.

(5) While the primary responsibility for ensuring response to significant critical infrastructure incidents rests with the Member States and the entities operating critical infrastructure and providing essential services, increased coordination at Union level is appropriate in case of disruptions with significant cross-border relevance. A timely and effective response is dependent not only on the deployment of national mechanisms by Member States but also on coordinated action supported at Union level, including having relevant cooperation in a swift and effective manner.

(6) The protection of European critical infrastructure is currently regulated by Council Directive 2008/114/EC[1], which covers only two sectors, namely transport and energy. That Directive establishes a procedure for the identification and designation of European critical infrastructure and a common approach on assessing the need to improve the protection of such infrastructure. It is the central pillar of the European Programme for Critical Infrastructure Protection[2] (''EPCIP'') adopted by the Commission in 2006 that has set out a European-level all-hazards framework for critical infrastructure protection.

(7) In order to go beyond the protection of critical infrastructure and to ensure, more broadly, resilience of critical entities operating such infrastructure that provide essential services in the internal market, Directive (EU) 2022/2557 of the European Parliament and of the Council[3] will replace Directive 2008/114/EC as of 18 October 2024. Directive (EU) 2022/2557 covers 11 sectors and provides for resilience-enhancing obligations for Member States and critical entities, cooperation between Member States and with the Commission as well as for support by the Commission for national authorities and critical entities and support from the Member States to the critical entities.

(8) Following the sabotage of the Nord Stream gas pipelines, there is a need for more resilience-enhancing measures for critical infrastructure to be adopted at Union level. Therefore, based on a Commission proposal, the Council adopted Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure (''Recommendation 2023/C 20/01'')[4], which aims at enhancing preparedness, response and international cooperation in this area. That Recommendation highlighted notably the need to ensure at Union level a coordinated and effective response to risks to the provision of essential services.

(9) Therefore, it is necessary to complement the existing legal framework by an additional Council Recommendation setting out a Blueprint on a coordinated response to disruptions of critical infrastructure with significant cross-border relevance (''the Critical Infrastructure Blueprint''), while making use of existing Union-level arrangements.

(10) This Recommendation should be aligned with Recommendation 2023/C 20/01, to ensure consistency and avoid duplication. Therefore, this Recommendation should not,

---

[1] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (OJ L 345, 23.12.2008, p.75).

[2] COM(2006) 786 final of 12 December 2006 – Communication from the Commission on a European Programme for Critical Infrastructure Protection.

[3] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (OJ L 333, 27.12.2022, p. 164).

[4] Council Recommendation of 8 December 2022 on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure 2023/C 20/01 (OJ C 20, 20.1.2023, p. 1).

as such, cover the other elements of the crisis management lifecycle, namely prevention, preparedness and recovery.

(11) This Recommendation should complement Directive (EU) 2022/2557, in particular in terms of coordinated response, and should be implemented whilst ensuring coherence with that Directive and any other applicable rules of Union law. Therefore, this Recommendation should also rely on and use, to the extent possible, the notions, tools and processes of that Directive, such as the Critical Entities Resilience Group, acting within the limits of its tasks as set out in that Directive, and points of contact. In addition, the notion of ''critical infrastructure'' as used in this Recommendation should be understood in the same way as set out in recital 7 of Recommendation 2023/C 20/01, that is, as comprising relevant critical infrastructure identified by a Member State at national level or designated as a European critical infrastructure under Directive 2008/114/EC, as well as critical entities to be identified under Directive (EU) 2022/2557. In order to ensure consistency with Directive (EU) 2022/2557, those notions used in this Recommendation should therefore be interpreted as having the same meaning as in that Directive. For instance, the concept of resilience, as defined in Article 2, point 2, of that Directive, should also be understood as referring to a critical infrastructure's ability to prevent, protect against, respond to, resist, mitigate, absorb, accommodate or recover from events that significantly disrupt or have the potential to significantly disrupt the provision of essential services in the internal market, that is, services which are crucial for the maintenance of vital societal and economic functions, public safety and security, the health of the population, or the environment.

(12) In addition, the notion of "significant disruptive effect" should be understood in light of the criteria provided by Article 7(1) of Directive (EU) 2022/2557, which refer to: i) the number of users relying on the essential service provided by the entity concerned; ii) the extent to which other sectors and subsectors as set out in the Annex to the Directive depend on the essential service in question; iii) the impact that incidents could have, in terms of degree and duration, on economic and societal activities, the environment, public safety and security, or the health of the population; iv) the entity's market share in the market for the essential service or essential services concerned; v) the geographic area that could be affected by an incident, including any cross-border impact, taking into account the vulnerability associated with the degree of isolation of certain types of geographic areas, such as insular regions, remote regions or mountainous areas; vi) the importance of the entity in maintaining a sufficient level of the essential service, taking into account the availability of alternative means for the provision of that essential service.

(13) In the interest of efficiency and effectiveness, the Critical Infrastructure Blueprint should be fully coherent and interoperable with the revised Union operational protocol for countering hybrid threats[5] and take into account the existing Blueprint on coordinated response to large-scale cross-border cybersecurity incidents and crises laid down by Commission Recommendation (EU) 2017/1584[6] (''Cyber Blueprint''), and the European cyber crisis liaison organisation network (''EU-CyCLONe'') mandate laid down in Directive (EU) 2022/2555 of the European Parliament and of the

[5] Joint Staff Working Document - EU Protocol for countering hybrid threats SWD(2023)116 final.

[6] 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).

Council[7] and avoid the duplication of structures and activities. It should also fully respect the Council's Integrated Political Crisis Response[8] (''IPCR'') arrangements for the coordination of the response.

(14) This Recommendation builds on and is, more broadly, consistent and complementary with the established Union crisis management mechanisms, notably the Council's IPCR arrangements, the Commission's internal crisis coordination process ARGUS[9] and the Union Civil Protection Mechanism (''UCPM'')[10], supported by the Emergency Response Coordination Centre (''ERCC''),[11] the European External Action Service (''EEAS'') Crisis Response Mechanism, as well as the Single Market Emergency Instrument[12], all of which may play a role in responding to a major disruption to critical infrastructure operations.

(15) In responding to a significant critical infrastructure incident, the above tools or mechanisms at Union level may be used, in accordance with the rules and procedures applicable thereto, which this Recommendation should complement but leave unaffected. For instance, the Council's IPCR arrangements remain the main tool for coordination of the response at political Union level among Member States. Internal coordination in the Commission takes place in the framework of the ARGUS cross-sectoral crisis coordination process. If the crisis entails an external or Common Security and Defence Policy (''CSDP'') dimension, the EEAS Crisis Response Mechanism can be used. In line with Decision No 1313/2013/EU on a Union Civil Protection Mechanism (''UCPM''), operational responses under the UCPM to actual or imminent natural and human-induced disasters within and outside the Union (including those affecting critical infrastructure) are organised by the ERCC, the Commission's single 24/7 operational hub managing crisis responses. In such instances, the ERCC can provide early warning, notification, analysis, and supports information-sharing and, in the event of a UCPM activation by a Member State, the deployment of operational assistance and experts to affected areas. In addition, the ERCC can facilitate sectoral and cross-sectoral coordination at both EU level and between the EU and relevant national authorities, including ones responsible for civil protection and critical infrastructure resilience.

(16) While the processes laid down in this Recommendation should be considered, where appropriate, in connection to those other tools or mechanisms once they are used, this Recommendation should also describe the actions that could be undertaken at Union level as regards shared situational awareness, coordinated public communication and

---

[7] 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 (OJ L 333, 27.12.2022, p. 80).

[8] 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).

[9] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Commission provisions on "ARGUS" general rapid alert system, COM(2005) 662 final.

[10] Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism (OJ L 347, 20.12.2013, p. 924).

[11] Decision No 1313/2013/EU on a Union Civil Protection Mechanism (UCPM), creates an all-hazards framework setting out Union-level prevention, preparedness, and response arrangements to manage all kinds of natural and human-induced disasters or imminent disasters within and outside the EU.

[12] Regulation …/… of the European Parliament and of the Council establishing a Single Market emergency instrument and repealing Council Regulation No (EC) 2679/98, COM(2022) 459 final.

effective response outside the framework of those Union crisis coordination mechanisms, in case they are not used.

(17) In order to better coordinate response in case of significant critical infrastructure incidents, there should be enhanced cooperation between Member States and Union institutions, relevant agencies, bodies and offices of the Union working through existing arrangements, in accordance with the framework of the Critical Infrastructure Blueprint. The Critical Infrastructure Blueprint should therefore apply when the threshold of six or more Member States provided for in Directive (EU) 2022/2557 as regards the identification of critical entities of particular European significance is met, as well as when incidents affecting a smaller number of Member States occur because such incidents could have a wide-ranging impact, due to cascading effects across borders and therefore Union-level response coordination would be beneficial.

(18) While a cooperation framework at Union level for a coordinated response to significant critical infrastructure incidents is deemed necessary, it should not divert resources of critical entities and competent authorities from incident handling, which should be the priority.

(19) The relevant actors involved in the implementation of the Critical Infrastructure Blueprint should be clearly identified so that there is a clear and comprehensive overview of the institutions, bodies, offices, agencies and authorities that could be responding to a significant critical infrastructure incident.

(20) Responding to critical infrastructure incidents, including significant ones, is the primary responsibility of the competent authorities of the Member States. This Recommendation should not affect Member States' responsibility for safeguarding national security and defence or their power to safeguard other essential State functions, in particular concerning public security, territorial integrity and the maintenance of law and order, in accordance with Union law. Further, this Recommendation should not affect national processes, such as the communication and liaison of operators of critical infrastructure with the competent national authorities. This Recommendation should apply without affecting relevant bilateral or multilateral arrangements concluded between Member States.

(21) Designating or establishing points of contact by the relevant actors is essential for an effective and timely cooperation within the framework of the Critical Infrastructure Blueprint. To ensure coherence, Member States should consider the possibility to have as the points of contact designated or established within this framework the single points of contact to be designated or established in the framework of Directive (EU) 2022/2557.

(22) In the interest of effectiveness, testing and practicing the Critical Infrastructure Blueprint, as well as reporting and discussing lessons learnt after its application, should be an essential part of maintaining a high level of readiness in the event of significant critical infrastructure incidents and of ensuring the ability to deliver a swift and well-coordinated response, with the involvement of the relevant actors.

(23) Considering the structure of the Council's crisis coordination mechanism IPCR and taking into account, more broadly, the potential activation of the crisis coordination mechanisms already existing at Union level, the Critical Infrastructure Blueprint should encompass two modes of cooperation to respond to a significant critical infrastructure incident. The first should consist of the exchange of information involving all relevant actors, coordination of public communication and, where used,

coordination via already existing mechanisms such as the IPCR arrangements in the Council, or ARGUS coordination within the Commission, supported by the ERCC as operational 24/7 contact point, and the EEAS Crisis Response Mechanism. The second should comprise further response action due to the scale of the incident. This cooperation should involve engagement at operational, strategic/political levels, which reflects the levels in Recommendation 2017/1584 and the Union Protocol for countering hybrid threats, in order to coordinate actions and respond to the significant critical infrastructure incident in an effective and efficient manner. Based on the principles of proportionality, subsidiarity, confidentiality of information and complementarity and in order to ensure effective cooperation, the Critical Infrastructure Blueprint should describe how shared situational awareness by the relevant actors takes place, as well as coordinated public communication and effective response.

(24) The exchange of information pursuant to this Recommendation should be carried out without jeopardising national security or the security and commercial interests of entities operating critical infrastructure. Therefore, sensitive information should be accessed, exchanged and handled prudently, in accordance with the applicable rules, and with particular attention to the transmission channels and storage capacities used,

HAS ADOPTED THIS RECOMMENDATION:

(1) The Member States, the Council, the Commission and, where appropriate, the European External Action Service (''EEAS'') and relevant Union bodies, offices and agencies should cooperate with each other in the framework of the Critical Infrastructure Blueprint contained in this Recommendation, in order to achieve the objectives set out in Section 1 of Part I of the Annex and, taking account of the principles set out in Section 2 of Part I of the Annex, provide a coordinated response to significant critical infrastructure incidents.

(2) The Member States, the Council, the Commission and, where appropriate, the EEAS and relevant Union bodies, offices and agencies should apply the Critical Infrastructure Blueprint without undue delay whenever a significant critical infrastructure incident occurs, that is, an incident involving critical infrastructure having one of the following effects:

(a) a significant disruptive effect on the provision of essential services to or in six or more Member States, including when it affects a critical entity of particular European significance within the meaning of Article 17 of Directive (EU) 2022/2557 on the resilience of critical entities[13]; or

(b) a significant disruptive effect on the provision of essential services in two or more Member States, where the Member State holding the rotating Presidency of the Council, in agreement with those other Member States and in consultation with the Commission, considers that timely coordination in the response at Union level is required, due to the incident's wide-ranging and significant impact of technical or political relevance.

[13] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (OJ L 333, 27.12.2022, p. 164).

(3) The relevant actors of the Critical Infrastructure Blueprint, identified at operational, strategic/political levels in accordance with Section 3 of Part I of the Annex, should endeavour to interact and cooperate in complementarity. They should ensure the adequate and timely exchange of information, including coordination of public communication, and the coordinated response as set out in Part II of the Annex.

(4) The Critical Infrastructure Blueprint should be applied having regard to and in coherence with other relevant instruments, in accordance with Section 4 of Part I of the Annex. In case an incident affects both physical aspects and the cybersecurity of critical infrastructure, synergies with relevant processes set up in the Cyber Blueprint should be ensured.

(5) Member States should ensure that they effectively respond, at national level, and in accordance with Union law, to disruptions of critical infrastructure following significant critical infrastructure incidents.

(6) Member States, the Council, the EEAS, the European Union Agency for Law Enforcement Cooperation (''Europol'') and other relevant Union agencies should, as well as the Commission, designate or establish a point of contact for matters relating to the Critical Infrastructure Blueprint. The points of contact should support the application of the Critical Infrastructure Blueprint by providing necessary information and facilitate coordination measures responding to a significant critical infrastructure incident. For Member States, where possible, those points of contact should be the same as the single points of contact to be designated or established pursuant to Article 9(2) of Directive (EU) 2022/2557. For the Commission, the ERCC ensures 24/7 operational contact and capacity and coordinates, monitors and supports in real-time the response to emergencies at Union level, while serving Member States and the Commission as the operational hub for crisis response promoting a cross-sectoral approach to disaster management.

(7) The Member State holding the rotating Presidency of the Council, in agreement with the affected Member States, should inform all relevant actors, via the points of contact referred to in point 6, of the significant critical infrastructure incident and the application of the Critical Infrastructure Blueprint. Exchange of information regarding a significant critical infrastructure incident should occur via appropriate communication channels, including, where applicable and appropriate, the Integrated Political Crisis Response[14] platform (''IPCR'') and the ERCC via the Common Emergency Communication and Information System (''CECIS''), a web-based alert and notification application enabling real-time exchange of information.

(8) If necessary, transmission channels should include secured ones in order not to jeopardise national security or the security and commercial interests of the entities concerned. The exchange of information that is described in Section 1 of Part II of the Annex to this Recommendation should also be done without jeopardising national security or the security and commercial interests of critical entities and in accordance with Union law, in particular Regulation (EU) …/… of the European Parliament and of the Council[15]. In particular, sensitive information should be accessed, exchanged

[14] Council Implementing Decision (EU) 2018/1993 of 11 December 2018 on the EU Integrated Political Crisis Response Arrangements, ST/13422/2018/INIT, (OJ L 320, 17.12.2018, p. 28).

[15] Regulation (EU) …/… on information security in the institutions, bodies, offices and agencies of the Union COM/2022/119 final.

and handled prudently. Available accredited tools as well as adequate security measures should be used for the handling and exchanging of classified information.

(9) The relevant actors should regularly practise and test the functioning of the Critical Infrastructure Blueprint and their coordinated response to a significant critical infrastructure incident at national, regional and Union level, for instance in the context of exercises. Such practices and tests may include, as appropriate, private sector entities. An exercise at Union level incorporating physical and cyber aspects should take place by [*the date of the adoption of this Recommendation + 12 months*].

(10) Following the application of the Critical Infrastructure Blueprint in respect of a significant critical infrastructure incident, the Critical Entities Resilience Group referred to in Article 19 of Directive (EU) 2022/2557 should discuss with the relevant actors, in a timely manner, the lessons identified that may indicate gaps and areas where improvements are necessary and subsequently prepare a report, including recommendations to achieve such improvements. The preparation of that report should be supported by the relevant actors involved in the application of the Critical Infrastructure Blueprint. The report should be adopted by the Commission.

(11) Member States should discuss the report referred to in point 10 in the relevant Council preparatory bodies or in the Council.

Done at Brussels,

For the Council
The President