Council of the European Union

Brussels, 17 June 2024
(OR. en)

10653/24

Interinstitutional File: 2023/0318(NLE)

PROCIV 53	ATO 41
ENV 582	CSC 337
JAI 936	ECOFIN 633
SAN 316	CSCI 99
COSI 106	DATAPROTECT 230
CHIMIE 40	MI 571
ENFOPOL 275	CODEC 1429
RECH 263	COPS 309
CT 64	JAIEX 42
DENLEG 37	COPEN 294
COTER 116	IND 295
RELEX 747	POLMIL 200
ENER 270	IPCR 44
HYBRID 92	DIGIT 150
TRANS 272	DISINFO 87
CYBER 181	CSDP/PSDC 411
TELECOM 201	MARE 12
ESPACE 54	POLMAR 23

LEGISLATIVE ACTS AND OTHER INSTRUMENTS

Subject:	COUNCIL RECOMMENDATION on a Blueprint to coordinate a response at Union level to disruptions of critical infrastructure with significant cross-border relevance

COUNCIL RECOMMENDATION

of …

on a Blueprint to coordinate a response at Union level 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 292 in conjunction with Article 114 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 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 between sectors and borders, there is a need to address and enhance 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, critical infrastructure incidents with significant cross-border relevance, as specified in this Recommendation.

(4) A coordinated response to such an incident with significant cross-border relevance might prove essential in order to avoid major disruptions in the internal market and to ensure the restoration of the provision of the affected essential services as soon as possible, since such an incident may have serious consequences on the economy and citizens in the Union. A timely and effective response at Union level to such an incident requires swift and effective cooperation amongst all relevant actors and coordinated action supported 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, bilateral, multilateral and, where relevant, 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 may be appropriate in case of disruptions with significant cross-border relevance. A timely and effective response may be 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) Responding to critical infrastructure incidents, including those with significant cross-border relevance, is the primary responsibility of the competent authorities of the Member States. This Recommendation does 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. This Recommendation, therefore, does not apply to critical infrastructures that carry out activities in those areas. Furthermore, this Recommendation does not affect national processes, such as the communication and liaison of entities operating critical infrastructure with the competent national authorities. This Recommendation applies without affecting relevant bilateral or multilateral arrangements concluded by and between Member States.

(7) 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 ("EPCIP") set up by the Commission in its Communication of 12 December 2006[2], that has set out a Union-level all-hazards framework for critical infrastructure protection.

---

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

(8) In order to go beyond the protection of critical infrastructure and to ensure, more broadly, resilience of critical entities operating critical infrastructure that provide essential services in the internal market, Directive (EU) 2022/2557 of the European Parliament and of the Council[3] replaces 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 to national authorities and critical entities and support from Member States to critical entities.

(9) Following the sabotage of the Nord Stream gas pipelines and based on a Commission proposal, the Council adopted a Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure[4] ('Recommendation 2023/C 20/01'), which aims at enhancing preparedness, response and Union and international cooperation in that area. That Recommendation highlighted notably the need to enhance at Union level a coordinated and effective response and operational preparedness to address the immediate and indirect effects of disruptions with significant cross-border relevance of relevant essential services provided by critical infrastructure.

---

[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).

(10) Therefore, this Recommendation, which is a non-binding act, is necessary to support and 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 EU Critical Infrastructure Blueprint'), while making use of existing arrangements at Union level.

(11) This Recommendation is aligned to Recommendation 2023/C 20/01, to ensure consistency and avoid duplication. Therefore, this Recommendation does not, as such, cover the other elements of the crisis and emergency management lifecycle, namely prevention, preparedness and recovery.

(12) 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. This Recommendation adopts an all-hazard approach and relies on and uses, to the extent possible, the existing structures and mechanisms, including the relevant Working Parties of the Council (namely the Working Party on Civil Protection – Critical Entities Resilience, 'PROCIV CER Working Party'), and also the existing 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.

(13) The scope of this Recommendation is limited to the sectors, subsectors and types of entities within the scope of Directive (EU) 2022/2557. The exclusions set out in that Directive apply within the scope of this Recommendation. Furthermore, this Recommendation should not duplicate already existing arrangements and structures within relevant sector-specific Union legal acts.

(14) 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 that 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.

(15) In the interest of efficiency and effectiveness, the EU Critical Infrastructure Blueprint should fully respect the Council's Integrated Political Crisis Response ('IPCR') arrangements for the coordination of the response[5]. It should also be fully coordinated, coherent and interoperable with all the other sectoral Union instruments or processes, such as the processes described in the EU Hybrid Toolbox[6] and in the revised EU Protocol for countering hybrid threats[7]. It should also take into account and respect the mandates of the European cyber crisis liaison organisation network ('EU-CyCLONe') and the Computer Security Incident Response Teams ('CSIRTs') Network as laid down in Directive (EU) 2022/2555 of the European Parliament and of the Council[8]. The Blueprint on coordinated response to large-scale cross-border cybersecurity incidents and crises laid down by Commission Recommendation (EU) 2017/1584[9] ('Cyber Blueprint') and the pan-European systemic cyber incident coordination framework for relevant authorities ('EU-SCICF') as recommended by the European Systemic Risk Board ('ESRB') should, where relevant, also be taken into account. To the extent possible, the duplication of structures and activities should be avoided.

---

5 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).

6 See the Council conclusions of 21 June 2022 on a Framework for a coordinated EU response to hybrid campaigns, and the Implementing guidelines approved by the Council on 13 December 2022 for the Framework for a coordinated EU response to hybrid campaigns.

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

8 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).

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).

(16) This Recommendation builds on and is, more broadly, consistent and complementary with existing bilateral or multilateral arrangements and the established Union crisis and emergency management mechanisms, notably the Council's IPCR arrangements, the Commission's internal crisis coordination process ARGUS[10] and the Union Civil Protection Mechanism[11] ('UCPM'), supported by the Emergency Response Coordination Centre ('ERCC'),[12] the European External Action Service ('EEAS') Crisis Response Mechanism as well as the Regulation establishing a framework of measures related to an internal market emergency and to the resilience of the internal market, all of which may play a role in responding to a major disruption to critical infrastructure operations.

---

[10] Communication from the Commission of 23 December 2005 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).

[11] 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).

[12] Decision No 1313/2013/EU 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 Union.

(17) In responding to a critical infrastructure incident with significant cross-border relevance, the above mentioned tools and mechanisms at Union level could 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 response at Union political level among Member States. Internal coordination within the Commission takes place in the framework of the ARGUS cross-sectoral crisis coordination process. If the crisis entails an external dimension, the EEAS Crisis Response Mechanism could be used. Under Decision No 1313/2013/EU, the UCPM can be activated to respond to actual or imminent natural and man-made disasters within and outside the Union (including those stemming from incidents affecting critical infrastructure) with the operational support from the ERCC. The ERCC works in close contact with national civil protection authorities and relevant Union bodies to promote a cross-sectoral approach to disaster management.

(18) 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 also describes the actions that could be undertaken at Union level as regards shared situational awareness, coordinated public communication and effective response outside the framework of those Union crisis coordination mechanisms, in case they are not used and relevant.

(19) In order to better coordinate, where relevant, the response in case of critical infrastructure incidents with significant cross-border relevance, there should be enhanced cooperation between Member States and Union institutions, relevant Union bodies, offices and agencies working on the basis of arrangements in effect, in accordance with the framework of the EU Critical Infrastructure Blueprint. The EU Critical Infrastructure Blueprint should therefore apply when there is a significant disruption of the provision of essential services as assessed and communicated by six or more Member States as well as when a disruption affects a critical entity of particular European significance, as coined in Directive (EU) 2022/2557, as assessed and communicated by the affected Member States. It should also apply when incidents have a significant disruptive effect on the provision of essential services to or in two or more Member States, and the Presidency of the Council assesses, in agreement with the affected Member States and in consultation with the Commission, that timely coordination in the response at Union level is required.

(20) While a cooperation framework at Union level for a coordinated response to critical infrastructure incidents with significant cross-border relevance is deemed necessary, it should not divert resources of critical entities and competent authorities from incident handling, which should be the priority and should not increase their liability.

(21) The relevant actors involved in the implementation of the EU 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 critical infrastructure incident with significant cross-border relevance.

(22) Designating or establishing points of contact by the relevant actors is essential for an effective and timely cooperation within the framework of the EU Critical Infrastructure Blueprint. To ensure coherence, Member States should consider the possibility of having 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.

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

(24) 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 EU Critical Infrastructure Blueprint should encompass two modes of cooperation to respond to a critical infrastructure incident with significant cross-border relevance. The first should consist of the exchange of relevant 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 24/7 contact point of IPCR and ARGUS, and the EEAS Crisis Response Mechanism. The second should comprise further response action due to the scale of the incident and the relevance of a coordinated response. This cooperation should involve engagement at operational, strategic/political levels, which reflects the levels described in Recommendation (EU) 2017/1584 and the EU Protocol for countering hybrid threats, in order to coordinate actions and respond to incidents with significant cross-border relevance 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 EU Critical Infrastructure Blueprint should describe how shared situational awareness by the relevant actors takes place, as well as coordinated public communication and effective response.

(25) This Recommendation should be without prejudice to Article 346 of the Treaty on the Functioning of the European Union. Information that is confidential pursuant to Union or national rules, such as rules on business confidentiality, should be exchanged with the Commission and other relevant authorities on a need to know basis and only where that exchange is necessary for the application of this Recommendation. No Member State should, pursuant to this Recommendation, be expected to supply information the disclosure of which would jeopardise its essential interests, national security, public security, defence or commercial interests of entities operating critical infrastructure. Therefore, sensitive information should be accessed, exchanged and handled prudently and be limited to that which is relevant and proportionate, in accordance with the applicable rules, and with particular attention to the transmission channels and storage capacities used.

RECOMMENDS HEREBY:

(1) 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 EU 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 should, taking account of the principles set out in Section 2 of Part I of the Annex, provide a coordinated response to critical infrastructure incidents with significant cross-border relevance.

(2) Member States, the Council, the Commission and, where appropriate, the EEAS and relevant Union bodies, offices and agencies should apply the EU Critical Infrastructure Blueprint without undue delay, whenever a critical infrastructure incident with significant cross-border relevance occurs and as long as the Member State hosting the affected critical infrastructure is in agreement. In the context of this EU Critical Infrastructure Blueprint, a critical infrastructure incident with significant cross-border relevance takes place when an incident involving critical infrastructure has one of the following effects:

(a) a significant disruptive effect on the provision of essential services, as assessed by six or more affected Member States, and communicated to the Presidency of the Council and to the Commission;

(b) a significant disruptive effect on the provision of essential services by a critical entity of particular European significance within the meaning of Article 17 of Directive (EU) 2022/2557 of the European Parliament and of the Council[13], as assessed by the affected Member State(s), and communicated to the Presidency of the Council and to the Commission; or

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

(3) The relevant actors of the EU 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 relevant information, including coordination of public communication and coordination of the response set out in Part II of the Annex.

---

[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).

(4) The EU 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, coordination and synergies with the provisions for coordinated management of large-scale cybersecurity incidents provided for by Directive (EU) 2022/2555 of the European Parliament and of the Council[14] 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, whether they have significant cross-border relevance or not.

(6) Member States, the Council, the EEAS, the European Union Agency for Law Enforcement Cooperation ('Europol') and other relevant Union agencies, as well as the Commission, should designate or establish a point of contact for matters relating to the EU Critical Infrastructure Blueprint. Information should be handled in accordance with established procedures and regulations, including the handling of classified information. The points of contact should support the application of the EU 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.

---

[14] 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).

(7) The Member State holding the Presidency of the Council should, in agreement with the affected Member States, inform the relevant actors involved in the response to the incident, via the points of contact referred to in point 6, of the critical infrastructure incident with significant cross-border relevance and the application of the EU Critical Infrastructure Blueprint. Exchange of information regarding a critical infrastructure incident with significant cross-border relevance should be limited to that which is relevant and proportionate to the purpose of that exchange and should occur via appropriate communication channels, including, where applicable and appropriate, the Integrated Political Crisis Response[15] ('IPCR') platform and the ERCC.

(8) When necessary, transmission channels should include secured ones in order not to jeopardise national security or the security and commercial interests of critical entities. The exchange of information in accordance with the Annex should not include information the disclosure of which would be contrary to the essential interests of Member States' national security, public security or defence or the security and commercial interests of critical entities and in accordance with Union law. In particular, sensitive information should be accessed, exchanged and handled prudently. Available accredited tools as well as adequate security measures should be used for the handling and exchanging of classified information.

[15] 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) The relevant actors should practise and test the functioning of the EU Critical Infrastructure Blueprint and their coordinated response to a critical infrastructure incident with significant cross-border relevance at national, regional and Union level, for instance in the context of exercises. Such practices and tests could include private sector entities, in agreement with all parties and in particular with the concerned Member States. Any contact with critical entities should be made through the Member States concerned. An exercise at Union level incorporating physical and cyber aspects should be organised by the Commission, in close cooperation with the Member States, including through the PROCIV CER Working Party and EU-CyCLONe, the CSIRTs network and with the support of ENISA. The objectives of the exercise should be agreed with the Member States beforehand. The exercise should take place by … [date of adoption of this Recommendation + 18 months]. Based on an exchange with the Member States about lessons learnt regarding that exercise, the need for further exercises and the appropriate scenarios should be considered.

(10) Following the application of the EU Critical Infrastructure Blueprint in respect of a critical infrastructure incident with significant cross-border relevance, the PROCIV CER Working Party should discuss the lessons learnt that may indicate gaps and areas where improvements are necessary. Other relevant Working Parties could be associated, as appropriate, to that lessons learnt process. Member States are encouraged to gather lessons learnt from all relevant actors directly involved in the response to the incident, as appropriate. Building on those discussions, the Presidency of the Council, with the support of the General Secretariat of the Council, in consultation with the Commission and with the affected Member States, should produce a report on lessons learnt. If necessary, the report should be classified at the adequate level.

Done at …, …

For the Council
The President

ANNEX

This Annex describes the objectives, the principles, the main relevant actors, the interplay with other relevant crisis and emergency management mechanisms, and the functioning of a Blueprint to coordinate the response to critical infrastructure incidents with significant cross-border relevance (‘EU Critical Infrastructure Blueprint’) and, where necessary, improve cooperation between Member States and the relevant Union institutions, bodies, offices and agencies as regards such incidents, in accordance with the applicable rules and procedures. This EU Critical Infrastructure Blueprint does not affect in any way the role and functioning of other arrangements.

Part I: Objectives, principles, actors and other instruments

1. Objectives

The EU Critical Infrastructure Blueprint aims to promote the following three main objectives in response to a critical infrastructure incident with significant cross-border relevance, where appropriate:

(a) **Shared situational awareness**, since a good understanding of the critical infrastructure incident with significant cross-border relevance in the Member States, of its origin and of its potential consequences for all relevant stakeholders at operational and strategic/political level is essential for an appropriate coordinated response.

(b) **Coordinated public communication**, since it helps to mitigate the negative effects of a critical infrastructure incident with significant cross-border relevance and to minimise discrepancies in the messages conveyed to the public among Member States, fully respecting national competences for crisis communication. Where it is in the interest of the public and where this communication does not hamper crisis and emergency management operations, clear public communication is also important to mitigate the consequences of disinformation.

(c) **Coordinated and effective response**, since strengthening the response of Member States and cooperation between them and with relevant Union institutions, bodies, offices and agencies can contribute to mitigating the effects of a critical infrastructure incident with significant cross-border relevance and to enabling swift reestablishment of essential services in a way that minimises vulnerability to further significant incidents.

2. Principles

Proportionality

Incidents that disrupt critical infrastructure and/or the provision of essential services often fall below the threshold of a critical infrastructure incident with significant cross border relevance as specified in point 2 of this Recommendation. As such, they can, in principle, be addressed effectively at national level. Therefore, the application of the EU Critical Infrastructure Blueprint should be limited to critical infrastructure incidents with significant cross-border relevance.

Subsidiarity

Member States have the primary responsibility in responding to disruptions of a critical infrastructure or of essential services provided by critical entities, in accordance with Union law. However, relevant Union institutions, bodies, offices and agencies, in particular the European External Action Service (‘EEAS’) can have an important complementary role in case of a critical infrastructure incident with significant cross-border relevance, since such an incident may impact several or even all sections of economic activity within the internal market, the life of citizens living in the Union, the security of the Union and its international relations with partners without prejudice to the Member States’ responsibility for safeguarding national security and defence.

Complementarity

The EU Critical Infrastructure Blueprint should take into account and reflect the working of existing crisis and emergency management mechanisms at Union level, namely the Council's Integrated Political Crisis Response ('IPCR') arrangements, the Commission's internal crisis coordination process ARGUS, the Union Civil Protection Mechanism ('UCPM'), supported by the Emergency Response Coordination Centre ('ERCC') established under the UCPM by Decision No 1313/2013/EU of the European Parliament and of the Council[1], and the EEAS Crisis Response Mechanism. It should also draw on sectoral arrangements, including the provisions for coordinated management of large-scale cybersecurity incidents provided for by Directive (EU) 2022/2555 of the European Parliament and of the Council[2], the EU-SCICF framework recommended by the European Systemic Risk Board[3] (ESRB), the Network of transport contact points[4], the European Aviation Crisis Coordination Cell[5] and the Coordination Groups for Electricity[6], Gas[7] and Oil[8].

---

1 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).

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

3 Recommendation of the European Systemic Risk Board of 2 December 2021 on a pan-European systemic cyber incident coordination framework for relevant authorities (ESRB/2021/17).

4 Communication from the Commission of 23 May 2022, A contingency plan for transport (COM(2022) 211 final).

5 Established under Article 19 of Commission Implementing Regulation (EU) 2019/123 of 24 January 2019 laying down detailed rules for the implementation of air traffic management (ATM) network functions and repealing Commission Regulation (EU) No 677/2011 (OJ L 28, 31.1.2019, p. 1).

6 Commission Decision 2012/C 353/02 of 15 November 2012 setting up the Electricity Coordination Group (OJ C 353, 17.11.2012, p. 2).

7 Regulation (EU) 2017/1938 of the European Parliament and of the Council of 25 October 2017 concerning measures to safeguard the security of gas supply and repealing Regulation (EU) No 994/2010 (OJ L 280, 28.10.2017, p. 1).

8 Council Directive 2009/119/EC of 14 September 2009 imposing an obligation on Member States to maintain minimum stocks of crude oil and/or petroleum products (OJ L 265, 9.10.2009, p. 9).

Furthermore, the EU Critical Infrastructure Blueprint should rely on and use the existing structures and mechanisms at Union level, including the relevant Working Parties of the Council (namely the PROCIV CER Working Party) and those established by Directive (EU) 2022/2557 of the European Parliament and of the Council[9], in particular as regards the cooperation between competent authorities of the Member States and with the Commission and in the Critical Entities Resilience Group ('CERG') established by Directive (EU) 2022/2557. It should also take into account the responsibilities of relevant Union institutions, bodies, offices and agencies under the legal framework applicable to them. Critical infrastructure crisis response activities are complementary with other crisis and emergency management mechanisms at Union, national and sectoral levels that support multi-sectoral coordination.

Confidentiality of information

The EU Critical Infrastructure Blueprint should take account of the importance of safeguarding the confidentiality of classified information and sensitive non-classified information related to critical infrastructure and critical entities.

---

9 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).

No Member State is expected to supply information the disclosure of which would be contrary to the essential interests of its national security, public security or defence. Without prejudice to Article 346 TFEU, information that is confidential pursuant to Union or national rules, such as rules on business confidentiality, should be exchanged with the Commission and other relevant authorities only where that exchange is necessary for the application of this Recommendation. The information exchanged should be limited to that which is relevant and proportionate to the purpose of that exchange. The exchange of information should preserve the confidentiality of that information and the security and commercial interests of critical entities, while respecting the security of Member States.

3. Relevant actors

Each Member State and relevant Union institutions, bodies, offices and agencies referred to in points (a) to (g) below should identify, in accordance with the rules and procedures applicable to them, the relevant actors for each critical infrastructure incident with significant cross-border relevance, where appropriate, depending on the sector affected and the type of incident.

(a) Member States

– Competent authorities (e.g., authorities in charge of critical infrastructure, relevant sectoral authorities, single points of contact designated or established pursuant to Article 9(2) of Directive (EU) 2022/2557, authorities designated or established pursuant to Article 9(1) of Directive (EU) 2022/2557).

– Other stakeholders, including entities or persons from the private sector holding specific functions, such as operators of critical infrastructure, including the ones identified as critical entities.

– Ministers responsible for critical infrastructure resilience and/or Ministers responsible for the sector or sectors most affected by the critical infrastructure incident with significant cross-border relevance in question.

(b) The Council

– The Presidency of the Council.

– COREPER, the Political and Security Committee and IPCR arrangements.

– The relevant Working Parties, such as the Working Party on Civil Protection – Critical Entities Resilience (‘PROCIV CER Working Party’) and the chairs of other relevant Working Parties.

– The General Secretariat of the Council.

(c) The European Council

– The President of the European Council.

(d) The Commission

– The designated lead service and the Directorate-General for Migration and Home Affairs as the service responsible in the area and, in case of a cross-sectoral incident, the Directorate-General for Migration and Home Affairs and other relevant Commission services.

– The Directorate-General for Communication and the Spokesperson's service.

– The Directorate-General HERA, European Health Emergency Preparedness and Response Authority.

– The CERG, chaired by a Commission representative (Directorate-General Migration and Home Affairs), and other relevant expert groups and committees.

– The ERCC established under the UCPM (24/7 operational emergency management hub under the UCPM located in Directorate-General European Civil Protection and Humanitarian Aid Operations).

– The Health Security Committee established by Article 4 of Regulation (EU) 2022/2371 of the European Parliament and of the Council[10].

[10] Regulation (EU) 2022/2371 of the European Parliament and of the Council of 23 November 2022 on serious cross-border threats to health and repealing Decision No 1082/2013/EU (OJ L 314, 6.12.2022, p. 26).

– The Secretariat-General of the Commission (ARGUS secretariat) and the (Deputy) Secretary-General (ARGUS process), the Directorate-General for Human Resources (Security Directorate).

– Other relevant Commission expert groups assisting the Commission in the coordination of measures in an emergency or a crisis situation.

– Other crisis and emergency management networks, including sectoral (e.g. Network of transport contact points managed by Directorate-General Mobility and Transport, the interinstitutional Cyber Crisis Task Force[11], the European Aviation Crisis Coordination cell).

– The President and/or the responsible Vice-President/Commissioner.

– Other Commission services which may have competence in specific areas of expertise.

(e) The EEAS

– The Single Intelligence Analysis Capacity (‘SIAC’) composed of the Intelligence and Situation Centre (‘IntCen’) and the EU Military Staff Intelligence Directorate (‘EUMS Int’).

– The Crisis Response Centre (‘CRC’).

[11] An informal group including relevant Commission services, the EEAS, the European Union Agency for Cybersecurity (“ENISA”), CERT-EU and Europol, co-chaired by Directorate-General Communications Network, Content and Technology and the EEAS.

– The High Representative of the Union for Foreign Affairs and Security Policy/Vice-President of the Commission (‘High Representative’).

(f) Relevant Union bodies, offices and agencies, such as Europol or ENISA, depending on the sector affected[12]

(g) Other relevant structures

– The European cyber crisis liaison organisation network (‘EU-CyCLONe’) established by Article 16 of Directive (EU) 2022/2555;

– The Computer Security Incident Response Teams (‘CSIRTs’) network established by Article 15 of Directive (EU) 2022/2555;

– The pan-European systemic cyber incident coordination framework (‘EU-SCICF’) as referred to in Recommendation ESRB/2021/17 of the ESRB.

[12] Such as, for transport: the European Union Aviation Safety Agency (‘EASA’), the European Maritime Safety Agency (‘EMSA’), the European Railways Agency (‘ERA’); for health: the European Centre for Disease Prevention and Control (‘ECDC’) and the European Medicines Agency (‘EMA’); for energy: the Agency for the Cooperation of Energy Regulators (‘ACER’); for space: the EU Space Programme Agency (‘EUSPA’); for the food sector: the European Food Safety Authority (‘EFSA’); for the maritime sector: the European Fisheries Control Agency (‘EFCA’); for cyber-security incidents: , Computer Security Incident Response Teams (‘CSIRTs’), the Computer Emergency Response Team for the Union institutions, bodies and agencies (‘CERT-EU’), ECB, ESRB, European Supervisory Authorities (‘ESAs’).

4. Interplay with other relevant crisis and emergency management mechanisms and instruments

The EU Critical Infrastructure Blueprint should be a flexible tool that maps various actions that could be taken partially or fully using different existing arrangements, depending on the nature and gravity of the critical infrastructure incident with significant cross-border relevance and on the need for operational or strategic/political coordination.

(a) Integrated Political Crisis Response arrangements ('IPCR')

In line with Council Implementing Decision (EU) 2018/1993[13], in case of a crisis for which the IPCR arrangements have been activated, measures under the EU Critical Infrastructure Blueprint could be part of the EU response at the political level. In such a case, the decision-making process of the IPCR would apply and the EU Critical Infrastructure Blueprint could be used as a complementary tool providing specific support on critical infrastructure to the IPCR to ensure a well-coordinated response. The IPCR arrangements are designed to allow a timely policy coordination and response at the Union political level (COREPER/Council) in the event of major emergencies or crises. The IPCR is also used to coordinate, at the strategic/political level, the response to the invocation of the solidarity clause (Article 222 TFEU) to ensure the coherence and complementarity of Union and Member State action. The arrangements for the implementation by the Union of the solidarity clause are defined by Council Decision 2014/415/EU[14].

[13] 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).

[14] Council Decision 2014/415/EU of 24 June 2014 on the arrangements for the implementation by the Union of the solidarity clause (OJ L 192, 1.7.2014, p. 53).

(b) The Union Civil Protection Mechanism ('UCPM')

Under Decision No 1313/2013/EU, the UCPM can be activated to respond to actual or imminent natural and man-made disasters within and outside the Union (including those stemming from incidents affecting critical infrastructure) with the operational support from the ERCC. The ERCC works in close contact with national civil protection authorities and relevant Union bodies to promote a cross-sectoral approach to disaster management.

(c) The EU Hybrid Toolbox and the EU Protocol for countering hybrid threats

The EU Protocol for countering hybrid threats[15] ('EU Protocol for countering hybrid threats') outlines processes and tools applicable in case of hybrid threats or campaigns throughout the whole crisis and emergency management cycle.

In case of a significant critical infrastructure incident with a hybrid dimension, the processes and tools described in the EU Protocol for countering hybrid threats apply in complementarity with the EU Critical Infrastructure Blueprint, where appropriate, e.g., for specific information, analysis or communication on hybrid aspects of the critical infrastructure incident with significant cross-border relevance and regarding cooperation with external partners. In particular, the EU Hybrid Toolbox[16] provides a framework for a coordinated response to hybrid campaigns. Since the primary responsibility for countering hybrid threats lies with the Member States, the decision-making process described in the Implementing guidelines for the Framework for a coordinated Union response to hybrid campaigns applies.

---

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

16 Council conclusions of 21 June 2022 on a Framework for a coordinated EU response to hybrid campaigns; Implementing guidelines for the Framework for a coordinated EU response to hybrid campaigns (15880/22).

(d) The provisions for coordinated management of large-scale cybersecurity incidents provided for by Directive (EU) 2022/2555

Directive (EU) 2022/2555 contains provisions for coordinated management of large-scale cybersecurity incidents through the existing cooperation networks, in particular the EU-CyCLONe and the CSIRTs network. EU-CyCLONe and the CSIRTs network cooperate on the basis of procedural arrangements that specify the details of that cooperation and avoid any duplication of tasks.

EU-CyCLONe works as an intermediary between the technical and political level during large-scale cybersecurity incidents and crises, and enhances cooperation at operational level and supports decision-making at political level. EU-CyCLONe builds on the CSIRTs network findings and use its own capabilities to create impact analysis of large-scale cybersecurity incidents and crises. In case of a critical infrastructure incident with significant cross-border relevance which coincides with, or appears to be related to a large-scale cybersecurity incident, the relevant Council Working Parties should determine appropriate coordination at an operational level, including in cooperation with EU-CyCLONe. The purpose of the coordination should be to determine which actor, tool(s) or mechanism(s) could contribute most effectively to responding to the critical infrastructure incident with significant cross-border relevance, while avoiding duplication and parallel work strands. Such coordination should be coherent with existing relevant arrangements at the time of the incident.

(e) Other sectoral or cross-sectoral mechanisms and instruments

The EU Critical Infrastructure Blueprint should not duplicate other sectoral or cross-sectoral crisis and emergency management tools or coordination mechanisms. Where such tools or mechanisms already exist, the EU Critical Infrastructure Blueprint, within its scope of application, should be used as a complementary tool to the sectoral or cross-sectoral tools or mechanisms, but should not replace them. The necessary coordination between the various actors would have to be ensured so as to avoid such duplication. In case of an activation of the IPCR, political and strategic coordination would take place in the IPCR. Within the Commission, internal crisis coordination is enabled by its internal crisis coordination process ARGUS, supported by the ERCC.

Part II: Information exchange and Coordinated response

The actions described below consist of modes of cooperation, namely information exchange, coordinated communication and response. This structure corresponds to the modes of the Council's crisis coordination mechanism IPCR and takes into account, more broadly, the potential use of the crisis coordination mechanisms already existing at Union level. This structure shows how those modes of cooperation would integrate therein if used. However, most of those actions can also be taken autonomously: they do not depend on the use of that mechanism but rather complement it. The actions are presented in a chronological order, while taking into consideration that, in case of a large-scale crisis that constitutes a critical infrastructure incident with significant cross-border relevance, several actions could be undertaken simultaneously and continuously.

1. Information exchange

(a) At operational level

The Member States affected by the critical infrastructure incident with significant cross-border relevance should apply their own contingency measures, ensure coordination with relevant national crisis and emergency management mechanisms, and ensure the involvement of all relevant national, regional and local actors, as appropriate.

Where relevant as regards civil protection assistance and the UCPM, the coordination between Member States and with the Commission is ensured through the ERCC and the contact points of the Member States in line with the legal provisions on the UCPM.

(i) Information sharing and notification by the national competent authorities

In addition to the notification and information obligations pursuant to Article 15 of Directive (EU) 2022/2557, and in line with the relevant national legal frameworks, national competent authorities responsible for critical infrastructure in Member States affected by a critical infrastructure incident with significant cross-border relevance should share with the Presidency of the Council and with the Commission, through their single points of contact and without undue delay, unless operationally unable to do so, relevant information, which could include information received from critical entities or operators of critical infrastructure, or from other sources, concerning the crisis and emergency management mechanisms that were activated.

Exchange of information regarding a critical infrastructure incident with significant cross-border relevance should be limited to that which is relevant and proportionate to the purpose of that exchange and should occur via appropriate communication channels to the relevant Commission services. Where applicable and appropriate, the IPCR platform and the ERCC could be used. Information should be handled in accordance with established procedures and rules, including the handling of classified information. The potential use of the ERCC should not affect UCPM resources nor the availability of the ERCC to continue to fully serve the UCPM.

Such information sharing could include, as appropriate, the nature and cause of the critical infrastructure incident with significant cross-border relevance, the observed or estimated impact of the disruption on the critical infrastructure and the provision of essential services, consequences of the incident across sectors and borders and the mitigation measures, either already taken or envisaged, nationally or with other relevant Member States and the Commission through existing arrangements, e.g. the information sharing arrangements under Articles 9 and 15 of Directive (EU) 2022/2557. This information sharing should be provided without diverting the critical infrastructure's or, in some cases, the critical entity's or the Member States' resources from activities related to incident handling, which is to be prioritised.

In order to ensure follow-up, the notified Commission services, including those responsible for the sector in which the critical infrastructure incident with significant cross-border relevance occurred, should inform the contact point in the Directorate for General Migration and Home Affairs and the Secretariat General of the Commission.

If the information could be relevant for addressing a cybersecurity dimension or be related to a cybersecurity incident, the Commission and the Presidency of the Council should share relevant information with EU-CyCLONe. The competent authorities under Directive (EU) 2022/2557 and those under Directive (EU) 2022/2555 should also cooperate and exchange information in relation to such incidents, without undue delay.

For the maritime domain, national competent authorities should consider the possibility of using the Common Information Sharing Environment (‘CISE’) to share information without undue delay.

(ii) Information sharing at Union level

The Commission convenes as soon as possible the CERG to facilitate exchanges of relevant information between national competent authorities responsible for critical infrastructure and relevant Union institutions, bodies, offices and agencies on the incident (nature, cause, impact and consequences across sectors and borders), and informs the Presidency of the Council thereof. As that CERG meeting would be focused on the relevant critical infrastructure incident with significant cross-border relevance and its consequences, Member States are reminded that they can request the Commission to invite national experts on the subject matter to that CERG meeting to facilitate the most suitable representation of Member States. Depending on the centre of gravity of the incident, relevant Commission services could be closely associated to the meeting of the CERG, with a view to sharing information gathered through existing sectoral instruments.

In case of incidents with a combination of cybersecurity aspects and non-cyber physical aspects, the CSIRTs Network and EU-CyCLONe would cooperate on the basis of procedural arrangements mentioned in Article 15(6) of Directive (EU) 2022/2555. Coordination should be ensured by the Presidency with the relevant Working Parties, the relevant Commission services, the EEAS, CERT-EU, ENISA and Europol. Where necessary, CERT-EU would share relevant information with the CSIRTs Network, while the Commission would share information with EU-CyCLONe. In agreement with the respective chairs, the Commission (Directorate-General for Migration and Home Affairs and the Directorate-General for Communications Network, Content and Technology) may, if appropriate, propose a joint meeting of the CERG with the EU-CyCLONe and the CSIRTs network, and inform the Presidency of the Council thereof.

In the event of a cross-sectoral critical infrastructure incident with significant cross-border relevance and with wide-ranging impact or political significance at Union level, the Presidency of the Council, on its own initiative and after having consulted the affected Member States, the Commission and the High Representative, or at the request of one or several Member States, may explore options for cross-sectoral coordination through the IPCR. In case of an activation of the IPCR, such as in information sharing mode, political and strategic coordination would take place in the IPCR, with the EU Critical Infrastructure Blueprint providing the necessary input on critical infrastructure in support of the IPCR's work.

In case a critical infrastructure incident with significant cross-border relevance also affects a third country, the Presidency of the Council, in consultation with the affected Member States and the Commission, should consider the suitability and modalities for collaborating with the third country.

(iii) Support by the Commission and Union's agencies

Where relevant and acting in accordance with its mandate, Europol presents an incident situation report at Union level. Other Union agencies, where relevant and acting in accordance with their respective mandates, report relevant information that contributes to the situational awareness or coordinated response to the critical infrastructure incident with significant cross-border relevance to their respective 'parent' Directorates-General which, in turn, report to the Commission (Directorate-General for Migration and Home Affairs) as the Chair of the CERG. The Commission keeps the Presidency of the Council adequately informed.

The Commission can provide a contribution to situational awareness using the assets of the Union Space Programme[17], such as Copernicus, Galileo or EGNOS, where relevant and in accordance with the applicable Union and national legal frameworks.

[17] Regulation (EU) 2021/696 of the European Parliament and of the Council of 28 April 2021 establishing the Union Space Programme and the European Union Agency for the Space Programme and repealing Regulations (EU) No 912/2010, (EU) No 1285/2013 and (EU) No 377/2014 and Decision No 541/2014/EU (OJ L 170, 12.5.2021, p. 69).

(b) At strategic level

(i) Production of reports based on Member States' contributions

The Commission prepares a report within the field of critical infrastructure resilience based on information (on the critical infrastructure incident with significant cross-border relevance and existing best practices regarding the handling of such incident) shared by national competent authorities in a CERG meeting, or joint meetings with relevant services, expert groups or networks, and other available information. This report will be distributed to CERG members, PROCIV CER Working Party members and, in consultation with the Presidency of the Council, to other relevant stakeholders. If necessary, the report will be classified at the adequate level and, in any case, distributed to relevant recipients in Member States, in accordance with rules and procedures regarding information security as set out in the applicable legal frameworks.

That report will, where appropriate, take into account the outcomes of the relevant Union-level risk assessments, evaluations and scenarios from a cybersecurity perspective, including those carried out by the Commission and the High Representative and the Cooperation Group.

In case of the activation of the IPCR, that report can contribute to the Integrated Situation Awareness Analysis ('ISAA') prepared by the Commission services and the EEAS.

The SIAC presents an up-to-date intelligence-based assessment on the incident, where relevant.

(ii) Activation of Union crisis coordination mechanisms and use of Union tools

In line with the legal provisions on the UCPM, the ERCC may begin providing situational awareness support surrounding the incident when the UCPM is activated[18]. In addition, affected Member States may request satellite imagery of their territory via the Copernicus Emergency Management Service.

Where considered appropriate to share information across the Commission with the EEAS and relevant Union agencies, the lead Directorate-General or the Directorate-General for Migration and Home Affairs, in coordination with the Secretariat-General, activates the Commission's internal crisis coordination process ARGUS Phase I by opening an event on the Argus IT tool. The Commission ensures that relevant information is shared with the Member States at the IPCR roundtables and via the IPCR platform.

The Presidency of the Council can activate the IPCR arrangements in information sharing mode, which entails the development of ISAA reports by the Commission and the EEAS, with contributions from national competent authorities and other sources, where appropriate. Even without activating the IPCR, a monitoring page on the IPCR web platform can be initiated by the Presidency of the Council. The General Secretariat of the Council, in agreement with the Presidency, can create a monitoring page possibly at the request of an affected Member State, the Commission services, or the EEAS.

[18] Such as the publication of media monitoring products, Civil Protection Messages, Analytical Briefs, ECHO Daily Maps, ECHO Daily Flashes, and other tailored products.

Other (sectoral) Union crisis and emergency management mechanisms and tools may be activated following the respective procedures, as appropriate. The Commission will ensure coordination between those mechanisms and tools.

If the physical incident coincides with or appears to be related to a large-scale cybersecurity incident, as defined in Article 6, point (7), of Directive (EU) 2022/2555, the Presidency of the Council may also apply the provisions for coordinated management of large-scale cybersecurity incidents laid down in Directive (EU) 2022/2555 to determine appropriate coordination involving, inter alia, the Horizontal Working Party on Cyber Issues, the PROCIV CER Working Party, the CERG, the EU-CyCLONe and the CSIRTs Network, in accordance with their own rules and procedures.

(iii) Coordination of public communication

The Member States affected by the critical infrastructure incident with significant cross-border relevance should coordinate their public communication on the crisis to the extent possible, while respecting national competences and administrative frameworks in this regard. The IPCR Crisis Communicators Network may be involved, as appropriate.

Based on the shared situational awareness, the PROCIV CER Working Party, in collaboration with the affected Member States and in consultation with the Commission, may organise an exchange of views on the public communication approaches of the Member States and the Commission. If needed, the PROCIV CER Working Party should try to identify common ground, to facilitate coordination among Member States.

This should be done keeping in mind that communication efforts should not undermine the national crisis and emergency management operations.

Europol and other relevant Union agencies coordinate their public communication activities with the Commission's Spokesperson's service, based on shared situational awareness and in consultation with the affected Member States. The ERCC will not have a role in crisis communication to the public under the Blueprint.

If the critical infrastructure incident with significant cross-border relevance entails an external or hybrid dimension, the public communication is coordinated with the EEAS and the Commission's Spokesperson's service, as described in the EU Protocol for countering hybrid threats.

2. Response (involving continuous actions described under Information exchange and additional actions at strategic/political level)

(a) At strategic level

(i) Continuous production of situational reports

The PROCIV CER Working Party should be informed of the production of the reports (e.g. the ISAA in case of IPCR activation or the report based on Member States' contributions within the field of critical infrastructure resilience prepared by the Commission) and should prepare the COREPER, in case the latter has not yet been convened, or the Political and Security Committee meeting, as appropriate.

The SIAC intensifies its outreach to Member States' intelligence services, aggregates the all-source information and prepares an analysis and assessment of the incident, as well as regular updates, if necessary.

(ii) Organisation of coordination meetings

Based on the shared situational awareness, the Presidency of the Council should convene as soon as possible meetings of the PROCIV CER Working Party to discuss, within the field of critical infrastructure resilience, gaps in the Union response to the critical infrastructure incident with significant cross-border relevance, and explore coordination options among Member States and the Union institutions, bodies, offices and agencies. If the IPCR were to be activated, the findings of those meetings could be fed by the Presidency into the IPCR crisis Roundtables. The IPCR crisis Roundtables can also identify some specific gaps in the response to the critical infrastructure incidents with significant cross-border relevance and direct, among others, the PROCIV CER Working Party to tackle those and report the results back to future IPCR crisis Roundtables to support the political and strategic coordination efforts of the IPCR.

(iii) Full activation of Union crisis coordination mechanisms and use of Union instruments

In case the IPCR is activated by the Presidency of the Council in full mode:

Coordination of the response at Union political level should be carried out by the Council, using the IPCR arrangements.

The Presidency of the Council calls for a timely informal Roundtable, gathering the relevant national, Union and international actors, where the affected Member State(s) can report on the incident, the Presidency can report on the findings of the relevant working parties of the Council, and the Commission services can report on the previously convened group's meeting(s), complemented by the EEAS, as appropriate.

The SIAC and the relevant Union agencies can be invited to present a situational update on the critical infrastructure incident with significant cross-border relevance in that meeting.

The ISAA lead service (the Commission lead service or the EEAS) prepares the ISAA report with contributions from relevant Commission services, relevant Union bodies, offices and agencies and national competent authorities. The Member States are also invited to provide input, through the IPCR web platform.

In case the President of the Commission activates the Commission's internal crisis coordination process ARGUS Phase II, Crisis Coordination Committee meetings involving the relevant Commission services, agencies, and the EEAS, where relevant, are convened on a short notice in order to coordinate as regards all aspects of the critical infrastructure incident with significant cross-border relevance.

In case of a critical infrastructure incident with significant cross-border relevance of common interest for the Union and NATO, the Commission services and the EEAS may convene an EU-NATO Structured Dialogue on Resilience meeting to contribute to shared situational awareness and exchange of information on measures taken by the Union and NATO, in full respect of Union and Member States' competences according to the Treaties and the key principles guiding the EU-NATO cooperation as agreed by the European Council, in particular reciprocity, inclusiveness and decision-making autonomy and in full transparency towards all Member States. Reaffirming the importance of unimpeded exchange of information between the Union and NATO, information on the incidents deemed sensitive by the affected Member State could be shared with NATO with the explicit consent of the affected Member State. Member States will be informed on the outcomes of the Structured Dialogue regarding the application of the EU Critical Infrastructure Blueprint.

(iv) Public communication

Where relevant, the Council should facilitate exchanges on public communication approaches and, if needed, try to find common ground in order to facilitate coordination among Member States and with the Commission. The informal network of crisis communicators established through the IPCR may support this work. The Commission's services also prepare public communication messages, as appropriate and in consultation with the affected Member States.

If the critical infrastructure incident with significant cross-border relevance entails an external or hybrid dimension, the public communication should be coordinated with the EEAS and the Commission's Spokesperson's service. The ERCC will not have a role in crisis communication to the public under the Blueprint.

(v) Support to Member States and effective response

The Presidency of the Council can convene more meetings of the PROCIV CER Working Party and other relevant working parties to support the activities in the framework of the IPCR, if activated.

Member States affected by the critical infrastructure incident with significant cross-border relevance may request the technical support of other Member States bilaterally or through the Presidency of the Council and/or PROCIV CER Working Party, e.g., specific expertise to mitigate the adverse impacts of the critical infrastructure incident with significant cross-border relevance.

Member States affected by the critical infrastructure incident with significant cross-border relevance may also request the technical and/or financial support of the Commission or relevant Union agencies. Upon such a request, the Commission, in coordination with the relevant Union agencies, assesses its possible support and activates, where appropriate and with the agreement of affected Member States, technical mitigation measures at Union level, in accordance with their respective procedures, and coordinates technical capacities needed to stop or reduce the impact of the critical infrastructure incident with significant cross-border relevance. The Commission and the Presidency should keep each other adequately informed of those requests, with the aim of effective coordination.

Affected countries may activate the UCPM to request for assistance, after which the ERCC would work with the contact points of the Member States in line with the legal provisions on the UCPM to coordinate the rendering of assistance.

Within their respective mandates and upon request, Europol and other relevant Union agencies can support Member States affected by a critical infrastructure incident with significant cross-border relevance in the investigation of the incident.

(b) At political level

The Presidency of the Council can consider the necessity to convene IPCR roundtables, meetings of Council Working Groups, COREPER, Council meetings to exchange on the possible origin and expected consequences of the critical infrastructure incident with significant cross-border relevance for the Member States and for the Union, agree on common guidelines, and adopt the necessary measures to support the Member States affected by such incident and mitigate its effects. The European Council may also address the matter.

Schematic Overview of the EU Critical Infrastructure Blueprint