Council of the European Union

Brussels, 7 September 2023
(OR. en)

12485/23
ADD 1

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:	ANNEX to the 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

ANNEX

ANNEX

to the

Proposal for a COUNCIL RECOMMENDATION

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

ANNEX

This Annex describes the principles, objectives, the main actors, the interplay with existing crisis response mechanisms, and the functioning of a Blueprint to coordinate the response to significant critical infrastructure incidents (''Critical Infrastructure Blueprint'') and 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 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 Critical Infrastructure Blueprint aims to achieve the following three main objectives in response to a significant critical infrastructure incident:

(a) **Shared situational awareness**, since a good understanding of the significant critical infrastructure incident in the Member States, its origin and 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 mitigate the negative effects of a significant critical infrastructure incident and minimise discrepancies in the messages conveyed to the public in and between Member States. Clear public communication is also important to mitigate the consequences of disinformation.

(c) **Effective response**, since strengthening the response of Member States and cooperation between Member States and with relevant Union institutions, bodies, offices, agencies, contributes to mitigating the effects of a significant critical infrastructure incident and 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 significant critical infrastructure incident 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 Critical Infrastructure Blueprint is limited to significant critical infrastructure incidents.

Subsidiarity

Member States have the primary responsibility in responding to disruptions of a critical infrastructure or of the essential services provided by critical entities, in accordance with Union law. However, relevant Union institutions, bodies, offices and agencies, and the European External Action Service (''EEAS'') have an important complementary role in case of a significant critical infrastructure incident with major 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 and the international relations of the Union.

Complementarity

The Critical Infrastructure Blueprint takes into account and reflects the working of existing crisis 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''), and the EEAS Crisis Response Mechanism. It also draws 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[1] and the framework set out in the Blueprint for coordinated response to large-scale cross-border cybersecurity incidents and crises (''Cyber Blueprint'')[2], the Network of transport contact points[3] and the European Aviation Crisis Coordination Cell[4].

Furthermore, the Critical Infrastructure Blueprint builds on, and is to be applied in accordance with the structures and mechanisms established by Directive (EU) 2022/2557 of the European Parliament and of the Council[5], in particular as regards the cooperation between competent authorities and with the Commission and in the Critical Entities Resilience Group. It also takes 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 management mechanisms at Union, national and sectoral levels that support multi-sectoral coordination.

Confidentiality of information

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

3. Relevant actors

Each Member State and relevant Union institutions, bodies, offices and agencies referred to under points a) to e) below will, in accordance with the rules and procedure applicable to them, decide on the relevant actor(s) for each significant critical infrastructure incident, depending on the sector(s) 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);

- Where appropriate, the European cyber crisis liaison organisation network (''EU-CyCLONe'') as referred to in Article 16 of Directive (EU) 2022/2555;

- The Cooperation Group as referred to in Article 14 of Directive (EU) 2022/2555;

---

[1] 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).

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

[3] Commission Communication - A contingency plan for transport (COM/2022/211 final).

[4] 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.

[5] 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).

- Where appropriate, other stakeholders, including entities or persons from the private sector such as operators of critical infrastructure, including the ones identified as critical entities;

- Ministers responsible for critical infrastructure resilience and/or the Minister(s) responsible for the sector or sectors most affected by the significant critical infrastructure incident in question.

b) The Council

- The rotating Presidency;

- The relevant Working Parties, such as the Working Party on Civil Protection including the subgroup on Critical Entities Resilience PROCIV-CER and the chair(s) of the relevant Working Party(ies) depending on the sector(s) affected and the nature of the incident, such as, the Horizontal Working Party on Cyber Issues and the Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats;

- COREPER, the Political and Security Committee, and IPCR, all supported by the General Secretariat of the Council.

c) The Commission, including Commission expert groups

- Designated lead service (depending on the affected sector) supported by the ERCC as the 24/7 operational hub managing crisis responses and Directorate-General for Migration and Home Affairs as the service responsible in the area and, in case of a cross-sectoral incident, Directorate-General Migration and Home Affairs and other relevant Commission services;

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

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

- The Critical Entities Resilience Group chaired by a Commission representative (Directorate-General Migration and Home Affairs), established by Directive (EU) 2022/2557, and, where appropriate, other relevant expert groups and committees;

- The ERCC established under the UCPM by Decision No 1313/2013/EU of the European Parliament and of the Council[6] (24/7 operational emergency management hub under the UCPM located in Directorate-General European Civil Protection and Humanitarian Aid Operations);

- The Cooperation Group as referred to in Article 14 of Directive (EU) 2022/2555;

- The Cyber Situational Awareness and Analysis Centre;

- The Health Security Committee, as referred to in Article 4 of Regulation (EU) 2022/2371[7];

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

---

[6] 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).

[7] 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).

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

- Other crisis management networks, including sectoral (e.g. Network of transport contact points managed by Directorate-General Mobility and Transport, the interinstitutional Cyber Crisis Task Force[8], the European Aviation Crisis Coordination cell);

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

d) EEAS

- Single Intelligence Analysis Capacity (''SIAC'') composed of the Intelligence and Situation Centre (''IntCen'') and the EU Military Staff Intelligence Directorate (''EUMS Int'');

- Crisis Response Centre (''CRC'');

- The High Representative of the Union for Foreign Affairs and Security Policy/Vice-President of the Commission.

e) Relevant Union bodies, and offices, and relevant Union agencies, such as Europol, depending on the sector(s) affected[9].

4. Interplay with other relevant crisis management mechanisms and instruments

The Critical Infrastructure Blueprint is 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 significant critical infrastructure incident and on the need for operational, strategic/political coordination.

a) The EU Protocol on countering hybrid threats[10] (''EU Protocol'')

The EU Protocol applies in the case of hybrid threats[11] by giving an outline of processes and tools applicable in case of such threats or campaigns.

In case of a significant critical infrastructure incident with a hybrid dimension, the EU Protocol applies in complementarity with the Critical Infrastructure Blueprint, where appropriate, e.g. for specific information, analysis or communication on hybrid aspects of the significant critical infrastructure incident and regarding cooperation with external partners.

---

8 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.

9 Such as Europol; 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); on maritime: the European Fisheries Control Agency (EFCA); for cyber incidents: the European Union Agency for Cybersecurity (ENISA), Computer Security Incident Response Teams (CSIRTs), the Computer Emergency Response Team for the EU institutions, bodies and agencies (CERT-UE).

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

11 Hybrid threats can be characterised as a mixture of coercive and subversive activity, conventional and unconventional methods, which can be used in a coordinated manner by state or non-state actors to achieve specific objectives, while remaining below the threshold of formally declared warfare, cf the EU Protocol on hybrid threats.

b) The Blueprint for coordinated response to large-scale cross-border cybersecurity incidents and crises

The Cyber Blueprint applies for large-scale cross-border incidents which cause disruption too extensive for a concerned Member State to handle on its own or which affect two or more Member States or EU 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.

In case of a significant critical infrastructure incident which coincides with, or appears to be related to, a large-scale cybersecurity incident, the relevant Council working groups determine appropriate coordination at an operational level, including with the EU-CyCLONe or through a joint meeting of the Critical Entities Resilience Group with the Cooperation Group. The purpose of the coordination is to determine which actor, tool(s) or mechanism(s) could contribute most effectively to responding to the significant critical infrastructure incident while avoiding duplication and parallel work strands.

c) Union Civil Protection Mechanism and the Emergency Response Coordination Centre

In line with Decision No 1313/2013/EU on a Union Civil Protection Mechanism, operational responses under the UCPM to actual or imminent natural and human-induced disasters (including those involving critical infrastructure disruptions) within and outside the Union are led 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 support 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 Union level and between the Union and relevant national authorities, including ones responsible for civil protection and critical infrastructure resilience.

d) Other sectoral or cross-sectoral mechanisms and instruments

The Critical Infrastructure Blueprint does not duplicate other sectoral or cross-sectoral crisis management tools or coordination mechanisms. Where such tools or mechanisms already exist in the affected sector, the Critical Infrastructure Blueprint, within its scope of application, can be used as a complementary tool to the sectoral or cross-sectoral tools or mechanisms but does not replace them. The necessary coordination between the various actors would have to be ensured so as to avoid such duplication. This could, for instance, be achieved in the Commission's internal crisis coordination process ARGUS, supported by ERCC, and/or IPCR coordination meetings.

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 EU level. This structure shows how these modes of cooperation would integrate therein if used. Yet, most of these 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 significant critical infrastructure incident, several actions may be undertaken simultaneously and continuously.

1. INFORMATION EXCHANGE

(a) At operational level

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

Where relevant as regards civil protection assistance, the coordination between Member States and with the Commission is ensured through the ERCC under 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, national competent authorities responsible for critical infrastructure in Member States affected by the significant critical infrastructure incident share with the rotating Presidency of the Council and the Commission, through their single points of contact and without undue delay, relevant information received from the operator(s) of critical infrastructure, critical entities, or from other sources as well as information concerning the crisis management mechanisms that were activated. 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.

Such information sharing concerns the nature of the significant critical infrastructure incident, its cause, 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 relevant other 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 notification is provided without diverting the critical infrastructure's or, in some cases, the critical entity's or the Member State's resources from activities related to incident handling, which is to be prioritised.

In order to ensure follow-up, the ERCC or the notified Commission services responsible for the sector(s) in which the significant critical infrastructure incident occurred, inform the contact point in Directorate General Migration and Home Affairs and the Secretariat General of the Commission. Meanwhile, if not already initiated, the ERCC begins monitoring events, especially in the event of a UCPM activation by one or more of the affected Member States.

If the information could be relevant for addressing a cybersecurity dimension or be related to a cybersecurity incident, the Commission shares relevant information with EU-CyCLONe.

National competent authorities under Directive (EU) 2022/2557 are to cooperate and exchange information with competent authorities under Directive (EU) 2022/2555 without undue delay, in relation to cyber incidents and incidents affecting critical entities, including the cybersecurity and physical measures taken by critical entities.

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

ii) Organisation of expert meetings

The Commission convenes as soon as possible the Critical Entities Resilience Group 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 on response actions, including mitigating measures and technical support to the affected Member States. Depending on the centre of gravity of the incident, relevant Commission services will be closely associated to the meeting of the Critical Entities Resilience Group with a view to share information gathered through existing sectoral instruments. In case of incidents with a combination of cybersecurity and physical non-cyber aspects, the relevant Commission services, CERT-EU and the EEAS, where relevant, notify and consult as soon as possible within the Cyber Crisis Task Force, as well as the respective chairs of the Cooperation Group as referred to in Article 14 of Directive (EU) 2022/2555, and EU-CyCLONe as appropriate, on the need for coordination activities. In agreement with the respective chairs, the Commission (Directorate-General Migration and Home Affairs and the Directorate-General Communications Network, Content and Technology) may propose a joint meeting of the Critical Entities Resilience Group with the Cooperation Group with a view to a shared situational awareness and to coordinate respective responses.

In case of a significant cross-sectoral critical infrastructure incident that requires or is likely to require consequence management at Union level, the Commission may convene cross-sectoral coordination meetings involving all relevant stakeholders.

In case a significant critical infrastructure incident also affects a third country, the Commission consults the competent authority of the affected third country and may invite them to a meeting of the Critical Entities Resilience Group.

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 significant critical infrastructure incident to their respective 'parent' Directorates-General which, in turn, report to the Commission (Directorate-General Migration and Home Affairs, as the Chair of the Critical Entities Resilience Group).

The Commission can provide a contribution to situational awareness using the assets of the Union Space Programme[12] such as Copernicus, Galileo and EGNOS, where relevant and in accordance with the applicable legal framework.

(b) At strategic level

i) Production of situational awareness reports

Based on information shared by national competent authorities in a Critical Entities Resilience Group meeting, or joint meetings with relevant services, expert groups or networks, the Commission prepares a situational awareness report based on the contributions of the competent national authorities and other available information.

[12] 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).

This report will, where relevant, take into account the outcomes of the relevant EU-level risk assessments, evaluations and scenarios from a cybersecurity perspective, including those carried out by Commission, the High Representative of the Union for Foreign Affairs and Security Policy and the Cooperation Group.

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

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

The ERCC begins providing situational awareness support surrounding the incident, where relevant, in particular if the event prompts a UCPM activation[13]. In addition, affected Member States may request satellite imagery of their territory via Copernicus Emergency Management Service.

Where considered appropriate to share information across the Commission with EEAS and relevant Union agencies, the lead Directorate-General or Directorate-General 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 rotating Presidency of the Council of the Union may 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 rotating Presidency of the Council or by the Commission, under certain conditions.

Other (sectoral) Union crisis management mechanisms and tools may be activated following the respective procedures, as appropriate. The Commission will ensure coordination between these 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(7) of Directive (EU) 2022/2555, the rotating Presidency of the Council may use the Cyber Blueprint to determine appropriate coordination at operational level involving, *inter alia,* the EU CyCLONe and the Critical Entities Resilience Group.

iii) Coordination of public communication

The Member States affected by the significant critical infrastructure incident coordinate their public communication on the crisis to the extent possible, while respecting national competence in this regard. The IPCR Crisis Communication Network may be involved, as appropriate.

Based on the shared situational awareness, the Critical Entities Resilience Group, and the affected Member States support the formulation of agreed public communication lines, where appropriate.

Europol and other relevant Union agencies coordinate their public communication activities with the Commission's Spokesperson's service, based on shared situational awareness.

If the significant critical infrastructure incident entails an external, hybrid or Common Security and Defence Policy dimension, the public communication is coordinated with the

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

EEAS and the Commission's Spokesperson's service in accordance with the EU Protocol for countering hybrid threats[14].

2. RESPONSE (INVOLVING CONTINUOUS ACTIONS DESCRIBED UNDER INFORMATION EXCHANGE AND ADDITIONAL ACTIONS AT STRATEGIC /POLITICAL LEVELS)

(a) At strategic level

i) Continuous production of situational reports

The Council Working Party on Civil Protection – Critical Entities Resilience (PROCIV-CER) is informed of the production of a politico/strategic situational report (e.g. the ISAA in case of IPCR activation or the shared situational awareness report prepared by the Commission) and prepares the COREPER, in case the latter has not yet been convened, or the Political and Security Committee meeting, as appropriate.

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

In case the President of the Commission activates the Commission's internal crisis coordination process ARGUS Phase II, Crisis Coordination Committee meeting(s) 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 significant critical infrastructure incident.

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

- The rotating Presidency of the Council calls for a timely informal roundtable, gathering the relevant national, European and international actors, where the Commission representative acting as the Chair of the Critical Entities Resilience Group (Directorate-General Migration and Home Affairs) can report on the previously convened group's meeting(s), complemented by other Commission services and EEAS, as appropriate.

- SIAC and relevant Union agencies can be invited to present a situational update on the significant critical infrastructure incident in this meeting.

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

In case of a significant critical infrastructure incident with international security relevance, 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, respectively.

iii) Public communication

The Council prepares common public communication messages. The informal network of crisis communicators established through the IPCR may support this work. The

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

Commission's Spokesperson's service also prepares public communication messages, as appropriate.

If the significant critical infrastructure incident entails an external, hybrid or Common Security and Defence Policy dimension, the public communication is coordinated with the EEAS and the Commission's Spokesperson's service.

iv) Support to Member States and effective response

The rotating Presidency can convene a meeting of PROCIV-CER to support the activities in the framework of the IPCR, if activated.

Member States affected by the significant critical infrastructure incident may request the technical support of other Member States or relevant Union institutions, bodies and agencies through the Critical Entities Resilience Group, e.g. specific expertise to mitigate the adverse impacts of the significant critical infrastructure incident.

Member States affected by the significant critical infrastructure incident may also request the technical and/or financial support of the Commission or relevant Union agencies. The Commission, in coordination with the relevant Union agencies, assesses its possible support and activates, where appropriate, 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 significant critical infrastructure incident.

In the context of the UCPM specifically, affected countries could request assistance via the Common Emergency Communication and Information System (''CECIS''), after which the ERCC would work to coordinate the rendering of assistance from Member States and UCPM Participating States, as well as via ''rescEU''.

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

(b) At political level

The Presidency of the Council could consider the necessity to convene IPCR Roundtables, meetings of Council Working Groups, COREPER, Council of Ministers and/or Summits to exchange on the possible origin and expected consequences of the significant critical infrastructure incident for the Member States and for the Union, agree on common guidelines, and adopt the necessary measures to support the Member States affected by the significant critical infrastructure incident and mitigate its effects.

Chart 1: Schematic Overview of the Critical Infrastructure Blueprint

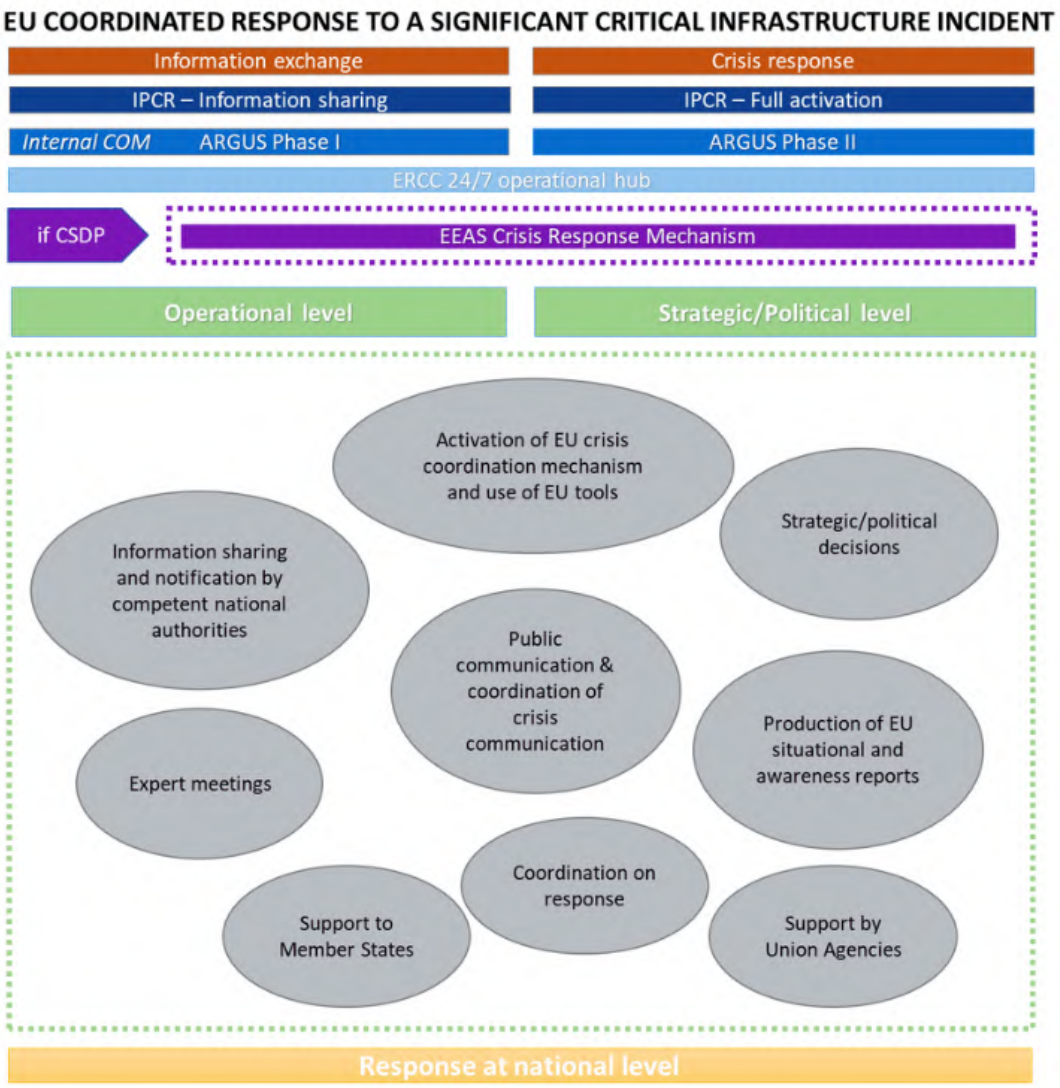

Chart 2: Critical Infrastructure Blueprint Decision