Council of the European Union

Brussels, 9 December 2022
(OR. en)

15623/22

Interinstitutional File: 2022/0338(NLE)

PROCIV 149	ATO 102
ENV 1248	CSC 561
JAI 1617	ECOFIN 1279
SAN 650	CSCI 189
COSI 315	DATAPROTECT 346
CHIMIE 100	MI 912
ENFOPOL 619	CODEC 1916
RECH 645	COPS 581
CT 220	JAIEX 103
DENLEG 93	COPEN 430
COTER 297	IND 533
RELEX 1657	POLMIL 297
ENER 654	IPCR 116
HYBRID 116	DIGIT 231
TRANS 768	DISINFO 102
CYBER 397	CSDP/PSDC 848
TELECOM 512	MARE 71
ESPACE 125	POLMAR 78

OUTCOME OF PROCEEDINGS

From:	General Secretariat of the Council
To:	Delegations
No. prev. doc.:	13713/22, 15454/22
Subject:	COUNCIL RECOMMENDATION on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure

Delegations will find in the annex the Council Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure, as adopted by the Council at its 3920th meeting held on 8 December 2022.

ANNEX

COUNCIL RECOMMENDATION (EU) 2022/…

of…

on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure

(Text with EEA relevance)

THE COUNCIL OF THE EUROPEAN UNION,

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

Having regard to the proposal from the European Commission,

Whereas:

(1) With the aim to secure the functioning of the internal market, it is in the interests of all Member States and the Union as a whole to clearly identify and protect relevant critical infrastructure that provides essential services within that market, especially in key sectors such as energy, digital infrastructure, transport and space, as well as critical infrastructure with significant cross-border relevance[1], the disruption of which could significantly impact other Member States.

[1] Member States should assess such relevance in line with their national practices and can do so based on, among other factors, a risk assessment and the impact and nature of the event.

(2) This Recommendation, which is a non-binding act, demonstrates the political will of the Member States to cooperate together and their commitment to the recommended measures, highlighted in a five-point plan issued by the President of the European Commission, while fully respecting Member States' competences. This Recommendation does not affect the protection of the essential interests of Member States´ national security, public security or defence and no Member State should be expected to share information that is detrimental to those interests.

(3) While the primary responsibility for ensuring the security and provision of essential services by critical infrastructure rests with the Member States and their critical infrastructure operators, increased coordination at Union level is appropriate, especially in light of evolving threats that may impact several Member States simultaneously, such as Russia's war of aggression against Ukraine and hybrid campaigns against Member States, or affect the resilience and good functioning of the Union's economy, internal market and society as a whole. Particular attention should be paid to critical infrastructure outside the territory of the Member States, such as undersea critical infrastructure or offshore energy infrastructure.

(4) The European Council has, in its conclusions of 20 and 21 October 2022, strongly condemned the acts of sabotage against critical infrastructure, such as those against the Nord Stream pipelines, indicating the Union's will to meet any deliberate disruption of critical infrastructure or other hybrid actions with a united and determined response.

(5) In view of the fast-evolving threat landscape, resilience-enhancing measures should be taken as a matter of priority in key sectors such as energy, digital infrastructure, transport and space, and in other relevant sectors identified by the Member States. Such measures should focus on enhancing the resilience of critical infrastructure taking into account relevant risks, especially cascading effects, supply chain disruption, dependence, impacts of climate change, unreliable vendors and partners, and hybrid threats and campaigns including foreign information manipulation and interference. Where national critical infrastructure is concerned, in view of the possible consequences priority should be given to critical infrastructure with significant cross-border relevance. Member States are encouraged to provide such resilience-enhancing measures, where appropriate, as a matter of urgency, while maintaining the approach set out in the evolving legal framework.

(6) The protection of European critical infrastructure in the energy and transport sectors is currently regulated by Council Directive 2008/114/EC[2], and security of network and information systems across the Union focused on cyber-related threats is assured by Directive (EU) 2016/1148 of the European Parliament and Council[3]. With a view to ensuring a higher common level of resilience and the protection of critical infrastructure, cybersecurity and the financial market, the existing legal framework is being amended and supplemented by the adoption of new rules applicable to critical entities (the "CER Directive"), reinforced rules for a high common level of cybersecurity across the Union (the "NIS2 Directive") and new rules applicable for digital operational resilience for the financial sector("DORA").

(7) Member States should, in accordance with Union and national law, use all available tools to move forward and help strengthen physical and cyber resilience. In this regard, critical infrastructure should be understood 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 the CER Directive or, where relevant, entities under the NIS2 Directive. The concept of resilience should 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.

---

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

3 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p. 1).

(8) National experts should be convened in order to coordinate work on achieving a higher common level of resilience and protection for critical infrastructure to be introduced by the new rules applicable for critical entities. That coordinated work would enable cooperation between Member States and information sharing regarding activities such as elaborating methodologies to identify essential services provided by critical infrastructure. The Commission has already started convening those experts and facilitating their work, and the Commission intends to continue this work. Once the CER Directive has entered into force and a Critical Entities Resilience Group under that Directive has been established, such anticipatory work should be continued by that group in accordance with its tasks.

(9) Acknowledging the changed threat landscape, the potential of conducting critical infrastructure stress tests at national level should be further developed as such tests could be useful for enhancing the resilience of critical infrastructure. With regard to the specific importance of the energy sector, and Union-wide consequences stemming from its possible disruption, that sector could benefit the most from conducting stress tests based on commonly agreed principles. Such tests fall within the competence of the Member States, who should encourage and support critical infrastructure operators to conduct such tests where assessed as beneficial and in accordance with their national legal frameworks.

(10) In order to ensure a coordinated and effective response to current and anticipated threats, the Commission is encouraged to provide additional support to Member States, in particular by providing relevant information in the form of briefings, non-binding manuals and guidelines. The European External Action Service (EEAS), in particular through the EU Intelligence and Situation Centre and its Hybrid Fusion Cell, with the support of the European Union Military Staff (EUMS) Intelligence Directorate under the Single Intelligence Analysis Capacity (SIAC) framework, should provide threat assessments. The Commission is also invited, in cooperation with Member States, to promote the uptake of Union-funded research and innovation projects.

(11) With the increasing interdependence of physical and digital infrastructure, it is possible for malicious cyber activities targeting critical areas to result in disruption or damage to physical infrastructure, or for sabotage of physical infrastructure to render digital services inaccessible. Member States are invited to accelerate preparatory work for the transposition and application of the new legal framework applicable to critical entities and of the reinforced legal framework for cybersecurity, building on the experience gained within the Cooperation Group established by Directive (EU) 2016/1148 (the "NIS Cooperation Group"), as soon as possible, while keeping in mind the time-limits for transposition and that such preparatory work should progress in parallel and in coherence.

(12) In addition to enhancing preparedness, it is also important to bolster the capabilities to respond swiftly and effectively to a disruption of essential services provided by critical infrastructure. Therefore, this Recommendation contains measures at both Union and national level, including by highlighting the supporting role and added value that can be obtained by introducing reinforced cooperation and exchange of information in the context of the Union Civil Protection Mechanism (UCPM) established by Decision No 1313/2013/EU of the European Parliament and of the Council[4] and by using relevant assets of the Union Space Programme established under Regulation (EU) 2021/696 of the European Parliament and of the Council[5].

(13) The Commission, the High Representative of the Union for Foreign Affairs and Security Policy (the 'High Representative') and the NIS Cooperation Group in cooperation with relevant civilian and military bodies and agencies and established networks, including the European cyber crisis liaison organisation network (EU-CyCLONe), are to conduct a risk evaluation and build risk scenarios. Moreover, following up on the Joint Ministerial Call of Nevers a risk assessment is currently being conducted by the NIS Cooperation Group, with the support of the Commission and the European Cybersecurity Agency (ENISA), and in cooperation with the Body of European Regulators for Electronic Communications (BEREC). Those two exercises will be consistent and coordinated with the scenario-building exercise under the UCPM, including cybersecurity events and their real-life impact, currently being developed by the Commission and Member States. In the interest of efficiency, effectiveness and consistency, and for the good application of this Recommendation, the outcomes of those exercises are supposed to be reflected at national level.

---

4 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).

5 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).

(14) In order to immediately reinforce preparedness and the capacity to respond to a large-scale cybersecurity incident, the Commission has set up a short-term programme to support Member States, through additional funding allocated to ENISA. Services proposed include, among others, preparedness actions, such as penetration testing of entities in order to identify vulnerabilities. The programme can also strengthen possibilities to assist Member States in the event of a large-scale cybersecurity incident affecting critical entities. This is a first step in line with the Council conclusions of 23 May 2022 on the development of the European Union's Cyber posture (the "Council conclusions on the EU´s Cyber posture") requesting the Commission to come forward with a proposal for a Cyber Emergency Fund. Member States should make full use of those opportunities, in accordance with the applicable requirements, and are encouraged to continue work in the area of Union cyber crisis management, in particular by regularly monitoring and taking stock of progress achieved in the implementation of the Cyber Crisis Management Roadmap recently developed in the Council. That Roadmap is a living document and should be revisited and updated when needed.

(15) Global undersea communications cables are essential for global and intra-EU connectivity. Due to the significant length of such cables and their installation on the seabed, underwater visual monitoring for most cable sections is extremely challenging. The shared jurisdiction and other jurisdictional issues relating to such cables represent a specific case for European and international cooperation concerning infrastructure protection and recovery. It is therefore necessary to complement ongoing and planned risk assessments concerning digital and physical infrastructure underpinning digital services with specific risk assessments and options for mitigating measures concerning undersea communications cables. The Member States invite the Commission to carry out studies for that purpose and share its findings with Member States.

(16) The energy and transport sectors can also be impacted by threats related to digital infrastructure, for example in relation to energy technologies embedding digital components. The security of the associated supply chains is important for the continuity of the provision of essential services and for the strategic control of critical infrastructure in the energy sector. Those circumstances should be taken into account when taking measures to enhance the resilience of critical infrastructure in accordance with this Recommendation.

(17) The growing importance of space infrastructure, space-related ground assets, including production facilities, and space-based services for security-related activities makes it essential to ensure resilience and the protection of the Union's space and its ground-related assets and services within the Union. For the same reasons, it is also essential, in the framework of this Recommendation, to make more structured use of space-based data and services, which are provided by space systems and programmes for surveillance and tracking and for protection of critical infrastructure in other sectors. The forthcoming EU Space Strategy for Security and Defence will propose appropriate actions in this regard, which should be taken into account when implementing this Recommendation.

(18) Cooperation at international level is also needed in order to effectively address risks to critical infrastructure, among others, in international waters. Therefore, the Member States are invited to cooperate with the Commission and the High Representative to take certain steps towards achieving such cooperation, keeping in mind that any such steps are only to be taken in accordance with their respective tasks and responsibilities under Union law, in particular the provisions of the Treaties regarding external relations.

(19) As established in its Communication of 15 February 2022 entitled ‘Commission Contribution to European defence’, in support of the Strategic Compass for Security and Defence - For a European Union that protects its citizens, values and interests, and contributes to international peace and security, the Commission will assess the Sectoral Hybrid Resilience Baselines in cooperation with the High Representative and the Member States, by identifying gaps and needs as well as steps to address them by 2023. That initiative should inform work under this Recommendation, helping to strengthen sharing of information and coordination of action on further strengthening of resilience, including that of critical infrastructure.

(20) The 2014 EU Maritime Security Strategy and its Revised Action Plan called for increased protection of critical maritime infrastructure, including underwater, and in particular maritime transport, energy and communication infrastructure, among others by enhancing maritime awareness through improved interoperability and streamlined information exchange (mandatory and voluntary). That Strategy and that Action Plan are currently being updated, and will include enhanced actions that aim to protect critical maritime infrastructure. Those actions should complement this Recommendation.

(21) Strengthening the resilience of critical infrastructure contributes to wider efforts to counter hybrid threats and campaigns against the Union and its Member States. This Recommendation builds upon the Joint Communication to the European Parliament and the Council entitled "Joint Framework on countering hybrid threats – a European Union response". Action 1 of the Joint Framework, namely the Hybrid Risk Survey, plays a key role in identifying vulnerabilities potentially affecting national and pan-European structures and networks. In addition, the implementation of the Council conclusions of 21 June 2022 on a Framework for a coordinated EU response to hybrid campaigns will provide for a stronger coordinated action through the application of the EU Hybrid Toolbox in all affected domains.

HAS ADOPTED THIS RECOMMENDATION:

CHAPTER I: AIM, SCOPE AND PRIORITISATION

(1) This Recommendation sets out a series of targeted actions at Union and national level to support and enhance the resilience of critical infrastructure, on a voluntary basis, with a focus on critical infrastructure with significant cross-border relevance and in identified key sectors, such as energy, digital infrastructure, transport and space. Those targeted actions consist of enhanced preparedness, enhanced response and international cooperation.

(2) Information shared in order to meet the objectives of this Recommendation, that is confidential pursuant to Union and national rules, as well as rules on business confidentiality, should be exchanged with the Commission and other relevant authorities only where that exchange is necessary for the good application of this Recommendation. This Recommendation does not affect the protection of essential interests of Member States´ national security, public security or defence, and no Member State should be expected to share information that goes against these interests.

CHAPTER II: ENHANCED PREPAREDNESS

Actions at Member State level

(3) Member States should consider an all-hazard approach when updating their risk assessments or their existing equivalent analyses, in line with the evolving nature of the current threats to their critical infrastructure, especially in identified key sectors and, where possible, in all sectors covered by upcoming new legal framework applicable to critical entities.

(4) Member States are invited to accelerate preparatory work and adopt resilience-enhancing measures, where possible, as mandated by the upcoming legal framework applicable for critical entities, with a particular focus on cooperation and relevant information sharing among Member States and with the Commission, on identifying critical entities with significant cross-border relevance and on enhancing support for identified critical entities in order to improve their resilience.

(5) Member States should support experts´ training and exercises and the sharing between experts of best practices and lessons learnt. Member States should encourage experts to participate in existing training platforms, both national and international, for example under the UCPM.

(6) Member States should encourage and support critical infrastructure operators, at least in the energy sector, to conduct stress tests, following principles commonly agreed at Union level where beneficial. Stress tests should assess the resilience of critical infrastructure against antagonistic man-made threats. Therefore, Member States should aim to identify relevant critical infrastructure to be tested and consult with relevant critical infrastructure operators as soon as possible, and no later than by the end of the first quarter of 2023. In addition, Member States should support the critical infrastructure operators so that they undertake those tests as soon as possible and aim to complete them by the end of 2023, in accordance with national law. The Council intends to assess the state of play on stress tests by the end of April 2023.

(7) Due to the rapidly evolving threats to critical infrastructure, maintaining its high level of protection is of vital importance. Member States are encouraged to allocate sufficient financial resources to strengthen the capacities of their relevant national authorities and to support them, in order to be able to enhance the resilience of critical infrastructure. Member States are also encouraged to allocate sufficient financial resources to authorities responsible for the management of large-scale cybersecurity incidents to support them, and to ensure that their computer security incident response teams (CSIRTs) and competent authorities are fully mobilised in the CSIRTs Network and EU-CyCLONe, respectively.

(8) Member States are invited, in accordance with the applicable requirements, to make use of potential Union and national-level funding opportunities to enhance the resilience of critical infrastructure in the Union for themselves, and also to encourage the critical infrastructure operators to make use of such funding opportunities, including for example trans-European networks, against the full range of significant threats, in particular under the programmes financed by the Internal Security Fund established by Regulation (EU) 2021/1149 of the European Parliament and of the Council[6], the European Regional Development Fund established by Regulation (EU) No 1301/2013 of the European Parliament and of the Council[7], the UCPM and the Commission's REPowerEU Plan. Member States are also encouraged to make best use of the results of relevant projects under research programmes, such as Horizon Europe established by Regulation (EU) 2021/695 of the European Parliament and of the Council[8].

---

6 Regulation (EU) 2021/1149 of the European Parliament and of the Council of 7 July 2021establishing the Internal Security Fund (OJ L 251, 15.7.2021, p. 94).

7 Regulation (EU) No 1301/2013 of the European Parliament and of the Council of 17 December 2013 on the European Regional Development Fund and on specific provisions concerning the Investment for growth and jobs goal and repealing Regulation (EC) No 1080/2006 (OJ L 347, 20.12.2013, p. 289).

8 Regulation (EU) 2021/695 of the European Parliament and of the Council of 28 April 2021 establishing Horizon Europe – the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination, and repealing Regulations (EU) No 1290/2013 and (EU) No 1291/2013 (OJ L 170, 12.5.2021, p. 1).

(9) As regards the communications and networks infrastructure in the Union, the NIS Cooperation Group is invited, whilst acting in accordance with Article 11 of Directive (EU) 2016/1148, to accelerate its ongoing work based on the Joint Ministerial Call of Nevers on a targeted risk assessment and should present first recommendations as soon as possible. That risk assessment should provide information to the ongoing cross-sector cyber risk evaluation and scenarios requested by the Council conclusions on the EU's Cyber posture. Moreover, that work should be carried out by ensuring coherence and complementarity with the work performed by the NIS Cooperation Group work stream on information and communication technology supply chain security as well as by other relevant groups.

(10) The NIS Cooperation Group is also invited, with the support of the Commission and ENISA, to continue its work on the security of the digital infrastructure, including in relation to undersea infrastructure, namely undersea communications cables. It is also invited to begin its work on the space sector, including by preparing, where necessary, policy guidance and cybersecurity risk management methodologies based on an all-hazard approach and risk-based approach for operators in the space sector aiming to increase the resilience of ground-based infrastructure supporting the provision of space-based services.

(11) Member States should make full use of the cybersecurity preparedness services offered in the Commission short-term support programme implemented with ENISA, for example penetration testing to identify vulnerabilities, and, in this context, are encouraged to prioritise entities operating critical infrastructure in the energy, digital infrastructure and transport sectors.

(12) Member States should make full use of the European Cybersecurity Competence Centre (ECCC). Member States should encourage their National Coordination Centres to proactively engage with the members of the cybersecurity community to build capacity at Union and national level to better support operators of essential services.

(13) It is important that the Member States achieve the implementation of the measures recommended in the EU Toolbox on 5G Cybersecurity and in particular that the Member States enact restrictions on high-risk suppliers, considering that a loss of time can increase vulnerability of networks in the Union, and also reinforce physical and non-physical protection of critical and sensitive parts of 5G networks, including through strict access controls. In addition, Member States in cooperation with the Commission should assess the need for complementary action in order to ensure a consistent level of security and resilience of 5G networks.

(14) Member States together with the Commission and ENISA should focus on implementing the Council conclusions of 17 October 2022 on ICT supply chain security.

(15) Member States should take into account the upcoming network code for cybersecurity aspects of cross-border electricity flows, building upon the experience gained with the implementation of Directive (EU) 2016/1148 and relevant guidance produced by the NIS Cooperation Group, especially its Reference document on security measures for Operators of Essential Services.

(16) Member States should develop the use of Copernicus, Galileo and the European Geostationary Navigation Overlay Service (EGNOS) for surveillance in order to share relevant information with the experts convened in accordance with point 15. Good use should be made of the abilities offered by the Union's Governmental Satellite Communications (GOVSATCOM) of the Union Space Programme for the monitoring of critical infrastructure and support to crisis prediction and response.

Actions at Union level

(17) Dialogue and cooperation between Member States' designated experts and with the Commission should be reinforced, with a view to enhancing the physical resilience of critical infrastructure, in particular by:

(a) contributing to the preparation, development and promotion of common voluntary tools to support Member States in enhancing such resilience, including methodologies and risk scenarios;

(b) supporting Member States in implementing the new legal framework applicable to critical entities, including by encouraging the Commission to adopt the delegated act in a timely manner;

(c) supporting the conduct of the stress tests referred to in point 6, based on common principles, starting with such tests focusing on antagonistic man-made threats in the energy sector and subsequently in-other key sectors, as well as supporting and advising on the conduct of such stress tests, upon request of a Member State;

(d) making use of any secure platform, once established by the Commission, to collect, take stock and share, on a voluntary basis, best practices, lessons learnt from national experiences and other information related to such resilience.

The work of those designated experts should pay particular attention to cross-sectoral dependencies and critical infrastructure with significant cross-border relevance, and should be followed up in the Council and the Commission, where appropriate.

(18) Member States are encouraged to make use of any support offered by the Commission, for instance through the preparation of manuals and guidelines such as a Handbook on Protecting Critical Infrastructure and Public Spaces against Unmanned Aircraft Systems, and tools for risk assessments. The EEAS, in particular through the EU Intelligence and Situation Centre and its Hybrid Fusion Cell, with the support of the EUMS Intelligence Directorate under the SIAC framework, is invited to conduct briefings on the threats to critical infrastructure in the Union in order to improve situational awareness.

(19) Member States should support actions undertaken by the Commission to take up results of projects on the resilience of critical infrastructure funded under the Union research and innovation programmes. The Council takes note of the Commission´s intention to increase, within the budget allocated to Horizon Europe under the 2021-2027 multiannual financial framework, funding on such resilience, without detriment to the funding of the other civil security related research and innovation projects under Horizon Europe.

(20) Due to the tasking stipulated in the Council conclusions on the EU´s Cyber posture, the Commission, the High Representative and the NIS Cooperation Group are invited to intensify, in accordance with their respective tasks and responsibilities under Union law, work with relevant networks and civil and military bodies and agencies in conducting risk evaluation and building cybersecurity risk scenarios, taking into account in particular the importance of energy, digital infrastructure, transport and space infrastructure and the interdependencies across sectors and Member States. That exercise should take into account the related risks to infrastructure on which those sectors rely. Where beneficial, the risk evaluation and scenarios could be carried out on a regular basis and should complement, build on and avoid duplication with existing or planned risk assessments in those sectors and inform discussions on how to strengthen overall resilience of entities operating critical infrastructure and to address vulnerabilities.

(21) The Commission is invited to accelerate its activities, in accordance with its respective tasks under cyber crisis management, on supporting the preparedness and response of Member States to the large-scale cybersecurity incidents, and in particular to:

(a) carry out, in order to complement relevant risk assessments in the context of Network and Information Security, a comprehensive study[9] taking stock of the undersea infrastructure, namely undersea communications cables, that connect Member States as well as Europe globally, findings of which should be shared with Member States;

(b) support the preparedness and response of Member States and Union institutions, bodies and agencies to large-scale cybersecurity incidents or major incidents, in accordance with the reinforced legal framework for cybersecurity and other relevant applicable rules[10];

(c) accelerate the main concept of the Cyber Emergency Fund with proper discussion with the Member States.

(22) The Commission is encouraged to: intensify work on forward-looking anticipatory action, including collaboration with Member States under Articles 6 and 10 of Decision 1313/2013/EU, and in the form of contingency planning to support the Emergency Response Coordination Centre's (ERCC) operational preparedness and response to disruptions of critical infrastructure; increase investments in preventative approaches and population preparedness; and increase support related to capacity building under the Union Civil Protection Knowledge Network.

---

9 This study should include mapping its capacities and redundancies, vulnerabilities, threats and risks to service availability, the impact of downtime of (trans-Atlantic) undersea cables for Member States and the Union as a whole and risk mitigation, while taking into account the sensitivity of such information and the need to protect it.

10 Particular attention should be also paid to all activities preparing for an effective Union-level coordinated response in the event of a cross-border major cyber incident or related threat that could have a systemic impact on the Union's financial sector, as mandated by the new legal framework on digital operational resilience.

(23) The Commission should foster the use of Union surveillance assets (Copernicus, Galileo and EGNOS) to support Member States in the monitoring of critical infrastructure, and their immediate vicinities where relevant, and to support other surveillance options provided for in the Union's Space Programme, such as Space Situational Awareness and EU Space Surveillance and Tracking frameworks.

(24) Where relevant and in accordance with their respective mandates, Union agencies and other relevant bodies are invited to provide support on matters relating to the resilience of critical infrastructure, in particular as follows:

(a) the European Union Agency for Law Enforcement Cooperation (EUROPOL) on information gathering, criminal analysis and investigative support in cross-border law enforcement actions and, where relevant and appropriate, sharing the outcomes with the Member States;

(b) the European Maritime Safety Agency (EMSA) on matters related to the security and safety of the maritime sector in the Union, including maritime surveillance services for matters related to maritime security and safety;

(c) the European Union Agency for the Space Programme (EUSPA) and the EU Satellite Centre (SatCen) may be able to assist through operations within the Union Space Programme;

(d) the ECCC as regards activities related to cybersecurity, also in cooperation with ENISA, could support innovation and industrial policy in cybersecurity.

CHAPTER III: ENHANCED RESPONSE

Actions at Member State level

(25) Member States are invited to:

(a) continue coordination of their response, where relevant, and maintain the overview of the cross-sectoral response to acute disruptions of essential services provided by critical infrastructure. This could be done in the framework of: a future Blueprint on a coordinated response to disruptions of critical infrastructure with significant cross-border relevance; the existing Integrated Political Crisis Response (IPCR) arrangements for the coordination of the political response when it comes to critical infrastructure with cross-border relevance; the Blueprint on large-scale cybersecurity incidents and crises under Commission Recommendation (EU) 2017/1584[11]; EU-CyCLONe; in the Framework for a coordinated EU response to hybrid campaigns and the EU Hybrid Toolbox in the case of hybrid threats and campaigns; and in the Rapid Alert System in the case of disinformation;

(b) increase operational-level information exchange with the ERCC within the context of the UCPM in order to enhance early warning and to coordinate their response under the UCPM in the event of disruptions of critical infrastructure with significant cross-border relevance, thus ensuring a faster Union-facilitated reaction when needed;

(c) increase their readiness to respond, where relevant, via existing or to-be-developed tools to such significant disruptions referred to in point (a);

[11] 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).

(d) engage in further developing relevant response capacities in the European Civil Protection Pool (ECPP) and rescEU;

(e) encourage critical infrastructure operators and relevant national authorities to enhance their capacities to be able to quickly restore a basic performance of the essential services provided by those critical infrastructure operators;

(f) encourage critical infrastructure operators, when rebuilding their critical infrastructure, to build it to be as resilient as possible, taking into account the proportionality of measures with regard to risk assessments and costs, to the full range of significant risks that may apply to it, including in adverse climate scenarios.

(26) Member States are invited to accelerate preparatory work, where possible, as mandated by the reinforced legal framework on cybersecurity, by aiming to enhance the national CSIRTs capabilities, in view of the new tasks of CSIRTs as well as the enlarged number of entities from new sectors, reviewing and updating their cybersecurity strategies in a timely manner and adopting as soon as possible national cybersecurity incident and crisis response plans, if not yet existing.

(27) Member States are invited to consider, at national level, the most relevant means to ensure that relevant stakeholders are aware of the need to advance the resilience of critical infrastructure by cooperation with trusted vendors and partners. It is important to invest in additional capacity, especially in the sectors where the current infrastructure is at the end of its lifespan, for example undersea communications cable infrastructure, to be able to ensure continuity of the provision of essential services in the event of disruptions, and to reduce unwanted dependencies.

(28) Member States are encouraged to pay attention to proactive strategic communication at national level in the context of countering hybrid threats and campaigns, and given the potential that adversaries may seek to engage in foreign information manipulation and interference by shaping the narratives around incidents targeting critical infrastructure.

Actions at Union level

(29) The Commission is invited to work closely with the Member States to further develop relevant bodies, instruments and response capacities, with a view to enhancing operational preparedness to address the immediate and indirect effects of significant disruptions of relevant essential services provided by critical infrastructure, in particular experts and resources available through the ECPP and rescEU under the UCPM or future Hybrid Rapid Response Teams.

(30) Taking into account the evolving threat landscape and in cooperation with Member States, the Commission is invited in the context of the UCPM to:

(a) continuously analyse and test the adequacy and operational readiness of existing response capacities;

(b) regularly monitor and identify potentially significant response capacity gaps in the ECPP and rescEU capacities;

(c) further intensify cross-sectoral collaboration to ensure adequate response at Union level, and organise regular training or exercises to test such collaboration in cooperation with one or more Member States;

(d) further develop the ERCC as the cross-sectoral emergency hub at Union level for the coordination of support to affected Member States.

(31) The Council is committed to initiating work with a view to approving a Blueprint on a coordinated response to disruptions of critical infrastructure with significant cross border relevance, that describes and sets out the objectives and modes of cooperation between the Member States and the Union institutions, bodies, offices and agencies in responding to incidents against such critical infrastructure. The Council looks forward to the Commission's draft for such a Blueprint, building on the support and contributions of relevant Union agencies. The Blueprint shall be fully coherent and interoperable with the revised Union operational protocol for countering hybrid threats ("EU Playbook") and take into account the existing Blueprint on coordinated response to large-scale cross-border cybersecurity incidents[12] and crises and EU-CyCLONe mandate stipulated in the NIS2 Directive and avoid the duplication of structures and activities. That Blueprint should fully respect the existing IPCR arrangements for the coordination of the response.

[12] Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises.

(32) The Commission is invited to consult with relevant stakeholders and experts on appropriate measures in relation to possible significant incidents regarding undersea infrastructure, to be presented in conjunction with the stock-taking study referred to in point 20(a), as well as to further elaborate contingency planning, risk scenarios, and Union disaster resilience goals set out in Decision No 1313/2013/EU.

CHAPTER IV: INTERNATIONAL COOPERATION

Actions at Member State level

(33) Member States should cooperate, where appropriate and in accordance with Union law, with relevant third countries as regards the resilience of critical infrastructure with significant cross-border relevance.

(34) Member States are encouraged to cooperate with the Commission and the High Representative in order to effectively address risks to critical infrastructure in international waters.

(35) Member States are invited to contribute, in cooperation with the Commission and the High Representative, to the accelerated development and implementation of the EU Hybrid Toolbox and the implementing guidelines referred to in the Council conclusions of 21 June 2022 on a Framework for a coordinated EU response to hybrid campaigns and subsequently use them, in order to give full effect to the Framework for a coordinated EU response to hybrid campaigns in particular when considering and preparing comprehensive and coordinated Union responses to hybrid campaigns and hybrid threats, including those against critical infrastructure operators.

Actions at Union level

(36) The Commission and the High Representative are invited to support, where appropriate and in accordance with their respective tasks and responsibilities under Union law, relevant third countries to enhance the resilience of critical infrastructure in their territory and in particular critical infrastructure which is physically connected to their territory and that of a Member State.

(37) The Commission and the High Representative, in line with their respective tasks and responsibilities under Union law, will strengthen coordination with NATO on the resilience of critical infrastructure of common interest through the EU-NATO structured dialogue on resilience, in full respect of Union and Member States' competences according to the Treaties and the key principles guiding EU-NATO cooperation as agreed by the European Council, in particular reciprocity, inclusiveness and decision-making autonomy. In this context, that cooperation will be taken forward within the EU-NATO Structured Dialogue on Resilience, embedded in the existing staff-to-staff mechanism for the implementation of the Joint Declarations, while ensuring full transparency and involvement of all Member States.

(38) The Commission is invited to consider the participation of representatives of relevant third countries, where necessary and appropriate, in the framework of the cooperation and information exchange between Member States in the area of resilience of critical infrastructure which is physically connected to the territory of a Member State and that of a third country.

Done at …, …

For the Council

The President