EUROPEAN
COMMISSION

Strasbourg, 18.10.2022
COM(2022) 551 final

2022/0338 (NLE)

Proposal for a

COUNCIL RECOMMENDATION

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

(Text with EEA relevance)

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

• Reasons for and objectives of the proposal

Security is an essential goal of the European Union. While Member States have the primary responsibility for protecting citizens, collective action at Union level makes a major contribution to the security of the EU as a whole. Coordination helps to reinforce resilience, to improve alertness, and to strengthen our collective response. In the context of the EU Security Union, important steps have been taken to build capabilities and capacities for prevention, detection and rapid response to many security threats, and to link players in the public and private sectors in a common effort.

Equipping the EU to deal with the ever-changing threat landscape requires constant vigilance and adaptation. Russia's war of aggression against Ukraine has brought new risks, often combined as a hybrid threat. One of these is the risk of disruption for the provision of essential services by entities operating critical infrastructure in Europe. This has become even more evident with the apparent sabotage of the Nord Stream gas pipelines and other recent incidents. Society relies heavily on both physical and digital infrastructure and the interruption of essential services, whether through conventional physical attacks or cyberattacks, or a combination of the two, can have serious consequences for citizens' well-being, our economies, and trust in our democratic systems.

Ensuring the smooth functioning of the internal market is another key goal of the EU, including when it comes to the essential services provided by entities operating critical infrastructure. The EU has therefore already taken a number of measures to reduce vulnerabilities and increase the resilience of critical entities, both in respect of cyber and non-cyber risks.

Action is urgently needed to step up the EU's capacity to stand up to potential attacks against critical infrastructure, principally in the EU itself but where relevant also in its direct neighbourhood.

The proposed Council Recommendation seeks to intensify the EU's support to increasing the resilience of critical infrastructure, and to ensuring an EU-level coordination, in terms of preparedness and response. It aims to maximise and accelerate work to protect those assets, facilities, and systems that are necessary for the functioning of the economy and to provide essential services in the internal market, which citizens rely on, as well as to mitigate the impact of any attack by ensuring the swiftest possible recovery. While all such infrastructure should be protected, the first priority is currently with the energy, digital infrastructure, transport and space sectors due to their particularly horizontal character for society and the economy, and to current risk assessments.

The EU has a particular role to play in respect of ensuring the resilience of infrastructure that crosses terrestrial or maritime borders impacting the interests of several Member States, or that is used to provide essential services that cross borders. Critical infrastructure with relevance for several Member States may, however, lie in one Member State alone or even outside the territory of a Member State, for example in the case of undersea cables or pipelines. Clear identification of the critical infrastructure and the entities operating them, as well as the risks threatening them, and a collective commitment to protect them, is in the interests of all Member States and the EU as a whole.

The European Parliament and the Council have already reached political agreement to deepen the legislative framework for the EU to help strengthen the resilience of entities operating

critical infrastructure. In the summer of 2022, agreements were reached on the Directive on the resilience of critical infrastructure ('CER Directive')[1] and the revised Directive on the security of network and information systems ('NIS2 Directive')[2]. These will represent a major intensification of capabilities compared to the existing legislative framework, 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 ('ECI Directive')[3] and Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union ('NIS Directive')[4]. The new legislation is expected to come into force in late 2022 or early 2023, and transposition and application should be prioritised by Member States, in accordance with Union law.

That being so, and given the potential urgency to address threats that are arising from Russia's war of aggression against Ukraine, the steps outlined in the new legislation should, where possible and appropriate, be frontloaded as of today. Intensifying mutual cooperation already now would also help to create the momentum for an effective implementation when the new legislation is fully in force.

The result would be to already move beyond the current frameworks, both in terms of the depth of action and the breadth of sectors covered. The new CER Directive puts forward a new framework for cooperation as well as obligations for Member States and critical entities aimed at strengthening the physical non-cyber resilience against natural and man-made threats of those entities that provide essential services in the internal market, with eleven sectors specified[5]. The NIS2 Directive will put in place a broad sectoral coverage of cybersecurity obligations. This will encompass a new requirement for Member States, to include, where relevant, undersea cables in their cybersecurity strategies.

The legislation requires the Commission to take on a substantial coordination role. Under the CER Directive, the Commission has a supporting and facilitating role, to be carried out with the support and involvement of the Critical Entities Resilience Group (CERG) established by that Directive, and should complement Member States' activities by developing best practices, guidance material and methodologies. As for cybersecurity, the Council has already in its Conclusions on the EU's Cyber Posture in summer 2022 invited the Commission, the High Representative, and the NIS Cooperation Group to work on risk assessments and scenarios from a cyber-security perspective. Such coordination can inspire an approach for other key critical infrastructure.

On 5 October 2022, President von der Leyen presented a 5-point plan, setting out a coordinated approach to the necessary work ahead**.** Its key elements were: enhancing preparedness; working with Member States with a view to stress test their critical infrastructure, starting with the energy sector and then followed by other high risk sectors; increasing the response capacity in particular, through the Union Civil Protection Mechanism; making good use of satellite capacity to detect potential threats; and strengthening cooperation with NATO and key partners on the resilience of critical infrastructure. The 5-point plan underlined the value of anticipating the legislation already enjoying political agreement.

---

1 COM(2020)829 final
2 COM(2020) 823 final
3 OJ L 345, 23.12.2008
4 OJ L194, 19.7.2016
5 Energy, Transport, Digital Infrastructure, Banking, Financial Market infrastructure, Health, Drinking Water, Waste Water, Public Administration, Space, and Food

The proposed Council Recommendation welcomes this approach, to structure support to Member States and coordinate their efforts in raising risk awareness, preparedness, and response to the current threats. In this regard, meetings of experts are convened to discuss the resilience of entities operating critical infrastructure in anticipation of the entry into force of the CER Directive and the CERG established thereby.

Strengthened cooperation with key partners and neighbouring and other relevant third countries on the resilience of entities operating critical infrastructure will be essential, in particular through the EU-NATO structured dialogue on resilience.

The focus of this Recommendation is the reinforcement of the Union's capacity to anticipate, prevent and respond to the new threats arising from Russia's war of aggression against Ukraine. The proposed recommendations therefore focus on addressing security-related risks and threats to critical infrastructure. Nevertheless, it should be noted that recent events have also underscored the pressing need to pay increased attention to climate change impacts on critical infrastructure and services in terms of, for example, seasonally compromised and unpredictable water supplies for nuclear power plant cooling, hydro power and inland navigation, or the risk of material damages to transport infrastructure, which may cause major disruptions in essential services. These concerns will continue to be addressed through relevant legislation and coordination.

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

This proposal for a Council Recommendation is fully in line with the current and future legal framework on the resilience of entities operating critical infrastructure, the ECI Directive and the CER Directive respectively, since it aims inter alia at facilitating cooperation between Member States in this area and supporting concrete measures to enhance resilience against the current imminent threats against entities operating critical infrastructure in the EU.

It also complements and anticipates the CER Directive by already inviting Member States to prioritise the timely transposition of the Directive, by cooperating through expert meetings convened as part of the 5-point plan announced by the Commission and by aiming at coordinating the way to a common approach on conducting stress tests on critical infrastructure in the EU.

The proposal is also in line with the NIS Directive and the forthcoming NIS2 Directive, which will repeal the NIS Directive, by calling for an early start to implementation and transposition work. It also reflects the Nevers Joint Call of March 2022 as well as the Council Conclusions on the EU cyber posture of May 2022 as regards the request of Member States to the Commission to develop risk assessments and risk scenarios.

The proposal is also in line with EU policy on civil protection, where in case of an overwhelming disruption to the operations of critical infrastructure/entities Member States and third countries can request assistance via the Emergency Response Coordination Centre (ERCC) under the Union Civil Protection Mechanism (UCPM). In the event of a UCPM activation, the ERCC is able to coordinate and co-finance the deployment of essential equipment, materials and expertise available in Member States (in part within the context of the European Civil Protection Pool) and under rescEU to the affected country. Assistance that can be made available upon request includes, for example, fuel, generators, electricity infrastructure, shelter capacity, water purification capacity, and emergency medical capacities.

The proposal is also in line with the EU acquis related to security of energy supply.

The nuclear energy sector is not specifically included in the proposed Council Recommendation, except for example related infrastructure (such as transmission lines to nuclear power plants) that may affect security of supply. Specific nuclear elements are

covered by relevant nuclear legislation under Euratom Treaty and/or national legislation[6]. Drawing from the lessons of the Fukushima accident, the European nuclear safety legislation was reinforced and consequently regular periodic safety reviews have to be conducted by national authorities for each installation to ensure continued compliance with the highest safety requirements and to identify further safety improvements as well as six yearly topical peer reviews at EU level.

The EU Maritime Security Strategy[7] and its action plan[8] highlight the changing nature of threats in the maritime domain and call for renewed commitment to the protection of critical maritime infrastructure, including underwater, and in particular maritime transport, energy and communication infrastructure, inter alia by enhancing maritime awareness through improved interoperability and streamlined information exchange.

The proposal is also in line with other relevant sectoral legislation. Therefore, the implementation of this Recommendation should be consistent with specific measures that regulate or may regulate in the future certain aspects of resilience of entities operating in concerned sectors, such as transport. This includes other relevant initiatives such as the contingency plan for transport[9] or the contingency plan for food supply and food security in times of crisis[10] and the related European Food Security preparedness and response Mechanism. More generally, the Recommendation should naturally be implemented in full respect for all applicable rules of EU law, including those laid down in the ECI and NIS Directives.

The proposal is also in line with the the Strategic Compass for Security and Defence, which emphasised the need to substantially enhance the resilience and ability to counter hybrid threats and cyber attacks, as well as the need to strenghten the resilience of partner countries and to cooperate with NATO. It is also in line with the Framework for a coordinated EU response to hybrid threats and campaigns affecting the EU, Member States and partners[11].

2. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY

• Legal basis

The proposal is based on Article 114 on the Treaty on the Functioning of the European Union (TFEU), which involves the approximation of laws for the improvement of the internal market, together with Article 292 TFEU. This is justified by the fact that the proposed Council Recommendation principally seeks to anticipate measures laid down in the new CER and NIS2 Directives, both of which are based on Article 114 TFEU as well. In line with the logic justifying the use of that Article as the legal basis for those Directives, EU action is needed to ensure the smooth functioning of the internal market in particular in view of the cross-border nature and scope of the services concerned and of the potential consequences in case of disruptions, as well as the actual and emerging national measures aimed at enhancing the resilience of entities operating critical infrastructure used to provide essential services in the internal market.

---

6 Recital 9 of Council Directive 2008/114/EC (ECI Directive)
7 11205/14
8 10494/18
9 COM(2022)211
10 COM(2021)689
11 Council of the European Union 10016/22, 21 June 2022

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

A way forward at European level in the area of the resilience of entities operating critical infrastructure is justified given the interdependent, cross-border nature of relationships between critical infrastructure operations and the essential services provided and by the need for a more common and coordinated European approach, in order to ensure that the entities concerned are sufficiently resilient in the current geopolitical context. Whereas, many of the common challenges, such as the apparent sabotage of the North Stream gas pipelines, are first and foremost addressed through national measures or by entities operating critical infrastructure, the support of the EU including relevant agencies where appropriate is necessary to reinforce resilience, to improve alertness, and to strengthen the EU's collective response.

- **Proportionality**

The present proposal is in conformity with the principle of proportionality as provided for in Article 5(4) Treaty on the European Union.

Neither the content nor the form of this proposed Council Recommendation exceeds what is necessary to achieve its objectives. The actions proposed are proportional to the pursued objectives as they respect Member States' prerogatives and obligations under national law.

Finally, the proposal accommodates a potential differentiated approach that reflects Member States' varying internal realities when it comes to preparedness and response to physical threats to critical infrastructure.

- **Choice of the instrument**

To achieve the objectives referred to above, the TFEU provides for the adoption by the Council of Recommendations notably in its Article 292, based on a proposal from the Commission. A Council Recommendation is an appropriate instrument in this case, having regard also to the current legislative context as explained above. As a legal act, albeit one of a non-binding nature, a Council recommendation signals the commitment of Member States to the measures included and provides a strong political basis for cooperation in these areas, while fully respecting Member State authority.

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

- **Stakeholder consultations**

In developing this proposal, the views of the Member State experts expressed at the meeting of 12 October 2022 were taken into account. There was a broad consensus on the usefulness of more coordination at Union level as regards preparedness and response in the current threat context and to anticipate certain elements of the CER Directive before its formal adoption. Member States expressed openness to share experiences and best practices on the measures and methodologies to enhance the resilience of entities operating critical infrastructure. Member States also expressed openness towards a coordinated approach to stress tests of entities operating critical infrastructure on a voluntary basis and based on common principles. Member States indicated that entities operating critical infrastructure in the energy, digital infrastructure, and transport sectors should be considered a priority for the purposes of this Recommendation, notably those with relevance for several Member States. Member States also welcomed the intention of the Commission to convene further meetings of Member State experts in the coming weeks.

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

The proposal for a Council Recommendation does the following:

– Chapter I lays down the aim of the proposal, what it covers and the prioritisation of measures recommended.

– Chapter II focuses on measures that should be taken on enhanced preparedness, both at Union and Member State level.

– Chapter III covers enhanced response, both at EU and Member State level.

– Chapter IV deals with international cooperation and the actions that should be taken for enhancing the resilience of entities operating critical infrastructure.

2022/0338 (NLE)

Proposal for a

COUNCIL RECOMMENDATION

on a coordinated approach by the Union 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 thereof,

Having regard to the proposal from the European Commission,

Whereas:

(1) The Union has a particular role to play in respect of infrastructure that crosses borders impacting the interests of several Member States, or that is otherwise used by entities to provide essential services on a cross-border basis. Such service provision and critical infrastructure with relevance for several Member States may, however, lie in one Member State alone or outside the territory of the Member States, for example in the case of undersea cables or pipelines. Clear identification of such infrastructure and entities and of the threats that they face, as well as collective commitment to protect them, is in the interests of all Member States and the Union as a whole.

(2) The protection of critical infrastructure in two sectors is currently regulated by Council Directive 2008/114/EC.[12] That Directive establishes a procedure for the identification and designation of European critical infrastructures and a common approach to the assessment of the need to improve the protection of such infrastructures in order to contribute to the protection of people. It covers the energy and transport sectors. In order to improve the resilience of critical entities and the essential services that they provide and the critical infrastructure that they rely on, a new Directive on the resilience of critical entities[13] ('CER Directive') is in the process of adoption by the Union legislator and will replace Directive 2008/114/EC, covering more sectors, including digital infrastructure.

(3) In addition, Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union[14] focuses on cyber-related threats. That Directive will be replaced by a new Directive on measures for a high common level of cybersecurity

[12] 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)

[13] COM(2020)829

[14] 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)

across the Union[15] ('NIS2 Directive'), which is also in the process of adoption by the Union legislator.

(4) In view of a fast-evolving threat landscape, in particular in the context of the apparent sabotage of the Nord Stream 1 and 2 gas infrastructure, entities operating critical infrastructure face particular challenges as regards their resilience against hostile acts and other man-made threats, while challenges from natural factors and climate change are increasing and may interact with hostile acts. Therefore, they need to take, with support from Member States, appropriate resilience-enhancing measures. Those measures should be taken and that support should be provided beyond measures under Directive 2008/114/EC and Directive (EU) 2016/1148 and even before the adoption, entry into force and transposition of the new CER and NIS2 Directives.

(5) Pending the adoption, entry into force, and transposition of those new Directives, the Union and the Member States are encouraged, in accordance with Union law, to use all available tools to move forward and help strengthen the physical and cyber resilience of those entities concerned and the critical infrastructure that they operate to provide essential services in the internal market, that is services, which are crucial for the maintenance of vital societal functions, economic activities, public health and safety or the environment. In this regard, the concept of resilience should be understood as referring to an entity's ability to prevent, protect against, respond to, resist, mitigate, absorb, accommodate and recover from events that have the potential to significantly disrupt, or that disrupt, the provision of the essential services in question.

(6) In order to ensure an approach that is both effective and as consistent as possible with the new CER Directive, the measures contained in this Recommendation should relate to infrastructure designated by a Member State as critical infrastructure, covering both national critical infrastructure and European critical infrastructure, irrespective of whether the entity operating the critical infrastructure has already been designated as a critical entity under that new Directive. For the purposes of this Recommendation, the term 'critical infrastructure' should be understood accordingly.

(7) In view of the existing threats, resilience-enhancing measures should be taken as a matter of priority in the key sectors of energy, digital infrastructure, transport and space, and such measures should focus on enhancing the resilience of entities operating critical infrastructure in respect of man-made risks. Where national critical infrastructure is concerned, in view of the possible consequences if the risks materialise, priority should be given to infrastructure that is of cross-border relevance.

(8) Accordingly, the measures laid down in this Recommendation principally aim to supplement the new CER and NIS2 Directives, which are based on Article 114 of the Treaty on the Functioning of the European Union (TFEU), by anticipating and complementing the measures that those new Directives will provide. Therefore, and in view of the cross-border nature and relevance of the essential services and critical infrastructure in question and of current and emerging disparities of national laws distorting the internal market, it is appropriate to base this Recommendation on Article 114 TFEU as well, together with Article 292 TFEU.

(9) The implementation of this Recommendation should not be understood as affecting, and should be consistent with, current and future requirements of Union law regarding

[15] COM(2020)823

certain aspects of the resilience of the entities concerned. Such requirements are laid down in general instruments such as Directive 2008/114/EC and Directive (EU) 2016/1148 and the new CER and NIS2 Directives replacing them, but also in certain sector-specific instruments, such as in the field of transport, where, amongst others, the Commission has taken an initiative regarding the contingency plan for transport.[16] In accordance with the principle of sincere cooperation, this Recommendation should be implemented in full mutual respect and assistance.

(10) The Commission announced on 5 October 2022 a five-point plan setting out a coordinated approach to address the challenges ahead, which includes working on preparedness by building on and anticipating the adoption and entry into force of the new CER Directive and which also includes working with Member States with a view to performing stress tests of entities operating critical infrastructure based on common principles, starting with the energy sector. This Recommendation, which will contribute to that plan, welcomes the approach proposed and sets out how it may be translated into action.

(11) Against the backdrop of a fast-evolving threat landscape and the current risk environment characterised by man-made risks, in particular as regards critical infrastructure with cross-border relevance, it is essential to have an accurate, up-to-date and complete picture of the most important risks that entities operating critical infrastructure are facing. Therefore, Member States should take the necessary measures to perform or update their assessments of those risks. While the focus of this recommendation is on security-related risks, in addition, efforts should continue to address climate change and environmental risks, in particular when natural events may further exacerbate man-made risks.

(12) Having regard to that threat landscape, Member States should be invited to take, as soon as possible, appropriate measures to enhance the resilience of critical infrastructure, also beyond the said risk assessments, that will subsequently be required under the new CER Directive.

(13) As part of the implementation of the five-point plan announced by the Commission, it is necessary to coordinate work by convening national experts to be brought together in anticipation of the establishment of the Critical Entities Resilience Group by the new CER Directive, to enable cooperation between Member States and the exchange of information as regards the resilience of entities operating critical infrastructure. This should include cooperation and exchange of information regarding activities such as identifying critical entities and infrastructure, preparing the development and promotion of a common set of principles to carry out stress tests and learning common lessons from stress tests, identifying vulnerabilities and possible capabilities. These processes should also benefit the resilience of entities operating critical infrastructure against climate and environmental risks. This work would also allow for common prioritisation of work on stress tests, with an emphasis on the energy, digital infrastructure, transport and space sectors. The Commission has already started convening those experts and facilitating their work, and the Commission intends to continue this work. Once the new CER Directive has entered into force and the Critical Entities Resilience Group has been established, such anticipatory work should be continued by that group in accordance with its tasks under the CER Directive.

[16] COM(2022)211

(14) The stress test exercise should be complemented by the production of a Blueprint on critical infrastructure incidents and crises that describes and sets out the objectives and modes of cooperation between the Member States and EU institutions, bodies, offices and agencies in responding to incidents against critical infrastructure, in particular where these entail significant disruptions of the provision of essential services for the internal market. This Blueprint should make use of the existing Integrated Political Crisis Response (IPCR) arrangements for the coordination of the response, should work in coherence and complementarity with the Blueprint on large scale cyber incidents, and should also provide for agreement on key public communication messages given that crisis communications play an important role in mitigating the negative effects of critical infrastructure incidents and crises.

(15) In order to ensure a coordinated and effective response to the current and anticipated threats, the Commission will provide additional support to Member States with a view to enhancing of resilience in the light of those threats, in particular by providing relevant information in the form of briefings, manuals and guidelines, promoting the uptake of Union-funded research and innovation projects, taking the necessary anticipatory action and optimising the use of the Union's surveillance assets. The EEAS, in particular through the EU Intelligence and Situation Centre, should provide threat assessments.

(16) Sector-relevant Union agencies and other relevant bodies should also provide support on resilience-related matters, insofar as their respective mandates as set out in the relevant instruments of Union law allow. In particular, the European Cybersecurity Agency (ENISA) could assist on cyber security matters, the European Maritime Safety Agency (EMSA) could assist with its expertise in supporting Member States via its maritime surveillance service for matters related to maritime security and safety, the European Union Agency for Law Enforcement Cooperation (EUROPOL) could provide support in relation to information-gathering and investigations in cross-border law enforcement actions, whereas 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.

(17) While the primary responsibility for ensuring security of critical infrastructure and the entities concerned rests with the Member States, increased coordination at Union level is appropriate especially in the light of threats that may impact on several Member States at a time, such as Russia's war of aggression against Ukraine, or affect on the resilience and good functioning of the Union's economy, single market and societies.

(18) This Recommendation does not entail the supply of information, the disclosure of which is contrary to the Member States' essential interests of national security, public security or defence.

(19) With the increasing interdependence of physical and digital infrastructures, malicious cyber activities targeting critical areas may result in disruption or damage to physical infrastructure, while sabotage of physical infrastructure may render digital services inaccessible. In view of the increased threat posed by sophisticated hybrid attacks, Member States should also include such considerations in their work in implementation of this Recommendation. In view of the interlinkages between the cybersecurity and the physical security of operators, it is important that the work to prepare for the transposition and application of the new NIS2 Directive starts as soon as possible and that such work under the new CER Directive also progresses in parallel.

(20) In addition to enhancing preparedness, it is also important to enhance the capabilities to respond swiftly and effectively in the event that risks affecting the provision of essential services provided by entities operating critical infrastructure materialise. Therefore, this Recommendation should contain the measures that should be taken both at Member State and at Union level, including reinforced cooperation and exchange of information in the context of the Union Civil Protection Mechanism and use of relevant assets of the Union Space Programme.

(21) Following the invitation of the Council in its Conclusions on the EU's cyber posture,[17] the Commission, the High Representative of the Union for Foreign Affairs and Security Policy ('High Representative') and the Cooperation Group established by Directive (EU) 2016/1148 ('NIS Cooperation Group') are, in coordination with relevant civilian and military bodies and agencies and established networks, including EU CyCLONe, conducting a risk evaluation and building risk scenarios from a cybersecurity perspective in a situation of threat or possible attack against Member States or partner countries. This exercise is focused on critical sectors including energy, digital infrastructure, transport and space.

(22) The Joint Ministerial Call of Nevers[18] and the Council conclusions on the EU's Cyber posture also called for reinforcing the resilience of the communications infrastructure and networks in the Union, by making recommendations to Member States and the Commission, based on a risk assessment. This risk assessment is currently being conducted by the NIS Cooperation Group, with the support of the Commission and ENISA, and in cooperation with the Body of European Regulators for Electronic Communications (BEREC). The risk assessment and gap analysis look at the risks of cyber-attacks for the various sub-sectors of communications infrastructures, including fixed and mobile infrastructures, satellite, sub-marine cables, internet routing, etc., thus providing a basis for work under this Recommendation. This risk assessment will feed information to the ongoing cross-sector cyber risk evaluation and scenarios requested by the Council, in the Council conclusions of 23 May 2022.

(23) Those two exercises will be consistent and coordinated with the exercise for scenarios focusing on civil protection in the context of a broad range of natural and man-made disasters, including cybersecurity events and their real-life impact, currently being developed by the Commission and Member States under Decision No 1313/2013/EU of the European Parliament and the Council.[19] In the interest of efficiency, effectiveness and consistency, this Recommendation should be implemented having regard to the outcomes of those exercises.

(24) The EU Toolbox on 5G Cybersecurity[20] sets out relevant measures and mitigation plans to reinforce the security of 5G networks. In view of the dependence of many essential services on 5G networks and the interconnected nature of the digital ecosystems, it is essential that all Member States urgently achieve the implementation of the measures recommended in the Toolbox and in particular apply the relevant restrictions on high-risk suppliers for key assets defined as critical and sensitive in the EU coordinated risk assessment.

---

17 Cyber posture: Council approves conclusions - Consilium (europa.eu)

18 https://www.regeringen.se/494477/contentassets/e5f13bec9b1140038eed9a3d0646f8cf/joint-call-to-reinforce-the-eus-cybersecurity-capabilities.pdf

19 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)

20 5g_eu_toolbox_72D70AC7-A9E7-D11D-BE17B0ED8A49D864_64468.pdf

(25) In order to immediately reinforce preparedness and capacities to respond to major cyber incident, the Commission has set up a short-term programme to support Member States, through additional funding allocated to ENISA. Services covered will include preparedness actions, such as penetration testing of critical entities in order to identify vulnerabilities. It will also strengthen possibilities to assist Member States in case of a major incident affecting critical entities. This is a first step in line with the Council conclusions on the 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.

(26) The global undersea data and electronic communications cable network is essential for global and intra-EU connectivity. Due to the significant length of these 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 these cables represent a particular 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 infrastructures underpinning digital services with particular risk assessments and options for mitigating measures concerning undersea cables. The Commission will therefore carry out studies for this purpose and share its findings with Member States.

(27) The priority sectors identified in this Recommendation of energy and transport can also be impacted by risks relating to digital infrastructure. Such an impact can exist, 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 operated by entities in the energy sector. Those circumstances should be taken into account when taking measures to enhance the resilience of entities operating critical infrastructure in accordance with this Recommendation.

(28) The growing importance of space infrastructure and of space-based services for security-related activities makes it essential to ensure resilience and the protection of the Union's space assets and services within the EU, but also in the framework of this Recommendation, to make more structured use of space-based data and services provided by space systems and programmes for surveillance and 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

(29) Cooperation at international level is also needed in order to effectively address risks to the resilience of entities operating critical infrastructure, either in the Union or in relevant third countries or in international waters. Therefore, the Member States should be invited to cooperate with the Commission and the High Representative, to take certain steps to that aim, it being understood that any such steps are only to be taken in accordance with their respective tasks and responsibilities under Union law, notably the provisions of the EU Treaties regarding external relations.

(30) As established in the Communication 'Commission Contribution to European defence',[21] in support of the Strategic Compass for Security and Defence - For a European Union that protects its citizens, values and interests and contributes to

[21] com_2022_60_1_en_act_contribution_european_defence.pdf (europa.eu)

international peace and security,[22] 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. This 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.

(31) The 2014 EU Maritime Security Strategy and its Action Plan called for increased protection of critical maritime infrastructure, including underwater, and in particular maritime transport, energy and communication infrastructure, inter alia by enhancing maritime awareness through improved interoperability and streamlined information exchange (mandatory and voluntary). The Strategy and Action Plan are currently being updated, and will include enhanced actions aimed at protecting critical maritime infrastructure. Those actions should inform and complement this Recommendation.

(32) Member States should take into account the full potential of the Union security research programme, notably leveraging its dedicated priority on critical infrastructure, in particular under the programmes financed by the Internal Security Fund as well as other potential funding opportunities at Union level, notably the European Regional Development Fund to the extent specific measures fulfil its eligibility requirements. REPowerEU may also offer possibilities for resilience funding. Any such use of the opportunities offered by Union funding is to take place in accordance with the applicable legal requirements.

HAS ADOPTED THIS RECOMMENDATION:

CHAPTER I: AIM, SCOPE AND PRIORITISATION

(1) This Recommendation invites Member States to take urgent and effective measures, and to cooperate loyally, efficiently, in solidarity and in a coordinated manner with each other, the Commission and other relevant public authorities as well as the entities concerned, to enhance the resilience of critical infrastructure used to provide essential services in the internal market.

(2) The measures set out in this Recommendation relate to infrastructure designated by a Member State as critical infrastructure, including as European critical infrastructure.

(3) When implementing this Recommendation, priority should be given to enhancing the resilience of entities operating in the sectors of energy, digital infrastructure, transport and space, and of the critical infrastructure that those entities operate that is of cross-border relevance, in respect of man-made risks.

CHAPTER II: ENHANCED PREPAREDNESS

Actions at Member State level

(4) Member States are invited to perform or update risk assessments regarding the resilience of entities operating European critical infrastructure designated in the transport and energy sectors under Directive 2008/114/EC and pursue cooperation among each other on such risk assessments and the resilience-enhancing measures resulting therefrom, as appropriate and in accordance with that Directive.

[22] Council of the European Union, 7371/22, 21 March 2022

(5) In addition, and in order to achieve a high level of resilience of entities operating critical infrastructure, Member States should accelerate preparatory work in order to transpose and apply, as soon as possible, the new CER Directive, by:

(a) speeding up the adoption of or updating national strategies for enhancing the resilience of entities operating critical infrastructure with a view to responding to the current threat. Relevant parts of this strategy should be communicated to the Commission;

(b) performing or updating risk assessments in line with the evolving nature of the current threats, as regards the resilience of entities operating critical infrastructure in relevant sectors beyond energy, digital infrastructure, transport and space, and where possible in those sectors in scope of the new CER Directive, namely, banking, financial market infrastructure, digital infrastructure, health, drinking water, wastewater, public administration, space and food production, processing and distribution, taking into account the potential hybrid nature of relevant threats, including cascading effects and the effects of climate change;

(c) informing the Commission of the types of risks identified per sector and sub-sector and the outcomes of the risk assessments, which may be done using a common reporting template developed by the Commission in cooperation with the Member States;

(d) accelerating the process of the identification and designation of critical entities, with priority as regards critical entities that:

i. use critical infrastructure, which is physically connected between two or more Member States;

ii. are part of corporate structures that are connected with, or linked to, critical entities in other Member States;

iii. have been identified as such in one Member State and provide essential services in or to six Member States or more and that are therefore of particular European significance, and inform the Commission accordingly;

(e) cooperating with each other, in particular when it comes to critical entities and essential services and critical infrastructure with cross-border relevance, notably, by engaging in consultations with each other for the purposes of point 5(d) and by informing each other in case of an incident with significant or potentially significant cross-border disruptive effect whilst keeping the Commission informed as appropriate;

(f) enhancing support for designated critical entities in order to improve their resilience, which may include providing guidance materials and methodologies, organising exercises to test their resilience and providing advice and training their personnel, as well as enabling background checks on persons with sensitive roles, in accordance with Union and national legislation, as part of employee security management measures by the critical entities;

(g) accelerate the designation or establishment of a single point of contact in the competent authority to exercise a liaison function for the purpose of ensuring cross-border cooperation relating to the resilience of entities operating critical infrastructure with the single points of contact of other Member States.

(6) Member States are encouraged to conduct stress tests of entities operating critical infrastructure. In particular, Member States are invited to advance their preparedness,

and that of the entities concerned, in the energy sector and conduct stress tests in this sector, where possible following principles commonly agreed at Union level, while ensuring effective communication with the entities concerned. Stress tests in other priority sectors, namely digital infrastructure, transport and space, where necessary, could be considered subsequently with due regard to inspections in the air and maritime sub-sectors pursuant to Union law, and taking account of relevant provisions under sectoral legislation.

(7) Member States are invited to cooperate, where appropriate and in accordance with Union law, with relevant third countries as regards the resilience of entities operating critical infrastructure with cross-border relevance.

(8) Member States are invited to make use, in accordance with the applicable requirements, of potential Union and national-level funding opportunities to enhance the resilience of entities operating critical infrastructure in the Union, including for example along trans-European networks, against the full range of significant threats, notably under the programmes financed by the Internal Security Fund and the European Regional Development Fund, subject to fulfilling the respective eligibility criteria, and the Connecting Europe Facility, including provisions on climate proofing. The Union Civil Protection Mechanism funding can also be used for that purpose, in accordance with the applicable requirements, in particular for projects related to risk assessments, investment plans or studies, capacity building or improving the knowledge base. REPowerEU may also offer possibilities for resilience funding.

(9) As regards the communications and networks infrastructure in the Union, the NIS Cooperation Group should, whilst acting in accordance with Article 11 of Directive (EU) 2016/1148 and subsequently Article 14 of the NIS2 Directive, accelerate its ongoing work on a targeted risk assessment and should present first recommendations in early 2023. 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, such as the Critical Entities Resilience Group to be established under the new CER Directive and the Oversight Forum to be established under the new Digital Operational Resilience Act (DORA)[23].

(10) The NIS Cooperation Group, which is to carry out its tasks in accordance with Article 11 of Directive (EU) 2016/1148 and subsequently Article 14 of the NIS2 Directive, is invited, with the support of the Commission and ENISA, to prioritise its work on the security of the digital infrastructure and the space sectors, including by preparing policy guidance and cybersecurity risk management methodologies and measures based on an all-hazard approach in relation to undersea communications cables, in anticipation of the entry into force of the NIS2 Directive, as well as on the development of guidance for cybersecurity risk management measures 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, notably penetration testing to identify vulnerabilities, and, in this context, are

[23] COM(2020) 595 final

encouraged to prioritise entities operating critical infrastructure in the energy, digital infrastructure and transport sectors.

(12) Member States should urgently achieve the implementation of the measures recommended in the EU Toolbox on 5G Cybersecurity[24]. Member States which have not yet enacted restrictions on high-risk suppliers should do so without further delay, considering that time lost can increase vulnerability of networks in the Union. They should 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, including legally binding requirements at Union level, in order to ensure a consistent level of security and resilience of 5G networks.

(13) Member States should implement as soon as possible the upcoming network code for cybersecurity aspects of cross-border electricity flows, building upon the experience gained with the implementation of the NIS directive and relevant guidance produced by the NIS Cooperation group especially its Reference document on security measures for Operators of Essential Services.

(14) Member States should develop the use of Galileo and/or Copernicus for surveillance and share relevant information within 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 response.

Actions at Union level

(15) The Commission intends to strengthen cooperation among Member States' experts, with a view to help enhancing the physical non-cyber resilience of entities operating critical infrastructure, notably by:

(a) preparing the development and promotion of common tools to support Member States in enhancing such resilience, including methodologies and risk scenarios.

(b) supporting the development of common principles on the conduct of the stress tests referred to in point 6 by Member States, starting with such tests focusing on man-made risks in the energy sector and subsequently in other key sectors, such as digital infrastructure transport and space; addressing other significant risks and hazards; as well as, where relevant, supporting and advising on the conduct of such stress tests.

(c) providing a secure platform to collect, take stock and share best practices, lessons learnt from national experiences and other information relating to such resilience, including on conducting those stress tests and translating the results thereof into protocols and contingency plans.

The work of those experts should pay particular attention to cross-sectoral dependencies and entities operating critical infrastructure with cross-border relevance, and should be continued by the Critical Entities Resilience Group once established.

(16) Member States should fully participate in the strengthened cooperation referred to in point 15, including by nominating contact points with relevant expertise and by sharing experience on methodologies used for the stress tests and protocols and

[24] 5g_eu_toolbox_72D70AC7-A9E7-D11D-BE17B0ED8A49D864_64468.pdf

contingency plans developed on the basis thereof. 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. This does not entail the supply of information the disclosure of which is contrary to the Member States' essential interests of national security, public security or defence.

(17) The Commission will support Member States by providing manuals and guidelines such as the preparation of 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, is invited to conduct briefings on the threats to critical infrastructure in the EU in order to improve situational awareness.

(18) The Commission will support the uptake of results of projects on the resilience of entities operating critical infrastructure funded under the Union research and innovation programmes. The Commission intends to increase, within the budget allocated to Horizon Europe under the 2021-2027 multiannual financial framework, funding on such resilience. This should allow current and future challenges in this area to be addressed, such as climate proofing of critical infrastructure, without detriment to the funding of the other civil security-related research and innovation funding under Horizon Europe. The Commission will also increase its efforts to disseminate results of relevant Union-funded research projects.

(19) The NIS Cooperation Group, in cooperation with the Commission and the High Representative, is invited to intensify, in accordance with their respective tasks and responsibilities under Union law, the work with relevant networks and civil and military bodies in conducting risk assessment and building cybersecurity risk scenarios with an initial focus on energy, communications transport and space infrastructure and the interdependencies across sectors and Member States. This exercise should take into account the related risks to physical infrastructure on which these sectors rely. The risk assessments and scenarios should be carried out on a regular basis and should complement, build on and avoid duplication with existing or planned risk assessments in these sectors and inform discussions on how to strengthen overall resilience of entities operating critical infrastructure and to address vulnerabilities.

(20) The Commission will accelerate its activities on supporting preparedness of Member States and response to the large-scale cybersecurity incidents, and notably:

(a) carry out, in complement to relevant risk assessments in the context of Network and Information Security, a comprehensive study taking stock of the subsea cable infrastructure that connects Member States and that connects Europe globally, including a mapping, its capacities and redundancies, vulnerabilities, risks for service availability and risk mitigation. The findings should be shared with Member States.

(b) support preparedness of Member States and EU institutions, bodies and agencies' (EUIBA) response to large-scale cybersecurity incidents.

(21) The Commission will intensify work on forward-looking anticipatory action, including under the UCPM, in 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 operational preparedness.

In particular, the Commission will engage as follows:

(a) further work in the Emergency Response Coordination Centre on anticipation and cross-sectoral prevention, preparedness and response planning to anticipate and prepare for disruptions of the provision of essential services by entities operating critical infrastructure;

(b) increase investments in preventative approaches and population preparedness in the event of such disruptions, with a particular focus on chemical biological radiological nuclear-explosives agents or other emerging man-made threats;

(c) reinforce the exchange of relevant knowledge, best practices, and improve the design and conduct of capacity development activities, such as training courses and exercises with the entities operating critical infrastructure, via existing structures and expertise, such as the Union Civil Protection Knowledge Network.

(22) The Commission will foster the use of EU surveillance assets (Copernicus and Galileo) 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.

(23) 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 entities operating critical infrastructure, notably for example as follows:

(a) EUROPOL on information gathering, criminal analysis and investigative support in cross-border law enforcement actions;

(b) 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) EUSPA as regards activities within the Union's space programme;

(d) ENISA as regards activities related to cybersecurity.

CHAPTER III: ENHANCED RESPONSE

Actions at Member State level

(24) Member States should:

(a) coordinate their response and maintain the overview of the cross-sectoral response to significant disruptions of the provision of essential services by entities operating critical infrastructure in the framework of the Council's crisis mechanism (IPCR) when it comes to critical infrastructure with cross-border relevance, the Blueprint on large-scale cybersecurity incidents and crises or in the Framework for a coordinated EU response to hybrid campaigns in the case of a hybrid campaign;

(b) increase information exchange within the Union Civil Protection Mechanism in order to enhance early warning and coordinate their response under the Mechanism in the event of such significant disruptions, thus ensuring a faster Union-facilitated reaction when needed;

(c) increase their readiness to respond via the Union Civil Protection Mechanism to such significant disruptions, in particular where they are likely to have significant cross-border or even pan-European, as well as cross-sectorial, implications;

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

(e) invite entities operating critical infrastructure and relevant national authorities to enhance the capacity of those entities to quickly restore a basic performance of the essential services provided;

(f) ensure that, when rebuilding critical infrastructure is necessary, such rebuilt infrastructure will be resilient to the full range of significant risks that may apply to it, including in adverse climate scenarios.

(25) Member States are invited to accelerate preparatory work for the transposition and application of the NIS2 Directive, by starting immediately to enhance the national Computer Security Incident Response Teams (CSIRTs) capabilities, in view of the new tasks of CSIRTs as well as the enlarged number of entities from new sectors, swiftly updating their cybersecurity strategies and adopting as soon as possible national cybersecurity incident and crisis response plans.

Actions at Union level

(26) Response to significant disruptions of the provision of essential services by entities operating critical infrastructure should be coordinated among Member State experts as regards the resilience of those entities and the responses to such disruptions that may contribute to the workings of the Council's crisis mechanism (IPCR).

(27) The Commission will work closely together with the Member States to further develop deployable emergency response capacities, including experts and rescEU stockpiles under the UCPM, with a view to enhancing operational preparedness to address the immediate and indirect effects of significant disruptions of the provision of essential services by entities operating critical infrastructure.

(28) Taking into account the evolving risk landscape and in cooperation with Member States, the Commission will in the context of UCPM:

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

(b) regularly review the potential need to develop new response capacities at the EU level through rescEU;

(c) further intensify cross-sectoral collaboration to ensure adequate response at the EU level, and organise regular exercises to test this collaboration;

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

(29) The Commission, in cooperation with the High Representative, and in close consultation with Member States and with the support of relevant Union agencies, will develop a Blueprint on critical infrastructure incidents and crises that describes and sets out the objectives and modes of cooperation between the Member States and EU institutions, bodies, offices and agencies in responding to incidents against critical infrastructure, in particular where these entail significant disruptions of the provision of essential services for the internal market. This Blueprint should make use of the existing Integrated Political Crisis Response (IPCR) arrangements for the coordination of the response.

(30) The Commission will work with stakeholders and experts on possible incident recovery measures regarding undersea cables 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 work on Union disaster resilience under the Union Civil Protection Mechanism.

CHAPTER IV: INTERNATIONAL COOPERATION

(31) The Commission and the High Representative will support, where appropriate and in accordance with their respective tasks and responsibilities under Union law, partner countries to enhance the resilience of entities operating critical infrastructure in their territory.

(32) 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 through the EU-NATO structured dialogue on resilience and will set up a Task Force for this purpose.

(33) 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 on a Framework for a coordinated EU response to hybrid campaigns[25] and subsequently use them, in order to give a full effect to the Framework for a coordinated EU response to hybrid campaigns in particular when considering and preparing comprehensive and coordinated EU responses to hybrid campaigns and hybrid threats, including those against entities operating critical infrastructure.

(34) The Commission will consider the participation of representatives of third countries where relevant and appropriate in the framework of the cooperation and information exchange between Member States' experts in the area of resilience of entities operating critical infrastructure.

[…]

Done at Strasbourg,

For the Council
The President

[25] Council conclusions on a Framework for a coordinated EU response to hybrid campaigns - Consilium (europa.eu)