EMERGENCY COMMUNICATIONS AS CRITICAL INFRASTRUCTURE IN EUROPE

May 2026

REPORT: Emergency Communications as Critical Infrastructure in Europe

Version: 1.0
Publication date: 19/05/2026
Status of the document: FINAL

European Emergency Number Association
EENA
Avenue de la Toison d'Or 79, Brussels, Belgium
T: +32/2.534.97.89
E-mail: info@eena.org

Author:

Maxime MIALON
(Advocacy Intern - EENA)

Contributors:

Benoît VIVIER
(Public Affairs Director - EENA)

Cristina LUMBRERAS
(Technical Director - EENA)

Peter LONERGAN
(Senior Policy Officer - EENA)

Liana MUSAT
(Knowledge Officer – EENA)

Table of contents

Executive summary

This paper aims to produce a comprehensive report on emergency communications as critical infrastructure and reveal the major legal, security and strategic implications this entails in Europe. It looks at EU frameworks around critical infrastructure, especially the CER and the NIS-2 Directives, and their impact on emergency communications systems. This includes focusing on PSAPs, providers of communication networks and services, supporting ICT infrastructures and interconnected sectors. The report intends to clarify whether and under which conditions emergency communications and related actors fall under critical infrastructure or essential entity regimes. It further analyses the impact of future EU legislation, such as the Cybersecurity Act 2 and the Digital Networks Act on the resilience of emergency communications. Moreover, it explores the broader security and resilience ecosystem, including NATO's perspective on critical infrastructure protection, resilience, and civil-military coordination, where relevant to emergency communications. This report also compares national transpositions and interpretations in six EU Member States to identify divergences, best practices, and open issues. It further examines interdependencies between emergency communications and other critical sectors such as telecoms, energy, cloud, data centres and public administrations. Finally, this paper underlines policy gaps, risks and unintended consequences, building on critical entities and national authorities' feedback.

Purpose of the document

- To analyse the EU framework and NATO's perspective on the European critical infrastructure resilience and cybersecurity.
- To understand how emergency communications fit in the EU critical infrastructure.
- To conduct a survey with emergency communications related entities and relevant national authorities to identify best practices and challenges.

List of acronyms

BEREC – Body of European Regulator for Electronic Communications
CER – Critical Entities Resilience
CERT – Computer Emergency Response Team
CSA – Cybersecurity Act
CSIRT – Computer Security Incident Response Team
DNA – Digital Networks Act
ECSF – European Cybersecurity Skills Framework
EECC – European Electronic Communications Code
ENISA – European Network and Information Security Agency (*currently European Union Agency for cybersecurity*)
EUDI – European Digital Identity
ICT – Information and Communication Technology
MNO – Mobile Network Operator
NCSS – National Cybersecurity Strategy
NIS – Network and Information Systems
ODN – Office for Digital Networks
PSAP – Public Safety Answering Point
SPOC – Single Point of Contact

I – Introduction

The critical infrastructure is the backbone of a society's proper functioning. Therefore, its protection and its ability to remain functional when facing threats are highly important. This report focuses on three main frameworks related to emergency communications as critical infrastructure: the European level, the national level, and the NATO level. This introductory part gives the definitions of the main concepts used in this report, and presents the structure, the scope and the methodology adopted to conduct this research.

1.1 – The emergency communication ecosystem

Emergency communications

The protection of citizens depends on the State's ability to organise emergency services effectively. This is made possible through stable and efficient emergency communications. Existing EU rules on emergency communications are set by the European Electronic Communications Code (EECC) which defines "emergency communication" as a "communication by means of interpersonal communications services between an end-user and the PSAP (Public Safety Answering Point) with the goal to request and receive emergency relief from emergency services"[1]. A PSAP is a physical location where emergency communications are received under the responsibility of a public authority or an organisation recognised by the State[2].

The EECC would be repealed by the Digital Networks Act (DNA), if adopted as a regulation. This new proposal would enhance the EU's ability to overcome several challenges affecting emergency communications such as implementing new communication technologies, deploying mobile-based public warning systems and improving the overall resilience and effectiveness of emergency communications during crises.

Critical infrastructure

The Critical Entities Resilience (CER) Directive defines the critical infrastructure as "an asset, a facility, equipment, a network or a system, or a part of an asset, a facility, equipment, a network or a system, which is necessary for the provision of an essential service".[3] Fundamentally, a critical

[1] DIRECTIVE (EU) 2018/1972 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 December 2018 establishing the European Electronic Communications Code, Art.2 (38)
[2] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on digital networks, amending Regulation (EU) 2015/2120, Directive 2002/58/EC and Decision No 676/2002/EC and repealing Regulation (EU) 2018/1971, Directive (EU) 2018/1972 and Decision No 243/2012/EU, part 1, Art.2 (37)
[3] DIRECTIVE (EU) 2022/2557 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, Art.2(4)

infrastructure includes physical and digital systems that are essential for a country to function. If these systems fail or are destroyed, they can seriously harm security, the economy, or public safety. The infrastructure considered as "critical" usually covers several sectors that are linked to vital areas such as public safety and public welfare[4].

Furthermore, related risks worsen as critical infrastructure disruption might spread globally. The ongoing digitalisation of many sectors such as energy, transports, and public services, also increases, for example, the exposure to cyberattacks[5] or blackouts affecting interconnected electricity systems, as seen in Spain and Portugal[6]. In a continually interconnected international system, cyberattacks causing power supply disruptions or internet shutdowns may propagate and extensively impact goods, people's lives, information and intelligence sharing across multiple countries.

Resilience

From a military standpoint, "resilience" means for a State to maintain and develop capacities to resist an armed attack[7]. When it comes to protecting the critical infrastructure, resilience entails both crisis preparedness and recovery. The CER Directive defines it as the "ability to prevent, protect against, respond to, resist, mitigate, absorb, accommodate and recover from an incident"[8]. It encompasses multiple concepts such as operational continuity in the long run, and the ability to face and overcome a threat quickly, for the sake of citizens' well-being.

Regarding emergency communications, resilience means being able to maintain functional communications between citizens and emergency services. It also means for a State to be prepared to face multifaceted threats and prevent communication systems from failing.

1.2 – Scope and methodology

To adopt a limited comparative approach, this report analyses the resilience and the cybersecurity frameworks of six EU Member States to assess their impact on emergency communications as critical infrastructure.

France's emergency communications follow a model 1 PSAP [9], where each department has its own PSAP that answers emergency calls and then dispatches relevant emergency services. The main threats France has faced include terrorism, cyberattacks, floods and heatwaves.

[4] SLAKAITYTE, Veronika, and SURWILLO, Izabela, «PROTECTING EU'S CRITICAL INFRASTRUCTURE The fight intensifies in the cyber realm», Danish Institute for International Studies, 2024, p. 3
[5] PARKES, Roderick, «NUTS AND BOLTS», *PROTECTING EUROPE: The EU's response to hybrid threats*, 2019, p.23
[6] Cf., Iberian Peninsula blackout of 28 April 2025
[7] NORTH ATLANTIC TREATY (NATO) OF THE NORTH ATLANTIC ALLIANCE ORGANISATION of 4 April 1949, Art. 3
[8] DIRECTIVE (EU) 2022/2557 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, Art.2(2)
[9] EENA (website) Emergency call handling service chain description (consulted on 5 May, 2026) - https://eena.org/wp-content/uploads/2020/12/2020_12_08_ServiceChainV2.1.pdf, p.11

Romania follows a model 3 PSAP[10]. Geographically, it is exposed to several natural risks, especially earthquakes, floods, and severe weather[11]. The country faces geopolitical threats with the war in Ukraine. The Special Telecommunications Service (STS) is the administrator of the national 112 emergency call system. It operates under the authority of the Romanian Government and is organised as a structure that is part of national defence.

Hungary is mainly exposed to regional flooding and hybrid security risks. Like Romania, it also faces geopolitical risks due to its location close to the ongoing conflict in neighbouring Ukraine. It uses a model 3 PSAP with centralised 112 call centres forwarding calls to emergency services.

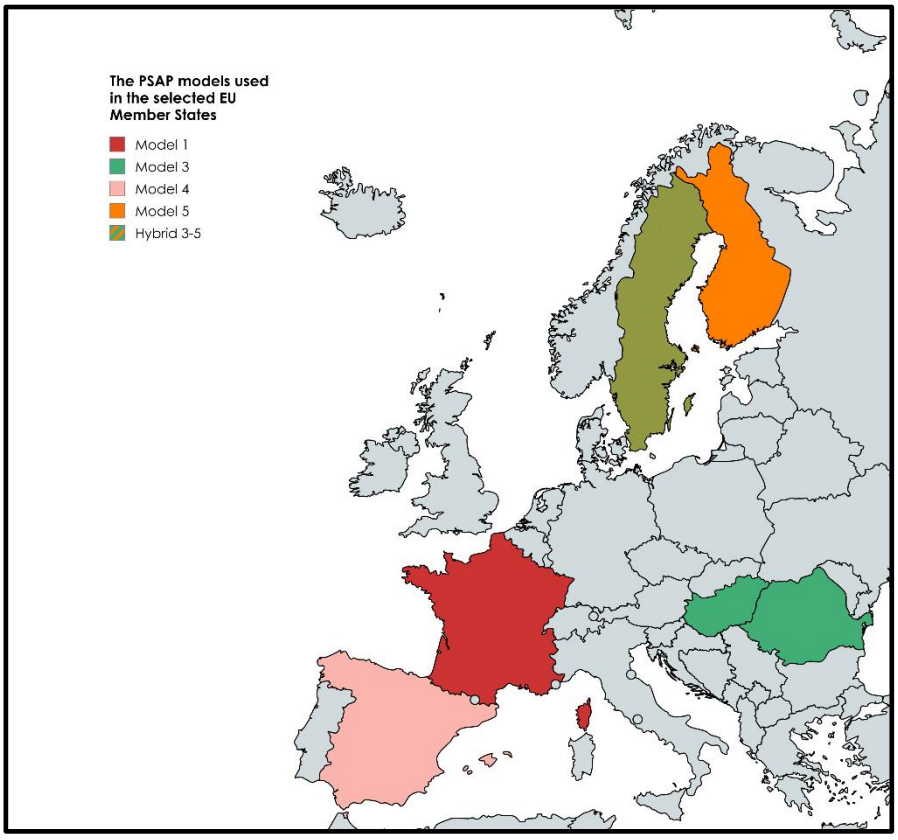
Finland follows a decentralised administrative system. It is directly exposed to geopolitical risks due to its border with the Russian Federation and places strong emphasis on national resilience and preparedness. To that extent, military and cyber threats are major concerns. While natural disasters are rather rare, wildfires or ice-related disruptions do occur. Finland operates a model 5 PSAP[12] with integrated regional emergency centres.

Sweden faces risks from floods, winter storms and wildfires, in addition to increasing security efforts since the war in Ukraine and the country's accession to NATO. The country uses a hybrid model 3-5 PSAP, with a national organisation (SOS Alarm) handling 112 emergency calls. Sweden follows a governance structure similar to Finland, with regions enjoying a relative level of autonomy to handle emergency communications.

Spain follows a decentralised regional political structure. It is highly exposed to natural disasters such as floods, wildfires and heatwaves. Spain mostly operates a model 4 PSAP[13], but this may vary from one region to another. Emergency communications fall under regional civil protection authorities, which shape differences in implementation processes across the country.

[10] EENA (website) Emergency call handling service chain description (consulted on 5 May, 2026) - https://eena.org/wp-content/uploads/2020/12/2020_12_08_ServiceChainV2.1.pdf, p. 15
[11] World Bank (website) Climate Change Knowledge Portal, *Global distribution of natural disasters* (consulted on May 15 2026) https://climateknowledgeportal.worldbank.org/country/romania/natural-disasters-historical
[12] EENA (website) Emergency call handling service chain description (consulted on 5 May, 2026) - https://eena.org/wp-content/uploads/2020/12/2020_12_08_ServiceChainV2.1.pdf, p. 18
[13] *Ibid*., p. 17

Figure 1 – PSAP models used by the selected EU Member States



Methodology: comparative approach

Part VI is based on a survey questionnaire that has been sent to various key actors, such as PSAPs, Mobile Network Operators (MNOs) and national cybersecurity authorities. The six EU Member States analysed in part IV are not necessarily the only ones that responded to our survey.

France, Sweden, Hungary, Spain, Romania and Finland were selected based on specific parameters that may influence differing approaches to the management of emergency communications as critical infrastructure. These selection parameters are:

- the geopolitical environment
- the geographical location in Europe
- the exposure to natural disasters and man-made threats
- the PSAP model used

II - Emergency Communications: qualification and resilience across the EU, NATO and beyond

2.1 – Definitions: "critical, essential, or important entities" and "essential services"

This subsection introduces the EU legislation and the following key concepts: "critical entities", "essential entities", "important entities", and "essential services".

The EU Directive 2022/2557 on Critical Entities and Resilience (CER) Directive entered into force in 2023. In its own words, it mainly aims at "harmonising minimum rules to ensure the provision of essential services in the internal market, to enhance the resilience of critical entities and to improve cross-border cooperation between competent authorities."[14] The CER Directive "lays down obligations on Member States to take specific measures aimed at ensuring that services which are essential for the maintenance of vital societal functions […] are provided in an unobstructed manner in the internal market, in particular obligations to identify critical entities and to support critical entities in meeting the obligations imposed on them". In all, the CER Directive lays down obligations for critical entities aimed at enhancing their resilience and ability to provide essential services.[15] EU Member States already manage their own critical infrastructure, but due to the cross-border impacts of some critical infrastructure, there is a need for all Member States to ensure that certain categories of entities are evenly considered and protected as critical infrastructure. Therefore, the CER Directive sets a common baseline for resilience in these categories. Member States have and should have additional categories of critical infrastructure.

The EU Directive 2022/2555 on Network and Information Systems (NIS-2) Directive entered into force in 2023. The NIS-2 Directive continues and strengthens the cybersecurity framework established by the 2016 NIS Directive. It enhances a framework to build cybersecurity capabilities across the Union, mitigate threats to networks and information systems used to provide essential services in critical sectors. In its own words, the NIS-2 Directive "lays down measures that aim to achieve a high common level of cybersecurity across the Union […]".[16] By setting harmonised minimum rules, the EU ensures that a failure in one State does not create cascading effects across the Union.

One should keep in mind that both the NIS-2 and the CER Directives establish a baseline of specific sectors

[14] DIRECTIVE (EU) 2022/2557 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, recital §7
[15] *Ibid.*, recital 1
[16] DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures aimed at ensuring a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148, Art. 1(1)

and categories of entities that all Member States must at least cover. Member States can then decide what other entities they want to include based on their specific needs. In other words, the Directives do not prevent the Member States from achieving a higher level of resilience and cybersecurity, rather they ensure the setting of a minimum harmonisation principle[17].

The Cybersecurity Act 2 (CSA-2) is a 2026 European Commission regulation proposal that would update and repeal the 2019 Cybersecurity Act. It would strengthen the EU cybersecurity certification scheme and ICT supply-chain security, and simplify compliance with the NIS-2 Directive. This draft legislation is relevant to introduce the potential future obligations and legal requirements concerning cybersecurity at the EU level for emergency communications entities.

As already mentioned, if adopted, the Digital Networks Act would be the main legislation regarding emergency communications. Its obligations would therefore apply to related entities, whose resilience is currently covered by the EECC and the CER Directive. The DNA's perspective on resilience is further analysed in section 3.2.

The NIS-2 and CER Directives serve as the twin pillars of the EU's resilience framework, while the CSA-2 proposal, if adopted, would be the newest text designed to modernise, harmonise and ensure cybersecurity rules. Once adopted, the DNA would be the main mandatory framework governing digital infrastructure and electronic communications.

Critical entities and essential services

Critical entities are defined in the CER Directive[18] as providers of "essential services" handling the critical infrastructure. They are the core units in the maintenance of vital societal functions, whose disruption would cause significant, sometimes cross-border, harm to society and public safety. Thus, "essential services" are considered outputs of critical entities. The CER Directive defines a critical entity as a "public or private entity which has been identified by a Member State […]"[19].

Critical entities are expected to be resilient. The text stresses that "critical entities should be in a position to reinforce their ability to prevent, protect against, respond to, resist, mitigate, absorb, accommodate and recover from incidents that have the potential to disrupt the provision of essential services".[20]

Finally, while the Directives may exclude certain entities from their scope to avoid legal duplication, the

[17] DIRECTIVE (EU) 2022/2557 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, Art. 3 - DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures aimed at ensuring a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148, Art. 5

[18] DIRECTIVE (EU) 2022/2557 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, Art. 1

[19] *Ibid*., Art.2(1)

[20] *Ibid*., recital 2

Member State remains the ultimate authority in determining what is critical for its own territory[21]. Uneven management frameworks of critical entities across Member States have effects on how the EU protects its critical infrastructure as a whole, as diverging security requirements create various levels of resilience.[22]

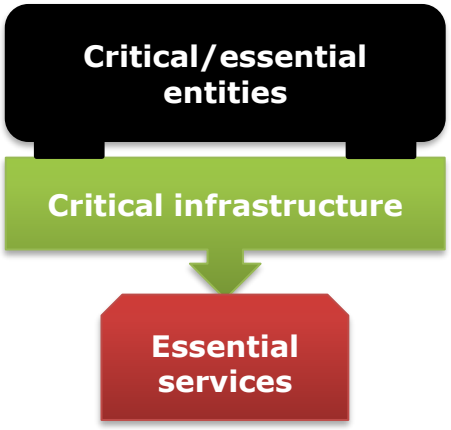
Critical entities and essential entities

The NIS-2 Directive follows the CER Directive by using the same definition of critical entities, adding a typological nuance: "entities identified as critical entities under Directive (EU) 2022/2557 (CER) should be considered to be essential entities under this Directive"[23], thus ensuring coherence between cyber and physical security. The term "essential" refers to a category of entities subject to the highest level of cybersecurity obligations and supervision. An entity's classification as "essential" is generally based on its size in high-criticality sectors, or the specific nature of the service it delivers.

Essential entities and important entities

The NIS-2 Directive distinguishes three different types of entities: "essential entities", "important entities", and "entities providing domain name registration services". As mentioned above, the difference between essential and important entities mostly lies in their size. This also mirrors the degree of impact their disruption could cause and the subsequent legal regime applied to them[24].
To sum up, the basic figure below illustrates how critical entities rely on the critical infrastructure, encompassing the physical or digital assets, to deliver essential services to society.

Figure 2 - The critical infrastructure pattern

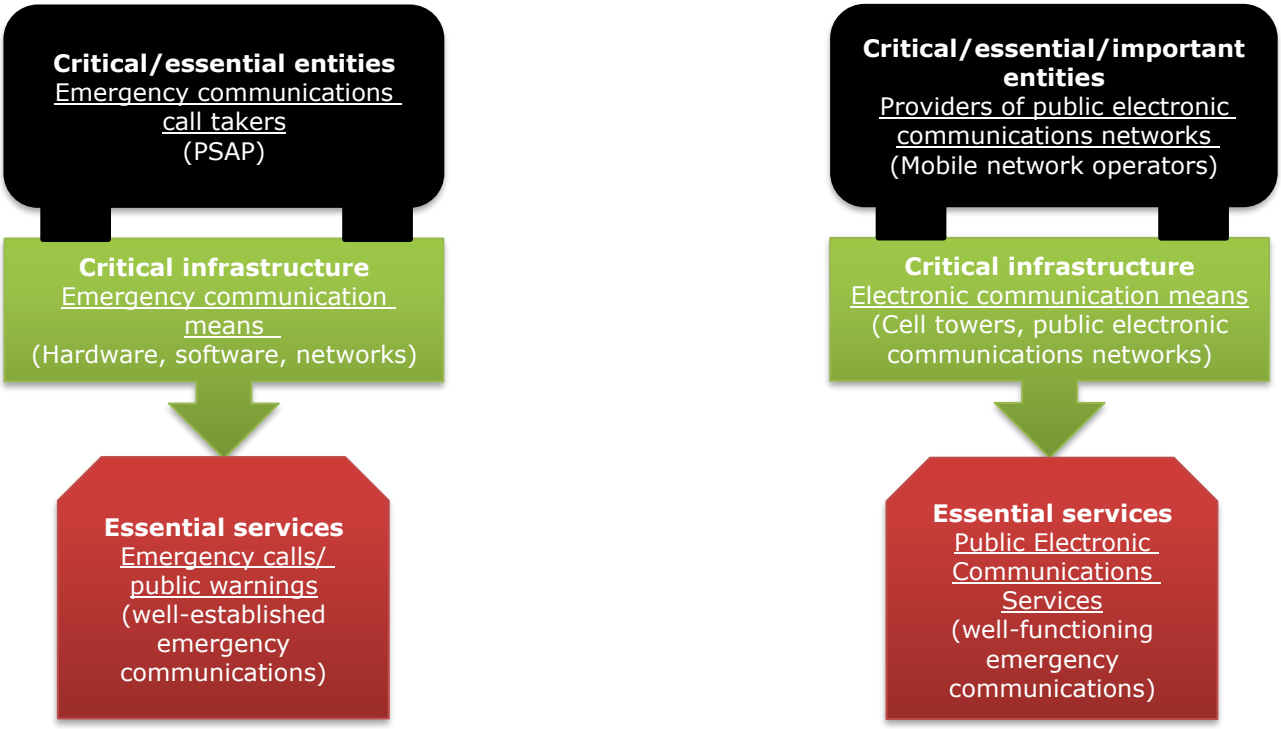


[21] DIRECTIVE (EU) 2022/2557 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, Art. 1(7)
[22] *Ibid*., recital 6
[23] DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures aimed at ensuring a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148, recital 1
[24] *Ibid*., Art. 3 (1-2)

2.2 – Positioning emergency communications within critical infrastructure frameworks

"Emergency communications" as such are not explicitly considered as critical infrastructure under EU law. However, the infrastructure they rely on is clearly identified as critical (e.g. public electronic communications networks). The entities managing this infrastructure are considered as critical (e.g. providers of public electronic communications networks). One may identify emergency communications as the essential service provided by a critical entity in the form of a well-established and functioning connection between an end-user and the emergency services.

Figure 3 - How emergency communications can fit in the critical infrastructure pattern



The figure above reveals interdependencies between critical sectors. For instance, the essential services provided by mobile network operators (MNOs), form part of the critical infrastructure that Public Safety Answering points (PSAPs) depend on to deliver their own essential services to society. Thus, the successful provision of one essential service by any critical entity is necessary for all the others to manage the delivery of their own.

Classification of emergency communications as critical infrastructure

Both the NIS-2 and the CER Directives classify the infrastructure emergency communications rely on as critical.

The Directives establish a list of sectors[25], each containing several critical entities which support the work of PSAPs. Providers of public electronic communications networks and providers of publicly available electronic communications services are explicitly classified as critical entities within the Digital Infrastructure sector in both Directives[26]. Information and Communication Technology (ICT) is also identified as a key infrastructure that needs special protection[27], while Network and information systems (NIS), understood as the basis of the Digital Infrastructure, are included in risk-management measures[28].

The "size" of an entity is also a primary parameter used to determine how strictly an organisation is regulated. The CER Directive notes that "critical entities" qualification may include small or medium-sized enterprises[29]. The NIS-2 Directive distinction between "essential" and "important" entities introduces the size cap rule. According to this rule, entities exceeding the ceilings for medium-sized enterprises are considered essential entities, while important entities are those considered smaller[30]. However, the NIS-2 Directive adds that if a disruption of the essential service provided by the entity has a significant impact on public safety, public security or public health, then the entity qualifies as essential.

Do PSAPs qualify as public administration entities under the EU Directives?

While both the CER and the NIS-2 Directives classify public administration entities of central governments as a category of critical entities, PSAPs do not appear to fall within their scope.
For an organisation to be classified as a public administration entity the CER Directive sets four cumulative criteria: to serve the general interest, have a legal personality (or act on behalf of one), be controlled or funded by the State[31], and have regulatory or administrative powers affecting cross-border movement of persons, goods, services or capital[32]. PSAPs do not appear to meet the final criterion, meaning they cannot be considered as a public administration entity under the CER Directive. However, this exclusion may not

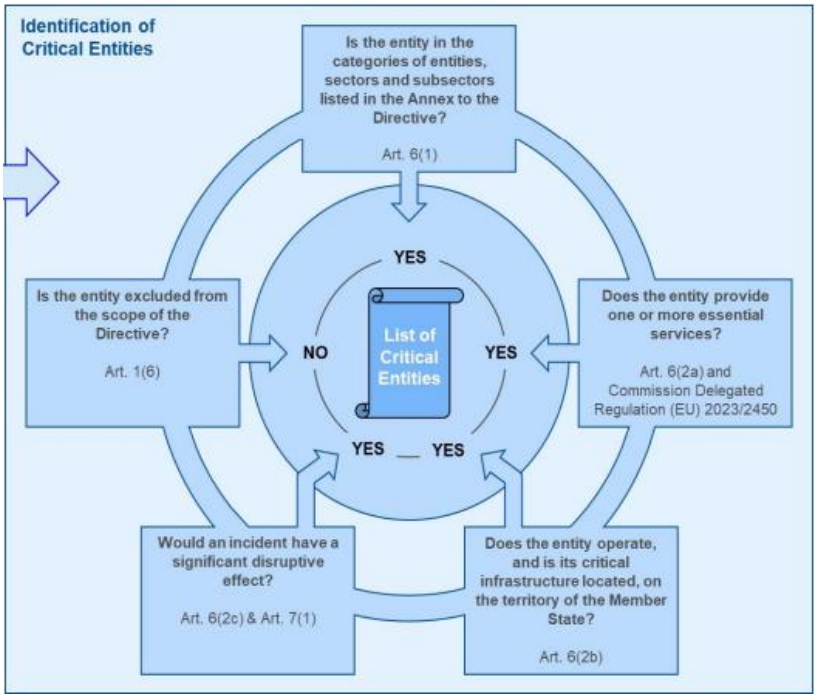
[25] See part V
[26] DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures aimed at ensuring a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148, Annex SECTORS, SUBSECTORS AND CATEGORIES OF ENTITIES (8) and Art.3(1) - DIRECTIVE (EU) 2022/2557 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, Annex (8)
[27] DIRECTIVE (EU) 2022/2557 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, recital 21
[28] DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures aimed at ensuring a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148, recital 31
[29] DIRECTIVE (EU) 2022/2557 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, recital 25
[30] DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures aimed at ensuring a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148, Art. 3 (1(a) – 2)
[31] DIRECTIVE (EU) 2022/2557 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, Art. 6 (2, c)
[32] *Ibid*., Art. 2(10)

be systematic across the whole Union, as some Member States seem to include PSAPs within public authorities that do have regulatory or administrative powers affecting cross-border movement. In other cases, PSAPs may also act on behalf of such authorities, which could influence their classification. PSAPs' legal classification as critical public administration entities may therefore appear legally ambiguous or inconsistent in practice.

In addition, the CER and NIS-2 Directives also exclude entities which predominantly carry out activities in the area of national or public security, or law enforcement, including the detection of criminal offences, from the scope of public administration entities, thereby removing PSAPs from their scope. Following discussions with ENISA, they also underlined that PSAPs would be outside the scope of the NIS-2 Directive and are generally supervised by national regulatory authorities.

2.3 - The European Commission guidelines for identifying critical entities

Figure 4 – Commission's criteria for critical entities identification



The lists of critical entities made by EU Member States are commonly kept secret. However, thanks to the guidelines developed by the European Commission[33], it is possible to know if an organisation most likely qualifies as a critical entity if it meets five requirements. While PSAPs appear as being excluded from the scope of this Directive, it gives insights into deciding if another entity related to emergency communications could be a "critical entity" under EU law.

[33] COMMUNICATION FROM THE EUROPEAN COMMISSION (2025), Commission Guidelines and reporting template developed pursuant to Articles 5(5), 6(6) and 7(3) of Directive (EU) 2022/2557 on the resilience of critical entities

How do mobile network operators qualify in the EU frameworks?

Both fixed and mobile network operators fall within the scope of the CER and NIS-2 Directives if the networks they operate are public. Public Electronic Communications Networks are defined as critical entities being part of the Digital Infrastructure[34]. The NIS-2 Directive identifies "providers of mobile electronic communications networks" as operators of highly critical infrastructure[35]. Even though MNOs are considered as critical entities under the CER, rules for these entities are exclusively covered by the NIS-2 Directive, which already imposes security requirements, in order to avoid legal duplication[36].

In other words, providers of public electronic communications networks and services are listed within the digital infrastructure sector and are clearly within the NIS-2 framework. The CER Directive remains relevant to the broader resilience framework, but active obligations for these entities are largely managed through the NIS-2 Directive. Their classification as either important or essential entities will depend on their size[37]. But even if they follow different supervisory regimes, MNOs must meet the NIS-2 requirements[38].

CER/NIS-2/CSA-2: classification of the emergency communications ecosystem

COMPONENT	CRITICAL SECTOR	KEY FUNCTION	CLASSIFY AS	MENTION
Public safety Answering Point (PSAP)	Not explicitly covered at EU level but may be covered at national level as public administration/…	Communicate with the end-user/dispatch first responders	Not explicitly covered at EU Directive level but may be covered by national implementation or through public administration/civil protection frameworks	None
PSAP Software	Digital Infrastructure	Enable the connection made by the end-user to the PSAP/reach the first responders	Relevant critical component/supporting service depending on national designation and legal basis	Covered as ICT products and services Recital 21 CER/ Art. 7(2) NIS-2
Providers of public electronic communications networks (MNOs)	Digital infrastructure	Monitor the access to the networks used by end-users and PSAPs	Critical/Essential/Important entities	Annex (8) CER/Annex I(8) NIS-2/Art. 117(1, a) CSA-2

[34] DIRECTIVE (EU) 2022/2557 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, Annex (8)
[35] DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures aimed at ensuring a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148, Annex I (8)
[36] DIRECTIVE (EU) 2022/2557 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, recital 20
[37] DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures aimed at ensuring a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148, Art. 3(1), c
[38] *Ibid*., Art. 2(2), a(i)

Electronic communication services	Digital Infrastructure	Internet access services, transmission of international communications and signals	Relevant critical component/supporting service depending on national designation and legal basis	Annex (8) CER/Annex I(8) NIS-2
NIICS (Number-Independent Interpersonal Communications Services)	Digital infrastructure	Enable communication through a number-independent interpersonal communication service (e.g. Snapchat, Facebook Messenger)	Infrastructure "of growing importance"	Recital 96 NIS-2
NBICS (Number-Based Interpersonal Communications Services)	Digital infrastructure	Enable communication through a number-based interpersonal communication service (e.g. phone number)	Relevant critical component/supporting service depending on national designation and legal basis	Recital 96 NIS-2
ICT (Information and Communication Technologies)	Digital infrastructure	Products, Services and processes enabling the Digital Infrastructure and secured systems required for real-time coordination, data sharing, and the maintenance of services essential for public safety and societal stability	Relevant critical component/supporting service depending on national designation and legal basis	Recital 21 CER/ Art. 7(2) NIS-2
Satellites	Space	Provide critical transmission infrastructure and space-based services for navigation and hazard monitoring that underpin resilient emergency communications	Relevant critical component/supporting service depending on national designation and legal basis	Chapter II CSA-2
Undersea communications cables	Digital infrastructure	Cross-border international communications and coordination.	Relevant critical component/supporting service depending on national designation and legal basis	Recital 97 + Art.7(2, d) NIS-2

Publicly available electronic communications networks	Digital infrastructure	Provide reliable ultra-fast connectivity and data transportation	Critical infrastructure	Annex (8) CER/Annex I(8) NIS-2/Art. 117(1, a) CSA-2
Electricity undertakings	Energy	Produce and distribute power to all kinds of end-users and enable the functioning of the digital infrastructure	Critical entities	Annex I (a) CER/Annex I (1, a) NIS-2

2.4 – NATO's perspective on critical infrastructure protection, resilience, and civil-military coordination

Given NATO's growing focus and recent investments in civil resilience and critical infrastructure protection, examining the Alliance's approach is particularly relevant to the resilience of emergency communications in Europe. In recent years, NATO has strengthened its work on the protection of critical infrastructure, including against cyber threats, hybrid operations and the disruption of essential civilian services. This section therefore analyses how NATO addresses critical infrastructure protection, resilience and civil-military cooperation, identifies the key NATO actors involved, and explores potential areas for EU–NATO cooperation to enhance the resilience of emergency communications against cyber and physical threats.

NATO's resilience framework and critical infrastructure protection

All NATO Member States are expected to be resilient to both military and non-military threats, including natural disasters, disruptions to critical infrastructure, and cyber or armed attacks. Resilience is both a national responsibility and a shared commitment based on Article 3 of the North Atlantic Treaty.

Although NATO's first conception of resilience is linked to resisting an armed attack, it may also combine both civil preparedness and military capabilities[39].

In its 2025 declaration in the Hague, the Alliance asked its members to invest 5% of Gross Domestic Product (GDP) annually on defence spending by 2035. While 3.5% is allocated to core defence requirements, 1.5% of GDP is invested to protect the critical infrastructure and to ensure civil preparedness and resilience[40]. NATO does not explicitly mention emergency communications as part of this civil resilience fund, nevertheless the 1.5% aims to defend the critical infrastructure and networks they rely on. These investments could indirectly benefit the infrastructure on which PSAPs depend, but NATO does not specify emergency communications or PSAPs as a dedicated category.

[39] European centre of excellence for civilian crisis management (website) (consulted on February 27, 2026)
[40] (NATO) Funding NATO, https://www.nato.int/en/what-we-do/introduction-to-nato/funding-nato

NATO identifies resilience as essential to ensure that States' critical infrastructure serves three core national functions: the continuity of government, the delivery of essential services for the population, and civil support for military operations. Through the 2016 Warsaw Summit, Allies committed to rebuilding these civil-military foundations to ensure they can withstand modern hybrid threats and strategic shocks[41]. At this summit, heads of State and Government agreed on "The Seven Baseline Requirements for National Resilience"[42] with guidelines and evaluation criteria that Allied Nations could use to conduct national resilience assessments and improve preparedness. New collective resilience objectives were agreed by Allies at the Vilnius Summit in 2023 to strengthen the Alliance's existing Resilience Commitment.

NATO's main actors relevant to emergency communications

One should keep in mind that there are no NATO bodies legislating, neither overseeing, EU emergency number 112. In this context, no NATO actors set standards for PSAPs working conditions, or have the authority over Member States' emergency services. Nevertheless, important NATO intergovernmental bodies can indirectly influence, or sometimes even assist, emergency communications and services.

Among these bodies, the Resilience Committee (RC), established in 2022, is NATO's main senior advisory body on resilience and civil preparedness. It decides NATO's priorities for resilience and turns them into practical actions and guidance. The RC reports to NATO's main decision-making body and helps countries plan, review, and improve their critical infrastructure's resilience. It promotes cooperation across governments and society, works with NATO military authorities, oversees disaster-response coordination, and supports cooperation with partner countries and international organisations.

This strategic role has recently been reinforced through analytical work. The RC, in cooperation with the Science and Technology Organisation (STO), published its NATO Chief research report on resilience in 2025. This paper sets resilience objectives that address collective vulnerabilities across the "Seven Baseline Requirements" mentioned above. Two of these requirements are particularly relevant to emergency communications. Baseline requirement no. 1 (Continuity of Government) includes the critical ability for leaders to make decisions and communicate with citizens during a crisis such as through public warning systems (PWS). Baseline requirement no. 6 (Resilient civil communications systems) indirectly covers the continuity of emergency communications. The sixth baseline requirement ensures that telecom networks keep working even during a crisis, with enough backup in place. This includes having reliable systems like 5G, strong ways to fix them quickly if they fail, giving priority access to authorities in emergencies, and carefully checking risks to these communication systems[43].

Building on this, the report outlines research projects for the STO to improve resilience. The STO has finalised many projects that could improve the resilience of emergency communications and the

[41] (NATO) Resilience – NATO Chief Scientist Research Report (19 December 2025) Science and Technology Organisation (STO), p. 8
[42] *Ibid*., p. 8
[43] *Ibid*., p. 9

communications networks that support them, including, developing emerging technologies to counter jamming, and using satellite communications networks to ensure backup capacities[44].

At a more specialised level, the Civil Communications Planning Group (CCPG) provides advice on building resilience in the communications sector. From a functional perspective, this planning group could be indirectly influential for emergency communications in Europe, playing a role in resilience, preparedness, and continuity planning. Its mandate focuses on civil communications resilience, telecommunications continuity during crises, civil–military interoperability and the protection of critical communications infrastructure. In that sense, emergency communications are part of the infrastructure it protects.

Alongside these planning structures, the Euro-Atlantic Disaster Response Coordination Centre (EADRCC), overseen by NATO's Resilience Committee, serves as the Alliance's main coordination body for disaster relief during major cross-border crises. It facilitates assistance, including military support, and provides situational awareness to Member States and partners, enabling informed decision-making in emergencies. The Centre distinguishes between "response" measured through coordination and operational effectiveness, and "resilience" which underpins response by ensuring the continuity of critical national systems such as government, energy, transport and communications.

This coordination role is further reinforced through regular large-scale crisis management exercises, such as those held in North Macedonia in 2021 and in Bulgaria in 2025. These simulations bring together military, scientific and civilian actors to test procedures and improve preparedness. While the EADRCC does not manage frontline emergency communications, it plays a key international coordination role, helping reduce pressure on national systems and supporting overall crisis management.

Potential for EU–NATO cooperation on emergency communications

In spite of tense EU-US geopolitical relations, NATO still perceives the European Union as an "essential partner". The two organisations are closely aligned on common values, strategic interests, and a significant overlap in membership. They collaborate closely on crisis management, capability development, and addressing hybrid threats and challenges.[45] For NATO countries that are also in the EU, resilience will follow both NATO and EU standards. The EU-NATO relationship on resilience is still parallel rather than integrated, there is an opportunity here to move toward harmonised or mutually recognised resilience benchmarks that includes the emergency communications infrastructure.

Moreover, a core task for the EADRCC is cooperation and dialogue with other authorities and organisations involved in disaster response and preparedness. The list of interlocutors includes the European Union's Emergency Response Coordination Centre (ERCC), which is the core operational hub of the European Union's Civil Protection Mechanism (UCPM). There is here an opportunity to develop more joint operational protocols between the ERCC and the EADRCC during cross-border crises.

[44] (NATO) Resilience – NATO Chief Scientist Research Report (19 December 2025) Science and Technology Organisation (STO), p. 22
[45] (NATO) (website) Relations with the European Union (consulted on 10 March 2026)

Concerning cybersecurity, the Technical Arrangement on Cyber Defence signed in 2016 between the NATO Cybersecurity Centre (CSC) and the CERT-EU provides a framework for exchanging information and sharing best practices between emergency response teams. Once again, opportunities to deepen this inter-institutional cooperation could be used to foster a common and strong approach toward cyber preparedness.

The EU-NATO cooperation also promotes information sharing between entities, which is a key aspect of the civil preparedness and European resilience. For instance, the EU Hybrid Fusion Cell and NATO's Hybrid Analysis Branch conduct Parallel and Coordinated Assessments (PACA) of the threat landscape concerning critical infrastructure[46]. There is here an opportunity for enhanced information sharing to make emergency communications more resilient, for example, by translating joint assessments into real-time operational guidance for critical entities.

The European External Action Service (EEAS) also supports NATO as part of the NATO-EU Task Force on the resilience of critical infrastructure. The EEAS produced a report dedicated to critical sectors resilience, among which the Digital Infrastructure sector encompasses emergency communications. These joint assessments are released to both EU Member States and NATO Allies simultaneously to ensure a shared understanding of risks. It concludes that the EU-NATO structured dialogue on resilience will oversee the implementation of the recommendations from joint reports[47].

The Digital Networks Act proposal also underlines the need for inter-organisational cooperation, in particular between the EU and NATO. The DNA highlights the role of the Office for Digital Networks as a central coordinator. In its own words, the "ODN should exchange and coordinate with […] international organisations such as NATO, on issues relating to Union-level assessment, monitoring, analysis and preparedness of electronic communications networks and services and their capability to contribute to the overall resilience of Union society and economy."[48]

The EU-NATO cooperation appears as essential to increase the resilience of the critical infrastructure emergency communications rely on. For instance, satellite systems can be used in case terrestrial infrastructure collapses, from which security can be monitored by space and air forces. It is just one example among others where the resilience of critical infrastructure is being reinforced through civil-military cooperation under the banner of NATO, fostering stable EU emergency communications[49]. As the CER Directive does, NATO highlights the need for its Member States to build national resilience strategies in order to face upcoming and ever-growing challenges. To that extent, "telecommunications grids" are regarded as crucial for NATO's operations and Member States' resilience[50]. They are the networks and infrastructure that enable information to travel between people and systems, such as mobile networks,

[46] (EU-NATO) EU-NATO task force on the resilience of critical infrastructure final assessment report (29 June 2023), p. 4
[47] *Ibid*., p. 9
[48] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on digital networks, amending Regulation (EU) 2015/2120, Directive 2002/58/EC and Decision No 676/2002/EC and repealing Regulation (EU) 2018/1971, Directive (EU) 2018/1972 and Decision No 243/2012/EU, recital 26
[49] (EU-NATO) EU-NATO task force on the resilience of critical infrastructure final assessment report (29 June 2023), p. 7 and 9
[50] (NATO) *NATO 2030 : United for a New Era*, Analysis and recommendations of the reflection group appointed by the NATO Secretary General (25 November 2020)

internet cables, antennas and satellites. They are essential for emergency communications because they carry calls and data.

The EADRCC also mentioned this point in its report on the 2025 exercise in Bulgaria. According to the centre, civil-military cooperation is a must, as "communications nodes that military forces depend on for movement, sustainment, and command are owned and operated by the private sector in every NATO Member State"[51]. Civil-military cooperation in this area is still emerging, there is an opportunity to deepen it during real-time exercises involving emergency communications entities. As examples from Ukraine highlighted that armed attacks also target PSAPs, these entities could therefore improve their physical protection capacities or redundancy and backup mechanisms through military assistance and material support.

To conclude, it is clear that emergency communications at the micro level remain a national competence, ultimately taking place between the PSAP and the end-user without NATO interfering. Nevertheless, NATO does contribute to a supranational emergency response structure that fosters international cooperation and, overall, builds new mechanisms to support emergency services. In today's interconnected security environment, reliance on complex, interdependent critical infrastructure, such as power grids and communications, heightens vulnerability to cascading disruptions and hybrid threats. NATO highlights its cooperation with the EU as a key factor in overcoming these challenges, underscoring once again multiple opportunities for cooperation between the two organisations to improve civil preparedness and resilience by pooling capacities, sharing information and training together.

2.5 – How emergency communications qualify outside of the EU

In its 2024 report, the Collaborative Coalition for International Public Safety (CCIPS) gave an overview of the qualification of emergency communications in a few non-European countries. In Australia, Canada and New Zealand emergency communications are not designated as critical infrastructure. However, Canada designated the 911 infrastructure as critical. The United Kingdom does not qualify explicitly emergency communications as critical infrastructure, but it does classify emergency services as one of its 13 national infrastructure sectors, entailing specific protection. In the United States, emergency communications and 911 are designated as part of the critical Emergency Services Sector (ESS) and the communications sector. In Ecuador and Costa Rica, one of the key pillars of the critical infrastructure cybersecurity frameworks officially encompass Public Safety and citizen security[52].

[51] (NATO) Emergency management exercise in Bulgaria – EADRCC Evaluation and Impact Report, 2025, p. 10
[52] CC:IPS, Public Safety Mission Critical Communications – Is it Critical Infrastructure? (July 2024), p. 2

III – The EU regulatory framework and concrete obligations

This section analyses the practical requirements arising from EU legislation and focuses mainly on risk management, incident reporting, supervision, and rules enforcement. It translates these legal obligations into concrete operational impacts for emergency communications. The CER and the NIS-2 Directives are both analysed as ongoing obligations that EU Member States have to transpose into national laws, while the CSA-2 and the DNA proposals reveal future potential obligations if they are adopted as regulations.

3.1 – Active legal obligations for entities and Member States

The Critical Entities Resilience Directive (CER)

In its own words, the CER Directive "lays down obligations on Member States to take specific measures aimed at ensuring that services which are essential for the maintenance of vital societal functions […] are provided in an unobstructed manner in the internal market, in particular obligations to identify critical entities and to support [them]" in meeting legal requirements. The CER Directive also lays down obligations directly on critical entities to enhance their resilience and ability to provide essential services.[53]

First, entities must conduct their own risk assessments at least every four years to identify all relevant risks that could disrupt the delivery of essential services[54]. Second, entities must implement technical, security, and organisational measures (e.g. physical protection of premises, incident response protocols, and supply chain management) to prevent disruption and recover from incidents[55]. Third, they are required to document their resilience measures in a formal resilience plan or an equivalent document[56]. Each entity must then designate a liaison officer or equivalent to serve as the point of contact with competent authorities[57]. Furthermore, entities must notify authorities of any incident that significantly disrupts or has the potential to disrupt essential services within 24 hours of becoming aware of it[58].

Member States must assist their critical entities to meet these legal obligations. The CER Directive mandated States to adopt a strategy for enhancing the resilience of critical entities by 17 January 2026[59]. They must then carry out a comprehensive risk assessment of natural and man-made risks at the national level at least every four years[60]. States must identify the specific critical entities for each sector by 17 July

[53] DIRECTIVE (EU) 2022/2557 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, recital 1
[54] *Ibid,* Art. 12
[55] *Ibid*., Art. 13
[56] *Ibid*., § 2
[57] *Ibid.*, § 3
[58] *Ibid*., Art. 15(1)
[59] *Ibid*., Art. 4(1)
[60] *Ibid*., Art. 5(1)

2026, and notify the entities of their status[61]. To supervise and ensure the correct application of the CER Directive, States must designate one or more competent authorities and a single point of contact (SPOC).[62] As an overall duty, States shall support entities through guidance, training, and exercises to help them meet their resilience requirements[63]. Finally, States must ensure relevant authorities have the power to conduct on-site inspections and audits, and can order entities to remedy infringements[64].

The Network and Information Systems Directive (NIS-2)

As discussed beforehand, this Directive creates a distinction between essential entities and important entities[65]. Although core legal obligations regarding cybersecurity risk management and incident reporting are similar for both types of entities, the primary difference between the two lies in the supervisory regime that is applied and the severity of penalties.

Essential entities are subject to a comprehensive supervisory regime, including both *ex ante* (before an incident) and *ex post* (after an incident) supervision[66]. Authorities can conduct audits, on-site inspections, and requests for evidence at any time to verify compliance.

Important entities are subject to a lighter, *ex post* only supervisory regime, meaning authorities generally only take action if they receive evidence of non-compliance[67]. Important entities must also align with the legal obligations stemming from the Directives. Some smaller MNOs (based on number of employees or annual turnover) may be classified as important entities.

As part of the Member States listing process, entities must provide specific details (name, contact info, IP ranges) to competent authorities to be included in national and EU-level registries[68]. Entities' management bodies must then approve and oversee the implementation of cybersecurity risk-management measures and can be held liable for non-compliance[69]. Entities must implement a baseline of technical, operational, and organisational measures, including incident handling or supply chain security.

Entities must follow a multi-stage reporting process for significant incidents: an early warning[70] within 24 hours, a full notification within 72 hours, and a final report within one month[71]. Each critical entity must manage its own cybersecurity at the micro level. In case of a cyberattack or technical failure causing the disruption of the essential services the entity delivers, the above-mentioned reporting process has to

[61] DIRECTIVE (EU) 2022/2557 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, Art. 6(1-3)
[62] *Ibid*., Art. 9(1-2)
[63] *Ibid*., Art. 10(1)
[64] *Ibid*., Art. 21(1)
[65] DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures aimed at ensuring a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148, recital 15
[66] *Ibid*., recital 122
[67] *Ibid*., Art. 33(1)
[68] *Ibid*., Art. 3(4)
[69] *Ibid*., Art. 20(1)
[70] *Ibid*., recital 102
[71] *Ibid*., Art. 23(1)

be done to the national Computer Security Incident Response Teams (CSIRT), even if the entity has an IT team or a specific internal organ that monitors cyber threats exposure. Finally, those internal bodies are required to undergo cybersecurity training to identify risks and assess management practices[72].

Similarly to the CER Directive, the main obligation for Member States under the NIS-2 Directive is to assist their entities in complying with the above-listed requirements. Concerning national cybersecurity, States must adopt a framework providing strategic objectives, resources, and policy measures to achieve a high level of cybersecurity[73]. States must appoint competent cyber-crisis management authorities, a single point of contact (SPOC), and CSIRT[74]. A CSIRT functions as an operational unit responsible for incident handling, which includes monitoring, analysing, and responding to cyber threats and vulnerabilities at the national level[75]. These national CSIRTs are members of the CSIRTs network, alongside the Computer Emergency Response Team for the EU institutions and bodies (CERT-EU)[76]. CSIRTs are supposed to cooperate, share information and risk assessments with the CERT-EU[77]. Moreover, States are required to foster cooperation and provide assistance to other Member States for supervision and enforcement, especially for cross-border entities[78]. At last, States must establish effective, proportionate, and dissuasive penalties, including administrative fines of up to €10 million or 2% of global turnover for essential entities in case of non-compliance with the Directive's rules[79].

3.2 – Future potential obligations

The Cybersecurity Act 2 (CSA-2)

The CSA-2 is a regulation proposal, which means that it does not impose any legal obligations yet. However, if adopted as a regulation, it would be directly applicable to all EU Member States. At the time of this report, the CSA-2 is under discussion in the European Parliament and Council of the EU. The EU already implemented a Cybersecurity Act in 2019 that the CSA-2 would officially repeal[80], once it is adopted. The CSA-1 regulation primarily established the European Cybersecurity Certification Framework (ECCF) and gave a permanent mandate to the European Union Agency for Cybersecurity (ENISA). The ECCF created a voluntary EU-wide certification scheme for ICT products and services that the CSA-2 intends to reinforce.

The CSA-2 would set rules for establishing managed security services, strengthen ENISA's operational role, address ICT supply-chain risks, and improve consistency with other EU cyber laws such

[72] DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures aimed at ensuring a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148, Art. 20(2)
[73] *Ibid*., Art. 7
[74] *Ibid*., Art. 1(2,a)
[75] *Ibid*., Art. 11(3)
[76] *Ibid*., Art. 10
[77] *Ibid*., Art. 15
[78] *Ibid*., Art. 37(1)
[79] *Ibid*., Art. 34
[80] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Union Agency for Cybersecurity (ENISA), the European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881, recital 171

as the NIS-2 Directive. The CSA-2 would also reinforce the already existing certification scheme by introducing mandatory prohibitions for "high-risk suppliers".

A high-risk supplier is either an entity linked to a designated third country or a specifically designated entity. The first category includes any entity established in, or controlled by, a third country that the European Commission has officially designated as posing cybersecurity concerns. The second case refers to specific entities that the Commission has prohibited through implementing acts due to exceptional circumstances where they pose a significant non-technical cybersecurity risk[81].

There would be no general obligation under the CSA-2 for critical entities to hold European cybersecurity certificates, as it would remain voluntary unless otherwise specified by separate Union or national law[82]. PSAPs would not be included within the mandatory scope of the CSA-2, as the trusted ICT supply chain framework only concerns entities that have been identified as essential under the NIS-2 Directive Annexes[83].

However, MNOs would be subject to the mandatory prohibitions of the trusted ICT supply chain framework as they would be obliged to completely remove high-risk ICT components within a specific transition period after a list of untrusted suppliers has been made[84]. Furthermore, the commission can adopt secondary legislation, stating that certain categories of critical entities cannot use high risk suppliers[85]. There would be a complementary restriction specifically for entities that choose to hold a certificate, barring them from including high-risk components in any certified ICT product, service, or process identified as a key asset to ensure the certificate remains a benchmark of trust[86]. While certification could be incentivised as a "compliance tool" to provide a presumption of conformity with other mandatory legislation like the NIS-2 Directive, the ban on high-risk supplier components for critical infrastructure would be an independent, mandatory risk-management obligation.

The Digital Networks Act (DNA)

This part does not cover all legal obligations incumbent on critical/essential entities related to emergency communications. Rather it underlines and synthesises the DNA's perspective on the resilience of communications infrastructure. Like the CSA-2, the DNA is still a regulation proposal, which does not impose any legal obligations yet.

Threats to electronic communications systems, whether from cyberattacks, physical damage, or wider system failures, naturally extend beyond national borders, and compromise security across the entire EU. At the same time, growing geopolitical tensions demand swift, coordinated action at EU level, which is

[81] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Union Agency for Cybersecurity (ENISA), the European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881, Art. 2(39)
[82] *Ibid*., Art. 71(3)
[83] *Ibid*., Art. 1(3)
[84] *Ibid*., Art. 110(3)
[85] *Ibid*., Art. 103(1)
[86] *Ibid*., Art. 85(9)

difficult to achieve if countries respond unevenly or pursue different levels of effort and timing. The DNA would therefore set out new mechanisms to improve telecom resilience and foster a Union-wide level of preparedness.

Moreover, the European Commission identifies the DNA as an opportunity to review EECC's limitations and to push for more requirements on security and preparedness. The text is presented as fostering simplification, legal harmonisation and as boosting resilience and integration in the European Single Market[87]. According to the proposal, increasing communications' resilience is tightly linked to the development of a single market for electronic communications[88].

The Digital Networks Act stresses that resilience goes through technological autonomy, where satellite connectivity plays a key role. The regulation directly links reducing technological dependencies with supporting the European Union's long-term competitiveness and resilience[89]. It underscores the importance of non-terrestrial networks (NTN) to avoid dependencies, long disruptions and to ensure redundancy. The proposal also underlines the risk of drone attacks on the critical infrastructure.

The DNA proposal acknowledges the standards set by the CER and NIS-2 Directives, but further explains that there is still a lot to accomplish to build a more resilient critical infrastructure. It identifies the absence of a sector-specific operational body, of a centralised EU-wide overview of preparedness, of an early warning crisis management mechanism, and the absence of a resilience mapping in electronic communications[90] as vulnerabilities pressing for actions. To ensure a strong resilience for the digital infrastructure, the DNA would advocate for implementing some of the recommendations stemming from 2022 Member States' risk assessments on communications infrastructure. The main recommendations are the "assessment of the resilience of international interconnections, criticality, resilience and redundancy of core Internet infrastructure, such as subsea communication cables", and also reinforcing "Union capabilities and coordinated action to strengthen the resilience of communications infrastructures"[91]. These recommendations need to be set through international coordination, information sharing and common guidance.

The Body of European Regulators for Electronic Communications (BEREC) and the ODN would play a central role in managing the resilience of the communications infrastructure. BEREC is described as a coordinating centre, entrusted with new tasks on resilience and preparedness, including the adoption of the Union Preparedness Plan for Digital Infrastructures, prepared by the ODN. It would also have to coordinate, share information and meet with many other regulatory bodies and stakeholders to collect information, analyse it and publish reports to provide guidelines and improve the communication infrastructure resilience[92]. BEREC, as the Commission or the ODN, would be expected to "reinforce the resilience and preparedness

[87] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on digital networks, amending Regulation (EU) 2015/2120, Directive 2002/58/EC and Decision No 676/2002/EC and repealing Regulation (EU) 2018/1971, Directive (EU) 2018/1972 and Decision No 243/2012/EU, explanatory memorandum, § 5
[88] *Ibid*., recital 17
[89] *Ibid*., 1.2 *Policy area(s) concerned*
[90] *Ibid*., § 14
[91] *Ibid*., recital 25
[92] *Ibid*., recital 357

of electronic communications networks and services at Union level, by fostering cooperation among public authorities and these providers in building the necessary resilience capacities, and in ensuring security and defence interests of the Union and its Member States"[93].

Part II of the Digital Networks Act proposal is the most relevant to emergency communications resilience. National authorities, cybersecurity bodies, and civil protection authorities would engage and coordinate together to "ensure the continuous availability of electronic communications networks and services as well as their necessary capabilities to anticipate, prevent, prepare for and respond to natural or man-made disruptions, crises or force majeure that may negatively affect the population"[94], which corresponds to the very definition of resilience itself.

[93] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on digital networks, amending Regulation (EU) 2015/2120, Directive 2002/58/EC and Decision No 676/2002/EC and repealing Regulation (EU) 2018/1971, Directive (EU) 2018/1972 and Decision No 243/2012/EU, Art. 3 (1, c)
[94] *Ibid*., Art. 5 (1)

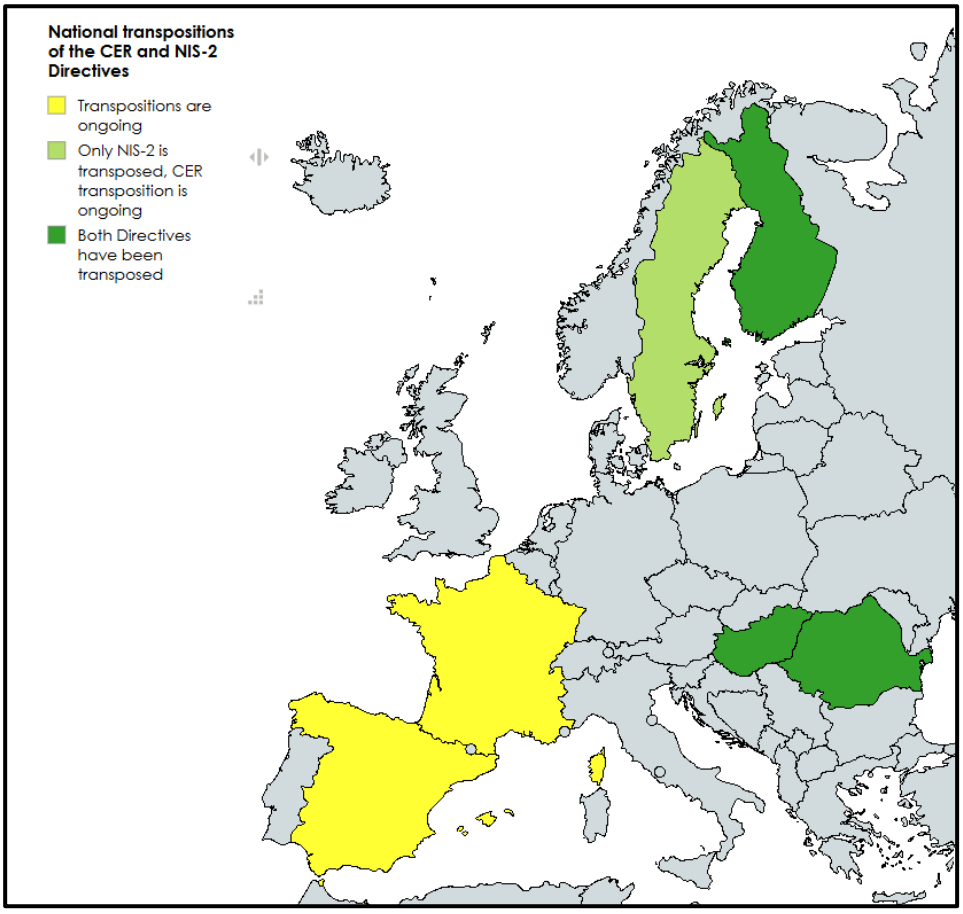
IV – National transpositions

This section compares the national transpositions of the above-mentioned legal frameworks to identify divergences, best practices, and open issues. It assesses how differing interpretations affect emergency communications in practice and highlights operational consequences for public authorities and service providers. It compares national implementations in France, Hungary, Finland, Romania, Sweden and Spain.

The analysis is divided according to the following requirements: the listing of critical entities, the designation of national competent authorities, the adoption of a national resilience strategy. The last subsection highlights emerging best practices among Member States.

In order to accomplish the above, the report analyses the main laws, bills, draft laws, acts and other legal texts that transposed, or will transpose, the CER and the NIS-2 directive into national law[95]. The state of national transposition is illustrated on the map below.

Figure 5 – National transpositions of the CER/NIS-2 Directives in the selected EU Member States



**data update (15/05/2026)*

[95] See Annex 1

France's national transposition of the CER and NIS-2 Directives is still under legislative negotiations. The national implementation will be completed through a single comprehensive law. It is the 2024 "draft law on the resilience of critical infrastructures and the strengthening of cybersecurity", discussed before the national assembly. The French national cybersecurity agency (ANSSI) already published guidelines to help future "essential entities" prepare for the NIS-2 implementation; PSAPs are not mentioned. In all, France is currently in a transitional phase awaiting the final vote.

Hungary passed two national laws to transpose the legal requirements of the CER and NIS-2 Directives. First, the "Act LXXXIV on the Resilience of Critical Organisations" transposed the CER Directive obligations. It entered into force in 2024. Then the 2025 "Act LXIX on the cybersecurity of Hungary" transposed the NIS-2 obligations.

Finland adopted the "Act 124/2025 on cybersecurity" to transpose the NIS-2 directive at national level. The country also adopted the "Act 310/2025 on the Protection of Infrastructure Critical to Society and on the Improvement of Resilience" to transpose the CER Directive. Both Acts entered into force in 2025.

Romania passed two distinct laws to transpose the CER and NIS-2 Directives. First, the "Law no. 294 on the resilience of critical entities and amending certain legislative acts", that entered into force in 2024, transposed the obligations from the CER Directive at national level. The NIS-2 Directive requirements were then transposed through the "Law no. 124 for the approval of Government Emergency Ordinance 155/2024 on establishing a framework for the cybersecurity of networks and information systems in the national civil cyberspace", which entered into force in 2025.

The Ministry of Defence confirmed that **Sweden** would most likely transpose the CER Directive around summer 2026. The transposition would be done through a specific act and accompanying regulation still under preparation and negotiations. A draft law should be proposed on the basis of an assessment report[96] (SOU 2024:64), which studies the impact of implementing the CER Directive in Sweden and includes both legislative proposal parts and an ordinance. The CER Directive formally required transposition by 17 October 2024, but like many other Member States, Sweden has not completed formal transposition by that deadline. However, Sweden did transpose the NIS-2 Directive into national law, and two legal texts have been adopted. One is the "Cybersecurity Act 1506:2025", the other is the "Cybersecurity ordinance 1507:2025". Both entered into force on January 15, 2026.

Spain implemented neither the CER nor the NIS-2 Directives at national level as of May 2026, despite the deadline. Both Directives' obligations have been transposed in two draft laws that have been approved in 2025 by the council of ministers and are still under negotiations. The first one focuses on "Cybersecurity Coordination and Governance" (to transpose the NIS-2 Directive), the other one aims at the "Protection and Resilience of Critical Entities" (to transpose the CER Directive). In all, Spain has not yet fully completed the formal transposition of the CER and NIS-2 Directives into binding national laws, although draft implementing legislation has been prepared and legislative processes are ongoing.

[96] (SWEDEN) Resilience in Essential Services, Final Report of the Inquiry on the Implementation of the NIS-2 and CER Directives (2024)

4.1 – Identification and listing of emergency communication entities

This section analyses whether Member States have met the obligation to establish a list of their critical/essential entities. It also examines if PSAPs and other emergency communications components have been included in these national registries.

France's draft laws follow the CER and NIS-2 Directives listing of critical sectors. The legislation mobilises the concept of "Operators of Vital Importance" (OIV)[97], which are organisations using the critical infrastructure to exercise activities of vital importance. In France, OIV is the broader legal status for critical entities. When such an operator provides services defined as "essential" by the EU, it is simultaneously qualified as a critical entity under the CER Directive[98].
Moreover, France explicitly identifies departmental fire and rescue services as critical entities, which implicitly rely on emergency communications as critical infrastructure[99]. France also specifies that the Prime Minister has the power to classify any entities as critical/essential regardless of its size, if the entity's disruption has significant impact on public safety, security and health[100]. In that sense, PSAPs could either already qualify as critical entities or might be by decree. Both Spanish and French draft laws include sectors of "high criticality" such as digital infrastructure, which encompasses the networks used for emergency calls.

Spanish draft laws say that entities of the Public Administration qualify as "essential entities". If it appears that PSAPs in **Spain** are public administration bodies or operate under their direct responsibility, once the draft laws are adopted, PSAPs would fall into this high-criticality category[101].
The nominative list of essential and critical entities is neither publicly available nor set in these countries, however, **France** developed an official simulator test that indicates to an entity if it qualifies as critical or not[102].

In **Hungary**, the adopted Acts establish a broad list of critical entities and critical sectors, following a similar structure to those of the EU Directives. The national law gives an explicit list of public administration entities, none of which refers explicitly to PSAPs[103]. However, if a PSAP is established as a unit within a Ministry (such as the Ministry of the Interior), it qualifies as a central state administration organ, which then qualifies as an essential entity. Furthermore, the law qualifies entities as "essential" if their disruption significantly impacts public safety[104] or if they provide services to at least 20,000 persons[105], which in both cases would be true for PSAPs.

[97] (FRANCE) Draft Law on the Resilience of critical infrastructures and the strengthening of cybersecurity (2025), Chap. I, Section 1, Art. L. 1332-2 (1)
[98] *Ibid*., Art. L. 1332-2. – I., 1(2)
[99] *Ibid*., Chap. II, Section 2 Art. 8(7, d)
[100] *Ibid*., Art. 10(2)
[101] (SPAIN) Draft Law on the Protection and Resilience of Critical Entities (2025), Annex 1, Sector 10
[102] French Government – ANSSI, *Mon Espace NIS-2*, (consulted on April 1st, 2026) https://monespacenis2.cyber.gouv.fr/simulateur
[103] (HUNGARY) ACT LXIX, on the Cybersecurity of Hungary, Annex 1
[104] *Ibid*., Section 1, 6(2)
[105] *Ibid*., Chap. I, Section 1, 6(7)

Finland appears to follow the EU Directives sectorial classification of critical/essential entities. The country classifies the sector of Digital Infrastructure as highly critical, which encompasses providers of publicly available electronic communications services and networks[106]. Moreover, Act 310/2025 follows the CER Directive classification covers which include "providers of public electronic communications networks" as critical entities[107]. Moreover, an essential service is also defined as any service crucial for maintaining "public safety" or "public health"[108], which would bring PSAPs under the scope of the resilience framework. The Finnish Ministry of the Interior confirmed that the identification of critical entities is currently underway. The nominative list requirement will be met by July 2026.

The **Swedish** legislation on cybersecurity does not provide a public list of critical entities. However, they do follow the obligation of establishing a mandatory registration process. Entities that meet the legal criteria must register themselves and notify the designated authority[109]. Furthermore, emergency communications critical infrastructure is partly covered as "public electronic communications networks" and "publicly available electronic communications services"[110]. The report (SOU 2024:64) sets the same broad list of critical entities and sectors as the CER Directive does, and mandates the production of a nominative list of critical entities in the future[111]. Overall, the report does not explicitly mention emergency communications, but critical infrastructure they rely on would fall in the Digital Infrastructure sector.

Romania also aligns with the EU Directives by identifying "providers of public electronic communications networks" and "providers of public electronic communications services intended for the public" as critical and essential entities under the Digital Infrastructure sector[112]. The specific list of identified critical entities must be approved by a decision of the Prime Minister, based on a proposal from the National Coordination Centre (CNCPIC)[113].

All of the selected EU Member States have adopted, or will adopt, the CER and NIS-2 Directives list of critical sectors. All States transposed the classification of MNOs as essential entities, but none directly mention PSAPs. Most countries have designated competent authorities in charge of listing critical entities, not all of them have yet produced a nominative list of their critical entities. There lies another inconsistency as many entities are not sure of their status concerning the ongoing transposition of the CER and NIS-2 Directives. The lack of an explicit designation for emergency communications entities may create a blurry common legal environment. The deadline for the Member States obligation to make the listing is set by the CER Directive for July 17, 2026.

[106] (FINLAND) Act 124/2025 Cybersecurity Act, Annex 1, Sector 6 (h, i)
[107] (FINLAND) Act 310/2025 on the Protection of Infrastructure Critical to Society and on the Improvement of Resilience, §1(1)
[108] *Ibid*., § 4(2)
[109] (SWEDEN) Cybersecurity Act 1506:2025, Chap. 2, § 2
[110] *Ibid*., Chap. I, § 6
[111] (SWEDEN) Resilience in Essential Services, Final Report of the Inquiry on the Implementation of the NIS-2 and CER Directives (2024), 1.6, § 10
[112] (ROMANIA) Law no.294/2024 on the resilience of critical entities and amending certain legislative acts, Annex, Sector 8
[113] *Ibid*., Art. 6(3)

4.2 – Designation of national competent authorities, SPOCs and CSIRTs

This section assesses the designation of national competent authorities, Single Points of Contact (SPOC), and Computer Security Incident Response Teams (CSIRT) in the selected Member States, as it is requested by each EU Directive.

France designated the National Authority for Security and Information Systems (ANSSI) to be the competent authority for the supervision of the NIS-2 Directive requirements transposition[114] which would make it the main SPOC and CSIRT coordinating with other CSIRTs[115]. Although the General Secretariat of Defence and National Security (SGDSN) is the French competent authority that manages the resilience of critical infrastructure, the draft law solely mentions an "administrative authority" as the competent body for monitoring the physical resilience and serving as the liaison for national oversight and cross-border coordination. This authority would have to designate operators of vital importance[116]. Also, sectoral ministries will be designated as competent authorities to implement and enforce resilience requirements in their respective sectors under the CER framework.

Hungary established two bodies for managing the cybersecurity of electronic information systems of critical entities, outside the scope of electronic information systems linked to national defence purposes. These agencies are the National Cybersecurity Centre and the Supervisory Authority for Regulatory Affairs (SARA)[117].

The cybersecurity of entities related to national defence is supervised by the National Defence Cybersecurity Authority, designated within the national defence sector by governmental decree[118]. The designated National Cybersecurity Centre serves as the main SPOC[119]. The Digital Infrastructure is mostly managed by SARA[120]. Hungary designates two different CSIRTs, the National Cybersecurity Incident Handling Centre and a separate National Defence Cybersecurity Incident Handling Centre[121].

Concerning the CER transposition, the authority competent for supervising the resilience of critical entities has to cooperate with sectoral ministers and is nominated by the government[122]. Government Decree no. 474/2024 (XII. 31.) officially designated the National Directorate General for Disaster Management (NDGDM) as the supervisory authority for the resilience monitoring of critical entities, carrying out inspections and oversight.

[114] (FRANCE) Draft Law on the Resilience of critical infrastructures and the strengthening of cybersecurity (2025), Art. 5
[115] *Ibid*., Section 4, Art. 23
[116] *Ibid*., Art. L. 1332-2
[117] (HUNGARY) ACT LXIX, on the Cybersecurity of Hungary, Section 23, 1(a, b)
[118] *Ibid*., Section 23(2)
[119] *Ibid*., Section 24(1) § 23
[120] *Ibid*., Section 23(1, b) cf. Section 1(1, e)
[121] *Ibid*., Section 63
[122] (HUNGARY) Act LXXXIV on the Resilience of Critical Organisations, Section 21(1)

In **Finland**, the Ministry of the Interior is designated as the competent authority for the overall guidance, monitoring, and coordination of the resilience framework implementation (CER)[123].

Regarding cybersecurity, the Finnish Transport and Communications Agency (TRAFICOM) is the primary supervisory authority for several key sectors, including the Digital Infrastructure sector. TRAFICOM functions as the national CSIRT and SPOC and shall report on incidents to the European Union Agency for Cybersecurity (ENISA)[124].

In **Sweden**, the Post and Telecom Authority (PTS) is designated as the supervisory authority issuing regulations over the Digital Infrastructure sector, including public electronic communications networks and services[125].

Furthermore, the Swedish Civil Contingencies Agency (MSB) serves as the national CSIRT and SPOC, as requested by the NIS-2 directive[126]. Also, "in order to strengthen [its] total defence and create clearer leadership of civil defence, the Swedish Civil Contingencies Agency "MSB" has become the Swedish Civil Defence and Resilience Agency "MCF" on 1 January 2026"[127].

Regarding the CER Directive, the report (SOU 2024:64) shows a decentralized supervision model where specific government agencies are designated as supervisory authorities based on the sector they already oversee. In addition, the MCF also serves as the SPOC for resilience and is requested to establish the list of critical entities.

Even though **Spain** has not implemented the CER and the NIS-2 Directives at the time of this report, its draft laws would designate the Secretariat of State for Security, within the Ministry of the Interior, as the competent national authority supervising critical entities' physical and operational resilience[128].

The National Centre for the Protection and Resilience of Critical Entities (CNPREC) shall serve as the SPOC and assist the Secretary of State for Security regarding its responsibilities, functions, and obligations related to critical entities' resilience[129]. Moreover, the National Cybersecurity Centre is designated as the national competent authority to supervise sectoral CSIRTs, and as the main SPOC regarding cybersecurity[130].

In **Romania**, the National Coordination Centre for Critical Infrastructure Protection (CNCPIC), within the Ministry of Internal Affairs, is the national competent authority responsible for coordinating the identification and resilience of critical entities[131].

[123] (FINLAND) Act 310/2025 on the Protection of Infrastructure Critical to Society and on the Improvement of Resilience, Chap. 2, § 7
[124] (FINLAND) Act 124/2025 Cybersecurity Act, Chap. 2, § 18-19
[125] (SWEDEN) Cybersecurity ordinance 1507:2025, § 7
[126] *Ibid*., § 23 - 27
[127] Swedish Civil Defence and Resilience Agency (website), *MSB will be Swedish Civil Defence and Resilience Agency as of January 1st, 2026* (consulted on February 20, 2026)
[128] (SPAIN) Draft Law on the Protection and Resilience of Critical Entities (2025), Art. 15(1)
[129] *Ibid*., Art. 16
[130] (SPAIN) Draft Law on Cybersecurity Coordination and Governance, Art. 6
[131] (ROMANIA) Law no.294/2024 on the resilience of critical entities and amending certain legislative acts, Art. 1

The national SPOC, functionally within the National Directorate for Cybersecurity (DNSC), is responsible for forwarding incident notifications to other Member States and ENISA[132]. The DNSC is the main CSIRT for entities in the Digital Infrastructure sector[133], including those related to emergency communications. Finally, the Special Telecommunications Service (STS) is responsible for cybersecurity and resilience related to its own special telecommunications networks and systems as explained in another law[134].

4.3 – Adoption of national resilience and cybersecurity plans and risk assessments

Under the requirements of the CER and NIS-2 Directives, Member States must adopt national strategies and conduct risk assessments for both the resilience and the cybersecurity of critical entities[135].

Five years before the implementation of the CER directive, the General Secretariat for Defence and National Security in **France** developed and coordinated the critical infrastructure protection (CIP) policy. It created a framework allowing public and private critical operators to help carry out the national security strategy by protecting against man-made malicious acts as well as natural, and health-related risks.

The 2025 French draft laws transposing CER and NIS-2 largely build upon and "europeanise" an already mature national model created by the SGDSN and pursued by ANSSI since the late 2000s. Once adopted, they would complete the designation of "Activities of Vital Importance", and delegate the plan of resilience to the critical entities themselves, which is called "*operator resilience plan*". In addition, France mandates operators of vital importance to conduct their own risk assessments[136]. ENISA published a French report in 2022 that highlights major stakes and sets broad objectives for resilience[137].

On cybersecurity, ANSSI is in charge of implementing the government policy for information system security[138]. ANSSI published its strategic plan for a "resilient nation" in 2025, which sets broad objectives for the cybersecurity of critical entities, without mentioning emergency communications as such[139]. Finally, France requires critical entities to take technical, operational, and organisational measures to manage network risks and ensure both resilience and cybersecurity. Those measures are supposed to reach specific objectives, that would be set by decree of the State Council and would determine the elaboration of a technical and organisational repository[140].

---

[132] (ROMANIA) Law no. 124/2025 for the approval of Government Emergency Ordinance No. 155/2024 on establishing a framework for the cybersecurity of networks and information systems in the national civil cyberspace, amendment to Art. 18, (10) Ordinance No. 155/2024
[133] *Ibid*., amendment to Art. 3(3) Ordinance No. 155/2024
[134] (ROMANIA) Law no. 58/2024 on the cybersecurity and defence of Romania, as well as for the amendment and completion of certain normative acts, Art. 16
[135] CER Directive Art. 4-5 and NIS-2 Directive Art. 7-21
[136](FRANCE) Draft Law on the Resilience of critical infrastructures and the strengthening of cybersecurity (2025), Art. L. 1332-3
[137] (FRANCE) National Strategic Review (2022)
[138] (FRANCE) Draft Law on the Resilience of critical infrastructures and the strengthening of cybersecurity (2025), Art. 5
[139] (FRANCE) ANSSI – Strategic Plan of the Agency of national security and information systems (2025)
[140] (FRANCE) Draft Law on the Resilience of critical infrastructures and the strengthening of cybersecurity (2025), Art. 14

Spain's draft laws include the approval of a "National Strategy for the Protection and Resilience of Critical Entities". The State Secretariat for Security will prepare the Strategy, setting objectives and measures based on existing plans to ensure and maintain a high level of resilience of critical entities[141]. In 2013 already, Spain published a set of objectives for the resilience of critical infrastructure. It underlined the need for the public authorities to ensure that the Information and Telecommunications Systems used by them have the appropriate level of security and resilience[142].

Regarding cybersecurity, a National Cybersecurity Strategy shall be established and its provision should contain the risk assessment measures[143]. While the National Cybersecurity Centre leads the direction and coordination of the strategy's activities, the National Security Council remains the high-level body responsible for its formal approval. Updated in 2019, the National Cybersecurity Strategy (NCSS) clearly identifies the components emergency communications rely on as critical infrastructure and mandates Spain to guarantee the secure and responsible use of information and communication networks and systems[144].

Hungary's resilience strategy, as requested by its Act LXXXIV of 2024[145], has been adopted under the Government Decision no. 1192/2025 (VI. 5.). The decision does not contain any explicit mention of emergency communications, but emergency communications related critical infrastructure is covered. Resilience risk assessments are distributed between the entities[146] and the national level authorities[147].

The Hungarian Cybersecurity Strategy is defined as a "document providing strategic objectives and priorities in the area of cybersecurity and the governance to achieve them"[148]. Hungary adopted the strategy on cybersecurity through a Government resolution[149] which does not mention emergency communications entities directly. The entities must conduct cybersecurity risk assessments to test their protective measures[150].

Finland transposed both the obligations of drafting a resilience strategy[151] and a cybersecurity strategy[152]. As of May 2026, the government has not adopted one final national CER resilience strategy, but it did adopt and updated a Cybersecurity strategy[153].

Concerning risk assessment, the document is used to determine which entities are considered critical. Under the Act, a national risk assessment of critical infrastructure and critical entities must be completed

[141] (SPAIN) Draft Law on the Protection and Resilience of Critical Entities (2025), chapiter 2, Art. 4
[142] (SPAIN) National Cybersecurity strategy (2013)
[143] (SPAIN) Draft Law on Cybersecurity Coordination and Governance, Art., 5 (d)
[144] (SPAIN) National Cybersecurity strategy (2019), preamble § 1
[145] (HUNGARY) Act LXXXIV on the Resilience of Critical Organisations (entered into force on January 1, 2024), Chap II, Section 3, § 4(1)
[146] *Ibid*., Section 10, § 18
[147] *Ibid*., Section 4, § 5(2)
[148] (HUNGARY) ACT LXIX, on the Cybersecurity of Hungary (2025), Section 4(78)
[149] (HUNGARY) Government resolution no. 1089/2025 (III. 31.) on Hungary's Cybersecurity Strategy
[150] (HUNGARY) ACT LXIX, on the Cybersecurity of Hungary (2025), Section 6, 3(10)
[151] (FINLAND) Act 310/2025 on the Protection of Infrastructure Critical to Society and on the Improvement of Resilience, § 5
[152] (FINLAND) Act 124/2025 Cybersecurity Act, Section 42
[153] (FINLAND) Finland's Cybersecurity Strategy 2024–2035

at least every four years[154]. The Finnish Ministry of the Interior indicated that the risk assessment of critical infrastructure and resilience of society has been adopted by Finland, but it is not publicly available. Nevertheless, a broader and available national risk assessment has been published in 2023. This report clearly stresses the necessity for "communications between people, emergency calls, authorities' communication channels, public administration's digital services and mass media [to] also function during society's severe disruptions and in emergency conditions"[155]. Moreover, the risk assessment sheds light on communications services being "particularly critical to society", including "emergency calls and the transmission of authorities' emergency warnings and targeted official announcements to the population"[156]. A broader national risk assessment will be published in autumn 2026[157].

The cybersecurity risk assessment is also requested by the law[158] and Finland publishes annual public cyber threat reports and conducts risk analysis with its national cybersecurity authorities, such as the national cybersecurity centre at TRAFICOM.

Sweden designated the MCF to cooperate with sectoral supervisory authorities to coordinate and achieve the effective and equivalent supervision[159] of the national cybersecurity strategies (NCSS).
Two Swedish NCSS have been published by ENISA, one in 2017[160], that has been "completed", and the other one in 2025[161]. CSIRTs are tasked with providing "dynamic risk and incident analysis" and situational awareness for the country[162]. While sectors' vulnerabilities and critical operators' lists remain classified[163], the MCF has conducted multiple risk assessments. In its 2025 National Risk and Vulnerability Assessment (NRVA), the MCF explicitly mentioned "warning systems"[164] as a critical infrastructure in case of disasters, implying the necessity of protecting the digital assets it relies on. Moreover, "Electronic Communications and Post" is identified as one of the ten specific preparedness sectors that undergo detailed vulnerability assessments in the report's appendices[165].

Romania tasked the CNCPIC to elaborate the "strategy for strengthening the resilience of critical entities", which will then be approved by a Government decision[166].
The CNCPIC is responsible for the risk assessment at national level[167], while critical entities also produce their own resilience risk assessment[168].

[154] (FINLAND) Act 310/2025 on the Protection of Infrastructure Critical to Society and on the Improvement of Resilience, § 6
[155] (FINLAND) National risk assessment (2023), Section 3.10
[156] *Ibid*., p. 60
[157] Finnish Government, *Government approves risk assessment of critical infrastructure* (website) (consulted on February 20, 2026)
[158] (FINLAND) Act 124/2025 Cybersecurity Act, Sections 8 and 10
[159] (SWEDEN) Cybersecurity ordinance 1507:2025, § 40
[160] (SWEDEN) A national cybersecurity strategy (2017)
[161] (SWEDEN) National Strategy for Cybersecurity 2025-2029 (2025)
[162] (SWEDEN) Cybersecurity ordinance 1507:2025 , § 33
[163] DIRECTIVE (EU) 2022/2557 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, Art. 8
[164] (SWEDEN) MSB - National Risk and Vulnerability Assessment (NRVA)(2025), p. 62
[165] *Ibid*. p. 161
[166] (ROMANIA) Law no.294/2024 on the resilience of critical entities and amending certain legislative acts, Article 4(1)
[167] *Ibid*., Art. 5(1)
[168] *Ibid*., Art. 12(1)

Important and essential entities shall train their staff to identify risks and assess cybersecurity risk-management practices, while cooperating with the DNSC[169]. ENISA published Romania's Cybersecurity strategy[170]. The report does not explicitly name "PSAPs" or "emergency communications", but it secures the critical infrastructure, essential services, and information systems they use.

4.4 – Emerging best practices and open issues

First, Member States are at different stages of implementing the EU requirements on resilience and cybersecurity, but all have either adopted or are developing national frameworks to transpose the CER and NIS-2 Directives. While some countries have already enacted comprehensive legislation and established detailed institutional arrangements, others are still finalising or preparing their legal reforms. Despite these differences in timing and maturity, most Member States already rely on functioning national structures for resilience and cybersecurity, demonstrating a shared commitment to transposition within an uneven but converging European framework.

Second, regardless of the stage of legal transposition, some similarities emerge in the designation of competent authorities, CSIRTs, and SPOCs among the selected Member States. **Finland** and **Sweden** have a relatively centralised model since the same primary agency combines the functions of EU liaison (SPOC) and operational responder (CSIRT). **France** follows a similar approach regarding cybersecurity through ANSSI, although the supervision of physical resilience under the CER framework also involves sectoral ministries. **Spain** and **Hungary** instead rely on a more decentralised operational structure, with multiple CSIRTs and authorities exercising specialised sectoral responsibilities. **Spain**, **Romania**, and **Hungary** also distinguish between the bodies responsible for cybersecurity coordination and those supervising physical resilience obligations under the CER framework. **Finland**, **Sweden**, and **Spain** further rely on multi-authority supervisory systems where oversight responsibilities are distributed among sector-specific regulators. Overall, the comparison shows that Member States broadly align with the objectives of the CER and NIS-2 Directives by combining national strategies with risk assessments conducted both at national and entity level. **Finland** and **Sweden** stand out for more explicit references to emergency communications systems and warning mechanisms in national risk analyses, linking them directly to crisis preparedness. **France** also explicitly identifies firefighting and rescue departments as essential entities. Overall, where risk assessments are continuous and shared between authorities and operators, emergency communications would appear more clearly integrated into preparedness and crisis-response planning.

To conclude, while emergency communications are rarely named explicitly, they are indirectly protected through critical infrastructure's resilience and cybersecurity frameworks. However, clearer recognition of their criticality would strengthen preparedness and coordination during crises, help clarify the entities' role and situate them within the whole resilience process and facilitate their legal obligations compliance.

[169] (ROMANIA) Law no.124/2025 for the approval of Government Emergency Ordinance No. 155/2024 on establishing a framework for the cybersecurity of networks and information systems in the national civil cyberspace, Art. 14(2,3)

[170] (ROMANIA) Decision no. 1.321/2021 regarding the approval of the Cybersecurity Strategy of Romania for the period 2022–2027, as well as of the Action Plan for the implementation of the Cybersecurity Strategy of Romania for the period 2022–2027.

V – Interdependencies between emergency communications and other critical sectors

All critical infrastructures are interconnected. While PSAPs are outside the scope of the CER and NIS Directives, both aim to set minimum standards in areas where the critical infrastructure can have a cross-border impact. This section will assess the interdependencies that PSAPs and other components in emergency communications have on some of these critical sectors.

Many interdependencies exist between emergency communications and the highly critical sectors like Energy and Public Administration, or sectors' components such as telecoms, the cloud and data services. Let's examine systemic risks and cascading failure scenarios, emphasising how disruptions in one sector can directly affect the continuity of emergency services. The CER and NIS-2 Directives, as well as the Cybersecurity Act 2 proposal, collectively emphasise the interconnected nature of critical sectors and the hazards it entails.

To address this, both CER and NIS-2 Directives establish harmonised framework setting out minimum rules for critical infrastructure across the Union, for sectors with cross-border impact. Member States retain the right to set rules for critical infrastructure outside the scope of these Directives.

The CER Directive identifies 11 sectors of vital importance[171], including Energy, Transport, Banking, Financial Market Infrastructure, Health, Drinking Water, Waste Water, Digital Infrastructure, Public Administration, Space, and the Production, Processing, and Distribution of Food. Network Operators which support emergency communications are under the Digital Infrastructure sector.

The NIS-2 Directive identifies eighteen sectors, divided into two categories. There are eleven sectors of High Criticality such as Energy, Transport, Banking, Financial Market Infrastructure, Health, Drinking Water, Waste Water, Digital Infrastructure, ICT Service Management, Public Administration, and Space.

On the other hand, there are seven critical sectors such as the Postal and Courier Services, Waste Management, Manufacture/Production/Distribution of Chemicals, Production/Processing/Distribution of Food, Manufacturing, Digital Providers, and Research. Emergency communications components would be covered by the highly critical category under the NIS-2 framework.

5.1 – Telecommunications dependencies

The Digital Infrastructure provides the buttress for communications, which underpins all essential functions in society. "Telecommunications" constitute a critical infrastructure, affecting different critical entities, within the Digital Infrastructure sector and beyond. "Electronic communications networks form the

[171] (ROMANIA) Decision no. 1.321/2021, Annex : *sectors, subsectors and categories of entities*

backbone for a wide range of services that are essential" [172] for the functioning of vital societal services. Public electronic communications networks support emergency communications, meaning that if these networks fail, people are unable to contact emergency services. These networks are recognised as critical infrastructure under the CER and NIS-2 Directives.

As Finland underlines in its National Risk Assessment, any outage in telecom networks immediately degrades emergency call routing, inter-agency coordination and public alert dissemination[173]. In Sweden, the MCF highlights that emergency services also rely on space services for communication, navigation and many other functions. These services use satellites that are exposed to solar storms or potential human spatial threats. As dependency on space services and data grows stronger, so do vulnerabilities linked to their disruption. Consequences of satellite communications disruption can curb emergency services due to positioning and communication difficulties, making it complex to handle all incoming calls. If satellites are completely disabled, some service disruptions could last for months[174] and backup solution in case of terrestrial infrastructure failure would no longer be accessible.

5.2 – Information and Communication Technology (ICT)

ICT systems increasingly act as control layers governing physical infrastructure operations. The NIS-2 Directive defines it either as a product, a service or a process[175]. They cover both hardware and software, data and networks conveying communications across society. They function as the primary infrastructure layer enabling emergency communications. Moreover, emergency communications (e.g., emergency calls or public warnings) depend directly on the availability, integrity and prioritisation of electronic communications networks.

MCF's risk assessment identifies IT incidents as crucial for emergency communications. An IT incident is an unwanted event that compromises the confidentiality, accuracy, or availability of information and curbs processing systems. Its most serious societal impacts are shared between the loss of connectivity and the collapse of Energy-related infrastructure. The MCF risk assessment stresses that such incidents critically impact the public's ability to contact healthcare in various ways, for example, by disrupting communications with SOS Alarm which manages emergency calls in Sweden [176].

[172] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Union Agency for Cybersecurity (ENISA), the European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881, recital 151
[173] (FINLAND) National Risk Assessment (2023), 3.10, p. 60
[174] (SWEDEN) MSB - National Risk and Vulnerability Assessment (NRSB)(2025), p. 46-49
[175] DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures aimed at ensuring a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148, Art. 6 (12,13,14)
[176] (SWEDEN) MSB - National Risk and Vulnerability Assessment (NRSB)(2025), p. 67

5.3 – Energy dependencies

The CER Directive identifies the Energy sector as a highly critical sector[177]. Emergency communications and telecommunications have considerable interdependencies on the energy sector, as energy is the foundational enabler for the critical infrastructure (hardware, software, networks and systems) required to provide essential services crucial for public health and safety[178].

A disruption in the Energy sector would generate cascading effects and potentially disable the electronic communications networks used by citizens to contact emergency services, and by first responders to communicate with one another[179]. This was for instance the case in Berlin, during the January 2026 power outage that negatively impacted emergency call centres operability. The emergency communications' infrastructure is entirely electricity-dependent, as base stations, dispatch centres, data routing nodes and satellite gateways require power supply. Energy disruptions rapidly cause telecom degradation and emergency communication failure, even where networks remain technically intact. Backup power mitigates but does not eliminate this dependency. Cyberattacks and natural disasters damaging energy infrastructure have in the past greatly disturbed emergency communications with relevant example from Ukraine since the beginning of the war.

Finland's risk assessment illustrates this idea noting that "approximately 10–20% of severe incidents in the functioning of communications networks and services result from power supply disruptions. It adds that these disruptions also usually last longer than other faults."[180] The report highlights that "communications services particularly critical to society," such as emergency calls and the transmission of authorities' emergency warnings, are jeopardised when power is lost[181].

Sweden's MCF risk assessment identifies power outages as a cross-sectoral vulnerability, noting that "in principle all socially important activities are dependent on electricity"[182], including emergency communications.

Without power, MCF notes that mobile networks and broadband services would go down across large parts of the country, especially in remote areas where redundancy is lower. A prolonged outage in the national transmission grid could also significantly impact the reliability and availability of internet and the services depending on it[183]. France's strategic review also stresses that power and self-sufficiency is linked to the protection and security of value chains and to the "assistance to the populations", which includes emergency communications and services[184].

[177] DIRECTIVE (EU) 2022/2557 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, Annex (1)
[178] *Ibid*., Art. 2 (4-5)
[179] *Ibid*., recital 5
[180] (FINLAND) National Risk Assessment (2023), p . 61
[181] *Ibid*., p. 60
[182] (SWEDEN) MSB - National Risk and Vulnerability Assessment (NRSB)(2025), p. 12
[183] *Ibid*., p. 87
[184] (FRANCE) National Strategic Review (2022), § 79

5.4 – Cloud and data centres infrastructure dependencies

Cloud computing and data centres are part of the Digital Infrastructure critical sector under NIS-2 and CER Directives. They are explicitly classified as the critical infrastructure provided by critical entities such as cloud computing service providers and Data centre service providers[185].

Emergency communications may rely on cloud computing services as it allows many people and services to access and share important data from anywhere. For instance, it may allow ambulance services, hospitals, and other emergency teams to access the same information remotely.

Emergency communications may also rely on Data centre services to store and send data and run the systems that keep alerts, calls, and messages working. Without the data centres, PSAPs' software would not work efficiently, and the emergency call would neither be registered nor sent properly.

Loss of cloud services may not just interrupt signal transmission but can disable command, coordination, and situational awareness functions. In this context, one of the main risks is a *kill-switch*. A kill-switch is a feature that allows a cloud provider or authority to remotely shut down or disable a service instantly. Such a phenomenon would be induced by the action of foreign governments, on which the national cloud service relies due to global interdependences. For instance, during discussions held at the 14th BEREC Stakeholder Forum on 31 March 2026, several participants voiced their concerns regarding the European critical infrastructure being partly dependent on the American Cloud.

The risk of foreign or third party interfering within the Cloud infrastructure is already alarming. Several countries implemented cybersecurity strategies to protect this critical sector, such as France with its *SecNumCloud*. *SecNumCloud* is a national cybersecurity certification scheme managed by the French cybersecurity agency (ANSSI). It sets strict requirements for cloud service providers, including rules on data sovereignty, meaning certified providers must ensure that foreign laws cannot grant third-party access to stored data. It effectively acts as a barrier against US tech giants dominating sensitive French public sector and critical infrastructure cloud contracts. Such a certification scheme could be fostered by the future CSA-2, but at the time of this report, EU level negotiations on the matter are not showing progress in that way[186].

A related concern on the cloud's dependencies is the concentration of essential digital services among a small number of global cloud providers sometimes called *hyperscalers*. A hyperscaler is a very large cloud company that runs massive data centres and provides computing services at global scale (e.g. Google Cloud or Amazon Cloud Services). Finland and France underline that the consolidation of emergency management platforms within a limited number of large data centres increases centralisation risks. Reliance on a small group of hyperscale providers creates systemic vulnerabilities and raises sovereignty concerns

[185] DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures aimed at ensuring a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148, Annex I, section 8

[186] Contexte, *Le DG de l'Anssi refuse de baisser les bras après la déconvenue de la France sur le CSA-2 (website) (consulted on March 25, 2026)*

where critical data or operational control depend on infrastructures subject to foreign jurisdictions[187].
In Sweden, the MCF risk assessment further explains that because multiple public and private services often share the same cloud environment, incidents such as cyberattacks, misconfigurations or software failures may propagate rapidly across sectors, potentially disrupting emergency coordination functions even when physical communication networks remain operational[188].

France's strategic review prioritises the protection of these Digital Infrastructure components to ensure the "sovereignty in the digital space" necessary for the continuity of the Nation's essential functions, especially during geopolitical tensions[189].

5.5 – The key role of the Public Administration sector

Public Administration is a highly critical sector under the NIS-2 Directive and a critical sector under the CER Directive when delivering essential public services. Finland's risk assessment report highlights that public safety depends on "authorities' communication channels" and the "public administration's digital services" to maintain leadership during crises[190].

Furthermore, both Sweden and Finland identify personnel shortage as a major vulnerability during pandemics or large-scale accidents, public administration may lack the staff to operate PSAPs or coordinate rescue services[191]. A staff shortage automatically impacts emergency communications as answering time for emergency calls increases and call takers become overloaded.

To meet synergy requirements, France's National Strategic review emphasises that resilience requires a "strengthened civil-military dialogue" and synergy between the Ministry for the Armed Forces and "all State services," including with regional administrative authorities. The armed forces should be able to help civilian entities dealing with any major crisis as part of a strengthened civil-military dialogue[192]. Finland notes that security threats are becoming so diverse and rapid that it is increasingly difficult to determine who is the competent authority in charge during the early stages of an incident[193], which might complicate the reaction of public administration entities in charge of supervising or issuing public warning for example.

Another challenge could be a competence clash between the national and a regional level when it comes to responsibilities and actions. Finland's assessment manages regional fragmentation by differencing national risk assessments from regional risk assessments, hence ensuring that threats characteristic of specific regions are not overlooked[194].

[187] (FINLAND) National Risk Assessment (2023), Section 2.4; (FRANCE) National Strategic Review (2022), Section 1.3(27)
[188] (SWEDEN) MSB - National Risk and Vulnerability Assessment (NRSB) (2025), p. 66
[189] (FRANCE) National Strategic Review (2022), § 98
[190] (FINLAND) National Risk Assessment (2023), p. 60
[191] (FINLAND) National Risk Assessment (2023), p. 73; (SWEDEN) MSB - National Risk and Vulnerability Assessment (NRSB) (2025), p. 13
[192] (FRANCE) National Strategic Review (2022), § 117-118
[193] (FINLAND) National Risk Assessment (2023), 1.3, p. 12
[194] *Ibid*., p. 10

Linking public administration to the economic aspect, the CER Directive mandates that Member States ensure their competent authorities have "adequate financial, human and technical resources" to perform their tasks[195]. However, the public administration faces systemic risks regarding its financial ability to maintain essential functions during a crisis, hence funding is a prerequisite to the good functioning of public administration and to the essential services it delivers.

Finland's risk assessment explicitly identifies "disruption of the public economy" as a threat scenario, noting that the availability of funding is a "precondition for safeguarding the vital functions of society"[196]. The assessment further warns that "increasing indebtedness and indirect liabilities" have already weakened the state's "freedom of action" and its ability to face negative shocks[197].

5.6 - Cyberattacks on emergency communications reveal critical interdependencies

The 2025 ENISA report on threat landscape in Europe identifies 5 major kinds of cyberattacks: Distributed Denial of Service (DDoS), ransomware, phishing, Foreign Information Manipulation and Interference (FIMI) and cyberespionage.

Ransomware is identified as the most impactful cybercrime tool in the EU. It involves deploying malicious software that can cause significant service disruptions. It remains a primary threat, particularly affecting public administration entities at municipal level.

DDoS attacks are high-volume but generally low-impact campaigns that target the websites of various organisations. Their primary goal is to overwhelm a service to make it unavailable. These attacks are understood as Hacktivism, it means they are largely ideology-driven rather than financially motivated.

Phishing is the dominant initial infection vector, used in approximately 60% of recorded cases to gain access to a system. It consists of several specific techniques such as *malspam* (unsolicited emails containing harmful links or attachments), *vishing* (use of phone calls to trick individuals into divulging sensitive information) and *malvertising* (malicious online ads distributing malware).

FIMI consists in campaigns designed to manipulate information and interfere with the public discourse while *cyberespionage* refers to state-aligned activities aimed at gathering intelligence. Emergency services are mostly threatened by ransomware, DDoS and phishing cyberattacks, each of these categories encompassing other subcategories of cyberattacks.

These attacks target European critical sectors for various reasons. A small part consists of cyberespionage.

[195] DIRECTIVE (EU) 2022/2557 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, Art. 9(4)
[196] (FINLAND) National Risk Assessment (2023), p. 48
[197] *Ibid*., p. 49

Others are financially motivated, such as the Iranian company *Emennet Pasargad* case[198], but most are ideology-driven and seek geopolitical destabilisation, with, for instance, services disruption or election interference caused by Russian hacker groups. ENISA reveals that critical sectors are not equally targeted. Public administration, transport, digital infrastructure and services, finance, and manufacturing are the most threatened critical sectors, with essential entities representing 53,7% of the total number of recorded incidents[199].

A 2024 report from the NIS Cooperation Group analysed the cybersecurity challenges faced by the communication infrastructure in Europe. It highlighted that "cyber-attacks on the telecom sector would have impact and spill-over effects in many critical sectors. Network outages, for instance, would disrupt the overall economy and society. Access to emergency services and numbers, and public warning systems would be disrupted, which would complicate emergency response in crisis situations. Additionally, the emergency services themselves may be disrupted, if their communications and systems depend on the public mobile networks"[200].

In 2022, a ransomware attack was conducted by *Qilin*, a Russian hacker group, targeting the information system of Slovenia's Administration for Civil Protection and Disaster Relief. This attack aimed at disrupting public services and stealing sensitive data. Overall, the attack failed since no PSAPs were directly affected, and no sensitive documents were published. The hacker used passwords and usernames from one of the civil servants to enter the information network. The group locked files from the Public Administration and asked for a ransom to unlock them, while also trying to upgrade malicious programmes on the administration servers. However, due to a lack of time before the cyber protection system was rebooted, the attackers were not able to succeed in continuing the attack[201].

To prevent future risks, the NIS cooperation group is urging Member States to assess the security of international communications, clarify which authorities oversee these links, and specifically map submarine cable infrastructure and secure satellite connectivity. The objective is to identify who is responsible for protecting them and what foreign legal obligations apply to operators managing this critical infrastructure on the Member States territory[202]. It also urges national authorities responsible for cybersecurity under the NIS Directive should share best practices with counterparts overseeing the critical infrastructure protection under the CER Directive. This would improve the coordination and preparedness against physical attacks directed towards the infrastructure that digital systems rely on[203].

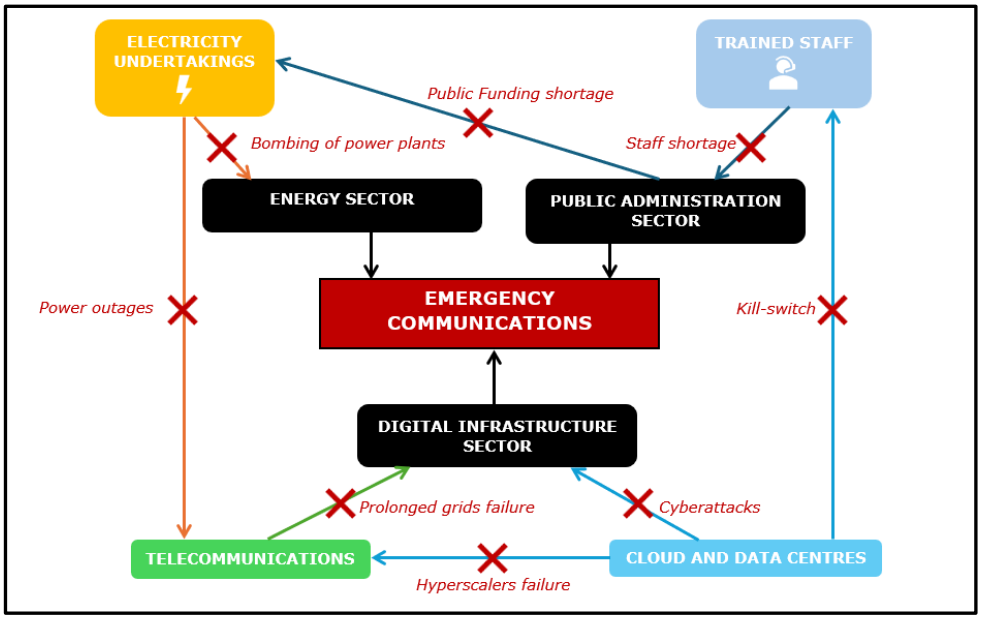
During EENA's visit of the 112 call centre in Brussels, the PSAP described its cybersecurity process. It has been targeted by a cyberattack in December 2025, and encountered technical issues which disrupted

[198] European Council - Cyber-attacks against the EU and its member states: Council sanctions three entities and two individuals (website) (consulted on 8 April, 2026)
[199] (ENISA) Threat Landscape (October 2025), p. 3
[200] (NIS Cooperation Group) Cybersecurity and resiliency of Europe's communications infrastructures and networks (21 February 2024), p. 13
[201] EENA (website) (consulted on 9 April, 2026)
[202] (NIS Cooperation Group) Cybersecurity and resiliency of Europe's communications infrastructures and networks (21 February 2024), p. 18
[203] (NIS Cooperation Group) Cybersecurity and resiliency of Europe's communications infrastructures and networks (21 February 2024), p. 20

emergency calls routing capacity during four hours. The cyberattack did not cause crucial damage but it triggered the cybersecurity management process and highlighted cyber exposure. The 112 PSAP has an Information Technology (IT) team, responsible for the security and supervision of the software used to convey emergency communications. An alert message was sent to Brussels-Capital region through the BE-Alert, a location-based SMS public warning system. The IT Team then conducted an inspection of the software. Similar to the risk assessment reporting requirement of the NIS-2 Directive, a report was sent to supervisory authorities. Since Belgium is a federal state, PSAPs report first to their regional authorities. If the crisis spreads and intensifies, the federal level gets involved.

Lastly, a rising concern for emergency communications is the growing use of AI during cyberattacks. ENISA notes that state-aligned intrusion sets and cybercriminal operators are increasingly leveraging AI to enhance their operations. Specifically, hackers use artificial intelligence for the productivity and optimisation of their malicious activities[204]. Another cyber threat is emerging with the introducing of AI systems in PSAPs, especially in the United States. These systems aim to manage non-emergency calls that normally put a burden on call takers during the triage process. Once hacked, such AI tools may pose a high-risk threat as misrouting or blocking calls, or even misclassifying "urgent calls" as "non-urgent" ones.

Figure 6 - Emergency communications dependencies across critical sectors



[204] (ENISA) Threat Landscape (October 2025), p. 4

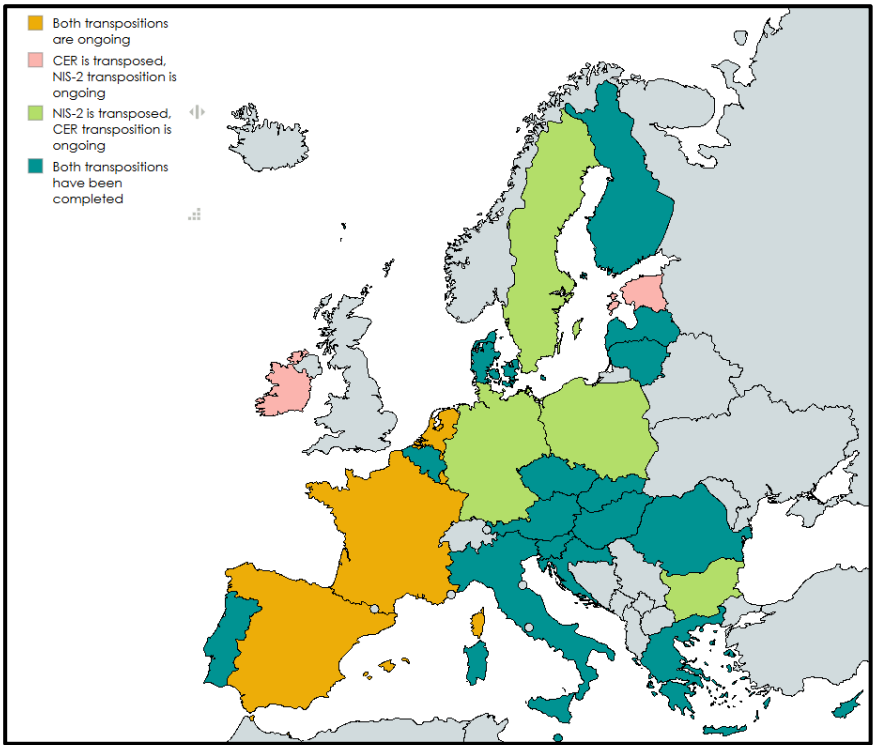
VI – Emergency communications entities feedback: identifying policy gaps and challenges

This section examines how the implementation process of both the CER and the NIS-2 Directives has influenced the work environment of PSAPs and MNOs. It highlights the different requirements, obstacles and also achievements or change induced by the laws.

In order to collect information to assess the real impact of the resilience and cybersecurity framework on the emergency communications' infrastructure, survey questionnaires were sent to PSAPs, MNOs and emergency communications software providers.

Since the EU Member States we have selected did not all transpose the CER and NIS-2 Directives, the questionnaires were sent more broadly to PSAPs and MNOs from other states. Concerning France and Spain, the questionnaires sent to cybersecurity national authorities asked for any information regarding the pending transposition. The map that follows displays the current state of the CER and NIS-2 Directives national transposition at the EU level.

Figure 7 – National transpositions of the CER and NIS-2 Directives at the EU level



Source: CER.com – NIS-2 tracker *ECSO (12/05/2026)*

The questionnaire was sent to several PSAPs, MNOs, and national authorities across around 20 different EU Member States. For both legal and technical reasons, only a few entities responded, giving an overview of the current impact the CER and NIS-2 Directives have on emergency communications.[205]

First, a majority of MNOs and PSAPs report that they qualify as critical entities under the CER Directive. Second, most of them specify they are considered essential entities under the NIS-2 Directive. Which means that all of the subsequent legal obligations analysed above are incumbent on them. For instance, several confirmed that risk assessments concerning physical resilience and cybersecurity had to be done. While MNOs do these reporting procedures under the supervision of a national authority, PSAPs appear to also conduct them internally.

Third, PSAPs generally stated that they belong to the Public Administration critical sector. However, others stated that they belonged to another sector in accordance with their Member State's specific framework. For instance, Lithuanian 112 call centres belong to the "public security" sector. When not kept confidential, MNOs' critical sector mostly is the Digital Infrastructure. Finally, both categories of critical entities, particularly mobile network operators, reported that their cooperation has increased moderately following the implementation of the CER and NIS-2 frameworks.

6.1 - Public Safety Answering Points

While it seems clear that PSAPs are outside the scope of CER and the NIS-2 Directives, many national rules on critical infrastructure, including on the implementation of the CER Directives, appear to interpret PSAPs as being within its scope.

First, it should be noted that some PSAPs preferred to remain confidential and were therefore unable to respond to the questionnaire. In Romania, although no official answers could be provided regarding the questionnaire, the national administrator of the 112 system stated that PSAPs are protected according to national legislation in the field.

Some PSAPs say they are already well prepared, as security and risk planning have long been part of their system. They affirmed regularly carrying out internal risk assessments and having added resilience measures, though many were already in place. For them, the EU Directives have led to some changes, mainly in reporting and crisis management, but daily work remains mostly unchanged and the overall impact is neutral. These respondents highlighted that cooperation with telecom operators has slightly increased, backup systems improved, and there are no major challenges or need for extra guidance.

It is important to flag that there currently are differences between EU Member States as many did not transpose the EU Directives. The pending transposition laws may create Union-wide divergences in the resilience scheme.

[205] see Annexes 2 and 3

Moreover, certain countries that have transposed one or both Directives are still finalising internal coordination with their critical entities. For example, in some countries where the NIS-2 Directive has been transposed, it may not be definitively clear whether emergency call centres are affected by the Directive.

There is a difference between transposition and full implementation. An EU Directive is "transposed" when a Member State turns it into national law, which most EU States did. However, the Directive is "implemented" when the rules are actually applied in practice.

Divergences among national frameworks are not only due to transpositions and implementations processes, but sometimes also to special regime covering the entities themselves. For example, in Bulgaria, which has transposed the NIS-2 Directive, the National Emergency Call System 112 does not seem to fit within the NIS-2 framework and would appear to be managed autonomously.

Furthermore, PSAPs responded to our questionnaire with relevant insights expressing different approaches to key aspects of the CER and NIS-2 requirements. Some of the PSAPs that did implement new resilience measures following CER risk assessments claimed they were now required to produce even more reports and risk assessments as part of their country security strategy, while national authorities and agencies continuously produce risk assessments. Others underlined that they planned to implement new video surveillance system to improve general security situation inside and outside the PSAP premises. A PSAP also highlighted implementing an "emergency button" to reach directly police services. Such a mechanism will improve the security measures and coordination of police help in case of armed attacks or any other man-made threats.

When asked about the changes induced by the CER and NIS-2 transpositions on their daily tasks, PSAPs revealed the planning of new reporting arrangements. Some also underlined the adoption of a cyber incident managing plan, according to which the PSAP provides data on cyber incidents to relevant services, monitors its security status and exchanges information with other public institutions. When asked about the Directives impact regarding reporting obligations, some PSAPs answered they were expected to report cyber incidents to national cybersecurity centre (i.e. CSIRTs). Some explained having set but not yet achieved series of reporting tasks, others underlined having at least defined the organisations that take in the reports.

About the Directives' impact on crisis management processes, some PSAPs answered that both the process of incident reporting and the need to develop resilience plans have expanded, while others noted that crises management processes, already there before the Directives, were modified accordingly with the new EU legal requirements.

PSAPs identified several challenges in complying with the national transpositions of the CER and NIS-2 Directives. Some stressed the lack of resources and the need for investments as major issues, since ensuring compliance may requires large financial resources for new technologies and qualified specialists who are currently in short supply on the market. Some acknowledged no challenges at all, while others identified the need to align the regulatory frameworks of the NIS-2 and CER Directives, as PSAPs provide

essential services to both the Digital Sector and Public Administration. PSAPs therefore claimed it is necessary to harmonise the EU legal frameworks on the critical infrastructure and avoid duplication.

When asked about new guidance and help from EU or national authorities to comply with the CER and NIS-2 Directives, some PSAPs underlined that both frameworks recognise third-party risk as a key vulnerability. The NIS-2 demands measures for managing digital supply chain risk (e.g. software providers) and the CER emphasises supplier dependencies for physical infrastructure and operations. There is a need for a "unified approach" such as risk assessments, contacts with security clauses, and access management systems.

In all, it appears that there is some confusion over how the CER and NIS Directives implementation apply to PSAPs. While it appears that EU rules were not intended to cover PSAPs, national implementations appear to sometimes cover such entities. It still aligns with the principle of minimum harmonisation, allowing Member States to achieve higher level of resilience than what is prescribed by the Directives. However, more guidance should be given to PSAPs on which new rules affect their sector, whether these are EU rules or national rules.

6.2 - Mobile network operators

Some MNOs underlined the role of national authorities in supervising both their resilience and cybersecurity work, to which most respondents report to them regularly.

MNOs indicated currently working on resilience risk assessments, while obligations connected to cybersecurity reports already apply. While mentioning providers of public electronic communications networks as entities it supervises, the Cybersecurity Act (2019) appears as less important into the cybersecurity reporting process in comparison to the NIS-2 Directive, since it relies on a voluntary basis.

Cooperation with emergency call centres has increased moderately since the EU rules, although a minority of MNOs stated that they do not cooperate at all with such entities.

Overall, the impact of EU rules is perceived positively by the operators. However, they unanimously believe public funding is needed to help cover the extra costs linked to these new obligations.

Although a minority of MNOs answered that the critical sector they have been assigned to under the Directives was confidential, most of the rest confirmed belonging to the sector of Digital Infrastructure.

6.3 – Cybersecurity authorities

After contacting national competent authorities, such as cybersecurity agencies, national CSIRTs and CERTs, we gathered interesting information on the national transposition process in Europe and how emergency communications entities fit in.

First, two representatives from **ENISA** gave us valuable insights into the monitoring of the European critical infrastructure cybersecurity.

Under the EU telecom framework (since the 2009 package and the EECC), and the NIS-2 Directive, the focus is on public electronic communications networks and services offered for a fee to end users. On that basis, 112 access, PSAPs, and the private networks used by police, fire, and ambulance services are generally not provided for a fee, although providers are required by law to ensure access. In the context of ENISA's observations on the application of the NIS-2 framework to the electronic communications sector, PSAPs would therefore generally be understood as falling outside its scope. Such entities would instead typically be addressed through national regulatory authorities (NRAs).

ENISA's representatives underlined that mobile network operators are formally within the scope as "essential entities", as part of the electronic communications sector in Annex I of the NIS-2 Directive (high criticality sectors). Essential entities do not report incidents directly to ENISA. They report to national authorities, CSIRTs or competent authorities, depending on national setup.

ENISA published two reports such as the already mentioned "Threat Landscape" and the "Telecom Security Incidents report"[206]. Each provide a solid overview of cyber threats and real incident trends across critical sectors. However, these are cross-sectoral, so they do not fully reflect the specific setup of emergency communications environments.

In practice, the threat profile depends heavily on the underlying infrastructure. For example, public telecom networks (mobile/fixed) are large, geographically distributed, and exposed systems, where major incidents are often linked to power outages, natural events (e.g. floods, fires, storms), or system failures, rather than purely malicious cyberattacks. Emergency call centres and PSAPs, as well as private networks used by police or fire services, tend to have more specialised architectures, so their risk profile may differ and should be assessed based on their specific technical and operational setup.

Finally, regarding the focus of authorities supervising PSAPs, ENISA's representatives underlined that it would likely include resilience, redundancy, power dependencies, the phase-out of 2G/3G, secure migration to 5G, and ICT supplier risks (including high-risk vendors).

A representative of the **Estonian Computer Emergency Response Team (CERT-EE)** also gave valuable insights on how emergency communications fit within the European legal Framework.
The CERT-EE is a department of Estonian Information System Authority that deals with cybersecurity

[206] (ENISA) Telecom Security Incidents (2024); (ENISA) Threat Landscape (October 2025)

incidents that occur in Estonian networks. It confirmed that police, firefighting, medical, and 112 emergency call centres are all considered critical/essential entities in Estonia under the CER and the NIS-2 Directives. The national team affirmed that the entities under the above-mentioned legal frameworks belong in both the Public Administration sector and the Digital Infrastructure sector.

The CERT-EE representative further explained that its duty is to assist Estonian Internet users in the implementation of preventive measures in order to reduce possible damage from security incidents and to help them respond to security threats.

The contact team deals with security incidents that occur in Estonian networks, start there, or which they have been notified about by citizens or institutions either in Estonia or abroad. It also affirmed that mobile network operators are considered critical/essential entities by the CER and the NIS-2 Directives. The overview of challenges the CERT-EE has observed, as an example throughout 2025, can be found within two articles it published[207].
The main challenges that emergency communications faced in 2025 in Estonia mostly were cable faults, service outages, Russian denial-of-service attacks and cyberattacks (e.g. phishing). These have direct concrete impacts on emergency communications, for instance in May 2025, some telecommunications provider experienced disruptions to its voice services, temporarily disabling voice calls to emergency services.

A contact at the **national CERT from Poland** confirmed that emergency call centres are subject to national regulations implementing the NIS-2 Directive. These entities fall within the constituency of another national-level Polish CSIRT, namely CSIRT GOV. All critical infrastructure entities in Poland belong to the CSIRT GOV constituency.

The **Centre for Cybersecurity in Belgium (CCB)**, responsible for supervising the NIS-2 Directive obligations, explained that Police services are excluded from the NIS-2 obligations.
On the one hand, firefighters and emergency services are included in the scope through the explicit inclusion of the Belgian "Emergency Zones" as important entities in the sector Public administration. On the other hand, ambulance/medical emergency services are covered if they provide healthcare services, as healthcare providers under annex I, sector health. If they are essential or important entities here depends on the organisation size. 112 emergency centres are covered as public administrations as they depend on the Federal Public Service (FPS) of Interior. The FPS of Interior itself is an essential NIS-2 entity.

The CCB works with these entities as with any other NIS-2 entities. If they fall under the NIS-2 Directive they are subject to supervision from the CCB inspection service and are obliged to report significant incidents. Mobile network operators that provide publicly available communication services or public electronic communications networks fall under the NIS-2 Directive as important entities if they are small or micro enterprises, and as essential entities if they are medium or larger enterprises.

[207] CERT-EE (website) (consulted on 7 April, 2026) - https://www.ria.ee/en/cyberspace-2025-year-fraud - https://www.ria.ee/en/how-make-public-services-more-resilient

These are the scope of application rules from the NIS-2 directive, which have been transposed as such in the Belgian law.

Our contact at the CCB has not yet observed any challenges that are specific to these entities. Nevertheless, the cybersecurity authority confirmed that the public sector in Belgium is currently the most targeted sector for cyberattacks.

A contact at **TRAFICOM** provided valuable insights from Finland. The contact team is responsible for supervising the security, redundancy and resilience issues in the telecommunications sector at the National Cybersecurity Centre Finland (NCSC). Their mission is to watch that the operators follow the obligations they have regarding the functioning of the emergency communications.

In Finland, the supervision of the obligations in the NIS-2 and CER Directives is divided between several competent authorities.

In the context of the NIS-2 Directive, the Finnish Transport and Communications Agency (TRAFICOM) supervises, for example, the transport sector and the digital infrastructure sector. The team also supervises part of the public administration sector, and the Single Point of Contact (SPOC) located in their CSIRT coordinates the NIS 2 supervision nationally. On the other hand, the Health sector (medical) is supervised by the Finnish Supervisory Agency. TRAFICOM told that the overall picture around the CER-directive is not so clear, as the identification of the critical entities is still in progress. The information about the identified entities is also going to be classified. TRAFICOM does not supervise the CER-related obligations of the sectors participating in the emergency communications.
In Finland, the police, as a law enforcement entity, is not in the scope of NIS-2 directive. The firefighting entities are not considered "essential" under the NIS-2 Directive, but they are considered "important". The medical entities, and PSAPs are classified as "essential entities".

All of the above belong to the Public Administration Sector. Since TRAFICOM supervises much of the Public Administration Sector, the firefighting entities and the PSAPs are required to report to them about cybersecurity incidents.

At the time of this report, the Agency has not received any incident notifications from these entities. In its supervisory actions, the Agency focuses on big scale proactive guidance for all the entities in different sectors. With limited resources, general guidance is considered the most efficient way to conduct supervisory actions.

The Finnish Supervisory Agency supervises the medical entities. According to TRAFICOM's representative, their situation regarding the supervision is quite similar. The NCSC very much work with the MNO's cybersecurity issues, and MNOs are considered "essential".

According to our contact, TRAFICOM has not observed remarkable problems when it comes to the

cybersecurity of the entities participating in the emergency communications and services (police, firefighting, ambulance, PSAPs).

The Agency sees that the lack of resources and knowledge poses challenges when it comes to the supervision of NIS-2 requirements, especially with the other competent authorities that do not have a strong experience, particularly in the field of cybersecurity. The overlap of the supervision competences between different authorities is also a problem that requires cooperation and coordination. For example, the Health sector is currently perceived as problematic, as some of the actions in that sector are supervised by TRAFICOM and some by the Finnish Supervisory Agency.

For the Czech Republic, a representative from the **National Cyber And Information Security Agency (*NUKIB*)** answered our questions. First, the police, firefighting, medical or 112 emergency call centres are considered essential entities under the Czech Act on Cybersecurity. The CER Directive is not fully implemented as of May 2026, but it is expected that these subjects will be deemed critical as well. In the Czech Republic, the Police and firefighting fit in the sector of Public Administration, while Emergency Medical Service units belong to the Health sector. None of them belong to the Digital Infrastructure, but the Czech Act on Cybersecurity requires regulated entities to regulate their key suppliers.

In addition to the fact that these suppliers will be subject to special requirements, those of them that provide key digital infrastructure will likely fall in the scope of the Czech Act on Cybersecurity in the sector of Digital Infrastructure themselves. These entities are required to report incidents to *NUKIB*.

If capacity allows, the Agency is available for consultations, this was much more common with the previous Act on Cybersecurity when the Agency had a much lesser number of regulated entities. With the NIS-2 Directive, that number has increased 15-fold without increasing the staffing capacity of NUKIB, for that reason personalised access will be quite limited.

MNOs are considered essential entities within the Digital Infrastructure sector along with other key providers of digital infrastructure. Finally, the cybersecurity maturity of these entities is at a relatively high level. NUKIB was not able to mention detailed challenges faced by the emergency communications.

VII – Conclusions

Emergency communications constitute a cornerstone of public safety in Europe. As this report has demonstrated, the physical resilience and cybersecurity of the critical infrastructure they rely on are formally codified within a layered European legal architecture. The CER and the NIS-2 Directives, both in force since 2023, together establish the twin pillars of this framework, addressing respectively the physical resilience of critical entities and the cybersecurity of the network and information systems they use. Should it be adopted, the CSA-2 would represent a significant step forward in harmonising cybersecurity requirements across the Union, strengthening certification schemes, addressing ICT supply-chain risks, and reinforcing ENISA's operational role.

In accordance with real-world feedback gathered through surveys, this report concludes that PSAPs are interpreted in some countries as qualifying as critical and essential entities under the CER and NIS-2 Directives, even if these entities do not appear to fall under the Directives' scope. Nevertheless, if their classification as critical entities is acted nationally, they are then subject to a comprehensive set of legal obligations, including regular risk assessments, incident reporting, cybersecurity risk management measures, and resilience planning. In any way, some components of the infrastructure they depend upon, from electronic communications networks and data centres to satellite systems and energy supply, is either explicitly classified as critical infrastructure or as an infrastructure that requires strong protection and close oversight.

At the time of this report, not all EU Member States have transposed the CER and NIS-2 Directives into national law within the deadlines. This uneven transposition creates a fragmented legal landscape across the Union, undermining the very harmonisation these Directives seek to achieve. Furthermore, even in Member States that have completed the transposition phase, the practical implementation varies considerably. Some countries explicitly recognise PSAPs as critical entities under their national frameworks, while others leave their classification ambiguous.

Beyond legal transposition, the report identifies major structural challenges that no regulatory text alone can fully resolve. Chief among these is the hybrid and multifaceted nature of contemporary threats. Cyberattacks, power outages, satellite disruptions, natural disasters and deliberate physical attacks on infrastructure rarely occur in isolation. They combine, cascade, and propagate across interdependent critical sectors in ways that are difficult to anticipate and even harder to contain. Emergency communications sit at the intersection of several sectors, such as Energy, Digital Infrastructure, Cloud services, and Public Administration. A prolonged power outage, a hyperscaler failure, or a coordinated cyberattack on telecom networks can each independently disable emergency communications and public warning systems. These interdependencies are well recognised in national risk assessments.

In this context, civil-military cooperation takes on growing strategic relevance. NATO perceives resilience as both a national responsibility and a collective commitment. While emergency communications at the micro level remain a national competence, the broader infrastructure that makes the critical infrastructure

more resilient is increasingly dependent on systems that intersect with military planning and NATO's baseline requirements. The Resilience Committee and the Euro-Atlantic Disaster Response Coordination Centre represent a framework within which civil and military actors can align their preparedness efforts, share threat assessments, and coordinate responses to large-scale disasters. The EU-NATO Task Force on the resilience of critical infrastructure, and the parallel assessments it produces, further demonstrate that structured dialogue between the two organisations already produces concrete results.

Ultimately, the picture that emerges from this report is one of significant progress made, but substantial work remaining. The resilience of emergency communications is not merely a technical or legal matter. It is a measure of a society's capacity to protect its citizens when they are most vulnerable, and to hold together when crises strike.

VIII - Key Recommendations

Several challenges have been identified all along this report. First, the diverging implementations of the CER and NIS-2 Directives in the Union creates various levels of resilience. On the one hand, we encourage Member States to take all measures to achieve the legal transposition process to ensure a coherent, clear and consistent set of cybersecurity and resilience rules to protect their critical infrastructure. On the other hand, we recommend that critical entities comply with their obligations.

The main legal problem identified in this report is the confusion over the scope of the CER and NIS-2 Directives regarding emergency communications entities. It seems from our reading and some Member States' practices that PSAPs are not covered by these supranational laws. However, in other Member States they are, which creates ambiguity. In addition, the piling up of legislation with the NIS-2 Directive, the CER Directive, the DNA regulation, and the CSA-2 regulation may confuse stakeholders. EU-level clarification explicitly defining the status and obligations of PSAPs within the critical infrastructure ecosystem would be useful. In any case, we recommend that PSAPs are efficiently supervised and protected through resilience and cybersecurity measures, either under national or supranational frameworks. We also recommend that all components of the emergency communications infrastructure vital to PSAPs' missions must be clearly identified as critical infrastructure and be supervised and protected accordingly.

Since cyberattacks target the Public Administration Sector the most, we recommend that Member States, with the support of the European Union, provide more staff and funding to the cybersecurity agencies and national CSIRTs to ensure uninterrupted assistance to essential entities and develop enhanced capabilities to face those ever-evolving threats.

Member States should help PSAPs to develop their communication technologies and to comply with the Directives' requirements. In addition, we recommend fostering enhanced cooperation between entities beyond CER and NIS-2 obligations, such as joint crisis protocols between PSAPs and MNOs.

Finally, the physical protection and defence of PSAPs premises is essential to prevent the disruption of the essential services they deliver. During the 2026 EENA Conference, Police Colonel Leonid Tymchenko, Deputy Minister of Internal Affairs in Ukraine, explained the preparation of emergency call centres during ongoing armed attacks. Ukraine built underground control rooms to protect call takers from bombing and ensure the continuity of emergency communications even under Russian missiles strikes. In both cybersecurity and physical protection, we recommend exploring the potential for civil–military cooperation, particularly through joint crisis management exercises and the sharing of resources.

IX – Bibliography

National legislation

(FINLAND) Act 124/2025 Cybersecurity Act (entered into force on April 8, 2025) https://www.finlex.fi/api/media/statute/690158/mainPdf/main.pdf?timestamp=2025-04-03T21%3A00%3A00.000Z

(FINLAND) Act 310/2025 on the Protection of Infrastructure Critical to Society and on the Improvement of Resilience (entered into force on July 1, 2025) https://www.finlex.fi/api/media/statute/690023/mainPdf/main.pdf?timestamp=2025-06-12T21%3A00%3A00.000Z

(FINLAND) Finland's Cybersecurity Strategy 2024–2035 (2024) https://julkaisut.valtioneuvosto.fi/server/api/core/bitstreams/e5575ec3-1ce2-4f0a-aaff-50154789cb6d/content

(FINLAND) National Risk Assessment (2023) https://julkaisut.valtioneuvosto.fi/server/api/core/bitstreams/072fa79a-f148-4fd2-af2d-38d925166a61/content

(FRANCE) ANSSI – Strategic Plan of the Agency of national security and information systems (2025) https://www.enisa.europa.eu/sites/default/files/ncssmap/strategies/reports/FR_NCSS_2025_fr.pdf

(FRANCE) Draft Law on the Resilience of critical infrastructures and the strengthening of cybersecurity (2025) (on negotiation) https://www.assemblee-nationale.fr/dyn/17/dossiers/DLR5L17N50731

(FRANCE) National Strategic Review (2022) https://www.sgdsn.gouv.fr/files/files/rns-uk-20221202.pdf

(HUNGARY) Act LXIX on the Cybersecurity of Hungary (entered into force on January 1, 2025) https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwi6ktqK7JWUAxW5P_sDHW5EKxEQFnoECBgQAQ&url=https%3A%2F%2Fnjt.hu%2Fjogszabaly%2Fen%2F2024-69-00-00&usg=AOvVaw16YlmqR40iT_89gSMqk73z&opi=89978449

(HUNGARY) Act LXXXIV on the Resilience of Critical Organisations (entered into force on January 1, 2024) https://www.vizmuvek.hu/files/public/new/torvenyek-jogszabalyok/2024-_evi_lxxxiv-_torv-ny-kozlonyallapot-20241220.pdf

(HUNGARY) Government Decree no. 474/2024 (XII. 31.) on implementing the Hungarian CER Act (Act LXXXIV of 2024)

(HUNGARY) Government resolution no. 1089/2025 (III. 31.) on Hungary's Cybersecurity Strategy https://www.enisa.europa.eu/sites/default/files/ncssmap/strategies/reports/HU_NCSS_2025_hu.pdf

(ROMANIA) Decision no. 1.321/2021 regarding the approval of the Cybersecurity Strategy of Romania for the period 2022–2027, as well as of the Action Plan for the implementation of the Cybersecurity Strategy of Romania for the period 2022–2027. https://legislatie.just.ro/Public/DetaliiDocument/250128

(ROMANIA) Decision *no. 55/2025* approving the list of sectoral competent authorities in the field of the resilience of critical entities (31 January 2025) https://legislatie.just.ro/Public/DetaliiDocument/294182

(ROMANIA) Law no. 124/2025 for the approval of Government Emergency Ordinance No. 155/2024 on establishing a framework for the cybersecurity of networks and information systems in the national civil cyberspace (entered into force on June 15, 2025) https://legislatie.just.ro/Public/DetaliiDocument/299675

(ROMANIA) Law no. 294/2024 on the resilience of critical entities and amending certain legislative acts (entered into force on October 29, 2024) https://legislatie.just.ro/Public/DetaliiDocument/291491

(ROMANIA) Law no. 58/2024 on the cybersecurity and defence of Romania, as well as for the amendment and completion of certain normative acts (entered into force on March 13, 2024) https://www.sri.ro/assets/files/legislatie/2024-eng/the_Law_No_58.pdf

(SPAIN) Draft Law on Cybersecurity Coordination and Governance (2025) (ongoing negotiation)

(SPAIN) Draft Law on the Protection and Resilience of Critical Entities (2025) (ongoing negotiation)

(SPAIN) National Cybersecurity strategy (2013)

(SWEDEN) A national cybersecurity strategy (2017)

(SWEDEN) Cybersecurity Act 1506:2025 (entered into force on January 15, 2026)

(SWEDEN) Cybersecurity ordinance 1507:2025 (entered into force on January 15, 2026)

(SWEDEN) MSB - National Risk and Vulnerability Assessment (NRSB) (2025)

(SWEDEN) National Strategy for Cybersecurity 2025-2029 (2025)

(SWEDEN) Resilience in Essential Services, Final Report of the Inquiry on the Implementation of the NIS-2 and CER Directives (2024)

Supranational corpus

(ENISA) Telecom Security Incidents report (2024)

(EU-NATO) EU-NATO task force on the resilience of critical infrastructure final assessment report (29 June 2023)

(NATO) 2022 STRATEGIC CONCEPT Adopted by Heads of State and Government at the NATO Summit in Madrid (29 June 2022)

(NATO) Emergency management exercise in Bulgaria – EADRCC Evaluation and Impact Report, 2025

(NATO) Funding NATO, https://www.nato.int/en/what-we-do/introduction-to-nato/funding-nato

(NATO) *NATO 2030 : United for a New Era*, Analysis and recommendations of the reflection group appointed by the NATO Secretary General (25 November 2020)

(NATO) Resilience – NATO Chief Scientist Research Report (19 December 2025) Science and Technology Organisation (STO)

(NATO) Supreme Headquarter Allied Powers in Europe (website) (consulted on March 03, 2026), https://shape.nato.int

(NATO) The European-Atlantic Disaster Response Coordination Centre, Factsheet (April 2025)

(NATO) TREATY OF THE NORTH ATLANTIC ALLIANCE ORGANISATION of 4 April 1949

(NIS Cooperation Group) Cybersecurity and resiliency of Europe's communications infrastructures and networks (21 February 2024)

COMMUNICATION FROM THE EUROPEAN COMMISSION (2025), Commission Guidelines and reporting template developed pursuant to Articles 5(5), 6(6) and 7(3) of Directive (EU) 2022/2557 on the resilience of critical entities

DECISION No 1313/2013/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 December 2013 on a Union Civil Protection Mechanism

DIRECTIVE (EU) 2018/1972 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 December 2018 establishing the European Electronic Communications Code

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures aimed at ensuring a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148

DIRECTIVE (EU) 2022/2557 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Union Agency for Cybersecurity (ENISA), the European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on digital networks, amending Regulation (EU) 2015/2120, Directive 2002/58/EC and Decision no. 676/2002/EC and repealing Regulation (EU) 2018/1971, Directive (EU) 2018/1972 and Decision no. 243/2012/EU

(NATO) Strengthened Resilience Commitment (14 June 2021)

(ENISA) Threat Landscape (October 2025)

Articles

Collaborative Coalition for International Public Safety (CC:IPS), Public Safety Mission Critical Communications – Is it Critical Infrastructure ? (July 2024)

HASHIMOTO, Taro, «Cooperation on Critical Infrastructure Cybersecurity and Resilience», *Operationalizing Japan-U.S. Cooperation on Critical Infrastructure Cybersecurity and Resilience*, 2024, pp. 23–41

PARKES, Roderick, «NUTS AND BOLTS», *PROTECTING EUROPE: The EU's response to hybrid threats*, 2019, pp. 23–33

SLAKAITYTE, Veronika, and SURWILLO, Izabela, «PROTECTING EU'S CRITICAL INFRASTRUCTURE The fight intensifies in the cyber realm», Danish Institute for International Studies, 2024, 5 p.

Websites

CERT-EE (website) (consulted on 7 April, 2026) - https://www.ria.ee/en/cyberspace-2025-year-fraud - https://www.ria.ee/en/how-make-public-services-more-resilient

Contexte, *Le DG de l'Anssi refuse de baisser les bras après la déconvenue de la France sur le CSA-2 (website) (consulted on 25 March, 2026) https://www.contexte.com/fr/actualite/tech/le-dg-de-lanssi-refuse-de-baisser-les-bras-apres-la-deconvenue-de-la-france-sur-le-csa-2_259509?go-back-to-briefitem=259509*

Critical Entities Resilience (CER) (website) (consulted on 16 March, 2026) https://www.critical-entities-resilience-directive.com/Critical_Entities_Resilience_Directive_Transposition.html

EENA (website) (consulted on 9 April, 2026) https://eena.org/webinar/lessons-from-the-cyber-attack-on-slovenias-civil-protection-system/

EENA (website) Emergency call handling service chain description (consulted on 5 May, 2026) - https://eena.org/wp-content/uploads/2020/12/2020_12_08_ServiceChainV2.1.pdf

European centre of excellence for civilian crisis management (website) (consulted on 27 February, 2026) https://www.coe-civ.eu

European Commission - Enhancing Europe's capacity to react – preparing the European Critical Communication System (consulted on 7 April, 2026) https://home-affairs.ec.europa.eu/news/enhancing-europes-capacity-react-preparing-european-critical-communication-system-2026-01-30_en

European Commission - List of single points of contact – Directive (EU) 2022/2557 on the Resilience of Critical Entities (consulted on 13 March, 2026) List of SPOC

European Commission – NIS-2 Directive transposition in EU countries (consulted on 19 March, 2026) https://digital-strategy.ec.europa.eu/en/policies/nis-transposition

European Council - *Cyber-attacks against the EU and its member states: Council sanctions three entities and two individuals* (website) (consulted on 8 April, 2026) https://www.consilium.europa.eu/en/press/press-releases/2026/03/16/cyber-attacks-against-the-eu-and-its-member-states-council-sanctions-three-entities-and-two-individuals/

European Cybersecurity Organisation (ECSO) (website) (consulted on March 16, 2026) https://ecs-org.eu/activities/nis2-directive-transposition-tracker/?utm_source=chatgpt.com

European Network and Information Security Agency (ENISA), (website) (consulted on 23 February, 2026) https://www.enisa.europa.eu/

Finnish Government, *Government approves risk assessment of critical infrastructure* (website) (consulted on 20 February, 2026) https://valtioneuvosto.fi/en/-/1410869/government-approves-risk-assessment-of-critical-infrastructure

French Government - ANSSI, *Mon Espace NIS-2*, (website) (consulted on 1st April, 2026) https://monespacenis2.cyber.gouv.fr/simulateur

Government Offices of Sweden, *SOS Alarm Sverige AB (SOS Alarm)* (website) (consulted on 26 February, 2026) https://www.government.se/government-agencies/sos-alarm-sverige-ab-sos-alarm/

Swedish Civil Defence and Resilience Agency - MCF (website) (consulted on 20 February, 2026) https://www.mcf.se/en/news/2025/december/msb-will-be-swedish-civil-defence-and-resilience-agency-as-of-januari-1-2026/

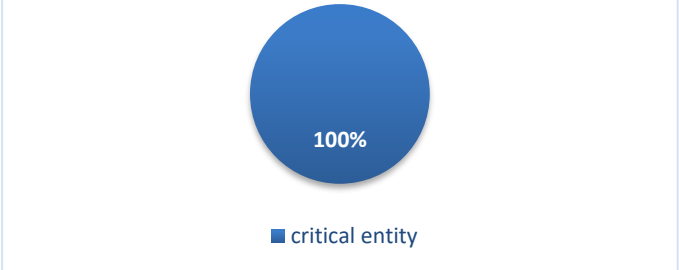
World Bank (website) Climate Change Knowledge Portal, *Global distribution of natural disasters* (consulted on May 15 2026) https://climateknowledgeportal.worldbank.org/country/romania/natural-disasters-historical

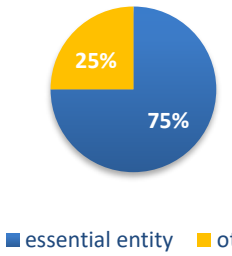
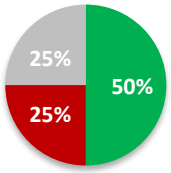
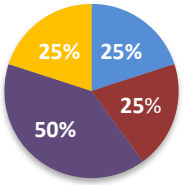
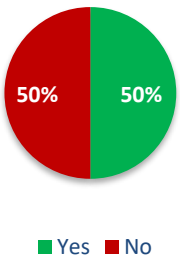
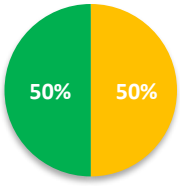
X - ANNEXES

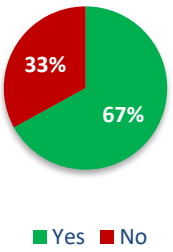
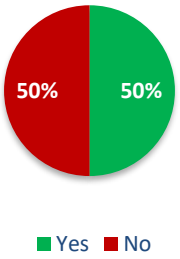
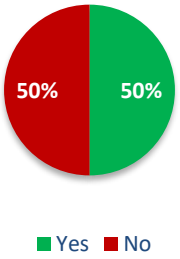
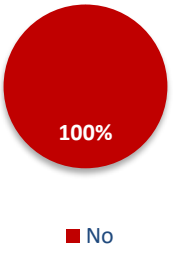
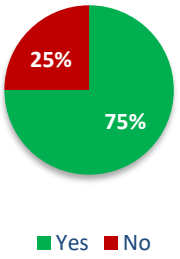
Annex 1 – National Transpositions of the CER and NIS-2 Directives

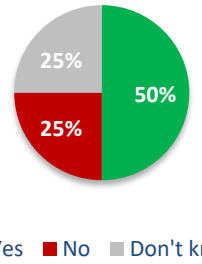
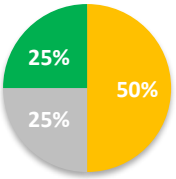
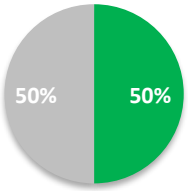
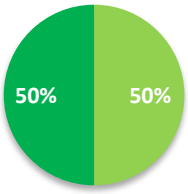
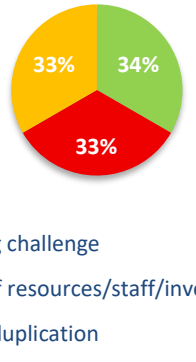
EU Member States	CER transposed	NIS-2 transposed	CER transposition	NIS-2 transposition
FRANCE	ongoing	ongoing	Draft Law on the Resilience of critical infrastructures and the strengthening of cybersecurity (2025)	*Ibid.*
HUNGARY	achieved	achieved	Act LXXXIV on the Resilience of Critical Organisations (2024)	Act LXIX on the Cybersecurity of Hungary (2025)
ROMANIA	achieved	achieved	Law no. 294/2024 on the resilience of critical entities and amending certain legislative acts	Law no. 124/2025 for the approval of Government Emergency Ordinance No. 155/2024 on establishing a framework for the cybersecurity of networks and information systems in the national civil cyberspace
FINLAND	achieved	achieved	Act 310/2025 on the Protection of Infrastructure Critical to Society and on the Improvement of Resilience	Act 124/2025 Cybersecurity Act
SWEDEN	ongoing	achieved	*NA (SOU 2024:64 report)*	Cybersecurity Act 1506:2025
SPAIN	ongoing	ongoing	Draft Law on the Protection and Resilience of Critical Entities (2025)	Draft Law on Cybersecurity Coordination and Governance (2025)

Annex 2 – PSAPs' answers to the questionnaire on critical infrastructure

QUESTIONS	ANSWERS
1. How do you qualify under CER? (*For the respondents from countries that have implemented the CER Directive*)	

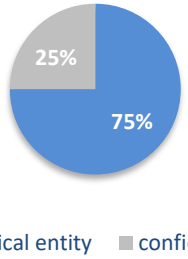
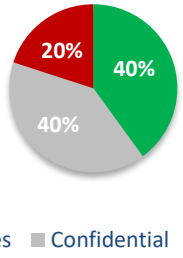
2. How do you qualify under NIS-2? (*For the respondents from countries that have implemented the NIS-2 Directive*)	
3. Are you officially a Public Administration entity?	
4. What is the primary critical sector you belong to?	
5. Have you carried CER risk assessment? (*For the respondents from countries that have implemented the CER Directive*)	
6. How were they conducted? *(If previous answer was yes)*	

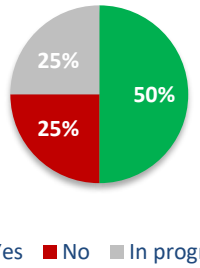
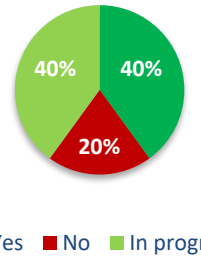
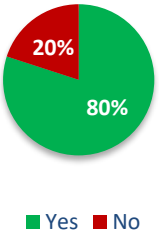
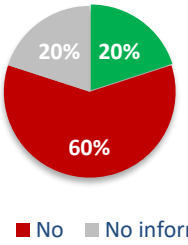
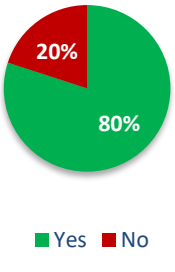
7. Following these, did you implement new resilience measure?	
8. Did cybersecurity governance, reporting obligations, or incident response procedures change as a result of NIS-2 implementation?	
9. Has the transposition or ongoing implementation of the CER and/or NIS-2 Directives in your country, resulted in changes to daily operational procedures?	
10. Has the transposition or ongoing implementation of the CER and/or NIS-2 Directives in your country, resulted in changes to coordination with telecom operators or regulatory authorities?	
11. Has the transposition or ongoing implementation of the CER and/or NIS-2 Directives in your country, resulted in changes to reporting obligations?	

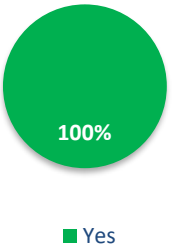
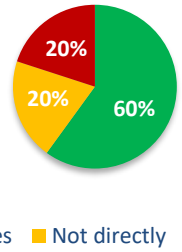
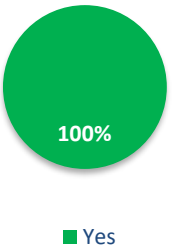
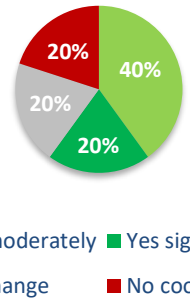
12. Has the transposition or ongoing implementation of the CER and/or NIS-2 Directives in your country, resulted in changes to crisis management processes?	
13. How would you say these changes have affected emergency communication operations mostly?	
14. Has cooperation with telecom operators or digital service providers increased in recent years?	
15. Has your organisation strengthened backup solutions for communication systems (e.g. alternative networks, redundancy, backup power)?	
16. What are the main challenges your organisation faces in complying with CER and NIS-2 requirements?	

17. What additional guidance or support from national or EU authorities would help PSAPs implement these frameworks more effectively?	

Annex 3 – MNOs' answers to the questionnaire on critical infrastructure

QUESTIONS	ANSWERS
1. How do you qualify under CER? (*For the respondents from countries that have implemented the CER Directive*)	
2. How do you qualify under NIS-2? (*For the respondents from countries that have implemented the NIS-2 Directive*)	
3. Have you received a formal confirmation of belonging to the Digital Infrastructure critical sector?	

4. Have you been mandated to conduct CER risk assessments? (*For the respondents from countries that have implemented the CER*)	
5. Have resilience risk assessments already been carried out?	
6(i). Has your organisation received specific obligations requiring cybersecurity risk assessments under the NIS-2?	
6(ii). Has your organisation received specific obligations requiring cybersecurity risk assessments under the CSA?	
7(i). Does a national authority assist or supervise the resilience management of your organisation?	

7(ii). Do you report to this authority on a regular basis? (*For the respondents whose resilience is assisted or supervised by a national authority*)	
8(i). Does a national authority assist or supervise the cybersecurity management of your organisation?	
8(ii). Do you report to this authority on a regular basis? (*For the respondents whose cybersecurity is assisted or supervised by a national authority*)	
9. Since the transposition or ongoing implementation of the CER, NIS-2, or CSA frameworks, has your organisation increased cooperation or coordination with PSAPs?	
10. Overall, how has the implementation of these EU frameworks affected your organisation's work?