AC-23-IAC-23, E5, 4, 4, x77300

Protecting Europe: How can space applications support European States to implement the new Critical Entities Resilience Directive

A. Donati*, V. Fedorchenko**

*Secretary General of the Association of European Space Agencies, Annalisa.donati@eurisy.eu
** Communications Officer of the Association of European Space Agencies, Veronika.fedorchenko@eurisy.eu

In preparation of the approval of the Critical Entities Resilience Directive, Eurisy and the Network of European Regions Using Space Technologies (NEREUS) organised a webinar series to underline the contributions that space applications can make to the implementation of the Directive. The webinars were organised around some of the sectors identified in the Directive, namely energy, transport, banking, financial market infrastructure, health, drinking water, wastewater, digital infrastructure, and public administration. Space-based data and signals offer opportunities to increase the resilience of critical infrastructure in each of such sectors. Indeed, satellite navigation and imagery can support the entire infrastructure life cycle, from site selection to building monitoring and post-construction operations. Galileo and Copernicus, the EU GNSS and EO satellite constellations, are already used by entities responsible for managing critical infrastructure in their daily activities. This paper provides hands-on examples of use of satellite data to increase the resilience of critical infrastructure in Europe, highlighting the potential for replication of the examples presented in other geographical regions. Furthermore, the paper will include recommendations to enhance the exploitation of already existing satellite-based services and to favour the development of new satellite-based services that better respond to the needs of the entities involved in the construction, monitoring and operation of critical infrastructure.

Keywords: space applications, satellite-enabled solutions, resilience, critical infrastructure, Galileo, Copernicus.

General context

Resilience has become a critical concept in shaping new European policies. As stated in the proposal of a Directive of the European Parliament and of the Council on the resilience of critical entities [1], to effectively protect Europeans, the European Union needs to continue to reduce vulnerabilities, including for the critical infrastructures that are essential for the functioning of societies and economy. For this purpose, the European Commission proposed to establish in December 2020 an all-hazards framework to support Member States in ensuring that physical and digital critical entities are able to prevent, resist, absorb and recover from disruptive incidents, no matter if they are caused by natural hazards, accidents, terrorism, insider threats, or public health emergencies. Taking into account the growing challenges in the cybersecurity field, the regulator faced a need for a comprehensive tool to bolster Europe's adaptability to new digital realities.

Although the European Union has long recognised the pan-European importance of critical infrastructures through such mechanisms as the European Programme for Critical Infrastructure Protection (EPCIP) adopted in 2006, and the European Critical Infrastructure (ECI) Directive approved in 2008, it became apparent that the established framework was not sufficient in the face of new challenges. Given an increasing interconnectedness among infrastructures, networks and operators delivering essential services across the internal market, it was necessary to fundamentally switch the current approach from protecting specific assets towards reinforcing the resilience of critical entities that operate them [1].

The environment in which critical entities operate has changed significantly in recent years.

- Firstly, the risk landscape is more complex than in 2008, involving today natural hazards [2] (in many cases exacerbated by climate change), state-sponsored hybrid actions, terrorism, insider threats, pandemics, and accidents (such as industrial accidents).
- Secondly, operators are confronted with challenges in integrating new technologies such as 5G and unmanned vehicles into their operations, while at the same time addressing the vulnerabilities that such technologies could potentially create.
- Thirdly, these technologies and other trends make operators increasingly reliant on one another. The implications of this are clear – a disruption affecting the service provision by one operator in one sector has the potential to generate cascading effects on service provision in other sectors, and also

potentially in other Member States or across the entire Union.

As evidenced by the 2019 evaluation of the ECI Directive [3], it was found to have only partial relevance. Due to the increasingly interconnected and cross-border nature of operations using critical infrastructure, protective measures relating to individual assets alone were recognised as insufficient to prevent all disruptions from taking place [3]. The evaluation also highlighted the need to update and further strengthen the existing rules in light of the new challenges facing the EU.

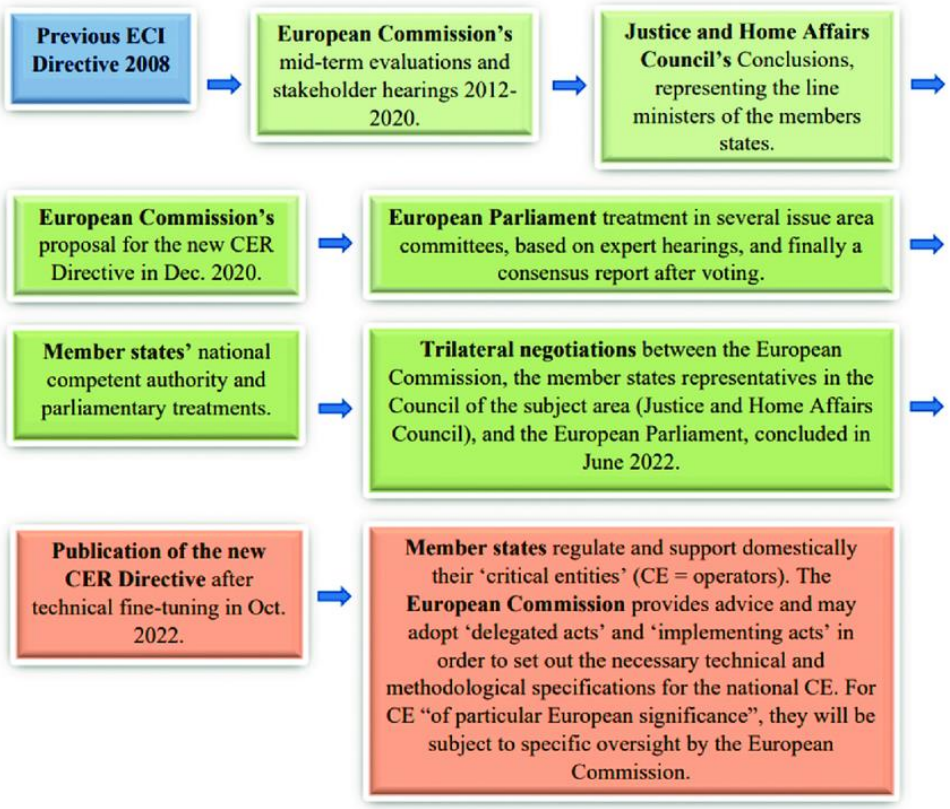

Fig.1. The policy process towards the CER Directive

Source: Christer Pursiainen and Eero Kytömaa, From European critical infrastructure protection to the resilience of European critical entities: what does it mean?

Highlight of novelties of the new directive: what has changed

The new Critical Entities Resilience Directive constituted a considerable change as compared to the ECI Directive, which applies only to the energy and transport sectors, focuses solely on protective measures, and provides a procedure for identifying and designating European critical infrastructures through cross-border dialogue. So what has changed?

- First of all, the new directive has a much wider sectoral scope, covering eleven sectors, namely energy, transport, banking, financial market infrastructure, health, drinking water, waste water, digital infrastructure, public administration, space and food.
- Secondly, the directive provides a procedure for Member States to identify critical entities using common criteria on the basis of a national risk assessment. Furthermore, on 25 July 2023 the

Commission adopted a list of essential services in the eleven sectors covered by the directive which entered into force on 16 January 2023. Member States will have to identify the critical entities for the sectors set out in the CER Directive by 17 July 2026. They will use the list of essential services to carry out risk assessments and to then identify the critical entities. Once identified, the critical entities will have to take measures to enhance their resilience [4].

- Thirdly, the directive sets out obligations on Member States and the critical entities that they identify, including ones with particular European significance, i.e. critical entities that provide essential services to or in more than one third of Member States that would be subject to specific oversight.

Where appropriate, the Commission would provide competent authorities and critical entities with support in complying with their obligations under the directive.

- In addition, *the Critical Entities Resilience Group*, which is a Commission expert group subject to the horizontal framework applicable to such groups, will provide advice to the Commission and promote strategic cooperation and the exchange of information.
- Finally, as the interdependencies do not stop at EU external borders, engagement with partner countries is also necessary. The proposed directive provided for a possibility of such cooperation, for instance, in the area of risk assessments.

Unlike ECI Directive which was based on Article 308 of the Treaty establishing the European Community (corresponding to the current Article 352 of the Treaty on the Functioning of the European Union), the CER directive is based on Article 114 TFEU, which involves the approximation of laws for the improvement of the internal market. This is justified by the shift of the directive's aim, scope and content, increased interdependencies and the need to establish a more level playing field for critical entities. To enforce the rules, the CER directive enables national authorities to conduct on-site inspections and introduce penalties in case of non-compliance.

The directive was presented together with the proposed review of the Network and Information Security Directive (NIS2), which aims to ensure robust cyber resilience on the part of a large number of entities. NIS2 aims to address the limitations of the previous directive, such as insufficient harmonization across Member States and critical sectors and the absence of a joint crisis-response mechanism. In order to ensure alignment between the two instruments, all critical entities identified under the CER directive would be subject to cyber resilience obligations under NIS2. Growing digitalisation of services increases the possibility of cybersecurity threats coming either from hackers, state entities or criminal organisations. A Distributed Denial-of-services (DDoS), for instance, has the potential to debilitate the targeted infrastructure, slowing down the system or causing severe delay in its regular functioning. Moreover, an attack could shut down an entire service, causing serious disruption within society. The 2015 attack against Ukraine represents a fitting example where malware infected the country's electrical infrastructure by targeting its control and data acquisition system, causing power outages in Kiev and other western regions of the state for roughly 230, 000 residents for duration of 1-6 hours [5]. The compromise of the Ukranian power grid was the first confirmed cyber operation to successfully take down energy infrastructure. This instance has also demonstrated how incidents taking place in EU neighboring countries could possibly have an impact on EU Member States due to cross-border interdependencies (European Parliament, 2021).

Why has the concept of protection been replaced by the concept of resilience, and why has the concept of critical infrastructure been replaced by the newly invented euro-concept of critical entities?

Switching to the concept of resilience, which became the cornerstone of the CER Directive, implies the rethinking of the assessment mechanisms. Modelling and the ensuing simulations make it possible to test the resilience of critical infrastructure with creation of digital twins where the space applications like Earth observation data may be of particular use. It may reveal some bottlenecks or weak points in a system and help in decision-making [6].

The new directive reflects not only the ability to protect against possible incidents, but also to bounce back into full operation afterwards. Rather than being limited to the physical assets and infrastructure, the emphasis lies on the entities making use of the infrastructure, as well as on its supply chains and processes. Additionally, as opposed to the preceding directive, Member States will identify critical entities at national level without the need for a cross-border physical connection [7].

On the other hand, there is a shift from a concept of critical infrastructure to that of critical entity. The CER Directive made mention of '*operators (referred to here as "critical entities")*'. Some policy analysts

argue that it aims at moving smoothly from critical infrastructure sectors (such as energy) towards more concrete operators (such as an energy company) or perhaps a facility (a power plant) to enhance and facilitate more detailed monitoring and regulation [6]. Another peculiarity of the CER Directive lies in the question on how to define the 'critical entities' within these 'critical infrastructure sectors'. The CER Directive is fundamentally based on the broader challenge of dependencies and interdependencies. These refer to at least three different types of interrelationships, namely those between different sectors, between countries, and between the physical-digital interfaces. The interdependencies create situations where disruptions in one sector lead to cascading effect in other related sectors. For instance, energy (especially electricity) and ICT sectors are the main cascading initiating sectors.

The webinar series

To reflect on the proposal of the CER Directive, Eurisy together with the Network of European Regions Using Space Technologies (NEREUS) launched in April 2022 a webinar series "Space4Critical Infrastructure". The series aimed at presenting how satellite-based solutions could contribute to the monitoring and maintenance of critical entities in the sectors outlined by the CER Directive. After three introductory webinars presenting the state of play of the legislative path and the rationale behind the enlargement of the scope of a new EU Directive on the resilience of critical entities, a set of thematic webinars were organised to illustrate operational solutions.These webinars were meant to sensitise and discuss with regional stakeholders, research and business community the dimension of space uses to better monitor and safeguard critical entities in different domains. The webinars also explored operational satellite-based applications per each sector identified in the proposed CER Directive and further elaborated on the benefits these solutions can bring to users to ensure more resilient environment to the citizens.

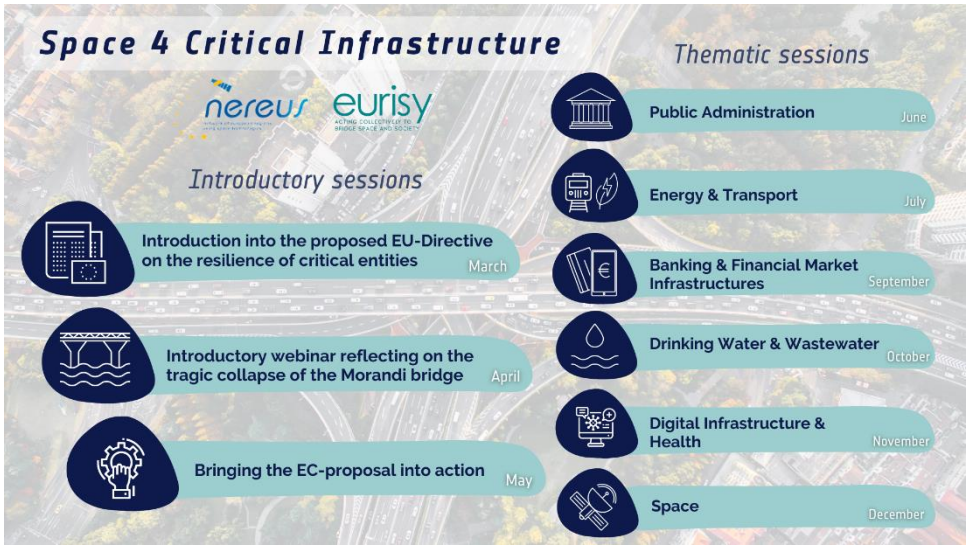

Fig. 2. Structure of Space 4 Critical Infrastructure Sessions

What space can do

With its enlarged scope, the Directive will directly apply to space, at least for what concerns the ground-based segment of space infrastructure. Nonetheless, space assets can also serve Member States to increase the resilience of their critical entities [8]. At ESRIN, the European centre of excellence for exploitation of Earth Observation missions, ESA hosts the International Charter on Space and Natural Disasters. The Charter is a global effort between space agencies to place their satellite resources at the disposal of civil protection authorities to keep an eye on critical infrastructure in the event of a disaster.

From Earth science missions and the sentinel constellation to meteorology in cooperation with Eumetsat, different Earth Observation data sources can help to monitor the status of critical infrastructure such as energy grids, transportation, health infrastructures, etc. One of the recent examples is the Rapid Action on Corona Virus and Earth Observation (RACE), an open platform measuring activities in industries, ports, commercial centres, and other areas to monitor the economic and environmental impact of the coronavirus crisis.

Other examples include regional initiatives (e.g. for the Alps, Atlantic, Black Sea/Sea Danube, Baltic) to enhance regional monitoring (e.g. landslide risk assessment) and environmental protection (e.g. real-time incident satellite imagery in oil and gas industry) in the event of natural or man-made disasters affecting the provision of essential services. Several examples of case studies illustrating the use of satellite derived information are presented in the below paragraph.

Case studies

As demonstrated by the first introductory webinar organised by Eurisy, with environmental regulations on one hand and the continuous maintenance of critical infrastructure on the other, operators and authorities likewise face an increasingly difficult balancing test [7]. A specific example of this was set out by Aurelie Dehouck, founder of i-Sea, a French start-up specialising in developing geo-information solutions in the domain of water and energy management for the use by public sector and industrial actors. To help the French Occitanie Region deal with the risk of turbidity during expansion works in the harbour of Port-la-Nouvelle, the start-up provided the port authorities with satellite data to monitor water quality and to forecast water turbidity during the works.

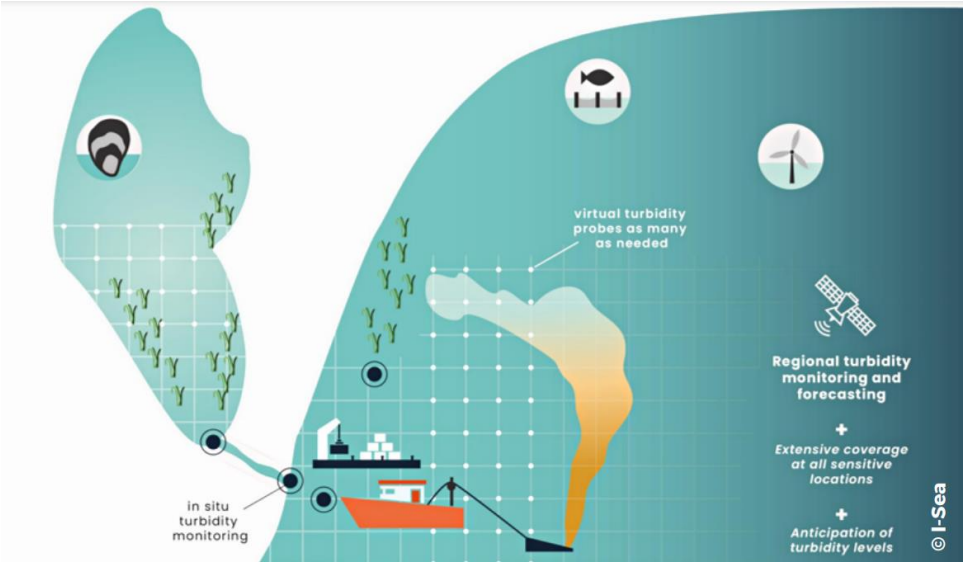

Fig. 3. Monitoring water turbidity during the port extension works at Port-la-Nouvelle, Occitanie region.

The historic port of Port-la-Nouvelle extends over 2.5 kilometres, representing a major economic asset in the area. Owned by the Region, it includes a commercial port, a fishing harbour and a marina. In 2018 the Occitanie region started massive construction works to adapt the commercial port to new traffics and allow for the development of new sectors. To avoid damage to the environment, the port authorities relied on Copernicus satellite imagery to monitor water quality and to rapidly intervene in the event that a turbid plume would spread towards vulnerable areas. Data from Sentinel-2 and Sentinel-3 provided a "Water turbidity weather forecast" nearby the works, in this way damage to the surrounding natural areas was avoided while extending the port [9]. This was the first time that the turbidity forecast model was used withing the context of operational works in the port.

During the second webinar on the introductory part of "Space for Critical Infrastructure" series, researchers and decision-makers shared concrete measures and practices on operational satellite services to support relevant entities with the maintenance of viaducts, tunnels, and highways. Special emphasis was put on lessons learnt from the collapse of the Morandi Bridge in 2018 and its impact on a European wide reflection on how to modernise critical infrastructure monitoring tools. After this incident, Genoa municipality adopted in 2019 "Genova Lighthouse", a sustainable and resilience strategy favouring the use of modern enabling technologies for the management of logistics and transport, the prevention of incidents, and the identification of mitigation actions. Satellite data was used to enhance the resilience of the local infrastructure and to identify landslides around the area of the Saint George Bridge, the viaduct which was inaugurated two years after the collapse of the

Morandi Bridge. Satellite data in combination with in-situ IoT sensors were also exploited to evaluate the oscillation in the bridge, just to mention couple of examples [10]. Thus, Rheticus Safeway, a digital platform for the continuous maintenance of roads and bridges developed by the Italian hi-tech company Planetek Italia, enables operators to move from a reactive approach to a proactive approach by understanding the trends of land movements that have an impact on the infrastructure.

Fig. 4. Ground motion service provides regularly updated nation-wide maps of millimetric ground mouvement based on data from Copernicus Sentinel-1 mission

The system relies on a combination of ground motion analysis and radar satellite data to provide a complete overview of an entire asset. This results in the abilities of critical entities to plan and prioritise inspections. The platform was activated by Anas S.p.A., an Italian company managing the complete cycle of design, maintenance and control of more than 32 000 km of roads and highways, 2100 tunnels, and 15 800 bridges. To complement its continuous surveillance activities, Anas relied on Rheticus Safeway developed with satellite technology. The service regularly provided Anas with information on the infrastructures with a high level of damage. This periodic reporting highlighted those assets on which further inspection had to be addressed to check their integrity. The predictive maintenance of the infrastructure offered by Rheticus Safeway produced concrete benefits for Anas operation, including better continuity and quality of services for road users, the decrease of overall costs of intervention and enhancement of the country's road heritage [11].

The third thematic webinar focused on the issue of cybersecurity as a critical challenge for the energy sector, the two main weaknesses being the software ecosystem in which many companies operate and social engineering attacks. To help companies face such challenges, Magellanic Space, a cybersecurity start-up, detects and prevents malicious behaviours by using satellite data. Apart from it, space technology (Copernicus and Galileo services in particular) can provide solutions to major threats, including software complex supply chain, access management, systems interoperability, and the existence of large-scale dynamic infrastructure. Earth observation data can be used for providing a high-level overview of infrastructure, while the Galileo geolocation system can be used for running drones to monitor the area [12]. Satellite data enables Magellanic to secure the distribution of oil and energy on a large scale by providing secure communications.

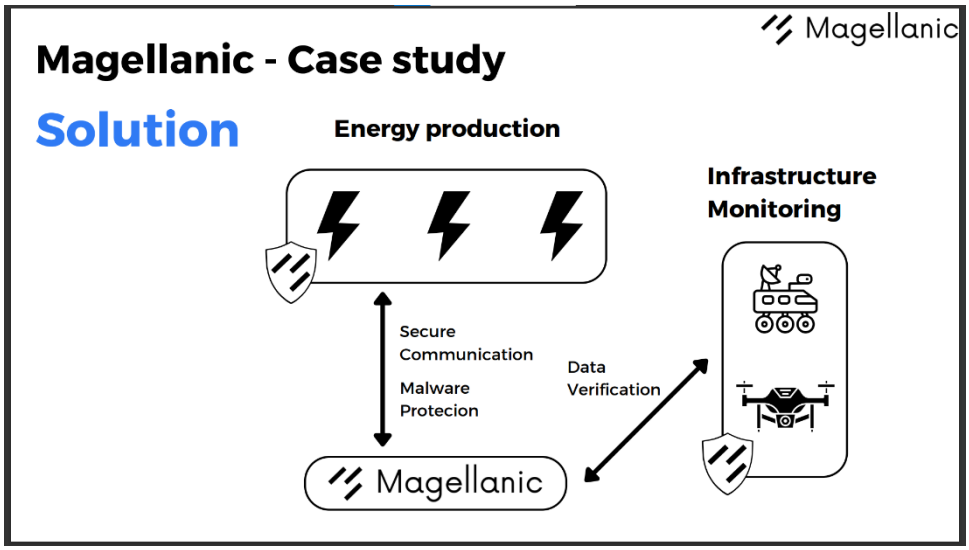

Fig. 5. Magellanic case study on energy production

Even though Europe is generally ready to face such challenge and despite of the significant steps taken by the industry to prepare for the cyberattacks, these continue to happen at both the European and global levels, and it is therefore essential to have real-time information on infrastructure with the help of space-derived data.

To conclude, the threats and challenges to critical entities are many. So are the solutions offered by space applications. From monitoring water quality to road construction and maintenance and ensuring cyber security of energy grids, the satellite data provide crucial and actionable information. The above case studies demonstrate how space-based data and signals offer opportunities to increase the resilience of critical infrastructure in the sectors covered by the CER Directive. Satellite navigation and imagery can support the entire infrastructure life cycle, from site selection to building, monitoring and post-construction operations. Galileo and Copernicus, the EU GNSS and EO satellite constellations, are already used by entities responsible for managing critical infrastructure in their daily activities. IRIS², Europe's new Infrastructure for Resilience, Interconnection & Security by Satellites, will provide secure communication services, as well as broadband connectivity, to the EU and its Member States, putting an end to dead zones in Europe. The use cases observed in this paper give concrete examples of how the resilience of critical entities in Europe can be achieved through application of satellite technologies and data.

List of references

[1] Proposal for a Directive of the European Parliament and of the Council in the resilience of critical entities (COM (2020) 829 final/2020/0365 COD), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0829, (accessed 14.08.2023)

[2] European Commission, *Overview of natural and man-made disaster risks the European Union may face* – 2020, Commission Stuff Working Document, SWD(2020) 330 final, https://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/swd/2020/0330/COM_SWD(2020)0330(PAR05)_EN.pdf, (accessed 23.08.2023).

[3] The Critical Entities Resilience Directive (CER), https://www.critical-entities-resilience-directive.com/, (accessed 25.08.2023)

[4] Enhancing EU resilience: A step forward to identify critical entities for key sectors. Press release, 25 July 2023, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3992 (accessed 07.08.2023)

[5] P. Tessari and K. Muti, Strategic or critical infrastructures, a way to interfere in Europe; state of play and recommendations, A study requested by the European Parliament's Special Committee on Foreign Interference in all Democratic Processes in the European Union, including Disinformation (INGE), July 2021, https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653637/EXPO_STU%282021%2965363 7_EN.pdf, (accessed 29.07.2023)

[6] Ch. Pursiainen and E. Kytomaa, From European critical infrastructure protection to the resilience of European critical entities: what does it mean?, Sustainable and resilient infrastructure 2023, VOL. 8, NO. S1, 85–101, https://www.tandfonline.com/doi/full/10.1080/23789689.2022.2128562?scroll=top&needAccess=true&role=tab, (accessed 25.08.2023)

[7] Introduction into the proposed EU-Directive on the resilience of critical entities - Eurisy, 15 April 2022, https://www.eurisy.eu/introduction-into-the-proposed-eu-directive-on-the-resilience-of-critical-entities/, (accessed 20.08.2023)
[8] Space for Critical Infrastructure: Putting the EC proposal into action, 24 May 2022, https://www.eurisy.eu/event/space-4-critical-infrastructure-putting-the-ec-proposal-into-action/about/, (accessed 19.08.2023)
[9] Monitoring water turbidity during the port extension works at Port-la-Nouvelle, Article produced by Eurisy with the support of the French National Centre for Space Studies within the Framework of the "Copernicus&Me" initiative, https://www.eurisy.eu/wp-content/uploads/2022/09/Monitoring-water-turbidity-in-Port-la-Nouvelle.pdf, (accessed 20.08.2023)
[10] Space for Critical Infrastructure – Reflecting on the collapse of the Morandi Bridge, Eurisy webinar, 12 May 2022, https://www.eurisy.eu/space-for-critical-infrastructure-reflecting-on-the-collapse-of-the-morandi-bridge/ (accessed 15.08.2023)
[11] Anas to monitor the stability of Italian roads and highways with Rheticus Safeway – Rheticus, https://www.rheticus.eu/news/anas-to-monitor-the-stability-of-italian-roads-and-highways-with-rheticus-safeway/, (accessed 21.08.2023)
[12] Space for Critical Infrastructure – Energy and Transport, 9 November 2022, Space 4 Critical Infrastructure – Energy & Transport – Eurisy, (accessed 20.08.2023)