Employers entrusted to deliver
Sustainability Growth Innovation

Opinion

Security Paper: The need for a multi-dimensional security approach to protect critical infrastructures in times of crisis

Adopted on 25 June 2025

SGI EUROPE GENERAL SECRETARIAT Rue des Deux Eglises, 26 bt 5, BE – 1000 Brussels
T: + 32 (0) 2 219 27 98 | F: + 32 (0) 2 218 12 13 | E: SGIeurope@SGIeurope.org | **www.SGIeurope.org**
Registered stakeholder
ID Nr 59513031434-92

SGI europe

Employers entrusted to deliver
Sustainability Growth Innovation

Opinion

Executive Summary

- The EU must shift from reactive protection to anticipatory resilience, embedding long-term planning and risk prevention into all relevant policies. **Empowering SGIs is essential to safeguard Europe's societal and economic foundations against interconnected threats**.

- SGI Europe welcomes the **EU Preparedness Strategy as a timely and necessary step towards strengthening Europe's ability to anticipate, manage, and recover from emerging threats**. However, clearer guidance is needed on what preparedness means for critical infrastructures and SGIs in the context of complex, multi-dimensional crises such as climate change, economic downturns, organised crime and geopolitical conflict.

- **Call for a "multi-dimensional resilience" approach**: The EU must move beyond protection alone and advance towards structural resilience that ensures continuity of essential services – including energy, healthcare, transport, water, waste management, telecommunication, media and public administration. **Resilience must be built into EU and national policy and infrastructure planning from the outset, ensuring that systems can respond to disruptions**.

- **Adopt the principle of "Preparedness by Design"**: Strengthening this multi-levelled resilience approach, SGI Europe urges to develop further on the principle of "preparedness by design," **under the forthcoming EU Climate Adaptation Plan, ensuring that SGIs are empowered to reinforce the EU's structural resilience.**

- **Ensure the coherence of implementation**: Key EU legislation and policy frameworks addressing critical infrastructures and cyber security measures provide a vital foundation for safeguarding critical services. However, **effective protection depends on the timely and coherent implementation** of these instruments across all EU Member States.

- **Establish a European digital platform for stakeholders:** Networking could facilitate continuous information exchange and enable practical insights to directly inform future revisions of the legal framework.

- **Build a shared EU responsibility governance**: Protecting cross-border critical infrastructures must be treated as a shared European responsibility, requiring harmonised security standards, flexible capacity mechanisms, and alignment with NATO's resilience principles. To ensure continuity of essential services under mounting geopolitical, climate, and digital threats, the EU must invest in adaptive infrastructure, secure communications networks, and maintain access to resilient information channels such as terrestrial broadcasting.

- **Ensure digital safety across sectors**: To safeguard public safety, **SGI Europe calls on the EU to retain Article 13(1) of the INSPIRE Directive, which exempts sensitive geodata from mandatory disclosure for critical infrastructures.** As digitalisation advances across sectors like water, energy, transport, and telecommunications, unrestricted access to infrastructure data increases the risk of hybrid threats, manipulation, and cascading failures. Protecting this data is essential not only for physical and cyber security, but also to avoid financial losses that could undermine vital investment in resilience and transformation.

Introduction

In light of the recently published EU Preparedness Union Strategy[1] and the growing challenges posed by climate change, economic instability, and broader multi-dimensional security threats, SGI Europe underscores the essential role of critical infrastructures and services of general interest. Their protection and resilience are fundamental to safeguarding societal continuity and cohesion in times of crisis.

SGI Europe warmly welcomes the adoption of **the EU Preparedness Strategy by the European Commission as a timely and necessary step toward strengthening Europe's ability to anticipate, manage, and recover from emerging threats**. By embracing an integrated, all-hazards, whole-of-government and whole-of-society approach, the Strategy marks a significant advancement in ensuring collective resilience across the Union. In particular, SGI Europe commends the Strategy's clear recognition of services of general interest (SGIs) – including energy, healthcare, transport, water, waste management, telecommunication, media and public administration – as vital societal functions. This **acknowledgment not only validates the critical role SGIs play in maintaining societal stability during crises but also highlights the need for continued investment in their resilience**.

This comprehensive approach to preparedness aligns closely with SGI Europe's longstanding call to embed resilience into the EU's policymaking frameworks. As vital operators of essential services, SGIs are indispensable in delivering stability, especially in times of disruption, and their centrality in the Strategy reflects growing awareness of their strategic importance. SGI Europe stands ready to contribute to the implementation of the Strategy's recommendations and looks forward to engaging actively in key initiatives such as the Social Partners Preparedness Summit. We also anticipate the forthcoming **European Climate Adaptation Plan and urge that it builds further on the principle of "preparedness by design," ensuring that SGIs are empowered to reinforce the EU's structural resilience** in a sustainable and future-proof way.

However, the Strategy can benefit from more clarity when it comes to defining what better preparedness truly means for critical infrastructures and SGIs, especially in the context of multi-dimensional crises such as climate change, economic downturns, organised crime and geopolitical conflict. This **position paper aims to help close that gap by outlining the specific needs and policy directions required to sustainably and structurally protect Europe's critical infrastructures**, ensuring their capacity to withstand and adapt to a rapidly changing risk landscape.

[1] EU Preparedness Strategy: https://webgate.ec.europa.eu/circabc-ewpp/d/d/workspace/SpacesStore/b81316ab-a513-49a1-b520-b6a6e0de6986/file.bin

The essential roles of critical infrastructures

Critical infrastructures (CIs) such as energy systems, water and wastewater networks, transport, telecommunications, and waste management are essential pillars of Europe's societal and economic stability. These interconnected systems form the backbone of public well-being and economic productivity. Their reliability underpins citizens' daily lives and enables industries to function, innovate, and grow, particularly in times of accelerated digital and green transitions.

The role of these infrastructures becomes even more vital in the context of multi-dimensional crises – ranging from pandemics and economic recessions to the impacts of climate change and geopolitical instability. Disruptions to one infrastructure can trigger cascading effects across other systems, amplifying societal vulnerability. As highlighted in the 2024 European Risk Assessment Report[2], ageing assets, increasing service demands, and the impacts of extreme weather events call for urgent and coordinated action to safeguard these vital systems.

In this context, **SGI Europe puts forward the view that a robust, multi-dimensional security and resilience strategy is urgently needed to protect critical infrastructures**. This strategy must integrate climate adaptation, economic stability, and geopolitical preparedness as interdependent pillars of future EU policy, ensuring that essential services remain secure, accessible, and sustainable in the face of mounting and overlapping threats.

A critical infrastructure protection approach

CI protection refers to policies, strategies, and operational frameworks designed to safeguard infrastructure systems against a wide range of physical and cyber threats. In the current environment of prevention**, the EU must move beyond protection alone and advance toward structural resilience that ensures continuity of service even under stress, disruption, or shock**.

Resilience in this context involves the ability of infrastructures to anticipate, absorb, adapt to, and rapidly recover from adverse events. It requires not only robust systems but also investment in quality, long-term infrastructure management. **SGI Europe underlines the importance of incorporating climate projections, cross-sectoral dependencies, and digital innovation into resilience planning**.

The protection of CIs must address therefore the following major threat dimensions:

- **Economic**: Cyberattacks, supply chain fragilities, and energy market volatility pose significant operational and financial risks to CI operators.
- **Climate Change**: Floods, droughts, and extreme weather events increasingly jeopardise the reliability of infrastructure networks. Climate adaptation must be mainstreamed into infrastructure planning, with particular attention to water-intensive sectors.
- **Conflict and internal insecurity**: Hybrid threats, disinformation, physical sabotage as well as daily violence can severely impact the functionality of key infrastructure systems and impose threads to the safety of personal operating SGIs, highlighting the need for both physical and cyber resilience.

[2] European Environment Agency (EEA). European Risk Assessment Report. March 2024: https://www.eea.europa.eu/en/analysis/publications/european-climate-risk-assessment

The EU's role in securing critical infrastructures

EU policy frameworks, such as the revised NIS2 Directive (EU 2022/2555), the Cyber Resilience Act (Regulation EU 2024/2847), and funding instruments like the Trans-European Transport Network (TEN-T) and the EU Cohesion Fund, provide a vital foundation for safeguarding critical services. However, **effective protection depends on the timely and coherent implementation of these instruments across *all* EU Member States**.

In light of the evolving threat landscape across Europe, securing critical infrastructures, ranging from public administration to drinking water and wastewater management, energy and mobility systems, and telecommunications have become increasingly urgent. The EU has made significant progress in recent years, notably through the **Critical Entities Resilience Directive (CER Directive, EU 2022/2557).** These efforts are helping to enhance both physical and digital resilience, while enabling smarter and more sustainable service delivery.

Additionally, in the context of the revision of the public procurement provisions, which affect both critical infrastructures and public local and regional authorities, SGI Europe deems it important to ensure that **public procurement rules allow for the protection of strategic data and thus industrial sovereignty**. In the cloud and artificial intelligence markets, it is essential to protect personal data and trade secrets. Therefore, it must be possible to stipulate in public procurement tenders that the **bidders cannot be subject to the US' Cloud Act** and that their data centres **must be located in the EU**.

Implementation and continuous review

To reinforce protection against emerging risks, **it is essential to swiftly implement and regularly update the common legal framework adopted during the last legislative period**. Establishing a European digital platform for stakeholder networking could facilitate continuous information exchange and enable practical insights to directly inform future revisions of the legal framework.

Ensuring coherent regulation

These legislative instruments are specifically designed to safeguard critical infrastructure. Yet, in some cases, such as the early drafting of the Gigabit Infrastructure Act, the importance of aligning with existing protective measures was initially overlooked. Going forward, it is crucial to ensure regulatory coherence and synergy between initiatives to fully embed infrastructure protection across all relevant EU policies.

A shared European responsibility

Finally, the protection of cross-border infrastructure systems remains a collective European responsibility. Harmonising security standards and allowing flexible application of capacity mechanisms, as proposed in the recent revision of the Electricity Market Regulation, are key steps toward ensuring a resilient and future-proof European infrastructure.

Furthermore**, applying NATO's resilience framework**[3] **to the protection of critical infrastructure offers a comprehensive approach to addressing the increasing complexity of today's economic, climate, conflict-related, and internal security threats**. As defined by NATO, resilience encompasses the capacity to prepare for, resist, respond to, and rapidly recover from disruptions. This is particularly relevant in the civilian domain, where critical infrastructure, energy, water, health, transport, communications, and food systems, form the backbone of national stability and security.

With the economic pressures i.e inflation, member states must prioritise the continuity of government and services together with the local and regional level, by securing supply chains, diversifying energy sources, and investing in digital redundancy (i. e. digital twins of electricity networks). **Climate change adds an unpredictable layer of risk**, making it essential to enhance the resilience of critical infrastructures such as water, energy, telecommunication, transport and waste management through risk mapping, scenario planning, and adaptive infrastructure. Meanwhile, increasing geopolitical tensions and internal security threats, such as physical attacks cyberattacks or disinformation campaigns, demand **secure civil communications networks and robust cyber defences**, in line with NATO's baseline requirements.

Meanwhile, in a context marked by increasing geopolitical tensions and internal security threats such as Foreign Information Manipulation and Interference (FIMI) and other disinformation campaigns, **ensuring that trusted general interest media content rises to the surface and is visible in the digital age, should remain a key goal of decision-makers to ensure citizens have access to trustworthy information**. However, IP networks are not enough to ensure access to reliable information. Increased infrastructure resilience requires a multilayer/multi-network approach. It is therefore key to preserve broadcasters' access to frequencies. Terrestrial broadcasting is indeed the only information infrastructure reliable even in cases of natural or man-made disasters.

Common identified challenges

To be efficient, resilience must be practiced as a cross-sectoral discipline within government bodies on all levels and through the support of the joint efforts of the EU. Ensuring continuity under stress from natural disasters to hybrid conflicts, requires that clear plans, interoperable systems, and redundancies are embedded into infrastructure strategies, whilst respecting the local and regional conditions and the national sovereignty.
Aligning national efforts with NATO's collective resilience goals allows for shared risk assessments, coordinated responses, and mutual support in crisis scenarios. It reinforces the **three pillars of civil preparedness, continuity of government, essential services, and civil support to the military**, ensuring that even when one domain is stressed, others can sustain the national and Allied response.

Yet, one of the most pressing challenges identified by the EEA is the **phenomenon of risk cascades, where the failure of one infrastructure element rapidly triggers disruptions across other systems**. For

[3] https://www.nato.int/cps/fr/natohq/official_texts_185340.htm?selectedLocale=en

example, power outages during climate-induced events can paralyse telecommunications, public transport, and essential health services. Conversely, disruptions in digital infrastructure, on which energy systems increasingly rely for operations, can themselves precipitate blackouts. **These interconnected vulnerabilities magnify the social and economic consequences of climate shocks.**
Inadequate climate adaptation, particularly in the structural design of buildings and networks, can further amplify human risks, such as heat stress during heatwaves.

The **Critical Entities Resilience (CER) Directive (EU 2022/2557) offers a key opportunity to advance these goals.** It can be leveraged to systematically evaluate resilience across essential services, regardless of ownership, and promote adaptation measures grounded in forward-looking climate projections. Updates to the Eurocodes (EU-wide standards for structural design) should also integrate future climate scenarios, especially for infrastructure with long operational lifetimes.

To address these vulnerabilities, **SGI Europe calls upon the European Commission to urgently enhance the resilience of critical infrastructures through systemic assessments, investment in climate-adaptive infrastructure, and stronger policy integration on all levels as outlined above**. In fact, resilience planning must shift from reactive to anticipatory.

Moreover, as an example of digitalisation in the water sector, sensitive data could, if exposed, compromise public safety and security. Information related to infrastructure operations, water supply networks, and consumption patterns is not only critical for service delivery but also poses risks if accessed by unknown third parties**. For this reason, it is crucial that all critical infrastructures arenot only protected from cyberattacks but that safeguards are put in place to prevent unauthorised access to such sensitive data. This requires a concerted effort to integrate comprehensive data protection measures into water utilities' digital systems** while ensuring compliance with emerging regulations and industry standards.
It is therefore important of maintaining existing exceptions under for example the INSPIRE Directive, particularly regarding access to data from critical infrastructures. **SGI Europe advocates for preserving the exemption in Article 13(1) of the INSPIRE Directive, which limits access to geodata from critical infrastructures for the sake of public safety**. According to the INSPIRE Directive, unrestricted access to such geodata could negatively impact public security.

Therefore, it is essential to ensure the ongoing security of critical infrastructures, and this exception should be retained in any revision of the INSPIRE Directive. By keeping this exception in place, the risk of manipulation and hybrid attacks, especially as more technical and geographical data becomes available, can be mitigated. Even seemingly unrelated datasets, when combined, could paint a comprehensive picture, heightening the risk of attacks on sensitive infrastructure. In addition to the general security risks, manipulations and intentional attacks often lead to significant financial losses for companies, resources that are urgently needed for transformation investments. This current exemption is deemed appropriate, proportional, and aligned with the requirements of the NIS2 Directive (2022/2555/EU) and the Critical Entities Resilience (CER) Directive (2022/2557/EU).

Technical security measures for critical infrastructures

Energy

Across all infrastructure sectors, digitalisation and decarbonisation are exposing systems to new forms of economic risk. Cyberattacks, energy price volatility, and unstable global supply chains are placing unprecedented financial and operational strain on CI operators. The energy sector exemplifies this complexity: according to the International Energy Agency (IEA)[4], **the shift toward clean energy technologies, particularly solar, wind, and battery storage, has increased demand for critical minerals, often sourced from a limited number of countries**. This geographical concentration amplifies geopolitical risks and market fluctuations, with ripple effects on the cost and security of energy systems across Europe.
Across all infrastructure sectors, digitalisation and decarbonisation are exposing systems to fresh and evolving economic risks. Cyber-attacks, energy-price volatility and fragile global supply chains already place unprecedented financial and operational strain on critical-infrastructure operators. The energy sector illustrates this complexity on two fronts:

Traditional fuels. Europe still relies on a small group of (often politically unstable) supplier countries for oil, gas and also through uranium (nuclear power), leaving it vulnerable to price shocks and deliberate supply disruptions, as the 2021-22 energy crisis made clear for gas.

Clean-energy technologies. According to the International Energy Agency, the rapid expansion of solar, wind and battery storage is driving demand for critical minerals whose production is likewise concentrated in a handful of countries. This concentration magnifies geopolitical and market risks, with knock-on effects for the affordability and security of Europe's future energy system.

The impacts of **climate change pose additionally escalating threats to Europe's energy infrastructure**. Southern Europe is already experiencing substantial stress on its energy systems due to prolonged droughts and extreme heat, affecting energy production, peak demand management, electricity grid stability. Both inland and coastal flooding also endanger the physical integrity of infrastructure across the continent, creating significant risks for energy production, distribution, and storage. Moreover, **hydrological forecasting and water-efficient design must be embedded into energy infrastructure planning**, particularly in water-stressed or arid regions.

Climate change also brings greater unpredictability to weather patterns, complicating forecasts and planning of energy supply. A more flexible planning and back-up capacities are therefore necessary, as well as cross-border infrastructure. **In view of the stability and resilience of the EU energy system, SGI Europe recommends to the European Commission to establish a strategic framework to ensure a resilient and diversified energy mix in line with the EU's climate targets, including maintaining sufficient dispatchable capacity and mechanisms for Member States** to coordinate system planning and crisis response.

Furthermore, **a coordinated European approach is urgently needed to build a systemic vision for the continent's energy future,** one that **prioritises cost optimisation, resilience, and decarbonisation**. As the

[4] International Energy Agency Outlook 2021- https://www.iea.org/reports/world-energy-outlook-2021/energy-security-and-the-risk-of-disorderly-change

EU accelerates its climate and energy transition, it must ensure that national efforts are not only effective in isolation but also coherent and complementary across borders.

This vision should be grounded in a cost-optimisation framework, focused on three key objectives:

- **Maximising efficiency in decarbonisation efforts**: This includes accelerating the decarbonisation path to reduce carbon emissions in transport, buildings, and industry. Achieving this requires a combination of (i) effective financial tools—such as the Connecting Europe Facility, a dedicated Decarbonisation Bank' mechanism as proposed by the European Commission (Citing needed) and updated state aid rules to ensure efficient allocation of funds; (ii) technologically neutral, incentive-based regulation; and (iii) smart consumer connection **accelerated handling of connection demands** to energy grids; (iv) the internalisation of external costs generated by fossil-fuelled transport modes, notably through the ETS.
- **Leveraging complementarities between Member States**: National energy systems possess different strengths, some with abundant renewable resources, others with more dispatchable baseload capacities. A truly European energy approach as proposed in the context of the EU Green Deal and the EU Energy Union should optimise these complementarities.

To structure this coordination, actions are needed at both political and technical levels:

- **At the political level**, a regular strategic orientation debate within the Council should be established with a particular focus on cross-border effects of national energy policies.
- **At the technical level**, the Energy Union Task Force, proposed in the Commission's Affordable Energy Action Plan, should be tasked with leading the technical groundwork, in close collaboration with relevant stakeholders (i.e ENTSO-E, ENTSO-G, EU DSO Entity) and market actors. This body could inform the political debate through shared data, modelling scenarios, and technical assessments of energy infrastructure needs and risks.

Together, these discussions would enable the development of collective regulatory and measures to optimise investments in energy networks and flexibility resources. Aligning new production capacities is key to maintaining system stability, preventing imbalances between supply and demand and reinforcing the resilience of the EU energy system in the face of increasing and multiplied climate and geopolitical challenges.

Water

The **water sector is an essential pillar of modern society, underpinning public health, economic prosperity, and environmental sustainability**. As a critical infrastructure, it ensures the reliable delivery of clean water for drinking, industry and agriculture as well as the provision of wastewater services. However, the sector faces increasing challenges, from the escalating impacts of climate change, demographic changes, economic downturns to rising cybersecurity threats, all of which pose significant risks to its ability to function effectively and meet the needs of communities.

These evolving pressures highlight the urgent need for comprehensive measures to safeguard water systems. In this context, the upcoming **EU Water Resilience Strategy will play a crucial role in guiding the protection and strengthening of water infrastructures across Europe**. By addressing both current and future risks, the strategy should aim to safeguard that water systems remain resilient, adaptable, affordable and capable of supporting the societies that depend on them**.**

The effects of climate change such as droughts and floods are impacting the water networks across Europe. Water supplies are disrupted by extreme weather events, infrastructure can get damaged and water

supply can experience stress. This necessitates a considerable expansion and reorganisation of the water infrastructure. This also includes wastewater infrastructure with separate and combined sewerage systems, flood protection facilities and stormwater overflow basins. In view of the increasing demand for water, interconnected and long-distance water pipelines are also of central importance. Drinking water providers and wastewater treatment operators must also be able to claim financial compensation for the associated maintenance work, and the Member States should make suitable funding programmes available. **Climate adaptation must become a common practice in infrastructure planning and investment, with a focus on making water systems more robust and capable of withstanding immediate shocks and future problematic issues.** The EEA also here emphasises the need to integrate climate risks into water infrastructure planning, **urging updates to standards and practices to safeguard future resilience against climate-induced problems**. This should be also not only seen from the water sectors perspective, but from a cross-sectoral side. This can also mean, that water reuse and water efficiency should become a more common practice to secure Europe's water quality and quantity. In addition to dealing with challenges of water quantity, external pollution from industries and the agricultural sector continues to negatively impact water quality, making the treatment processes even more challenging. These disruptions have the potential to not only undermine service reliability but also challenge the long-term viability of water as a sustainable resource for communities and agriculture. Control at source must therefore be fully implemented.

Lastly, as **digitalisation** advances, the water sector increasingly relies on sophisticated IT systems for managing operations, water quality, distribution, and metering. **While these technological advancements hold significant potential to enhance efficiency and sustainability, they also introduce new vulnerabilities**. The sector's dependence on interconnected systems heightens its exposure to cyber threats, making it essential to prioritise robust cybersecurity protocols. However, the implementation of the latest cybersecurity measures often faces challenges, including insufficient support and resources to keep pace with rapidly evolving threats. See page 5 under Common identified challenges.

Waste management

The EU Preparedness Strategy identifies the waste management sector as critical infrastructure due to its essential health and safety functions. As such, it should be recognised as a vital public service. **However, waste operators are not yet clearly acknowledged within the official definition of critical infrastructure.**

There is a general lack of awareness and urgency regarding compliance with cybersecurity protocols in the sector. These requirements are often perceived as mere administrative obligations rather than necessary safeguards. Unlike the energy and water sectors, waste management does not rely on a fixed physical network infrastructure such as pipelines or cables. Instead, it depends on collection logistics and treatment facilities that are functionally interlinked but not physically connected. Digitalisation in the waste sector is gradually advancing, yet its development remains limited in scope.

From the point of view of possible risks to the operation of the waste facilities and, therefore, to the functioning of the entire supply chain, **fire remains one of the sector's most significant threats** and is only now receiving broader recognition. Common causes of fires include self-heating, thermal runaway in batteries, friction, human error in the disposal of municipal waste, technical failures, new storage requirements The growing presence of new waste types, such as lithium batteries, introduces further fire hazards.

As a result, insurance companies often consider waste facilities to be high-risk. They may offer prohibitively expensive policies, or refuse coverage altogether**. This lack of insurability hinders facilities' access to capital grants and loans, where insurance is often a prerequisite**. The insurance issue is, in fact, becoming

a structural challenge across several EU Member States. The impossibility of having insurance coverage could even compromise the functioning of the waste facilities themselves.
SGI Europe firmly believes that the waste management sector should be formally recognised as critical infrastructure and benefit from appropriate insurance coverage at a reasonable cost.

Transport

CIs such as public transport and rail systems are fundamental to the resilience and functionality of modern societies. As providers of essential public services, they enable safe and sustainable mobility, connect communities, and support economic and social participation. In times of increasing geopolitical tensions, rail infrastructure plays a crucial role in the defence capability of the European Union. Heavy and dangerous military goods can sometimes only be transported by rail.

However, these sectors face an evolving set of threats that increasingly jeopardise their ability to operate effectively. **To safeguard these services, we must shift towards a proactive to preventative approach to infrastructure protection, that reflects their critical role and unique vulnerabilities.**

Protecting critical infrastructure is about embedding resilience through prevention and strategic investment and reacting to crises when needed. This includes funding the modernisation, and climate resilience of rail infrastructure, the renovation of stations and stops to improve visibility and safety, also for women in particular. It further includes, strengthening cyber capabilities, enhancing emergency response tools, and providing support for staff safety and well-being.

With increasing digitalisation, train and public transport companies are becoming more reliant on complex IT systems for operations, safety management, signalling, and ticketing. This dependence also heightens their exposure to cyberattacks.
However, stakeholder consultations during the development of the NIS2 Directive revealed that the need to reenforce **cybersecurity preparedness across the EU remains, especially in sectors like rail.** This fragmented approach leaves systems vulnerable to disruption and highlights the need for a more harmonised and risk-based cybersecurity framework across Member States.
In parallel, supply chain fragilities and energy price volatility continue to strain budgets and disrupt operations. **Designating rail and public transport as critical infrastructure is a crucial step toward ensuring they receive the targeted support needed to strengthen cyber and economic resilience**.

The effects of climate change, heatwaves, floods, storms, are already impacting rail networks across Europe. Tracks buckle under extreme temperatures, stations are flooded, and overhead lines are damaged, leading to major delays, increased costs and safety risks. **These disruptions not only undermine service reliability but also threaten the long-term viability of rail as a sustainable alternative to road transport** and rail transport's ability to contribute to European prosperity and competitiveness.

The European Environment Agency (EEA) underscores this growing challenge. In its March 2024 report[5], the EEA emphasises the **urgent need to integrate climate risk into infrastructure planning and investment. It recommends updating engineering standards, such as the Eurocodes**, to incorporate forward-looking climate data and ensure that new infrastructure is resilient to future climate conditions. This forward-planning approach is essential to avoid constructing assets that exacerbate vulnerabilities to extreme weather events.

[5] European Environment Agency (EEA). European Risk Assessment Report. March 2024: https://www.eea.europa.eu/en/analysis/publications/european-climate-risk-assessment

Furthermore, the EEA's Climate-ADAPT platform highlights that climate change impacts, such as torrential rainfall, storms, and heatwaves, have a particularly pronounced effect on transport infrastructure, especially rail. Moreover, the European Commission study on climate adaptation published in December 2024 estimated that €71 billion are needed for adapting the TEN-T network to cope with mid-century climate conditions[6]. **These events compromise not only the reliability but also the safety of transportation systems.** The platform reinforces the necessity of embedding climate adaptation measures across the transport sector to build more robust and shock-resistant networks.

Internal security threats also continue to rise. Frontline staff in public transport and rail services face frequent verbal and physical assaults, leading to significant challenges in staff recruitment and retention. **A lack of perceived safety deters passengers from using trains and buses, undermining efforts to promote modal shift for climate and urban sustainability goals.** Beyond everyday security concerns, the risk of hybrid threats such as sabotage, disinformation campaigns, and coordinated attacks underscores the need for closer cooperation between infrastructure operators, police, and public authorities. Both physical and cyber resilience must be enhanced to protect the people who operate and rely on these systems.

Telecommunication

Telecommunications networks form the backbone of digital communication and are fundamental to maintaining societal stability, emergency response, and economic continuity, especially during crises such as natural disasters, conflicts, or cyber incidents. As a designated CIs sector under EU law, telecom operators are entrusted with safeguarding network security, ensuring data integrity, and maintaining service continuity under stress. To support this mission, **SGI Europe deems it as important to ensure the implementation of the EU regulatory framework and update rules, where deemed necessary, to follow adequate standards and condition for a future competitive digital network to enhance the resilience of these essential services.**

The NIS2 Directive (2022/2555/EU) significantly expands cybersecurity obligations for operators of essential services, including telecommunications providers. It mandates comprehensive risk management practices, incident reporting, and supply chain security protocols. By classifying telecom operators as "essential entities," the directive ensures they receive prioritised regulatory attention, technical support, and coordinated responses in times of large-scale cyber threats such as DDoS attacks, sabotage, or coordinated hacking campaigns. During emergencies, whether environmental or geopolitical, communications are vital for public safety, civil protection, and emergency coordination. Recognising this, the CER Directive (2022/2557/EU) reinforces the protection of telecom infrastructure as part of a wider strategy to ensure continuity of essential services. It supports resilience planning through vulnerability assessments, emergency planning, and physical and cyber risk mitigation.

Together, these EU legislative tools form a comprehensive EU-level approach to telecom cybersecurity. As digital threats escalate, **SGI Europe recommends that telecoms must be further supported through EU investment, cross-border coordination, and continual unbureaucratic threat monitoring to ensure resilient communications infrastructure in Europe**.