EUROPE’S DIGITAL BACKBONE: WHY SECURE CONNECTIVITY IS NOW A CORE PILLAR OF DEFENCE

1. Summary

Europe’s security is now inseparable from the security of its connectivity. Essential national services, such as hospitals, energy grids, transport networks, logistics chains, financial markets, as well as, armed forces’ command and control systems, all rely on resilient digital connectivity. If that infrastructure is disrupted or compromised, the consequences can spread far beyond any single sector, undermining economic stability and defence readiness.

The war in Ukraine demonstrates that military action can severely test connectivity. When it holds, it can dramatically strengthen a country’s ability to resist. The conflict shows that digital networks are strategic assets, not only supporting security but also playing a role in countering hybrid and electronic warfare.

Yet in policy and investment terms, connectivity is frequently treated as a commodity for the economy, rather than a core pillar of defence. Responsibilities are spread across civil and military authorities, EU and national structures, and public and private sectors. Critical investments are delayed or underfunded, and coordination in crisis remains ad-hoc. Addressing these challenges requires a pro-investment, pro-innovation framework, underpinned by coherent and consistent policy across Europe.

Europe has a choice. If it continues to treat connectivity as a basic, low-cost utility, it will expose citizens, democratic institutions and allies to escalating risks. But if it prioritises connectivity as central to its security, it can strengthen one of its most important lines of defence against modern warfare.

The stakes are clear, as shown in recent reviews of Europe’s competitiveness by Enrico Letta and Mario Draghi, and of civil-military preparedness by Sauli Niinistö. Without major investment in secure, pan-European connectivity, Europe will remain vulnerable to hybrid threats. Indeed, the European Commission has identified a need for €200 billion more investment to meet its 2030 connectivity targets.[1]

To put connectivity at the heart of Europe’s security, leaders should take five actions.

a. **Recognise secure connectivity as a strategic security asset,** and reflect this in national security strategies, EU and NATO planning, and defence capabilities.

b. **Establish permanent, trusted mechanisms** for collaboration between governments, operators, and allies to coordinate crisis response, share intelligence, protect subsea, satellite and cyber systems, and strengthen cross-border resilience at the pan-European level.

c. **Close investment gaps in critical digital infrastructure** where markets alone do not deliver the resilience and redundancy Europe needs. Europe must use targeted incentives and harmonised policies that strengthen network protection, including via the upcoming Digital Networks Act.

d. **Pursue strategic openness by partnering with trusted allies,** such as the UK, to co-develop critical technologies and align standards that reinforce Europe’s security and technological sovereignty.

e. **Invest in digital inclusion and literacy** to help citizens recognise disinformation and sustain trust in democratic institutions, reinforcing Europe’s societal resilience.

This approach will enable Europe to use its dense and robust networks for strategic gain, deterring adversaries, supporting allies and protecting the safety and prosperity of its citizens.

2. Introduction - Europe's new security reality

For three decades after the Cold War, large-scale conflict on the continent seemed farfetched. War in Ukraine, increased cyber and hybrid threats and growing geopolitical competition have prompted Europe to reassess its security.

High intensity state-on-state warfare has returned to Europe's neighbourhood, while hybrid threats, such as cyber-attacks, infrastructure sabotage and disinformation targeting democratic institutions, are now commonplace across the continent. In 2025, global cyber-attacks rose by 21% and the International Institute for Strategic Studies recorded a 246% increase in Russian sabotage operations against European critical infrastructure from 2023 to 2024.[2]

The European Commission has recognised that today's instability requires greater investment in defence innovation and digital infrastructure, including AI, quantum and secure communications.[3] NATO has similarly demanded that its members dedicate 1.5% of GDP to resilience, including the protection of critical digital infrastructure.[4]

Strategic reviews, such as the 2024 Niinistö report on Europe's preparedness, recommend allocating 20% of the overall EU budget to security and crisis preparedness.[5] The 2025 Eurobarometer survey also shows strong public support for a more active EU role in security and defence.[6] They together show a growing recognition that Europe's security is inseparable from the infrastructure that sustains its economies and societies. In this context, secure connectivity, and the telecoms infrastructure that underpins it, will be a critical test of whether this ambition can be translated into capability.

3. Connectivity as a strategic security asset

Connectivity was historically regarded as an economic tool for delivering services and connecting citizens. While these remain important, connectivity is now also integral to societal resilience and defence readiness.

a. Connectivity as the backbone of societal resilience

Europe's essential services, from energy grids and transport systems to hospitals and public administration, all rely on digital connectivity.

During crises such as natural disasters or cyber attacks, connectivity allows emergency services to coordinate, citizens to get help, and authorities to provide guidance and maintain order. The COVID-19 pandemic showed how robust connectivity networks supported millions of Europeans to work remotely and kept essential services running, even when traditional business methods were disrupted.

However, when connectivity is disrupted, the effects can spread quickly across interconnected sectors. Modelling of natural disasters show that hospitals' ability to function depends on the availability of critical infrastructure. When these are compromised, emergency care begins to break down.[7]

Recent events highlight how disruption across different infrastructure layers can have cross-sector and cross-border consequences.

- In April 2025, the hours-long power outage across Iberia was estimated to cost Spain 0.1% of its quarterly GDP.[8] Expert commentary noted that the outage had widespread effects on critical infrastructure, including transportation, and on industrial activity and retail.[9]
- The 2022 Viasat satellite attack, initially targeting Ukraine, disrupted internet access for thousands of users across Europe and temporarily caused German wind turbines to lose remote monitoring access.[10]
- GPS jamming in the Baltic region has affected civil aviation and shipping, demonstrating how attacks on digital signals can create real-world safety risks.

Connectivity underpins societal cohesion. Disinformation campaigns allow hostile actors to undermine institutional and public trust, as Europe continues to experience during election campaigns. Recent research by the UN and the

World Economic Forum rank mis- and disinformation among the most serious short-term threats to democracy, highlighting why secure connectivity helps defend society.[11]

Connectivity enables economies to function, governments to serve and citizens to communicate. It is one of the main foundational systems, alongside energy, transport and finance, on which many other services rely. Today, Europe's digital backbone spans across underground fibre, mobile networks, subsea cables, satellite links, data centres and cloud services. Telecoms networks have long been part of critical national infrastructure. What has changed is the extent to which other critical sectors depend on them, and the complexity of the technologies involved.

b. Connectivity as the nervous system of modern defence

Modern armed forces rely on secure, high-capacity telecoms for command and control, logistics and intelligence gathering. As the Chatham House study on NATO's command, control and communication systems notes, 'communication forms one of three building blocks of any deterrent strategy' and any disruption to communications networks has 'serious implications on the exercise of command and control'.[12]

Mobile and fixed networks carry data between sensors, drones and decision-makers in the field. For example, the Portuguese Navy used a private 5G network from Vodafone to test drones and unmanned vessels, allowing ships to coordinate them in real time without land-based control for the first time.[13]

In Finland, the 2024 government defence report noted that 'the Finnish Defence Forces strengthened cooperation with telecoms operators and key allies', leading to innovations like cross-border 5G network slicing for military use.[14] These examples show that modern military capability depends on secure, high-capacity communications networks, many of which are built and operated by civilian providers.

NATO recognises resilient civil communication as a key element of national resilience, with armed forces depending on civilian networks for capabilities like unmanned aerial systems, which require high-bandwidth and ultra-low latency for real-time data exchanges.[15] The European Commission's *White Paper for European Defence* also notes that AI, cloud computing and secure connectivity are transforming warfare by enabling the development of autonomous systems such as drones, robotics, and ground vehicles.

As the Arel report *Telecoms as the Bedrock of European Defence* highlights, 'modern armed forces rely on digital infrastructure for virtually every core function… Without robust telecoms capabilities, a coordinated and effective European defence architecture is structurally impossible.'[16]

Lessons from Ukraine

Ukraine's experience since February 2022 offers stark lessons for Europe about the role of connectivity in modern conflict. From the beginning of its invasion, Russia tried to disable Ukraine's networks through physical strikes, cyber-attacks and electronic warfare. Yet the country's operators worked tirelessly to keep connectivity running, with far better results than many expected. Drawing from the experience of Vodafone Ukraine – one of Vodafone Group's non-equity partner markets – and public reports, several factors contributed to this resilience.

1. **Diversity and redundancy mattered.** Ukraine's networks drew on multiple technologies, routes and providers, including mobile, fixed, subsea and satellite connectivity. This created alternative paths to restore connectivity in a matter of hours after damage to the network.
2. **Rapid reconfiguration was critical.** Vodafone Ukraine deployed more than 3,000 generators and solar-powered base stations, keeping 90% of sites online during blackouts.
3. **Close public-private cooperation.** Regular dialogue between Ukrainian authorities and operators enabled swift, coordinated responses to incidents and the distribution of verified information via SMS, helping to counter risks of disinformation during the war.
4. **Agile regulation.** Authorities enabled emergency spectrum use, roaming and the fast deployment of temporary infrastructure.
5. **Cyber protection:** Proactive resilience measures enabled uninterrupted operation of Vodafone's network during the 2023 Kyivstar cyberattack incident, ensuring millions of Ukrainians stayed connected.
6. **Innovation in time of crisis.** A new R&D lab from Vodafone Ukraine and the National Aviation University will focus on 5G, cyber security, drone systems and mobile-space communications, increasing collaboration between industry and academia and contributing to Ukraine's tech sovereignty and European solutions for secure, resilient connectivity.

The result was that Ukraine retained the ability to coordinate defence, maintain essential services and communicate with its citizens. Connectivity became a key pilar of its overall resilience and resistance.

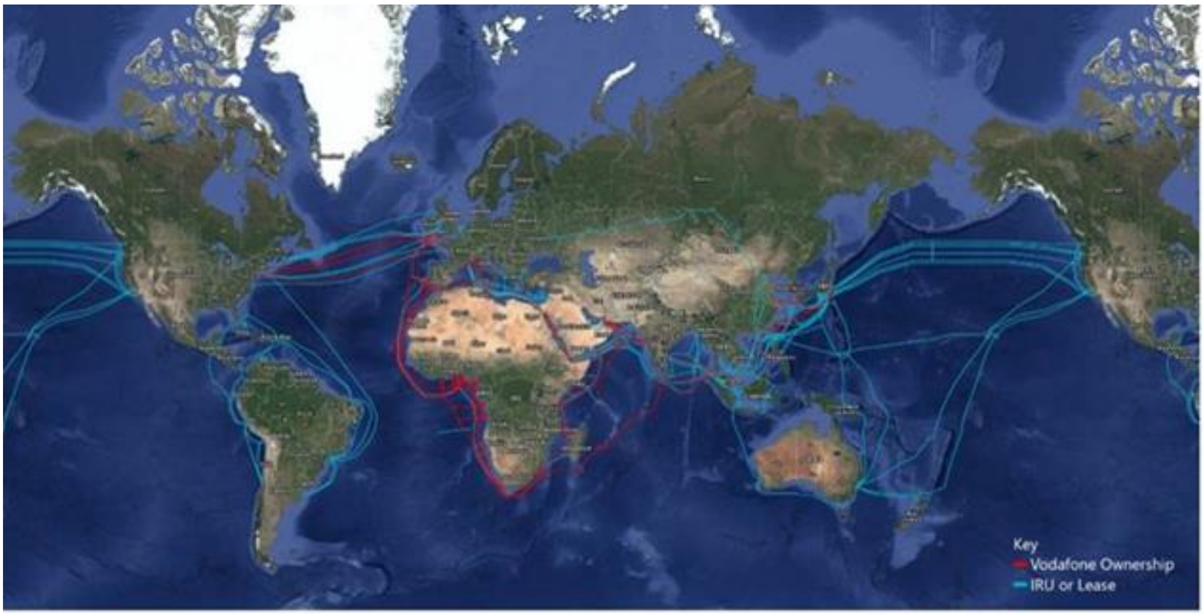
4. How connectivity providers contribute to Europe's security

Adversaries understand the value of connectivity, and so do the operators defending it every day. Hybrid campaigns against open societies routinely include efforts to disrupt, degrade or compromise networks and services. Operators like Vodafone sit on the front line, investing continuously in resilience, response and adaptation to protect Europe's critical systems across physical, cyber and satellite domains.

a. Protecting physical assets

Subsea cables, landing stations, terrestrial fibre routes, mobile masts and data centres are attractive targets. 97% of global internet traffic data now travels over subsea cables, carrying around €8.5 trillion in daily financial transfers.[17] Cable systems experience around 150-200 faults a year, even without hostile action. Three European member states – Ireland, Malta and Cyprus – rely entirely on subsea cables for their connectivity. All this is why redundancy, repair and landing sites matter.

To manage these risks, European operators, including Vodafone, focus on strengthening resilience. This includes diversifying routes, increasing redundancy of key corridors, hardening critical sites, improving backup power and repair capabilities, and planning alternative options for remote or hard to reach areas. National governments and allies increasingly acknowledge this, as seen in NATO's critical undersea infrastructure cooperation and recent North Sea commitments to safeguard underwater energy and data assets. Close coordination with authorities and other critical infrastructure providers helps prioritise repairs and protect key assets in a crisis.



Vodafone's subsea cable network. Vodafone manages one of the most extensive subsea cable networks in Europe, providing secure and resilient connectivity to one hundred countries. Vodafone owns and manages twin cables connecting Europe (via the UK and France) to the USA, and is a partner in developing 2Africa, the world's largest subsea cable. [18]

b. **Countering cyber attacks**

Cyber attacks are increasing in scale and sophistication, affecting governments, businesses and citizens. In Germany, for example, cyber crime and sabotage cost companies €267 billion in 2024.[19]

Telecoms operators are among Europe's most experienced cyber defenders. They work 24/7 to deploy advanced monitoring and threat detection tools, share intelligence with trusted partners and rehearse incident responses. Vodafone runs a cyber security team of over 900 professionals, proactively hunting threats and handling billions of events across our global footprint.

With ongoing threats to data, services and supply chains, secure digital connectivity from responsible large-scale operators is critical for Europe's security.

The 2022 cyber attack on Vodafone Portugal demonstrates the importance of scale and leveraging pan-European capabilities. [20] Though the attacks aimed to disrupt services, Vodafone resumed mobile data services and operator interconnections within eight hours, mobilising and coordinating resources from across our European operations and our global security team.[21] This rapid reaction highlights the value of scale, expertise and cross-border collaboration to counter modern, hybrid threats.

c. **Satellite connectivity for security and resilience**

Connectivity goes beyond cables and towers. Satellite communications and positioning, navigation and timing signals, including GPS, are critical to sectors such as aviation, shipping and logistics. As telecom operators such as Vodafone add satellite connectivity to their terrestrial networks, Europe must prioritise network security. Vodafone's SatCo joint venture, by virtue of its wholesale open model, helps operators maintain service continuity during natural disasters or outages, enabling emergency services and ensuring citizens retain access to basic connectivity. [22]

Security of satellite communications is increasingly important. In recent years, interference, manipulation and jamming of GPS has become more common. In the Baltic, planes and ships have been repeatedly targeted. The

Swedish Transport Agency has reported frequent signal jamming and disruption, with 733 incidents from January to August 2025. [23]

The telecoms sector is preparing for future threats by pioneering next-generation security standards such as post-quantum cryptography. Vodafone's partnership with IBM aims to update ICT systems to be quantum-safe, showing how industry innovation helps strengthen Europe's defences against future threats.

5. Closing Europe's preparedness and resilience gap

Civilian critical infrastructure operators invest heavily in resilience, from redundant capacity to fast response teams, and by adapting technologies to detect and contain evolving threats. Taken together, these efforts turn connectivity from a static target into a living system that can withstand pressure, recover quickly and emerge stronger from every incident.

Yet, maintaining and strengthening this advantage requires an enabling policy framework that supports long term investment in security, fosters innovation and deepens collaboration with governments and trusted operators.

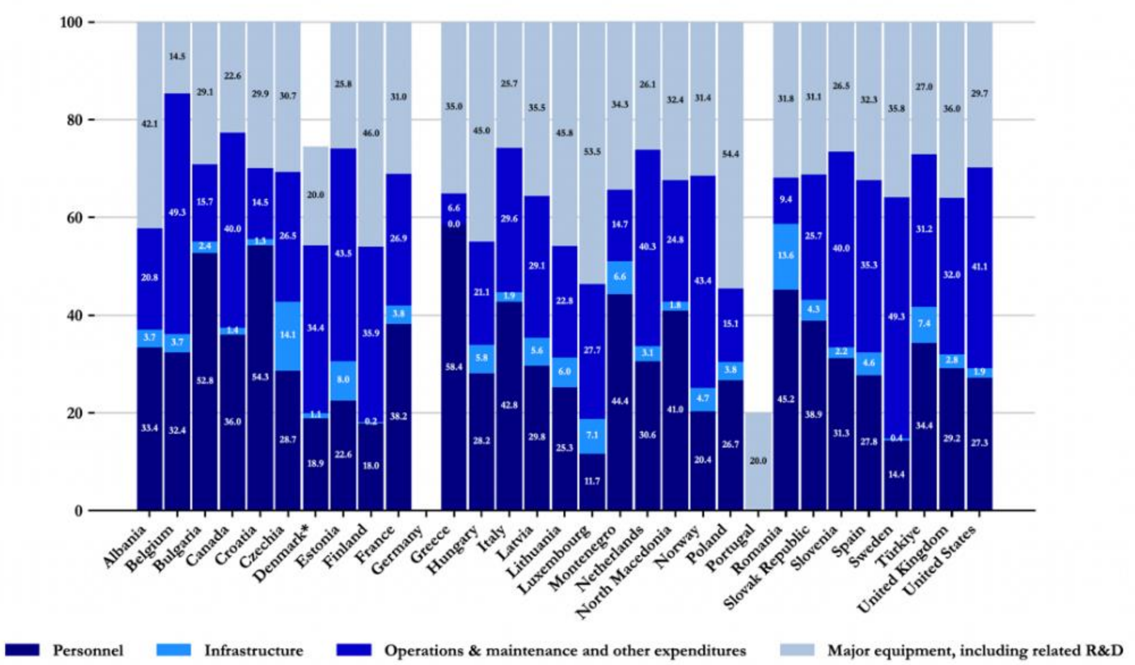
Ensuring secure connectivity should not be the sole responsibility of operators. The 2024 Niinistö report similarly notes that preparedness requires a 'whole of society' approach, with communications infrastructure fully integrated into civilian and military planning. [24]

Political action is therefore required. The Arel report, *Much More than a Network*, points to a structural investment gap in European communications networks. The European Commission has estimated that €200 billion more investment is required for Europe to meet its 2030 connectivity targets. Connectivity technology is one of the last parts of the digital ecosystem where Europe maintains true global leadership, but this competitive advantage will fade without a sustainable model for growth and investment. As the Arel paper argues, there can be no credible European defence without a genuinely continental, secure and resilient telecoms market. The two now rise or fall together.

Over time, fragmentation across Europe will weaken the sector's ability to respond and adapt efficiently to emerging threats, limit innovation and prevent the scale of investment needed for secure, dual-use networks. Digital infrastructure requires pan-European coordination with trusted partners, not simple national strategies, to counter cross-border, state-sponsored threats. Closer EU-UK cooperation is essential, as both face common threats and bring complementary strengths.

Treating connectivity as a strategic security asset, and as part of wider societal resilience, requires Europe to acknowledge these realities in its planning and investment, while not adding unnecessary regulatory burdens.

Graph 8: Main Categories of defence expenditure (%) 2025e
(percentage of total defence expenditure)



Notes: Data as at 3 June 2025, based on 2021 prices and exchange rates. Figures for 2025 are estimates. For those Allies that did not provide estimates for 2025, the respective estimates are shown as blank. * Denmark has declared that it has allocated more than 20% of defence expenditure to major equipment.

This chart from NATO illustrates the main categories of defence expenditure across Allies (2024 actuals, with 2025 estimates).[25] Infrastructure remains the smallest share, defined narrowly as military construction and NATO common facilities. Yet NATO Allies have committed to dedicate 1.5% of GDP to resilience, including the protection of critical civilian infrastructure. This will require increases in, and reallocation of, spending.

6. Solutions for European leaders

Europe' strengths include technologically advanced operators and suppliers, dense networks and a growing recognition that resilience matters. As threats grow more complex and targeted, Europe must resist the temptation to introduce extra regulatory burdens – it should instead collaborate with trusted operators to fully integrate connectivity into its defence infrastructure.

Five priorities stand out for European leaders.

a. Embed secure connectivity in national security strategy

Secure connectivity should be explicitly recognised as a strategic asset in national strategies, EU strategic documents and NATO planning. Both the EU and NATO already acknowledge the importance of communications networks for resilience, yet they must treat them as core capabilities on a par with energy and transport infrastructure. This involves making digital infrastructure a core part of defence supply chains and planning, and ensuring connectivity investment is prioritised with other defence and resilience spending.

b. Strengthen pan-European coordination and collaboration between governments and operators

Ad-hoc coordination is no longer sufficient. To counter hybrid threats, governments and operators need formal mechanisms for collaboration, linking national, European and NATO structures. These should include cross-border crisis forums, shared incident reporting protocols and regular joint exercises to ensure coordinated responses throughout all event phases.

Leaders should prioritise collaboration with trusted operators that have cross-border capabilities. Hybrid threats cross borders, so resilience relies on partners whose scale improves detection, response and service continuity.

The EU and national leaders should reinforce pan-European coordination to protect critical network infrastructure such as subsea cables, satellites, and cyber systems. For example, there should be shared response capacity for subsea cables, as well as repair mechanisms under European control. Pan-European collaboration should extend to satellite spectrum, ground station resilience and common cyber standards and certification.

c. **Invest in resilience where markets alone fall short**

Competitive markets drive innovation, but Europe's fragmented telecoms sector and sub-scale operators make it harder to invest in the redundancy and hardening that security now demands. Governments should identify critical corridors and nodes where additional resilience is needed and use targeted funding, guarantees and regulatory incentives to close this investment gap. Leaders should recognise and support the investments operators make in security and resilience, including through stable, predictable and coherent policy frameworks across the EU.

d. **Adopt a strategically open approach to technological sovereignty**

European leaders recognise that sovereignty over critical digital infrastructure is essential for Europe's long-term security. AI, cloud computing and advanced connectivity are critical enablers of modern defence.

Today, a handful of non-European providers dominate the market for cloud and AI. This has led to urgent calls to favour sovereign 'made in Europe' solutions. But ambition must be tempered with pragmatism. Cutting off access to these technologies would slow digital transformation and undermine productivity. Europe must embrace mitigation over exclusion – a risk-based approach that strengthens control without isolating it from world-leading innovation. Rather than focusing on a company's headquarter, its approach to sovereignty should prioritise local investment, R&D, jobs and production in Europe. By incentivising companies to build and maintain capabilities at home, Europe can reinforce its industrial base, supply chains and long-term competitiveness, in turn securing its economic security.

Europe's long-term security, and that of its allies, depends on its ability to develop world leading capabilities in emerging fields such as advanced connectivity, quantum and cyber security. Europe should partner with like-minded countries, like Japan, South Korea and the UK, to develop key technologies together, share resources and align standards.

Europe's long-standing defence, security and economic partnerships must evolve to reflect the connected nature of modern warfare; investment must follow. The recent treaty between Germany and the UK, which strengthens cooperation in defence and critical technologies, offers an excellent template.

e. **Build societal resilience through digital literacy**

As information warfare intensifies in Europe, investing in digital inclusion and literacy will help Europeans identify disinformation, resist manipulation and maintain confidence in democratic institutions during crises. Vodafone's September 2025 report, *A Bridge Across Communities*, provides greater detail on the importance of democratic resilience, as well as how Europe might strengthen it.[26]

7. Conclusion – a new pillar of European defence

Secure connectivity is the foundation on which Europe's defence, resilience and prosperity now rest. If neglected, it will be a point of strategic failure.

As adversaries probe and attack the digital arteries of open societies, Europe cannot afford to treat connectivity as just another utility provided at the lowest possible cost. Networks, data and services should be treated with the same seriousness as land, sea, air, space and cyber defences.

Europe brings together world-class operators, cutting-edge technologies, a tradition of allied cooperation, and unmatched expertise in shaping regulation and global standards. The opportunity now is to harness these strengths into a bold, integrated strategy, one that elevates secure connectivity as a cornerstone of Europe's strategic power.

Europe's security framework needs a fundamental shift. Connectivity must become a core element of planning, complemented by crisis coordination and resilience measures that extend beyond national borders. Greater protection against hybrid threats and institutionalised public-private collaboration will be critical to lasting security.

Decisions on connectivity, how we invest, regulate and collaborate, will shape Europe's security for the decades ahead. Secure connectivity must stand as a core pillar of defence, not an afterthought. It is a good foundation for protecting citizens and reinforcing democratic values in a world defined by complexity and constant information challenges.

8. Endnotes

[1] European Commission, *Investment and funding needs for the Digital Decade connectivity targets*, July 2023

[2] Check Point Research, *Global Cyber Attacks Surge 21% in Q2 2025, Europe Experiences the Highest Increase of All Regions*, July 2025, and Charlie Edwards, Nate Seidenstein, *The scale of Russian sabotage operations against Europe's critical infrastructure,* International Institute for Strategic Studies, August 2025

[3] European Commission, *White paper for European defence - Readiness 2030,* March 2025

[4] NATO, *The Hague Summit Declaration,* June 2025

[5] European Commission*, Safer Together: Strengthening Europe's Civilian and Military Preparedness and Readiness*, October 2024

[6] In the Spring 2025 Eurobarometer survey, 'defence and security' was the top priority Europeans want the EU to strengthen, chosen by 37% of respondents. Eurobarometer survey, *EP Spring 2025 survey,* September 2025

[7] Poudel, A., Argyroudis, S., and Pitilakis, K, *Systemic seismic risk assessment of urban healthcare system considering interdependencies to critical infrastructures. International Journal of Disaster Risk Reduction*, 2024

[8] Joan Faus, *Post-blackout in Spain and Portugal, companies count the cost*, Reuters, April 2025

[9] El País, *What remains unknown about the massive blackout in Spain*, April 2025

[10] Cyber Peace Institute, *Case Study Viasat,* June 2022

[11] UNESCO, *Survey on the impact of online disinformation and hate speech,* September 2023, and World Economic Forum, The *Global Risks Report 2025,* 15 January 2025

[12] Chatham House, *Ensuring cyber resilience NATO's command, control and communication systems*, July 2020

[13] Vodafone, *Offshore connectivity extends defence capabilities, A case study with the Portuguese Navy,* January 2025

[14] Government of Finland, *New Security Strategy for Society enhances Finland's comprehensive security*

[15] NATO's Baseline Requirements for National Resilience (2016, updated 2023) and NATO - Topic: Resilience, civil preparedness and Article 3

[16] Andrea Lamberti (Arel), *Much More than a Network Telecoms as the Bedrock of European Defence*, Single Market Lab, October 2025

[17] Elisabeth Braw, *Financial institutions should prepare for subsea cable sabotage, Financial Times,* July 2025

[18] Vodafone, *Global network resilience: a deep dive into our subsea cable infrastructure*, 18 August 2025

[19] According to ENISA's Threat Landscape 2025, Europe faces an increasingly complex and convergent threat environment marked by the blurring of state, criminal, and hacktivist activities, the mainstream use of AI, and cybercrime targeting public administrations and critical infrastructure. Sources: ENISA, *2025 Threat Landscape*, October 2025, and Bitkom, *Study Corporate Security 2024*, 2024

[20] Vodafone*, Case study incident, Vodafone Portugal*, February 2022

[21] Other services were recovered over the next 48 hours (see Vodafone Group*, Cyber Security Factsheet 2023* and *Case study incident, Vodafone Portugal,* ibid.)

[22] Vodafone, *Vodafone and AST SpaceMobile choose Luxembourg as joint venture headquarters to drive European-wide space-based mobile broadband coverage*, 30 June 2025

[23] Franciszek Beszłej/jk, *Sweden warns of almost daily GPS jamming in Baltic region, traced to Russia*, TVP World, September 2025

[24] European Commission, *Safer Together: Strengthening Europe's Civilian and Military Preparedness and Readiness*, ibid.

[25] NATO, *Defence Expenditure of NATO Countries (2014-2025),* August 2025

[26] Vodafone, *Digital inclusion key to tackling Europe's €1.3 trillion digital transformation gap,* September 2025