Digital Security:
Resilience, Innovation, and Trust

Digital Public Policy, Regulation and Competition

2025

Telefónica

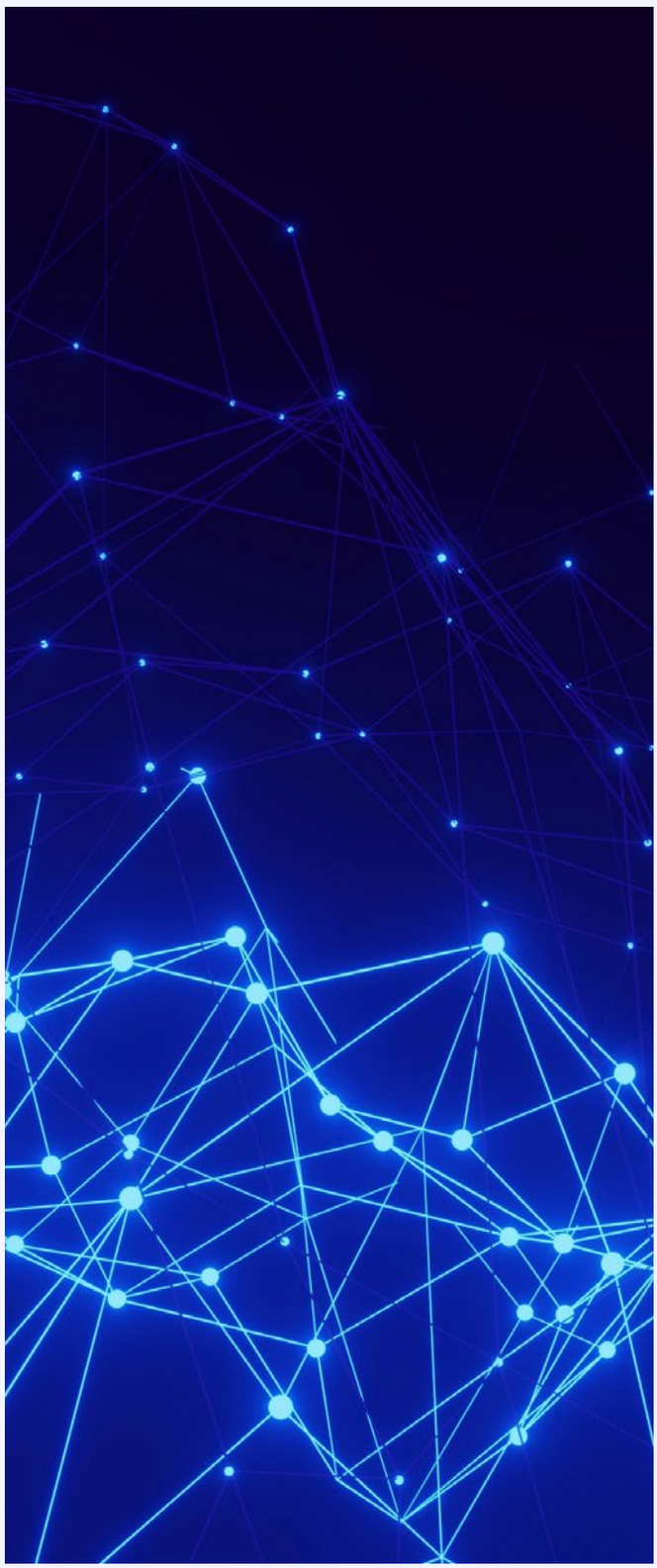
Foreword

Amidst unprecedented cyber threats and a complex regulatory landscape, the need for a technological and strategic partner has never been more critical. At Telefónica, we believe that digital security is no merely a business imperative – it is a foundational pillar for a resilient and prosperous society.

The digital revolution has transformed every aspect of our lives, but with progress comes a new frontier of risk. We have witnessed the exponential growth of cyberattacks, the widening skills gap, the funding shortfall, and the challenges posed by a fragmented and complex policy environment. These issues underscore a fundamental truth: securing our digital future requeres a new model of collaboration. It demands a partnership between the public and private sectors, where the technical expertise of the telecommunications industry is leveraged to inform and strenhthen public policy.

As a global telecommunications leader, our role extends beyond providing connectivity. Our secure network and our cutting-edge capabilites place us at the heart of this challange. We are uniquely positioned to serve as a trusted ally for goverments, public administrations, and business of all sizes in building the resi-lience and security needed to thrive in an increasingly connected world.

This document is our contribution to that critical conversation. It offers a comprehensive analysis of the current security landscape and presents clear, actionable recommendations for policymakers. It is our hope that this paper serves as a catalyst for a more secure, innovative, and trus-ted world, one built on a foundation of shared responsability and collaboration.



Index

1. Executive summary

Strategic security ambitions must be supported by an enabling environment

Regulatory complexity and unfunded obligations threaten to undermine the resilience we seek to build. A sustainable telecoms sector —a strategic partner— and a streamlined, well-funded framework are essential for achieving security, resilience and sovereignty. Telefónica, with its decades of experience in securing and managing vast digital infrastructure and services, is uniquely positioned as a strategic partner to help governments, businesses, and society build resilience.

Security is a fundamental pillar of society: a shared responsibility and a key driver of innovation

Digital security and technological sovereignty have become central to the policy agenda, driven by growing concerns. Moreover, the digital security industry is a key cornerstone, providing essential capabilities and generating significant spill-over effects. This reinforces the need for greater coordination, long-term policy commitment and sustained investment.

Preparedness is more urgent than ever, while improving resilience entails overcoming political, technical and economic challenges

Amid a new era of growing risks and uncertainty, the continued surge in cyber-attacks, data breaches, fraud, and cyber-espionage underscores the critical need for effective security frameworks and industrial policy.

The protection of strategic infrastructure holds critical value

Resilient networks are essential, as they underpin critical services across society. The telecoms industry has long been committed to implementing robust security measures to safeguard its assets, customers, and services—yet its positive contributions and sustained investments often go unrecognised. Regulatory

obligations that extend beyond market-driven considerations risk undermining the long-term sustainability of telecoms operators, if not matched by adequate funding, as seen in other sectors.

The telecoms sector, with Telefónica as a trusted and strategic partner, plays a crucial role in strengthening security and trust across society

Telefónica leverages experience, skilled workforce, extensive partnerships, and strong operational capabilities not only to protect its own infrastructure, but also to strengthen the resilience of society at large—including businesses and public administrations—while actively raising awareness and combating fraud.

The telecoms sector also acts as a key driver of security innovation

It accelerates cutting-edge tech —such as AI and quantum—and best-in-class operations to boost its own efficiency, resilience, and innovative services, while also driving digital transformation across industries and public services.

It's a time for action, with policies that effectively support a secure, innovative, and trustworthy digital environment

Recommendations

To enhance digital security and capabilities, increase societal resilience, and reduce dependencies:

1. **Ensure a robust and economically sustainable telecoms sector**, anchored in trusted operators and serving as a key regional technology partner of governments and businesses.

2. **Boost investment in security, resilience, and dual-use technologies** by leveraging public funding, targeted tax incentives, and strategic use of public procurement.

3. **Implement a streamlined, proportionate, and risk-based security regulatory framework**, grounded in facts and developed in close collaboration with the private sector, ensuring coherence across standards and policies.

4. **Advance cybersecurity and technology skills development**, while promoting greater public awareness and understanding of digital security to foster a more resilient digital society.

5. **Enhance coordination in cyber intelligence, defence, and the deterrence of cybercrime**, backed by increased resources and reinforced through stronger cooperation.

2. Unlocking the value of *digital security* and resilience

A. Security as a fundamental pillar of society: a shared responsibility, and a key driver of innovation

In an era of evolving digital complexity and rising geopolitical tensions, digital security and technological sovereignty have moved to the forefront of the policy agenda.

For organisations, building digital security is fundamentally about developing a comprehensive approach, protecting business continuity and maintaining trust through strategies that go beyond purely technical solutions. For policymakers, it is about ensuring economic stability, sovereignty and public confidence by embedding resilience into broader policy frameworks[2].

Digital security is a shared responsibility, requiring coordinated efforts between governments, public administrations, the private sector, and international bodies[3]. Moreover, the digital security industry is a strategic driver of innovation, sovereignty and regional modernisation, with spill-over effects. This demands stronger coordination, long-term policy commitment and sustainable funding.

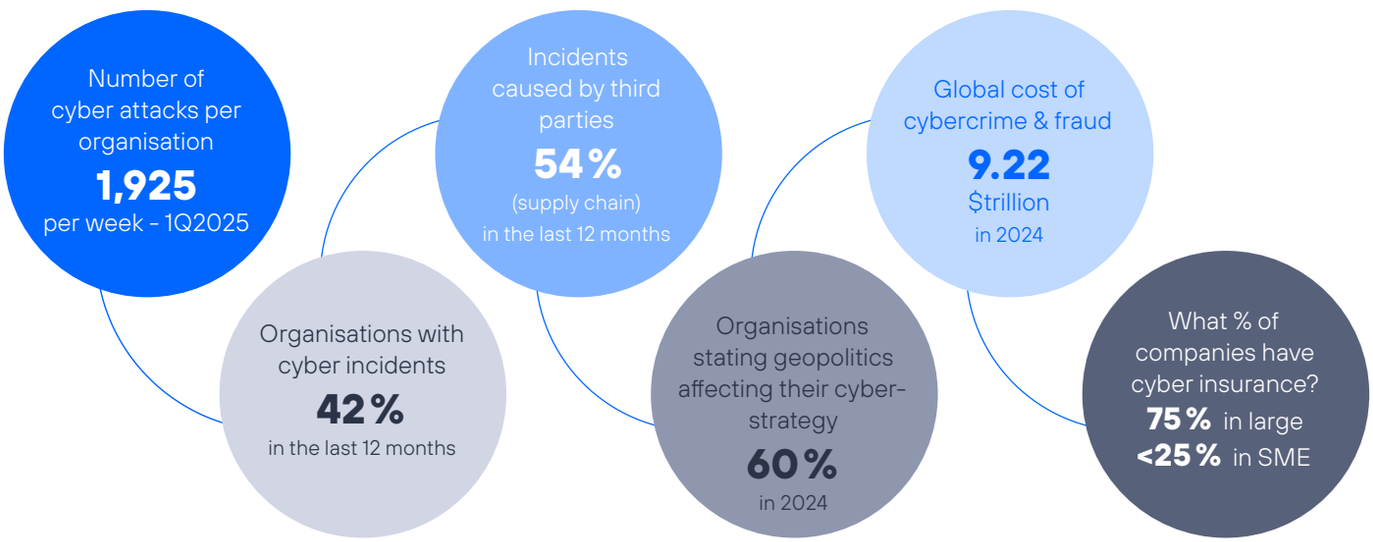
Amidst unprecedented cyber threats and regulatory complexity, the need for a technological strategic partner has never been more critical.

> **Security is the foundation on which everything is built [...] Security is a public good [...] It is the precondition for maintaining our values, as well as being a necessity for our economic success and competitiveness**
>
> *Adviser Niinistö Report on the Preparedness and Readiness of the EU - October 2024*[1]

B. The growing concern over digital security defines today's digital landscape

The World Economic Forum[4] identifies cyber insecurity (misinformation, disinformation, cyber espionage and warfare) as top 10 global risks. The cyber landscape is increasingly complex. Data breaches, ransomware attacks[5], and cyber-espionage continue to increase. The world faces a new reality of growing risks and uncertainty, making preparedness more urgent than ever.

Figure 1. Global landscape of digital security[6]



Sources: Telefónica based on: Checkpoint (April 2025)- Q1 2025 Global Cyber Attack Report. Checkpoint - The state of Cybersecurity | World Economic Forum (WEF) (January 2025) - Global Cybersecurity Outlook 2025 | GSMA (February 2025) - Fraud and Scams: Staying Safe in the Mobile World | International Monetary Fund (IMF) (April 2024) - Chapter 3 Global Financial Stability Report, Cyber Risk: A Growing Concern for Macro financial Stability

The number of cyberattacks has surged by 50% over the past year, reaching an average of 1,925 weekly attacks per organization in the first quarter of 2025[7]. Some 42% of organizations experienced a successful social engineering attack in 2024, a number that can only increase with the malicious adoption of AI[8]. The supply chain is particularly critical, as 54% of cyber incidents originated from third parties.

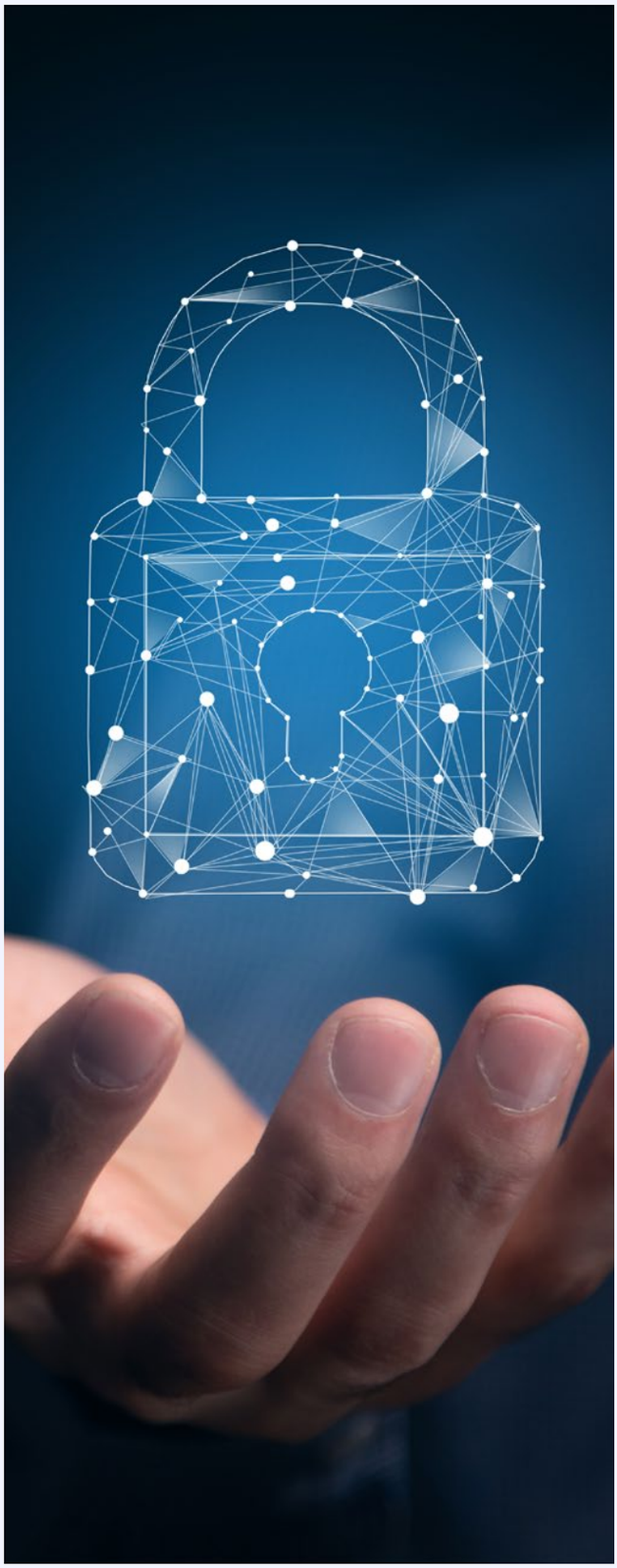
The global financial cost of cybercrime, including fraud[9], is projected to escalate from 9.22 trillion in 2024 to USD 15.63 trillion by 2029. The cost of cyberattacks or data breaches is increasingly high: the average total cost per incident is estimated over €4 million[10].

According to the IMF's Cyber Risk Report[11], the organisations most at risk are those in highly connected

sectors, those with attractive assets but weaker protection (such as SMEs), and those operating in countries with high geostrategic risk or inadequate cyber legislation. Attackers are driven by a range of motives, most commonly financial gain—as seen with organised criminal groups—but also by the pursuit of recognition or the advancement of political and social causes.

There is a widening gap between organisations that are cyber resilient and those that are not. Small organizations can no longer adequately secure themselves against the growing complexity of cyber risks, according to 71% of cyber leaders. Less than a quarter of SMEs have cyber insurance in place, compared to 75% of larger organisations, and more than twice as many SMEs as large organisations report that they lack the cyber resilience needed to meet their critical operational requirements, delaying their evolution in the digital world. In the telecoms sector, the root causes of service disruptions—measured in terms of hours of lost communication—are primarily system failures (60%), followed by human errors (19%), natural phenomena (13%), and malicious actions (8%)[12].

Strengthening preparedness and combating cyber threats has become more urgent than ever. In summary, the consequences of information incidents, cyber threats and fraud can include significant financial loss, jeopardised business viability and loss of confidence in digital services- ultimately hindering the adoption of otherwise beneficial technologies. Moreover, countering foreign manipulation and interference has become critical to ensuring stability and the sovereign protection of individual rights, businesses, democratic processes and fundamental values.



C. Improving resilience entails overcoming geopolitical, technical, policy and economic challenges

In today's context, building resilience requires confronting a range of **critical challenges**[13].

Figure 2. Major Challenges Shaping the Security Landscape

Telefónica

Skills - High priority for **71%** of EU companies[4]

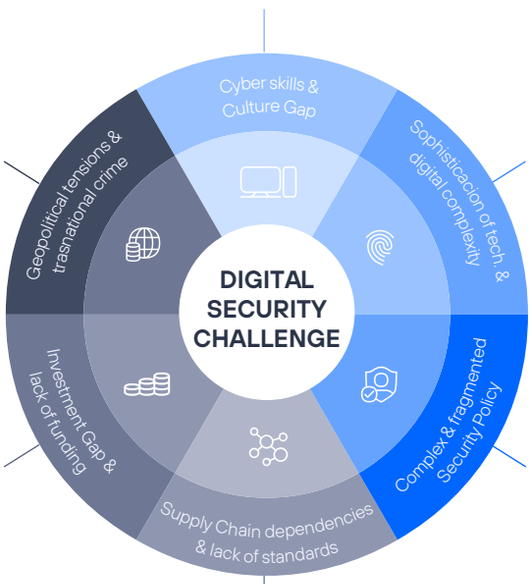
Only **14%** of orgs. feel confident about their skills[1]

Shortage of cybersecurity professionals: **500,000 experts** in EU and **2.8 to 4.8 million** globally[1]

60% of orgs. state geopolitical tensions affecting their cybersecurity strategy[1]

Over **$1 trillion** stolen in 2023[2]

Difficult international **law enforcement**



Tech leveraged by both defenders and attackers (e.g. AI & quantum)

Tech Gap paradox[1]: 66% expect AI impact on cybersecurity in 2026, but only **37%** have processes for security of AI

Complexity: misconfigurations & IT vs OT

Investment Gap in digital security[3]

	Digital security spending	
	Per employee / Year	% of IT spending
Global Average	$ 709	5.6%
Public. Admin.		
Local & Regional	$ 520	4.6%
Nat. & Internat.	$ 1,346	5.7%
Telecoms	$ 1,851	7.3%

Lack of economic analysis and **funding strategies**, while resilience comes at a cost

Regulatory complexity: 76% of companies report[1] that **regulatory fragmentation** impairs their ability to maintain compliance & cybersecurity effectiveness

Risk of ***de-coupling*** *or* ***de-risking*** beyond market-driven approach, requiring public funding

Sources: Telefónica base on: (1) World Economic Forum (WEF) (January 2025) - Global Cybersecurity Outlook 2025 | (2) GSMA (February 2025) - Fraud and Scams: Staying Safe in the Mobile World. | (3) Gartner (December 2024) – IT Key Metrics Data 2025: IT Security Measures Analysis; ENISA (November 2024) - NIS Investments | (4) Eurobarometer (May 2024) - Survey on cyber-skills | EU Mind the Cyber Skills Gap (August 2023): a deep-dive

Geopolitical tensions and transnational crime continue to complicate efforts to address insecurity and fraud. The shortage of cybersecurity professionals and the absence of a strong cybersecurity culture further exacerbate these challenges. While emerging technologies offer new opportunities for defence and resilience, the growing complexity of digital systems hinder end-to-end security. Additionally, supply chain interdependencies and the lack of common or open standards remain significant barriers to building long-term, resilient infrastructures.

Resilience remains underfunded in both public and private sectors, partly due to limited incentives to address spill-over effects, as seen in R&D. Government targets often exceed risk-based, proportionate or market-driven approach and lack the economic analysis and funding strategies needed for implementation. Enhancing resilience is costly — e.g., the cost of providing one hour of backup in UK mobile RAN across all four mobile networks would be £0.9 - £1.8bn, plus ongoing maintenance[14].

A fragmented and highly complex regulatory landscape hinders effective strategies. While regulations are increasingly recognised as key to strengthening baseline cybersecurity, their growing number and lack of alignment pose major challenges. Duplicative, conflicting, or unnecessary regulations require companies to devote more resources to fulfilling technical compliance requirements without improving cybersecurity outcomes[15].

BOX 1

EUROPE'S CYBERSECURITY POLICY LANDSCAPE: COMPLEX AND FRAGMENTED

In the European Union, the NIS2 (*Network and Information Systems*) Directive significantly raises cybersecurity standards across 18 sectors—requiring risk management, incident response and reporting, business continuity planning, tighter supply chain oversight, and greater board-level accountability.

However, it operates within a **complex regulatory landscape**[16], overlapping with national or European frameworks such as DORA (*Digital Operational Resilience Act*), CRA (*Cyber-Resilience Act*), CSA (*Cybersecurity Act-certification framework*), CER (Critical Entities Resilience), telecoms sector regulations, GDPR (General Data Protection Regulation), the AI Act or the EU 5G Toolbox, alongside a growing number of security standards that organisations must comply with.

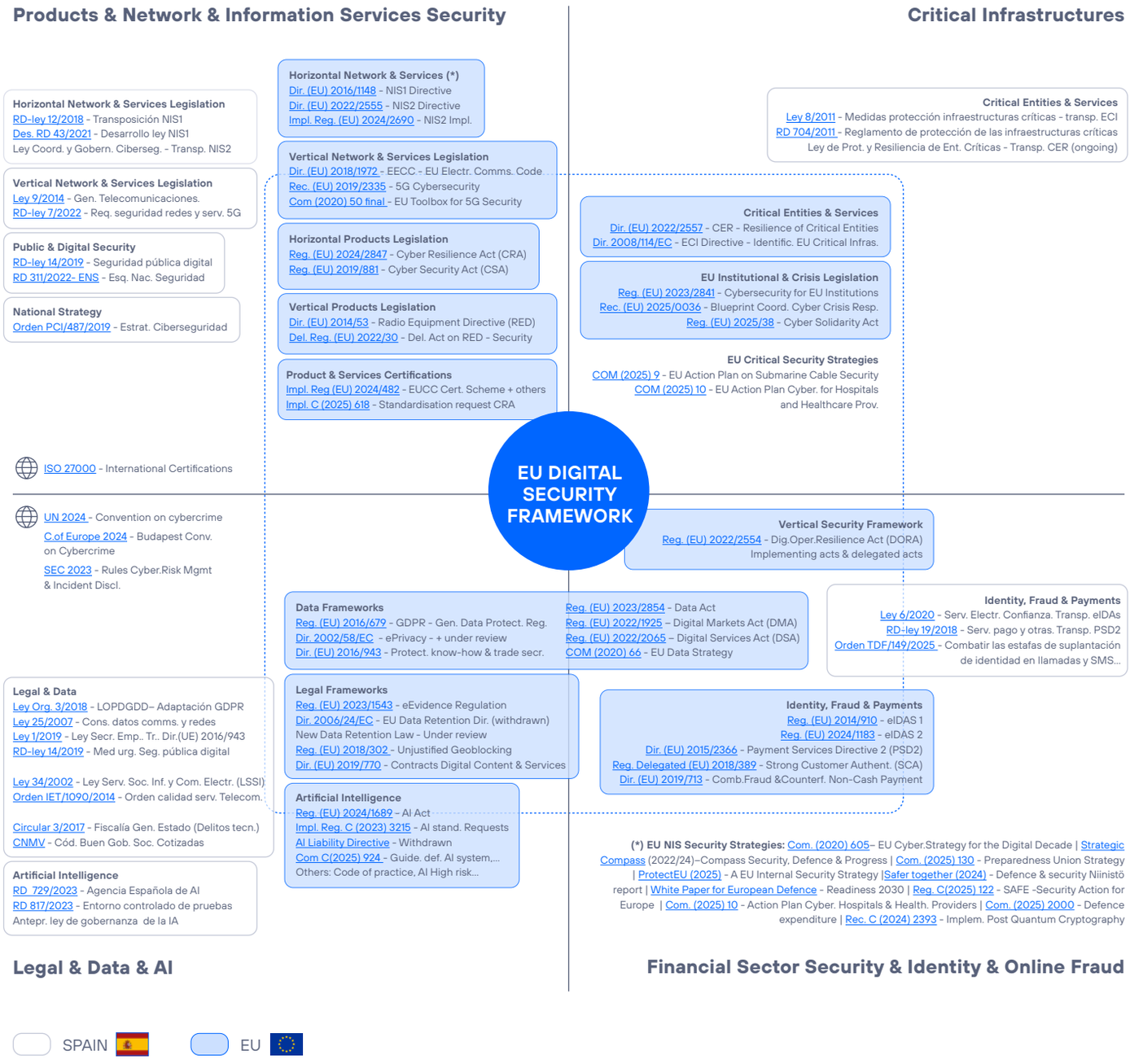
Complementing these frameworks are **national and European security strategies**[17], including the recent action plan on defence[18], the cybersecurity proposals for hospitals, initiatives to protect submarine cables, the European Protect EU, or the Cybersolidarity Act[19]. Finally, the EU cyber defence policy aims to enhance cooperation and investments to better detect, deter, and protect and defend against a growing number of cyberattacks.

An additional development is the launch of the **ENISA Vulnerability Database (EUVD)**[20] in May 2025. While not as extensive as the United States' publicly funded CVE-MITRE[21] database, the EUVD seeks a high level of interconnection by aggregating publicly available information from various sources, including CSIRTs, vendors, and existing vulnerability databases.

This complex and fragmented policy landscape highlights the need for a simplified and proportionate approach to effectively address cybersecurity threats across the EU.

Telefónica

Figure 3. A complex & fragmented EU security policy framework for digital infrastructures



Sources: Telefónica based on legal framework and blog posts. (January 2025) - DORA, NIS2 and CRA: Decoding Europe's Cybersecurity Regulatory Landscape | Telefónica (April 2025) - Defence, security and preparedness: an EU action plan

BOX 2

OTHER REGIONS' CYBERSECURITY POLICY LANDSCAPE: BRAZIL & CHILE EVOLUTION

Globally, regulatory approaches to cybersecurity vary widely[22]. In Latin America, several legislative initiatives are underway; however, their maturity varies considerably, and the strength of protective measures often correlates with whether a country has previously faced major cyber incidents—such as in the case of Costa Rica.

BRAZIL

Brazil has laid the foundations for a robust cybersecurity framework, particularly through the General Data Protection Law (LGPD) and the National Cybersecurity Strategy (E-Ciber)—which is currently under review by the National Cybersecurity Committee (CNCiber) according to the guidelines of Decree N° 11.856/2023, which established the National Cybersecurity Policy (PNCiber).

Regarding sectorial regulation, Anatel approved in 2020 and updated in 2024 the Cybersecurity Regulation applied to the Telecommunications Sector (R-Ciber), which establishes rules for telecommunications networks and services, focusing on the protection of critical infrastructures, requiring preventive measures, incident response and risk management, under the coordination of GT-Ciber, a technical group responsible for defining deadlines, procedures and equipment covered.

CHILE

Amid this diverse landscape, Chile stands out with the adoption in March 2024 of Law N° 21.663 on Cybersecurity and Critical Information Infrastructure[23], representing a major step forward in the region. It marks Chile's first comprehensive regulatory response to the threat of cyber-attacks. It complements the National Cybersecurity Policy 2023–2028, creating a foundational framework for a cohesive national cybersecurity strategy. The core principles:

- Creation of the National Cybersecurity Agency (ANCI), a National CSIRT (civilian incidents), and a Defence CSIRT — each with clearly defined mandates, specific cybersecurity functions, and dedicated financial resources, all governed by the principle of rationality. The agency began operations on 2 January 2025.
- Obligation to cooperate with authorities in managing incidents.
- Damage control and rapid response protocols to mitigate impacts.
- Commitment to security and privacy by design and by default.
- Emphasis on information security consistent with international standards.

From May 28 to 30, 2025, government representatives and experts from 10 countries in the region met in Puerto Varas to launch the project *"Strengthening Cybersecurity Capacities in Latin America and the Caribbean"*[24]. This EU-funded initiative, part of the **EU-LAC Digital Alliance**, will support Chile in advancing its cybersecurity policies, while also sharing this experience to help improve regional digital security readiness.

The evolution of cybersecurity policy in Brazil and Chile demonstrates the global recognition of digital security as a national priority and a key driver of economic growth.

Sources: Cyber Policy Portal https://cyberpolicyportal.org/ | Telefónica (June 2024)- Chile: a frontrunner in cybersecurity in Latin America | EU-Chile (June 2025) ANCI lanza en la Patagonia Chilena proyecto de fortalecimiento de la ciberseguridad de América Latina y el Caribe | Brazil - Decreto nº 11.856, de 26 de Dezembro de 2023

3. The telecoms sector — and Telefónica as a *strategic partner* — in safeguarding digital infrastructure and strengthening security and trust across society

A trusted and sustainable telecoms sector is an essential partner in ensuring the security and resilience of society. The telecommunications industry has long been committed to developing and deploying robust security measures to protect its assets, customers and services.

Beyond this core responsibility, it is using its extensive expertise and technical capabilities to play a key role in strengthening the resilience of all sectors and public administration. At the same time, it acts as a driver of innovation, encouraging the adoption of cutting-edge digital technologies and best-in-class operational practices - including cloud computing, artificial intelligence or quantum technologies.

Building upon decades of experience, Telefónica is uniquely positioned to assist governments, businesses, and society in building resilience.

A. The value of protecting strategic infrastructures

Resilient telecommunications networks are crucial for consumers, businesses and governments, as our increasing reliance on digital communications underpins critical services such as emergency response, digital payments, healthcare, the operation of critical sectors, energy grid connectivity or the protection of sensitive data.

The telecommunications industry is playing a key role in this effort, making significant investments to strengthen the security and resilience of its infrastructure[27]. This includes implementing stringent security requirements, applying supply chain best practices[28], minimising single points of failure and establishing robust processes, tools and training to support operational resilience.

Despite its critical role in securing digital networks, the telecoms sector's positive contributions often go unrecognised - particularly at a time when it faces major investment challenges to meet connectivity targets. Inadequate investment in security and resilience would leave networks increasingly vulnerable to evolving threats, weakening both the telecoms sector's operational capabilities and the essential services that depend on them.

The imposition of new regulatory obligations that go beyond market-driven considerations - without thorough cost-benefit analysis or adequate funding as seen in the energy sector's approach to resilience – would risk significantly increasing costs and further undermining the long-term sustainability of telecom operators.

> **Critical infrastructure such as telecommunications networks and digital services are of utmost importance to many critical functions in our societies and are therefore a prime target for cyberattacks**
>
> *Informal Meeting of the Telecommunications Ministers Nevers, March 9, 2022*[26]

BOX 3

TELEFÓNICA'S DIGITAL SECURITY GOVERNANCE

Telefónica understands **security**[29] as a comprehensive concept whose purpose is to preserve assets, interests and strategic objectives, guaranteeing their integrity and protecting them from potential threats. All markets where Telefónica operates have a local security organisation, which is coordinated by the global security and intelligence area.

Comprehensive security encompasses:

- Physical and operational security (of people and property)
- Digital security
- Business continuity
- Fraud prevention
- Supply chain security
- Any other relevant area or function whose objective is corporate protection against potential damage or loss.

In turn, **digital security** involves information security and cybersecurity, and applies to the means, systems, technologies and elements that make up the network and information systems. To meet stakeholders' information needs, in a clear, concise, and accessible way, Telefónica provides a dedicated 'Security' section within its Global Transparency Centre, available on its website [30]. This section also enables the reporting of vulnerabilities or threats that could impact Telefónica's technological infrastructure.

Early protection of Telefónica's assets is achieved through the definition of security policies based on international standards, and the implementation of robust security architectures tailored to the business environment. Over that, Telefónica's approach to **cyber defence** is rooted in a comprehensive and proactive model that leverages the company's advanced capabilities across key areas:

- **Anticipation**. Telefónica adopts a Cyber Intelligence driven strategy focused on proactivity and foresight. By continuously identifying emerging trends, threats, and suspicious activity patterns, the company enhances early breach detection. The integration of advanced technology and expert knowledge ensures timely identification of risks.

- **Prevention**. Dedicated internal expert teams, such as the Red Team, actively search for digital vulnerabilities to identify and mitigate risks before they can be exploited.

- **Detection and Response**. Telefónica maintains a rapid and effective incident response capability through a network of Computer Security Incident Response Teams (CSIRTs). These teams are coordinated to manage security incidents efficiently, minimizing impact. They also collaborate with national and international CSIRTs and CERTs across both public and private sectors, strengthening global cybersecurity resilience.

Telefónica's progressive strengthening of security capabilities and resources has been complemented by the decision to internally develop specific capabilities in the fields of cryptography, cyber intelligence, and cyber defence.

Telefónica's robust governance model, combining a top-down and bottom-up approach, ensures that cybersecurity is a core component of its business strategy and operations.

Sources: Telefónica – Global Security Transparency Center www.telefonica.com/en/global-transparency-center/security/ | Telefónica - Cybersecurity www.telefonica.com/en/about-us/public-policy-and-regulation/public-positioning/cybersecurity/

BOX 4

BUILDING A POSITIVE CYBERSECURITY CULTURE: TELEFÓNICA GERMANY

Cybersecurity is often seen as the domain of specialists working in silos—but real resilience depends on every employee[31]. The concept of the *"weakest link"* illustrates that even the best defences can fail if everyday practices across the organisation aren't aligned with basic cyber hygiene.

At Telefónica, we are embedding a security-first mindset across the business. Our approach combines continuous awareness, tailored training, and modern engagement formats to help all staff adopt secure behaviours. From self-paced learning via intranet and knowledge hubs to interactive presentations delivered by our security experts, we aim to make cybersecurity relevant and accessible.

To further engage employees, Telefónica has introduced formats like the **Security Arena**—an on-site event mixing mini-games and discussion—as well as a browser-based game exploring social engineering tactics. For management, tabletop exercises help test and refine processes and responsibilities. People remain one of our most important resources. By offering diverse learning formats, encouraging open communication, and reinforcing shared responsibility, Telefónica is building a culture of cybersecurity that supports innovation and long-term resilience.

Complementing this cultural foundation, Telefónica Germany established a virtual, interdisciplinary **Threat Intelligence Squad** in early 2024. The team analyses key geopolitical and cyber risks and publishes an evolving threat landscape, such as the Threat Intelligence Radar 2024–2025.

By focusing on awareness, training, and internal communication, Telefónica Germany successfully fosters a positive cybersecurity culture that empowers employees to be the first line of defence.

Sources: UK National Cybersecurity Centre - Cyber Security Toolkit for Boards | Telefónica Germany - Threat Intelligence Radar 2024–2025

BOX 5

PROTECTING SUBMARINE CABLES: TELXIUS

In light of the growing number of hybrid threats, including recent incidents in the Baltic and North Seas, subsea cables[32] emerge as an essential asset for digital resilience.

Telxius[33] implements a holistic security model that ensures an effective management through up-to-date policies, a combination of robust physical and cybersecurity measures, regular audits, and ongoing evaluation of security practices. Internal regulations are aligned with legal frameworks and international standards and supported by employee training and awareness programmes.

In this regard, Telxius ensures the resilience of its subsea cables landing stations by operating a Business Continuity Management System in accordance with Telefónica Group regulations and guidelines based on the ISO 22301 standard. It also maintains an active Integrated Management System for its main landing stations, ensuring the application of market best practices in line with ISO 27001 for information security management, ISO 14001 for environmental management and ISO 50001 for energy efficiency.

Business continuity is strengthened through route diversification, enhanced physical security, robust continuity plans, regular testing, and well-defined disaster recovery procedures. Crisis management includes structured response plans, trained personnel, established communication channels, and post-crisis evaluations. Physical and personnel security are addressed through access controls, surveillance, asset protection, emergency protocols, and the promotion of a safe work environment.

In cybersecurity, Telxius adopts a multi-layered approach—covering data, applications, devices, networks, and perimeters—leveraging AI and machine learning for real-time threat detection. Measures include end-to-end encryption, network segmentation, protection of corporate devices, and safeguards against credential theft, ensuring secure communications, data protection, and risk mitigation.

Increasing resilience through enhanced coordination

There is an urgent need for coordinated action and effective cross-border dialogue to protect this vital infrastructure. The EU Action Plan on Cable Security outlines a framework to further increase the resilience and security of subsea cables[34]. Active engagement with industry stakeholders will be key to ensure a comprehensive and practical response.

A harmonised approach to the subsea cable ecosystem must align security objectives with operational feasibility, sustainable business models and the strategic use of public funding. This approach must be underpinned by proportionate, risk-based best practices co-developed in close collaboration with industry partners.

The case study demonstrates how public-private partnerships are essential for protecting critical, global infrastructure like submarine cables from a wide range of physical and digital threats.

Sources: Telxius, a leading global connectivity provider |Telefónica (December 2024)- Invisible infrastructure that drives the digital world: submarine cables

B. Leveraging telecoms' security expertise to strengthen protection across sectors

The telecoms sector plays a key cross-cutting role in securing a wide range of sectors. It uses its experience, skilled workforce, extensive partnership networks and robust operational capabilities not only to protect its own infrastructure, but also to strengthen the resilience of wider society, businesses and public administrations. With deep technical expertise and high operational readiness, the industry makes a vital contribution to securing services in defence, banking, energy, healthcare, finance, transport, manufacturing and other key sectors.

The surge in the volume and value of cyber-enabled fraud has attracted organised crime groups into the international cybercrime market, where they are difficult to trace and prosecute. In an effort to combat fraud, operators invest significant resources in identifying, filtering and blocking fraudulent traffic, but these crimes often involve a sophisticated and organised chain of events - so technical measures alone are not enough. Despite industries best efforts, criminals have found a way to bypass technical defences and target human behaviour through 'social engineering'.

BOX 6

TELEFÓNICA'S SECURITY SERVICES FOR COMPANIES & PUBLIC ADMINISTRATIONS

Telefónica delivers an end-to-end suite of cybersecurity solutions. As a trusted Managed Security Service Provider (MSSP), Telefónica Tech focuses on prevention, detection, and rapid, effective response to mitigate cyberattacks, safeguard businesses and public digital services, and strengthen cyber resilience across sectors and geographies. It also provides specialised protection for Operational Technology (OT) systems, which govern industrial processes and demand tailored cybersecurity approaches adapted to their specific architectures and constraints. This mission is driven by a multidisciplinary team of highly skilled cybersecurity professionals, backed by extensive experience in delivering services to third parties.

Telefónica Tech's 24/7 capabilities are anchored in state-of-the-art Digital Operations Center (DOC) and Security Operations Centers (SOCs), strategically positioned across Europe and the Americas. Telefónica Tech delivers global protection backed by local expertise, supporting customers across the entire threat lifecycle. Its adaptable service portfolio combines proprietary technologies with best-in-class third-party solutions, ensuring comprehensive and flexible protection against evolving threats.

Telefónica Tech's cybersecurity capabilities are widely recognised by clients across a broad range of industries, reinforced by a strong network of strategic partners and consistently acknowledged by leading industry analysts. Complementing its core security services, Telefónica also offers cyber-insurance solutions to enhance protection and support risk management. Additionally, it regularly publishes reports and cyber intelligence analyses, providing valuable insights into emerging threats and trends.

Telefónica's comprehensive suite of security services for businesses and public administrations positions it as a key partner in building a secure and resilient digital ecosystem.

Sources: Telefónica Tech | Telefónica Tech – Cyber Security services | Telefónica Tech – Case Studies | Telefónica Tech (July 2025) - Cyber Security Report 2025 H1 | Telefónica Tech (2025) - Cyber Resilience in Critical Infrastructures | Telefónica - Cyber Insurance services | Telefónica Empresas - Cybersecurity and Technological Security for Companies | Telefónica Empresas - Cybersecurity for Small Businesses

Telefónica Tech

A global Managed Security Service Provider with a complete portfolio of cybersecurity capabilities

~ 5.5M B2B customers
Across full portfolio services in Telefónica Tech

~7,000 professionals
Working in Telefónica Tech

24x7 support service
1 Digital Operations Center (DOC) with 2 locations and a global network of SOCs

+50 technologies
Cybersecurity tech. managed by our SOCs

+6,500 certifications
In all third-party technologies

Top-tier partner
Highest partnership level

Experience, reliability and continuous innovation

INDUSTRY RECOGNITION

AVASANT · IDC Analyze the Future · GlobalData. · FORRESTER

CUSTOMER RECOGNITION

Telefónica - CASE STUDIES
Success Stories

TECHNICAL SCALE

+290k Threats identified

+350k Tickets managed per year

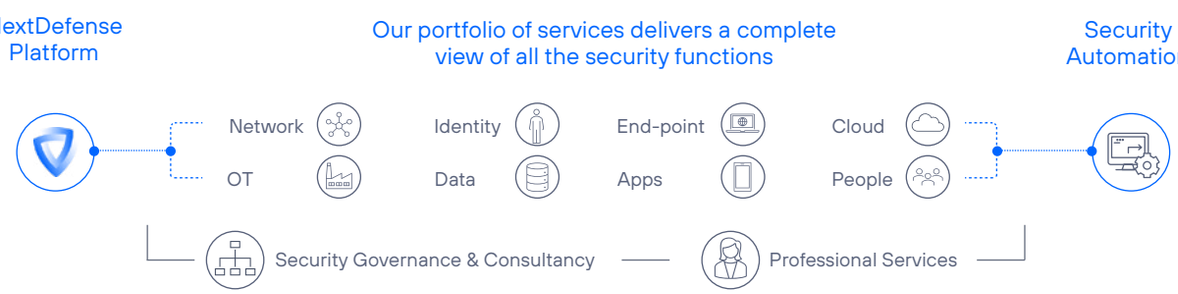
+370k EDR agents deployed

+50k h. Pentesting and Red Team

+4,150 TB Logs ingested into SIEM

HIGHEST LEVEL PARTNERSHIP

aws · CHECK POINT · CROWDSTRIKE · FORTINET · Microsoft · paloalto NETWORKS



Sources: Telefónica Tech | Telefónica Tech – Cyber Security services | Telefónica Tech – Case Studies | Telefónica Tech (July 2025) - Cyber Security Report 2025 H1 | Telefónica Tech (2025) - Cyber Resilience in Critical Infrastructures | Telefónica - Cyber Insurance services | Telefónica Empresas - Cybersecurity and Technological Security for Companies | Telefónica Empresas - Cybersecurity for Small Businesses

BOX 7

TELEFÓNICA'S ROLE IN STRENGTHENING DEFENCE SECTOR'S TECH CAPABILITIES

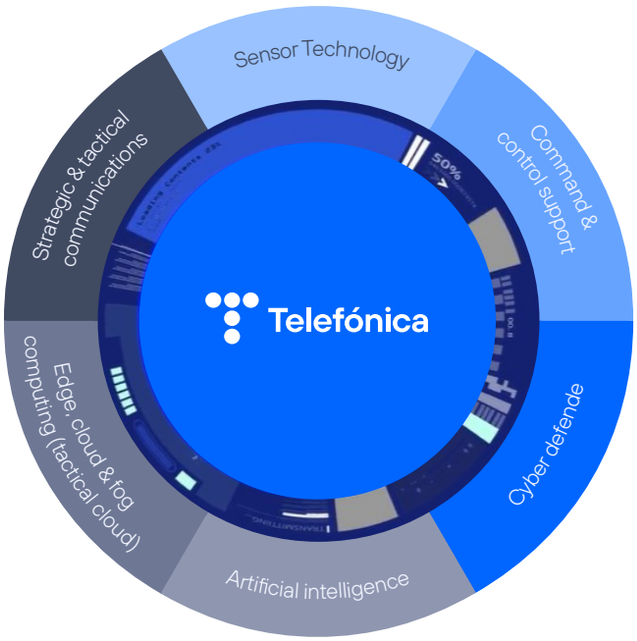
No defence capability can operate securely without advanced, resilient digital infrastructure and trusted technology partners. At the Spanish Defence and Security Fair (FEINDEF 2025)[35], Telefónica presented its comprehensive technology strategy aimed at strengthening strategic, operational, and tactical capabilities, while reinforcing security across the defence sector. Modern defence and military operations require modern communications and technologies.

Telefónica brings its extensive expertise to the integration of defence technologies in key areas such as hypersensing, strategic and tactical connectivity—including 5G tactical bubbles[36] and spectrum dominance—, and secure data transport with post-quantum readiness. These capabilities are further complemented by advanced cloud, edge, and fog computing architectures, the latter acting as a decentralised layer between edge and cloud environments. Together, they enable the efficient organisation and management of mission-critical information.

When combined with AI-driven data processing, robust digital security, advanced cyber defence capabilities, and next-generation command posts enhanced with extended reality, this comprehensive technological ecosystem delivers a decisive advantage in both protecting and strategically exploiting information.

On a related front, drones have emerged as a growing concern in national security reports[37] due to their potential misuse by terrorist or criminal organisations. In response, Telefónica offers a wide-ranging portfolio of solutions, from drone-in-a-box systems to advanced counter-drone technologies, all designed to enhance airspace security and provide effective threat mitigation[38].

Integration of technologies for information superiority



In parallel, Telefónica fosters innovation both internally and through open innovation models, with Wayra—its corporate venture vehicle. The company has established several agreements, including with NATO's Defence Innovation Accelerator for the North Atlantic (DIANA), integrating six Telefónica laboratories into DIANA's international network of test centres. These laboratories specialise in cutting-edge fields such as quantum technologies, next-generation networks, the Internet of Things (IoT), and cybersecurity.

Telefónica's collaboration with the defence sector exemplifies the crucial role of private-sector innovation and technological expertise in enhancing national security and defence capabilities.

Sources: Telefónica Defensa y Seguridad | Telefónica (May 2025)- The FEINDEF defence and security fair: technology, talent and innovation

BOX 8

THE FIGHT AGAINST FRAUD: RAISING STANDARDS AND AWARENESS

The rise in fraud is a growing concern, prompting players in the digital ecosystem to intensify their efforts to combat this threat. Criminals are finding ways to exploit the human factor through social engineering. At the same time, the rise of transnational cyber-enabled crime is making it increasingly complex for law enforcement to combat fraud.

Telefónica has consistently supported the fight against fraud, with a range of initiatives across regions. Included are some non-exhaustive examples.

GSMA Open Gateway initiative[39]

Operators have launched various network APIs (Application Programming Interfaces) designed to enhance digital security and combat fraud (e.g. device status, device location, SIM swap, scam signal...). These APIs enable developers and partners to build intelligent layers of customer authentication, verification, and protection within mobile networks. This innovation helps businesses—such as financial institutions and online retailers—strengthen user authentication and better prevent fraud.

SPAIN

In February 2025, the Spanish Government, in broad consensus with the industry, approved a Ministerial Order to combat fraud in voice calls and SMS[40], establishing measures to combat identity spoofing scams — in which the source number is modified so that the destination number shows a trusted number, a known number, or an institution.

The plan includes several technical measures: blocking unauthorised numbers, such as those that have not been assigned to any service, operator or customer; preventing spoofed Spanish numbers received from international calls or messages, except for users who are roaming abroad legitimately; creating a national registry for alphanumeric sender IDs, managed by the National Commission for Markets and Competition (CNMC), to prevent the impersonation of legitimate entities, such as banks or public agencies; and banning the use of mobile numbers for customer service or unsolicited telemarketing, requiring businesses instead to use geographic numbers or 800/900 lines, which are now authorised for outgoing calls.

BRAZIL

Brazil is increasingly using biometric identification in some products, including behavioural biometrics to combat fraud in various sectors, including social security, banking, telecoms and government services. By verifying identities accurately, biometric systems can help detect and prevent fraud, such as identity theft, account takeover, and unauthorized transactions.

Vivo additionally offers a variety of products and services to fight scams. An example is Vivo Anti-Spam[41]: this free service for mobile users analyses call behaviour across the network and uses intelligent algorithms to block unwanted calls. Or through *"Modo Seguro"*[42] platform, which allows Vivo users to remotely lock the device and erase data in case of theft or loss.

UK

Virgin Media O2 (VMO2) is taking a proactive and multi-faceted approach to tackling fraud through technology, industry collaboration, and customer awareness. As a contributor to the UK Government's Telecoms Fraud Sector Charter, VMO2 supports joint efforts to improve scam call and SMS detection, number misuse prevention, and data sharing with law enforcement. On the consumer side, the company launched DAISY[43], an innovative awareness campaign using simulated customer numbers to attract and study fraudulent calls—helping reduce the likelihood of real customers being targeted. Combined with tools like AI-based SMS filtering and enhanced call screening, these efforts reflect VMO2's strong commitment to protecting users and reducing fraud across the telecoms' ecosystem.

A holistic approach to combat fraud

Cooperation and a holistic approach are key in the fight against fraud. To deploy advanced tools effectively, companies need both flexibility and timely access to relevant data—without excessive or disproportionate restrictive data protection policies hindering this fight. This requires addressing the entire value chain, as well as prioritising user awareness[44] and law enforcement[45]. Cross-sector collaboration is crucial for achieving collective goals and requires a flexible, pragmatic and future-proof approach that avoids overly prescriptive measures, given the dynamic nature of fraud.

Telefónica's proactive approach to combating fraud, using advanced technology and intelligence, highlights the need for a collaborative, public and industry-wide effort to build digital trust.

Sources: UK VMO2 (May 2025) - New report calls for overhaul of fraud policing as majority of police believe officers lack the resources and skills to investigate the crime | INCIBE. Qué hacer si eres víctima de un fraude | GSMA – GSMA Open Gateway | Government of Spain (February 2025)- Spain plan to combat pone and text messages scam | VIVO – Antispam service | Vivo (May 2025) - Vivo Seguro | UK VMO2 (November 2024) - O2 unveils Daisy, the AI granny wasting scammers' time

C. A key innovator sector in advanced technologies and a catalyst for adoption

The telecoms sector is a key driver of innovation, continuously adopting and integrating cutting-edge digital technologies and best-in-class operational practices. This includes the use of cloud computing, artificial intelligence and emerging quantum technologies - not only to improve its own efficiency, resilience and service delivery, but also to enable secure digital transformation across industries and public services.

> **Technology will be the main feature of competition in the new geopolitical environment. A handful of critical and foundational technologies like AI, quantum, biotech, robotics, and hypersonic are key inputs for both long term economic growth, and military preeminence**
>
> *White Paper on European Defence Readiness 2030 – March 2025*

BOX 9

FUTURE OF SOCs: INCREASING DIGITAL SECURITY WITH AI

Telefónica Tech is leading a significant transformation in how organizations tackle cybersecurity challenges by advancing the evolution of the Security Operations Center (SOC) through the **strategic use of artificial intelligence (AI) and automation**.

In the face of a hostile and an increasingly complex digital landscape – marked by hybrid infrastructures - a combination of on-premises systems and multiple public and private cloud environments, the proliferation of connected devices, and a critical shortage of specialised talent—Telefónica Tech promotes a modern, efficient, and proactive SOC architecture.

Through its NextDefense solution[46], the company integrates advanced capabilities such as behavioral analytics, automated alert management, and enriched threat intelligence, enabling a significant reduction in false positives, better prioritisation of critical incidents, and faster response times.

This approach provides organizations with comprehensive visibility across their entire digital ecosystem, including multi-cloud and operational technology (OT) environments, allowing for early risk detection, contextual threat analysis, and preemptive mitigation. In addition, Telefónica Tech complements its technological capabilities with expert services such as threat hunting, cybersecurity posture assessments, and strategic consulting, helping businesses define tailored security strategies that optimize resources and reduce operational costs.

By fully integrating AI into the SOC[47], repetitive and low-value tasks are automated, freeing analysts to

focus on higher-impact actions, enhancing operational efficiency, and actively strengthening resilience against increasingly sophisticated cyber threats: integrating AI and automation into cybersecurity enables organizations to proactively detect and neutralize threats boosting detection speed and response times, and shifting from a reactive to a preventive approach. AI systems analyse large volumes of data to identify anomalies and emerging risks in real time, while automation handles repetitive tasks, freeing up human analysts for complex decision-making. Machine learning enhances these capabilities by continuously learning from new threats, making defences more adaptive and efficient.

The integration of AI into Security Operations Centers (SOCs) will be crucial for managing the growing volume and complexity of cyber threats, enabling more efficient detection and response.

Sources: Telefónica Tech – Next Defense | Telefónica Tech - The SOC of the future: How AI and automation are redefining the future | Telefónica Tech - Cybersecurity automation with AI to anticipate and neutralize threats

BOX 10

QUANTUM OPPORTUNITIES AND THREATS

Quantum technologies will offer transformative opportunities, enabling computational breakthroughs, ultra-secure communications and unparalleled measurement precision. However, the development of quantum computing presents a serious threat, particularly through '*store-now, decrypt-later*' strategies that could exploit **cryptographic vulnerabilities**. To mitigate this risk, the most effective short-term countermeasure is the adoption of post-quantum cryptography (PQC) or hybrid cryptographic systems.

In this context, the 2024 joint declaration signed by 18 EU Member States[48] urged the prioritisation of the transition to post-quantum cryptography, based on the European Commission Recommendation[49] . These initiatives were followed by the release of the Roadmap for the Transition to Post-Quantum Cryptography in June 2025[50].

In 2024 the first standards were published. Amid standardisation efforts in different regions, the concept of **crypto-agility**[51] — the ability to adapt security solutions dynamically to incorporate new standards or encryption algorithms — is becoming increasingly important for resilience.

Telefónica's role in quantum

Telefónica has established a dedicated Centre of Excellence for quantum technologies[52] . The company is already making strides towards quantum-safe[53] networks by integrating an additional layer of protection through quantum-resistant technologies, combining traditional cryptographic methods with post-quantum cryptography (PQC). Going beyond the lab, Telefónica is also advancing future technologies such as Quantum Key Distribution (QKD), having deployed them operationally within the EuroQCI network[54] , to accelerate their maturity. This effort has been carried out in close collaboration with leading academic and research institutions, as well as in partnership with top network equipment manufacturers.

Telefónica is also collaborating with third parties. Several use cases were showcased at MWC25[55], including applications in healthcare[56], defence, and utilities, as well as broader efforts to build a robust quantum ecosystem. This includes partnerships with quantum computing manufacturers and collaboration with the Provincial Council of Biscay[57].

The relevance of funding

Collaboration and testbeds are key to developing secure, innovative services. Enhanced resilience should be market-driven and backed by a sustainable telecom sector. Targeted public funding can fill investment gaps where private incentives fall short, while public procurement can drive adoption of strategic, long-term technologies.

Telefónica's early engagement in quantum technology positions it at the forefront of preparing for both the security risks and the new opportunities that quantum computing will bring.

Sources: EU Commission (April 2024) - Recommendation on Post-Quantum Cryptography | EU Member States declaration (Nov.2024) - Securing tomorrow today: transitioning to Post-Quantum Cryptography. | EU Commission (June 2025)- A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography |Telefónica Tech (June 2025) – Strategic preparation for Post Quantum Cryptography | Telefónica (March 2025) - Telefónica opens a dedicated Centre of Excellence for quantum technologies | Telefónica - Quantum-Safe Networks | Telefónica (October 2024) - QKD, cryptographic keys and quantum networks |Telefónica (March 2025) - Telefónica anticipates quantum challenges with an innovative demo at MWC |Telefónica (March 2025) - Telefónica and Vithas test shielding against quantum attacks in two hospitals |Telefónica (March 2025) - partner of Government of Biscay for development of its quantum technology industrial strategy

4. Public policy *recommendations* for a more secure, innovative, and trusted world

Regions are working to enhance security, strengthen its capabilities, boost societal resilience, make substantial investments, and reduce strategic dependencies. In this context, a robust and sustainable telecommunications sector—anchored in trusted operators and serving as a key technology partner—will be essential.

But even a strong private sector cannot meet these challenges alone. Unlocking the full potential of digital and security ambitions requires: a streamlined, proportionate and coherent regulatory framework; targeted support for the development of a competitive ecosystem in strategic network technologies; public funding for security and resilience as a public good; and the strategic use of public procurement. Equally important are the development of cyber skills, greater coordination and cooperation between public authorities, sustained engagement with the private sector, and increased resources and international cooperation to combat fraud and cybercrime.

Strategic ambitions must be supported by an enabling environment. A coordinated, simplified and well-funded framework is not just an option: it is a prerequisite for achieving resilience and security objectives. Following are recommendations to foster a more secure and trusted digital world.

> **Robust preparedness does not come for free. Investments in preparedness imply costs, but these are outweighed by the long-term gains in resilience, reduced disruptions, lower recovery expenditures, and long-term competitiveness**
>
> *European Preparedness Union Strategy – March 2025*

A. Ensure a robust and economically sustainable telecoms sector, anchored in trusted operators and serving as a key regional technology partner

No capability can operate securely without a trusted digital infrastructure and strategic partners with technological leadership. This is where the telecommunications sector plays a critical role - not only as an enabler of connectivity, but also as a guardian of strategic autonomy. The economic sustainability of the telecoms sector is therefore a cornerstone of society's overall digital resilience. To reinforce this role, the following policy actions are essential:

- **Recognise the strategic importance of the telecoms sector** in strengthening the resilience of all industries
- **Acknowledge the costs of maintaining secure and resilient telecoms infrastructure**, operational capabilities and rapid incident response into the wider conversation about the future of connectivity.
- **Adopt a modernised regulatory framework and forward-looking competition policy that strengthens the fundamentals of the sector.** This should enable the scalability and long-term investment capacity needed to maintain security and resilience in the face of escalating cyber and physical threats.

B. Boost investment in security, resilience, and dual-use technologies by leveraging public funding, targeted tax incentives, and strategic use of public procurement

The private sector should not bear sole responsibility for delivering public goods or financing resilience beyond commercially reasonable expectations. Governments must step up by implementing effective industrial policies, making public investments, and using public procurement strategically.

- **Increase public funding and provide tax** incentives to support defence, cybersecurity, and resilience efforts—similar to measures applied in other strategic sectors such as energy, to close the investment gap.
- **Support the deployment of essential technologies** that enhance innovation and long-term resilience, such as artificial intelligence and quantum-safe solutions.
- **Strengthen public procurement as a strategic lever to drive technological innovation, and resilience**—focusing not solely on the lowest cost, but prioritising security and the adoption of European technologies and long-term value.

.

C. Adopt a streamlined, proportionate, fact-based, risk-based and coherent security regulatory and standards framework, in close cooperation with the private sector

Reducing regulatory complexity, promoting best practices, and ensuring a coherent, proportionate, and predictable framework—paired with a mindset that trusts and empowers the private sector—will be key to achieving lasting success. To support this goal, policymakers should:

- **Promote cybersecurity best practices alongside the development of minimum standards** -particularly in regions where they are lacking-, independent oversight bodies, and well-resourced strategic frameworks that support implementation and compliance.
- **Streamline the fragmented security landscape and reporting obligations**, ensuring a level playing field across the ecosystems, prioritising alignment with international standards, and assessing the interplay between regulatory frameworks and different points of contact, to enable more effective resource allocation toward meaningful security outcomes.
- **Ensure that all regulatory obligations are fact-based, risk-based, and proportionate**, and that they are consistently accompanied by thorough cost-benefit analyses and clear funding strategies.

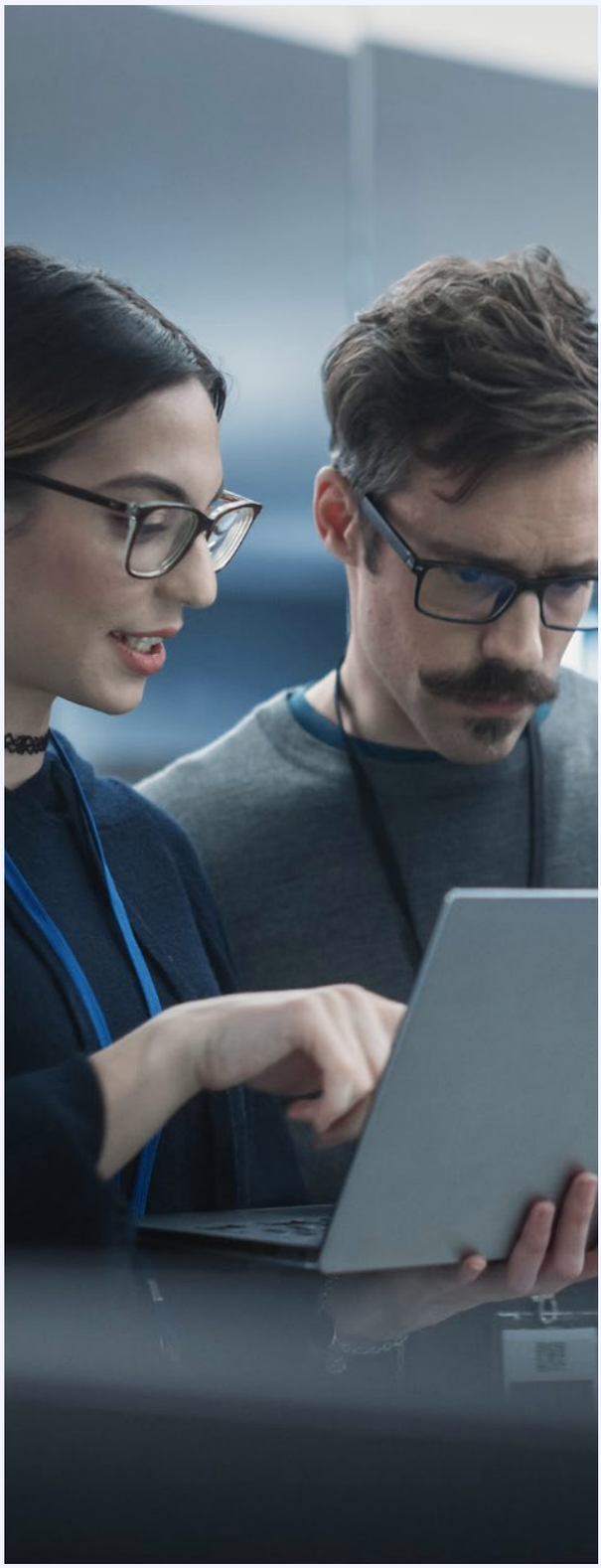
D. Advance cybersecurity and technology skills development, while promoting greater public awareness and understanding of digital security

- **Invest in education and training** at all levels to build a strong pipeline of cybersecurity and technology professionals.
- **Promote lifelong learning and upskilling** through targeted initiatives for the current workforce, particularly in critical sectors.
- **Support awareness campaigns** to educate citizens and businesses—especially SMEs—on basic cyber hygiene, digital risks, fraud, and safe practices online.

E. Enhance coordination in cyber intelligence, defence, and the deterrence of cybercrime, backed by increased resources and reinforced cooperation

Cyber resilience is a shared responsibility that requires a clear understanding of what is at stake for society, along with strong cooperation in combating cybercrime and fraud.

- **Strengthen public-private coordination** by involving the private sector early in the policy development process and fostering collaboration in cyber threat intelligence sharing, the creation of actionable guidelines, and capacity-building—going beyond purely sanction-based approaches.
- **Enhance multilateral cooperation** to enable the effective sharing of cyber threat information and to support the prevention, detection, containment, investigation, and prosecution of cybercrime and fraud, including through the allocation of additional resources.



5. Glossary of key concepts

Cyber intelligence generally refers to the process of collecting, analysing, and applying information about cyber threats to inform decision-making and improve cybersecurity.

Cyber threat means any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons[59].

Cybersecurity means the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats.

Deterrence means the action of discouraging an action or event through instilling doubt or fear of the consequences.

Digital security encompasses information security and cybersecurity, and applies to the means, systems, technologies and elements of the network and information systems.

Essential service is a service which is crucial for the maintenance of vital societal functions, economic activities, public health and safety, or the environment[60].

Incident means an event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems.

Resilience means the ability to prevent, protect against, respond to, resist, mitigate, absorb, accommodate and recover from an incident. In the broadest sense it is the ability of an organisation, resource, or structure to be resistant to a range of known and future internal and external threats, to withstand the effects of a partial loss or degradation of platform, system, or service, to recover and resume service with the minimum reasonable loss of performance, and adopt lessons learnt from any incidents[61]. **Cyber resilience** goes beyond traditional cybersecurity; it is an organization's ability to minimize the impact of significant cyber incidents on its primary business goals and objectives[62]. Recognising that 100% security is unattainable, organisations must adopt adaptive strategies and a '*when, not if*' mindset, acknowledging that incidents are inevitable.

Security of network and information systems is the ability of network and information systems to resist, at a given level of confidence, any event that may compromise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, those network and information systems[63].

Sources: Definitions as set in: Regulation (EU) 2019/881 on ENISA; Directive (EU) 2022/2557 on the resilience of critical entities (CER); Directive (EU) 2022/2555 - NIS 2 on measures for a high common level of cybersecurity across the Union; Deterrence definition from Oxford Languages.

6. References

1. EU Commission (October 2024) - Sauli Niinistö report - Safer Together: Strengthening Europe's civil and military preparedness and readiness

2. Spanish Government (2021) - Spanish National Security Strategy

3. German Government (2022) - German National Security Strategy | UK Government (2022)– UK Cyber Security Strategy 2022-2030

4. World Economic Forum (WEF) (January 2025) - Global Risk report 2025

5. ENISA (September 2024) - ENISA Threat Landscape 2024

6. Sources Figure 1: Checkpoint (April 2025) - Q1 2025 Global Cyber Attack Report. Checkpoint - The state of Cybersecurity | World Economic Forum (WEF) (January 2025) - Global Cybersecurity Outlook 2025 | GSMA (February 2025) - Fraud and Scams: Staying Safe in the Mobile World | International Monetary Fund (IMF) (April 2024) - Chapter 3 Global Financial Stability Report, Cyber Risk: A Growing Concern for Macro financial Stability

7. Checkpoint (April 2025) - Q1 2025 Global Cyber Attack Report. Checkpoint - The state of Cybersecurity 2025

8. World Economic Forum (WEF) (January 2025) - Global Cybersecurity Outlook 2025

9. GSMA (February 2025) - Fraud and Scams: Staying Safe in the Mobile World

10. ENISA (November 2024) - NIS Investments

11. International Monetary Fund (IMF) (April 2024) - Chapter 3 Global Financial Stability Report, Cyber Risk: A Growing Concern for Macro financial Stability.

12. ENISA (July 2025) - Telecom Security Incidents 2024

13. Sources Figure 2: (1) World Economic Forum (WEF) (January 2025) - Global Cybersecurity Outlook 2025 | (2) GSMA (February 2025) - Fraud and Scams: Staying Safe in the Mobile World. | (3) Gartner (December 2024) – IT Key Metrics Data 2025: IT Security Measures Analysis; ENISA (November 2024) - NIS Investments | (4) Eurobarometer (May 2024) - Survey on cyber-skills | EU Mind the Cyber Skills Gap (August 2023): a deep-dive

14. Ofcom (February 2025) - Mobile RAN Power resilience

15. US Office of the National Cyber Director (June 2024) – Summary 2023 cybersecurity regulatory harmonization request for information

16. Telefónica (January 2025) - DORA, NIS2 and CRA: Decoding Europe's Cybersecurity Regulatory Landscape. References to NIS2, DORA, CRA, CSA GDPR, CER legislations

17. Telefónica (April 2025) - Defence, security and preparedness: an EU action plan. References: Niinistö Report on the Preparedness and Readiness of the EU, October 2024; White Paper on European Defence Readiness 2030, March 2025; European Preparedness Plan Strategy, March 2025; Protect EU: EU Internal Security Strategy, April 2025; ReArm Europe Budget Plan, March 2025; work programmes for Multi annual framework

18. Telefónica (April 2025) - Defence, security and preparedness: an EU action plan

19. The EU Cyber Solidarity Act entered into force on 4 February 2025. It aims to strengthen capacities in the EU to detect, prepare for and respond to significant and large-scale cybersecurity threats and attacks. The Act includes a European Cybersecurity Alert System, and a comprehensive Cybersecurity Emergency Mechanism to improve the EU's cyber resilience.

20. ENISA - European Vulnerability Database

21. MITRE CVE Vulnerability data base - https://www.cve.org/

22. Cyber Policy Portal - https://cyberpolicyportal.org/

23. Telefónica (June 2024) - Chile: a frontrunner in cybersecurity in Latin America

24. EU-Chile (June 2025) - ANCI lanza en la Patagonia Chilena proyecto de fortalecimiento de la ciberseguridad de América Latina y el Caribe

25. GSMA (February 2025) - Mobile Telecommunications Security Landscape 2025.

26. European Commission - Report on the cybersecurity and resiliency of the EU communications infrastructures and networks; Informal meeting of the telecommunications Ministers - Joint call. March 2022

27. NIS Cooperation Group (February 2024)- Cybersecurity and resiliency of Europe's communications infrastructures and networks | OECD (May 2025) - Enhancing the resilience of communication networks | World Bank (December 2024) - Resilient telecommunications infrastructure: A practitioner's guide

28. International Chamber of Commerce (ICC) (July 2024) - Protecting the cybersecurity of critical infrastructures and their supply chains; ENISA (June 2023) - Good practices for supply chain cybersecurity

29. Telefónica (February 2025) - Consolidated annual report 2024

30. Telefónica – Global Security Transparency Center

31. UK National Cybersecurity Centre - Cyber Security Toolkit for Boards

32. Telefónica (December 2024)- Invisible infrastructure that drives the digital world: submarine cables

33. Telxius, a leading global connectivity provider - https://telxius.com/en/inicio-en/

34. EU (February 2025) - Joint Communication to strengthen the security and resilience of submarine cables

35. Telefónica (May 2025) - The FEINDEF defence and security fair: technology, talent and innovation

36. Telefónica (February 2024) - Tactical 5G bubbles and network slicing in public networks

37. España (May 2025) - Informe Anual de Seguridad Nacional 2024

38. Telefónica (March 2025) - Telefónica revolutionizes the use of drones with a comprehensive and secure service

39. GSMA - GSMA Open Gateway

40. Government of Spain (February 2025) - Spain plan to combat pone and text messages scam

41. Vivo (December 2024) - Antispam service

42. Vivo (May 2025) - Vivo Seguro

43. UK VMO2 (November 2024) - O2 unveils Daisy, the AI granny wasting scammers' time

44. INCIBE - Qué hacer si eres víctima de un fraude

45. VMO2 (May 2025) - New report calls for overhaul of fraud policing as majority of police believe officers lack the resources and skills to investigate the crime

46. Telefónica Tech - Next Defense

47. Telefónica Tech - The SOC of the future: How AI and automation are redefining the future

48. EU Member States declaration (Nov.2024) - Securing tomorrow today: transitioning to Post-Quantum Cryptography

49. EU Commission (April 2024) - Recommendation on Post-Quantum Cryptography

50. EU Commission (June 2025) - A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography

51. Telefónica Tech (June 2025) - Strategic preparation for Post Quantum Cryptography

52. Telefónica (March 2025) - Telefónica opens a dedicated Centre of Excellence for quantum technologies

53. Telefónica - Quantum-Safe Networks

54. Telefónica (October 2024) - QKD, cryptographic keys and quantum networks

55. Telefónica (March 2025) - Telefónica anticipates quantum challenges with an innovative demo at MWC

56. Telefónica (March 2025) - Telefónica and Vithas test shielding against quantum attacks in two hospitals

57. Telefónica (March 2025) - Telefónica partner of Government of Biscay for development of its quantum technology industrial strategy

58. EU (March 2025) - European Preparedness Union Strategy

59. EU (2019) - Regulation (EU) 2019/881 (CSA) on ENISA and on ICT cybersecurity certification

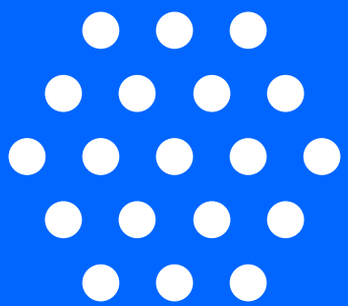
60. EU (2022) - Directive (EU) 2022/2557 on the resilience of critical entities (CER)

61. OFCOM - Statement on Network and Service Resilience Guidance

62. World Economic Forum (WEF – April 2025) - The Cyber Resilience Compass: Journeys Towards Resilience.

63. EU (2022) - Directive (EU) 2022/2555 - NIS 2 on measures for a high common level of cybersecurity across the Union

Digital Security:
Resilience, Innovation, and Trust



Follow the conversation on:
our Web, Linkedin or
subscribe to our Newsletter

Telefónica

Digital Public Policy, Regulation and Competition

2025