Digitale Sicherheit:
Widerstandsfähigkeit, Innovation und Vertrauen

Digitale öffentliche Politik, Regulierung und Wettbewerb

2025

Telefónica

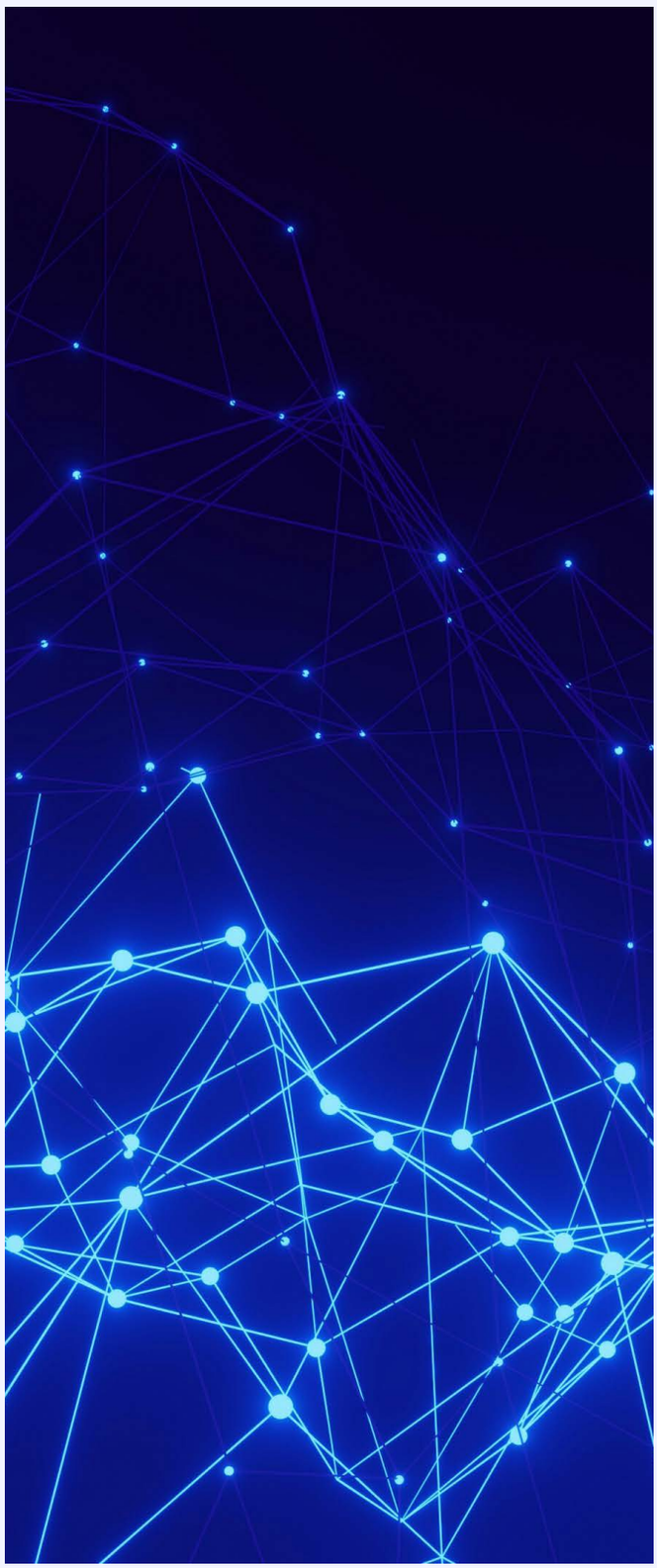
Vorwort

Angesichts beispielloser Cyber-Bedrohungen und eines komplexen regulatorischen Umfelds ist der Bedarf an einem technologischen und strategischen Partner so groß wie nie zuvor. Wir bei Telefónica sind davon überzeugt, dass digitale Sicherheit nicht nur eine geschäftliche Notwendigkeit ist, sondern ein öffentliches Gut und eine tragende Säule für eine widerstandsfähige und wirtschaftlich starke Gesellschaft.

Die Digitalisierung hat jeden Aspekt unseres Lebens verändert, aber mit diesem Fortschritt gehen auch neue Risiken einher. Wir haben ein exponentielles Wachstum von Cyberangriffen, eine sich vergrößernde Qualifikationslücke, Finanzierungsengpässe und die Herausforderungen einer fragmentierten und komplexen politischen Landschaft erlebt. Diese Probleme unterstreichen eine grundlegende Wahrheit: Die Sicherung unserer digitalen Zukunft erfordert ein neues Modell der Zusammenarbeit. Es erfordert eine Partnerschaft zwischen dem öffentlichen und dem privaten Sektor, in der das technische Know-how der Telekommunikationsbranche genutzt wird, um die Öffentlichkeit und die Politik zu informieren und zu stärken.

Als weltweit führendes Telekommunikationsunternehmen geht unsere Rolle über die Bereitstellung von Konnektivität hinaus. Unser sicheres Netzwerk und unsere hochmodernen Fähigkeiten machen uns zu einem zentralen Akteur bei dieser Herausforderung. Telefónica steht als vertrauenswürdiger Partner Regierungen, öffentlicher Verwaltungen und Unternehmen jeder Größe beim Aufbau der Widerstandsfähigkeit und Sicherheit im digitalen Raum zur Seite, und hilft damit anderen, in einer zunehmend vernetzten Welt erfolgreich zu sein.

Dieses Dokument ist unser Beitrag zur öffentlichen Diskussion rund um Resilienz und Cybersicherheit. Es bietet eine umfassende Analyse der aktuellen Sicherheitslage und enthält klare, umsetzbare Empfehlungen für politische Entscheidungsträger. Wir hoffen, dass dieses Papier als Katalysator für eine sicherere, innovativere und vertrauenswürdigere Welt dient, die auf gemeinsamer Verantwortung und Zusammenarbeit basiert.



Index

1. Zusammenfassung

Strategische Sicherheitsziele müssen durch ein förderliches Umfeld unterstützt werden

Komplexe Vorschriften und ungedeckte Verpflichtungen drohen die von uns angestrebte Widerstandsfähigkeit zu untergraben. Ein stabiler Telekommunikationssektor und gute politische und finanzielle Rahmenbedingungen sind unerlässlich, um Sicherheit, Widerstandsfähigkeit und Souveränität sicherstellen zu können. Telefónica verfügt über jahrzehntelange Erfahrung im Aufbau, der Absicherung und dem Betrieb umfangreicher digitaler Infrastrukturen und Dienste und ist damit als strategischer Partner ein überaus verlässlicher Partner, um Regierungen, Unternehmen und die Gesellschaft beim Aufbau ihrer Resilienz zu unterstützen.

Die digitale Sicherheit ist eine grundlegende Säule der Gesellschaft: ein öffentliches Gut, eine gemeinsame Verantwortung und ein wichtiger Motor für Innovation

Digitale Sicherheit und technologische Souveränität sind zu zentralen Themen der politischen Agenda geworden. Darüber hinaus ist die digitale Sicherheitsbranche ein wichtiger Eckpfeiler. Dieser Eckpfeiler bedarf einer gezielteren Koordinierung aller Beteiligten, dazu gehören Unternehmen ebenso wie Behörden, sowie eines langfristigen politischen Engagements und Investitionen, die sich nachhaltig auf die Sicherheitsstruktur auswirken.

Vorbereitung ist dringender denn je, eine Stärkung der Resilienz benötigt einen einheitlichen Rahmen

In einer Ära wachsender Sicherheitsrisiken und geopolitischer Unsicherheiten unterstreicht die anhaltende Zunahme von Cyberangriffen, Datenverstößen, Betrug und Cyberspionage die dringend erforderliche und Schaffung einheitlicher Sicherheitsrahmenbedingungen und einer zielgerichteten Industriepolitik.

Der Schutz strategischer Infrastruktur ist von entscheidender Bedeutung

Robuste ITK-Netzwerke sind unverzichtbar, da sie wie das Fundament eines Hauses wichtige Funktionen und Dienste für die gesamte digitale Welt bereitstellt. Die Telekommunikationsbranche engagiert sich seit langem

für eine Umsetzung gezielter Sicherheitsmaßnahmen - zum Schutz ihrer Vermögenswerte, Kunden und Dienste. Doch ihre positiven Beiträge für Wirtschaft und Gesellschaft und nachhaltigen Investitionen werden oft nicht anerkannt. Regulatorische Verpflichtungen, die über marktwirtschaftliche Erwägungen hinausgehen, können die langfristige Planungssicherheit von Telekommunikations-Netzbetreibern gefährden, wenn sie nicht durch eine angemessene Gegenfinanzierung ausgeglichen werden, wie dies in anderen Sektoren der Fall ist.

Telefónica als vertrauenswürdiger und strategischer Partner spielt eine entscheidende Rolle bei der Stärkung der Sicherheit und des Vertrauens in der gesamten Gesellschaft

Telefónica nutzt seine Erfahrung, qualifizierte Mitarbeiter, umfangreiche Partnerschaften und starke operative Fähigkeiten nicht nur zum Schutz seiner eigenen Infrastruktur, sondern auch zur Stärkung der Resilienz der gesamten Gesellschaft – einschließlich Unternehmen und öffentlicher Verwaltungen –, während es gleichzeitig aktiv das Bewusstsein für mehr Sicherheit in der ITK schärft und Betrugsversuche aktiv bekämpft.

Telekommunikationssektor ist wichtiger Motor für Sicherheitsinnovationen

Der Sektor unterstützt die Entwicklung von Spitzentechnologien – wie KI und Quantencomputern – und effizienten Prozessen, um seine eigene Effizienz, Widerstandsfähigkeit und innovative Dienstleistungen zu steigern und gleichzeitig die digitale Transformation in allen Branchen und öffentlichen Diensten voranzutreiben.

Es ist Zeit zu handeln - mit Maßnahmen, die eine sichere, innovative und vertrauenswürdige digitale Umgebung schaffen

Empfehlungen zur Verbesserung der digitalen Sicherheit und Fähigkeiten, zur Erhöhung der Resilienz und zur Steigerung der Souveränität:

1. **Sicherstellung eines stabilen und wirtschaftlich starken Telekommunikations,** sektors, der auf vertrauenswürdigen Betreibern basiert und als wichtiger Technologiepartner für Regierungen und Unternehmen fungiert.

2. **Erhöhung der Investitionen in Sicherheit, Widerstandsfähigkeit und Dual-Use-Technologien** durch den gezielten Einsatz öffentlicher Mittel, gezielter steuerlicher Anreize und den strategischen Einsatz öffentlicher Beschaffungsmaßnahmen.

3. **Einführung eines angemessenen, verhältnismäßigen und risikobasierten Sicherheitsregelungsrahmens**, der von Fakten gestützt und in enger Zusammenarbeit mit der Privatwirtschaft entwickelt wird.

4. **Stärkung der Cybersicherheit und Ausbau der technologischen Kompetenzen** bStei gleichzeitiger Sensibilisierung und Aufklärung der Öffentlichkeit zur digitalen Sicherheit, für eine resiliente digitale Gesellschaft.

5. **Gezielte Koordinierung zwischen Beteiligten in den Bereichen Cyber-Intelligence, Verteidigung und Strafverfolgung** zur Abschreckung von Cyberkriminalität, unterstützt durch mehr Ressourcen und eine verstärkte Zusammenarbeit.

2. Den Wert der *digitalen Sicherheit* und Widerstandsfähigkeit erschließen

A. Sicherheit als grundlegender Pfeiler der Gesellschaft: ein öffentliches Gut, eine gemeinsame Verantwortung und ein wichtiger Motor für Innovation

In einer Zeit zunehmender digitaler Komplexität und wachsender geopolitischer Spannungen sind digitale Sicherheit und technologische Souveränität in den Vordergrund der politischen Agenda gerückt.

Für Organisationen geht es beim Aufbau digitaler Sicherheit im Wesentlichen darum, einen umfassenden Ansatz zu entwickeln, die Geschäftskontinuität zu schützen und das Vertrauen durch Maßnahmen zu erhalten, die über rein technische Lösungen hinausgehen. Für politische Entscheidungsträger geht es darum, wirtschaftliche Stabilität, Souveränität und öffentliches Vertrauen zu gewährleisten, indem sie Resilienz zum Bestandteil von umfassenderen politischen Rahmenbedingungen zu machen[2].

Digitale Sicherheit ist ein öffentliches Gut und eine gemeinsame Verantwortung, die koordinierte Anstrengungen von Regierungen, öffentlichen Verwaltungen, der Wirtschaft und internationalen Gremien erfordert[3]. Darüber hinaus ist die digitale Sicherheitsbranche ein strategischer Motor für technologische Innovation und Souveränität. Um ein Zusammenwirken dieser Akteure zu gewährleisten sind eine stärkere Koordinierung, langfristiges politisches Engagement und eine nachhaltige Finanzierung erforderlich.

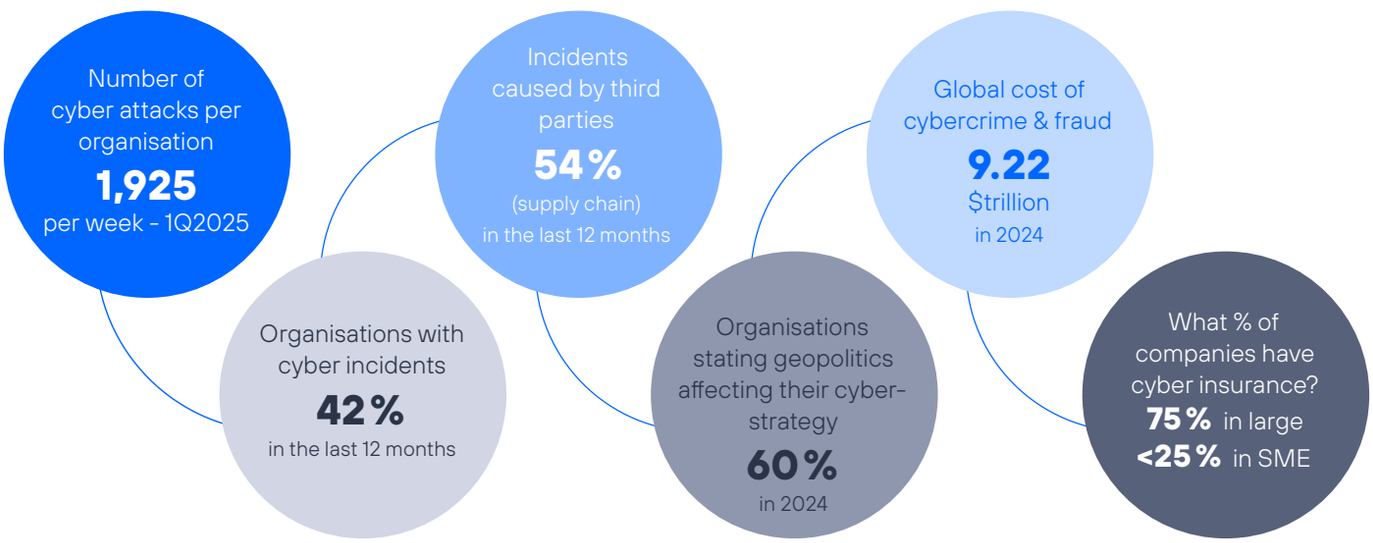
Angesichts beispielloser Cyberbedrohungen und kom-plexer regulatorischer Rahmenbedingungen ist der Bedarf an einer strategischen Partnerschaft zwischen Unter-nehmen und staatlichen Stellen so groß wie nie zuvor.

> **Sicherheit ist das Fundament, auf dem alles aufgebaut ist [...] Sicherheit ist ein öffentliches Gut [...] Sie ist die Voraussetzung für die Wahrung unserer Werte und eine Notwendigkeit für unseren wirtschaftlichen Erfolg und unsere Wettbewerbsfähigkeit.**
>
> *Niinistö-Bericht „Safer Together" über die Vorsorge und Bereitschaft der EU – Oktober 2024[1]*

B. Die wachsende Sorge um die digitale Sicherheit prägt die heutige digitale Landschaft

Das Weltwirtschaftsforum[4] identifiziert Cyber-Risiken (Fehlinformationen, Desinformation, Cyberspionage und Cyberkrieg) als eines der zehn größten globalen Gefahren. Die Cyberlandschaft wird immer komplexer. Datendiebstähle, Ransomware-Angriffe[5], und Cyberspionage nehmen weiter zu. Die Welt sieht sich einer neuen Realität mit wachsenden Risiken und Unsicherheiten gegenüber, die eine Vorbereitung dringender denn je machen.

Abbildung 1. Globale Landschaft der digitalen Sicherheit[6]



Quellen: Telefónica basierend auf: Checkpoint (April 2025) – Global Cyber Attack Report für das 1. Quartal 2025. Checkpoint – Der Stand der Cybersicherheit | Weltwirtschaftsforum (WEF) (Januar 2025) – Global Cybersecurity Outlook 2025 | GSMA (Februar 2025) – Betrug und Scams: Sicherheit in der mobilen Welt | Internationaler Währungsfonds (IWF) (April 2024) – Kapitel 3 Global Financial Stability Report, Cyber Risk: A Growing Concern for Macro financial Stability

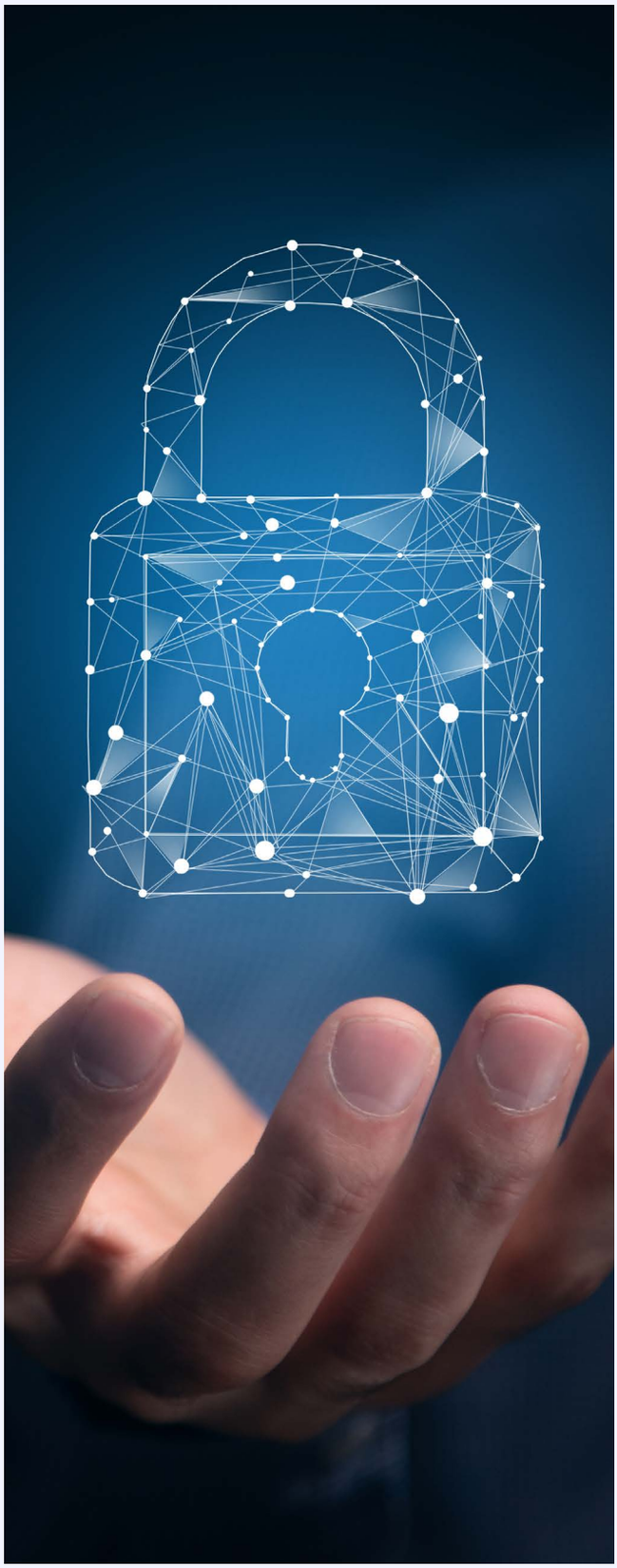
Die Zahl der Cyberangriffe ist im vergangenen Jahr um 50 % gestiegen und erreichte im ersten Quartal 2025 durchschnittlich 1.925 Angriffe pro Woche und Organisation[7]. Rund 42 % der Organisationen waren 2024 von einem erfolgreichen Social-Engineering-Angriff betroffen, eine Zahl, die mit dem böswilligen Einsatz von KI nur noch steigen kann[8]. 54 % der Cyberangriffe in Unternehmen ist entlang der Lieferkette ausgeführt worden.

Die weltweiten Kosten von Cyberkriminalität, einschließlich Betrug[9], werden voraussichtlich von 9,22 Billionen im Jahr 2024 auf 15,63 Billionen US-Dollar im Jahr 2029 steigen. Die durchschnittlichen Gesamtkosten pro Vorfall werden derzeit auf über 4 Millionen Euro geschätzt[10].

Laut dem Cyber-Risiko-Bericht des IWF[11], sind die am stärksten gefährdeten Organisationen jene in stark vernetzten Branchen, mit attraktiven Vermögenswerten, aber schwächerem Schutz (wie KMU) und jene, die in Ländern mit hohem geostrategischem Risiko oder unzureichender Cyber-Gesetzgebung tätig sind. Angreifer werden von einer Reihe von Motiven angetrieben, am häufigsten von finanziellen Gewinnen – wie bei organisierten kriminellen Gruppen –, aber auch vom Streben nach Anerkennung oder der Förderung politischer und sozialer Ziele.

Die Kluft zwischen cyberresilienten und nicht cyberresilienten Organisationen wird immer größer. Kleine Organisationen können sich nach Aussage von 71 % der IT-Führungskräfte nicht mehr angemessen gegen die wachsende Komplexität von Cyberrisiken schützen. Weniger als ein Viertel der KMU verfügt über eine Cyberversicherung, verglichen mit 75 % der größeren Organisationen. Mehr als doppelt so viele KMU wie große Organisationen geben an, dass ihnen die erforderliche Cyber-Resilienz fehlt, um ihre kritischen betrieblichen Anforderungen zu erfüllen, was ihre Entwicklung in der digitalen Welt verzögert. Im Telekommunikationssektor sind die Hauptursachen für Dienstunterbrechungen – gemessen in Stunden verlorener Kommunikation – in erster Linie Systemausfälle (60 %), gefolgt von menschlichen Fehlern (19 %), Naturereignissen (13 %) und böswilligen Handlungen (8 %)[12].

Die Stärkung der Vorsorge und die Bekämpfung von Cyberbedrohungen sind dringender denn je geworden. Zusammenfassend lässt sich sagen, dass die Folgen von Informationsvorfällen, Cyberbedrohungen und Betrug erhebliche finanzielle Verluste, die Gefährdung der Wirtschaftlichkeit von Unternehmen und den Verlust des Vertrauens in digitale Dienste umfassen können, was letztlich die Einführung ansonsten vorteilhafter Technologien behindert. Darüber hinaus ist die Bekämpfung ausländischer Manipulationen entscheidend geworden, um Stabilität und den souveränen Schutz individueller Rechte, Unternehmen, demokratischer Prozesse und grundlegender Werte zu gewährleisten.



C. Die Verbesserung der Resilienz erfordert die Bewältigung geopolitischer, technischer, politischer und wirtschaftlicher Herausforderungen

Im heutigen Kontext erfordert der Aufbau von Resilienz die Bewältigung einer Reihe **zentraler Herausforderungen**[13].

Abbildung 2. Wichtige Herausforderungen, die die Sicherheitslandschaft prägen

Telefónica

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

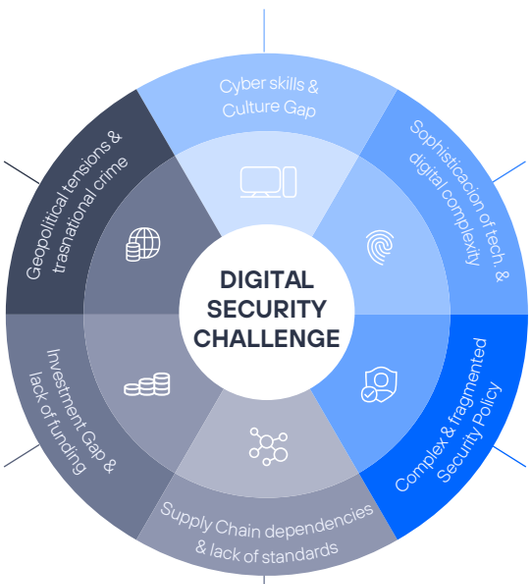
Only **14%** of orgs. feel confident about their skills[1]

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

Quellen: Telefónica basierend auf: (1) Weltwirtschaftsforum (WEF) (Januar 2025) – Global Cybersecurity Outlook 2025 | (2) GSMA (Februar 2025) – Betrug und Scams: Sicherheit in der mobilen Welt. | (3) Gartner (Dezember 2024) – IT Key Metrics Data 2025: IT Security Measures Analysis; ENISA (November 2024) – NIS Investments | (4) Eurobarometer (Mai 2024) – Umfrage zu Cyber-Kompetenzen | EU Mind the Cyber Skills Gap (August 2023): eine eingehende Untersuchung

Geopolitische Spannungen und grenzüberschreitende Kriminalität erschweren weiterhin die Bemühungen zur Bekämpfung von Unsicherheit und Betrug. Der Mangel an Fachkräften für Cybersicherheit und das Fehlen einer starken Cybersicherheitskultur verschärfen diese Herausforderungen zusätzlich. Während neue Technologien neue Möglichkeiten für Verteidigung und Widerstandsfähigkeit bieten, behindert die zunehmende Komplexität digitaler Systeme die End-to-End-Sicherheit. Darüber hinaus stellen die gegenseitigen Abhängigkeiten in der Lieferkette und das Fehlen gemeinsamer oder offener Standards erhebliche Hindernisse für den Aufbau langfristiger, widerstandsfähiger Infrastrukturen dar.

Der Bereich der Cybersecurity ist sowohl im öffentlichen als auch im privaten Sektor nach wie vor unterfinanziert. Zugleich gehen die regulatorischen Ziele von Regierungen oft über einen risikobasierten, verhältnismäßigen oder marktorientierten Ansatz hinaus und es mangelt ihnen an den für die Umsetzung erforderlichen Analysen der Wirtschaftlichkeit. Die Verbesserung der Resilienz ist kostspielig – beispielsweise würden die Kosten für die Bereitstellung eines Backups im britischen Mobilfunk-RAN für alle vier Mobilfunknetze 0,9 bis 1,8 Milliarden Pfund betragen, zuzüglich laufender Wartungskosten[14].

Eine fragmentierte und hochkomplexe Regulierungslandschaft behindert wirksame Strategien. Zwar werden Vorschriften zunehmend als Schlüssel zur Stärkung der grundlegenden Cybersicherheit anerkannt, doch ihre wachsende Zahl und mangelnde Abstimmung stellen große Herausforderungen dar. Doppelte, widersprüchliche oder unnötige Vorschriften erfordern von den Unternehmen den Einsatz zusätzlicher Ressourcen zur Erfüllung technischer Compliance-Anforderungen, ohne dass sich dadurch die Cybersicherheit verbessert[15].

KASTEN 1

EUROPAS CYBERSICHERHEITSPOLITIK: KOMPLEX UND FRAGMENTIERT

In der Europäischen Union erhöht die NIS2-Richtlinie die Cybersicherheitsstandards für 18 Sektoren und verlangt von den regulierten Unternehmen Risikomanagement, Reaktion auf Vorfälle und Berichterstattung, Planung der Geschäftskontinuität, strengere Überwachung der Lieferkette und eine größere Rechenschaftspflicht auf Vorstandsebene.

Sie wirkt jedoch in einem **komplexen regulatorischen Umfeld**[16], das bereits durch zahlreiche andere Europarechtlich vorgaben reguliert ist, wie z.B. DORA (Digital Operational Resilience Act), CRA (Cyber-Resilience Act), CSA (Cybersecurity Act-Zertifizierungsrahmen), CER (Critical Entities Resilience), Vorschriften für den Telekommunikationssektor, DSGVO (Datenschutz-Grundverordnung), dem AI-Act oder der EU-5G-Toolbox.

Ergänzt werden diese Rahmenwerke durch **nationale und europäische Sicherheitsstrategien**[17], idarunter der Aktionsplan zur Verteidigung[18], die Cybersicherheitsvorschläge für Krankenhäuser, Initiativen zum Schutz von Unterseekabeln, das europäische Programm „Protect EU" oder der 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.

Eine weitere Entwicklung ist die Einführung der **ENISA-Schwachstellendatenbank (EUVD)**[20] im Mai 2025. Die EUVD ist zwar nicht so umfangreich wie die öffentlich finanzierte CVE-MITRE-Datenbank der Vereinigten Staaten, strebt jedoch ein hohes Maß an Vernetzung an, indem sie öffentlich zugängliche Informationen aus verschiedenen Quellen, darunter CSIRTs, Anbieter und bestehende Schwachstellendatenbanken, zusammenführt.

Diese komplexe und fragmentierte Politiklandschaft unterstreicht die Notwendigkeit eines vereinfachten und verhältnismäßigen Ansatzes, um Cybersicherheitsbedrohungen in der gesamten EU wirksam zu bekämpfen.

KASTEN 2

CYBERSICHERHEITSPOLITIK IN ANDEREN REGIONEN: ENTWICKLUNGEN IN BRASILIEN UND CHILE

Weltweit variieren die regulatorischen Ansätze zur Cybersicherheit stark[22]. In Lateinamerika sind mehrere Gesetzesinitiativen im Gange, deren Reifegrad jedoch erheblich variiert. Die Stärke der Schutzmaßnahmen hängt oft davon ab, ob ein Land zuvor mit größeren Cybervorfällen konfrontiert war – wie beispielsweise im Fall von Costa Rica.

BRASILIEN

Brasilien hat die Grundlagen für einen robusten Rahmen für Cybersicherheit geschaffen, insbesondere durch das Allgemeine Datenschutzgesetz (LGPD) und die Nationale Cybersicherheitsstrategie (E-Ciber), sowie durch die Schaffund eines Nationalen Cybersicherheitskomitees (CNCiber).

Im Hinblick auf die sektorale Regulierung hat die Regulierungsbehörde Anatel im Jahr 2020 die Cybersicherheitsverordnung für den Telekommunikationssektor (R-Ciber) verabschiedet und im Jahr 2024 aktualisiert, die Regeln für Telekommunikationsnetze und -dienste festlegt, wobei der Schwerpunkt auf dem Schutz kritischer Infrastrukturen liegt. Zudem werden vorbeugende Maßnahmen festgelegt, welche die Reaktion auf Vorfälle und das Risikomanagement vorschreiben.

CHILE

Chile sticht mit der Verabschiedung des Gesetzes Nr. 21.663 über Cybersicherheit und kritische Informationsinfrastruktur[23] im März 2024 hervor. Es ist Chiles erste umfassende regulatorische Antwort auf die Bedrohung durch Cyberangriffe. Es ergänzt die Nationale Cybersicherheitspolitik 2023–2028 und schafft einen grundlegenden Rahmen für eine kohärente nationale Cybersicherheitsstrategie. Die Kernprinzipien:

- Gründung der Nationalen Cybersicherheitsbehörde (ANCI), eines nationalen CSIRT (zivile Vorfälle) und eines Verteidigungs-CSIRT – jeweils mit klar definierten Aufgaben, spezifischen Cybersicherheitsfunktionen und zweckgebundenen Finanzmitteln, die alle dem Grundsatz der Rationalität unterliegen.

- Verpflichtung zur Zusammenarbeit mit den Behörden bei der Bewältigung von Vorfällen.

- Protokolle zur Schadensbegrenzung und schnellen Reaktion, um die Auswirkungen zu mildern.

- Verpflichtung zu Sicherheit und Datenschutz durch Design und durch Voreinstellungen.

- Betonung der Informationssicherheit im Einklang mit internationalen Standards.

Vom 28. bis 30. Mai 2025 trafen sich Regierungsvertreter und Experten aus 10 Ländern der Region in Puerto Varas, um das Projekt *„Stärkung der Cybersicherheitskapazitäten in Lateinamerika und der Karibik"*[24]. zu starten. Diese von der EU finanzierte Initiative, die Teil der **EU-LAC-Digitalallianz** ist, wird Chile bei der Weiterentwicklung seiner Cybersicherheitspolitik unterstützen und gleichzeitig diese Erfahrungen weitergeben, um die regionale digitale Sicherheitsbereitschaft zu verbessern.

Die Entwicklung der Cybersicherheitspolitik in Brasilien und Chile zeigt, dass digitale Sicherheit weltweit als nationale Priorität und wichtiger Motor für das Wirtschaftswachstum anerkannt ist.

Quellen: Cyber Policy Portal https://cyberpolicyportal.org/ | Telefónica (Juni 2024) – Chile: Vorreiter in Sachen Cybersicherheit in Lateinamerika | EU-Chile (Juni 2025) ANCI startet in der chilenischen Patagonien ein Projekt zur Stärkung der Cybersicherheit in Lateinamerika und der Karibik | Brasilien – Dekret Nr. 11.856 vom 26. Dezember 2023

3. Der Telekommunikationssektor – und Telefónica als *strategischer Partner* – ibeim Schutz der digitalen Infrastruktur und der Stärkung von Sicherheit und Vertrauen in der Gesellschaft

Ein vertrauenswürdiger und nachhaltiger Telekommunikationssektor ist ein unverzichtbarer Partner für die Gewährleistung der Sicherheit und Widerstandsfähigkeit der Gesellschaft. Die Telekommunikationsbranche engagiert sich seit langem für die Entwicklung und den Einsatz robuster Sicherheitsmaßnahmen zum Schutz ihrer Vermögenswerte, Kunden und Dienste[25].

Über diese Kernaufgabe hinaus nutzt sie ihr umfangreiches Fachwissen und ihre technischen Fähigkeiten, um eine Schlüsselrolle bei der Stärkung der Widerstandsfähigkeit aller Sektoren und der öffentlichen Verwaltung zu spielen. Gleichzeitig fungiert die TK-Branche als Motor für Innovationen und fördert die Einführung modernster digitaler Technologien und erstklassiger Betriebsverfahren – darunter Cloud Computing, künstliche Intelligenz oder Quantentechnologien.

Aufgrund seiner jahrzehntelangen Erfahrung ist Telefónica einzigartig positioniert, um Regierungen, Unternehmen und die Gesellschaft beim Aufbau von Resilienz zu unterstützen.

A. Der Wert des Schutzes strategischer Infrastrukturen

Resiliente Telekommunikationsnetze sind für Verbraucher, Unternehmen und Regierungen von entscheidender Bedeutung, da eine zunehmende Abhängigkeit von digitaler Kommunikation im Bereich kritischer Dienste besteht. Dies Umfasst z.B. Bereiche wie digitale Zahlungen, die Gesundheitsversorgung, den Betrieb kritischer Sektoren, die Steuerung des Energienetzes oder den Schutz sensibler Daten.

Die Telekommunikationsbranche spielt dabei eine Schlüsselrolle und tätigt erhebliche Investitionen, um die Sicherheit und Widerstandsfähigkeit ihrer Infrastruktur zu stärken[27]. Dazu gehören die Umsetzung strenger Sicherheitsanforderungen, die Anwendung bewährter Verfahren in der Lieferkette[28], die Minimierung einzelner Fehlerquellen und die Einrichtung robuster Prozesse, Tools und Schulungen zur Unterstützung der betrieblichen Widerstandsfähigkeit.

Trotz seiner entscheidenden Rolle bei der Sicherung digitaler Netzwerke werden die positiven Beiträge des Telekommunikationssektors oft nicht anerkannt – insbesondere in einer Zeit, in der er vor großen Investitionsherausforderungen steht, um die politisch definierten Konnektivitätsziele zu erreichen. Unzureichende Investitionen in Sicherheit und Widerstandsfähigkeit würden die Netzwerke zunehmend anfällig für neue Bedrohungen machen und sowohl die Betriebsfähigkeit des Telekommunikationssektors als auch die davon abhängigen wesentlichen Dienste schwächen.

Die Auferlegung neuer regulatorischer Verpflichtungen, die über marktwirtschaftliche Erwägungen hinausgehen – ohne gründliche Kosten-Nutzen-Analyse oder angemessene Finanzierung –, würde das Risiko einer erheblichen Kostensteigerung und einer weiteren Untergrabung der langfristigen Nachhaltigkeit der Telekommunikationsbetreiber mit sich bringen.

> **Kritische Infrastrukturen wie Telekommunikationsnetze und digitale Dienste sind für viele wichtige Funktionen in unseren Gesellschaften von größter Bedeutung und daher ein bevorzugtes Ziel für Cyberangriffe.**
>
> *Informelles Treffen der Telekommunikationsminister in Nevers, 9. März 2022*[26]

KASTEN 3

DIGITALE SICHERHEITS-GOVERNANCE BEI TELEFÓNICA

Telefónica versteht Sicherheit[29] als ein umfassendes Konzept, dessen Zweck darin besteht, Vermögenswerte, Interessen und strategische Ziele zu bewahren, ihre Integrität zu gewährleisten und sie vor potenziellen Bedrohungen zu schützen. Alle Märkte, in denen Telefónica tätig ist, verfügen über eine lokale Sicherheitsorganisation, die vom globalen Bereich für Sicherheit und Intelligence koordiniert wird.

Umfassende Sicherheit beinhaltet:

- Physische und operative Sicherheit (von Personen und Eigentum)
- Digitale Sicherheit
- Geschäftskontinuität
- Betrugsprävention
- Schutz der Lieferkette
- Alle anderen relevanten Bereiche oder Funktionen, deren Ziel der Schutz des Unternehmens vor potenziellen Schäden oder Verlusten ist.

Die digitale Sicherheit umfasst wiederum die Informations- und Cybersicherheit und gilt für die Mittel, Systeme, Technologien und Elemente, aus denen das Netzwerk und die Informationssysteme bestehen. Um den Informationsbedarf der Stakeholder auf klare, prägnante und zugängliche Weise zu decken, bietet Telefónica in seinem Global Transparency Centre einen eigenen Bereich „Sicherheit" an, der auf seiner Website[30] verfügbar ist. In diesem Bereich können auch Schwachstellen oder Bedrohungen gemeldet werden, die sich auf die technologische Infrastruktur von Telefónica auswirken könnten.

Der frühzeitige Schutz der Vermögenswerte von Telefónica wird durch die Festlegung von Sicherheitsrichtlinien auf der Grundlage internationaler Standards und die Implementierung robuster, auf das Geschäftsumfeld zugeschnittener Sicherheitsarchitekturen erreicht. Darüber hinaus basiert der Ansatz von Telefónica zur Cyberabwehr auf einem umfassenden und proaktiven Modell, das die fortschrittlichen Fähigkeiten des Unternehmens in folgenden Schlüsselbereichen nutzt:

- **Antizipation.** Telefónica verfolgt eine auf Cyber Intelligence basierende Strategie, die sich auf Proaktivität und Weitsicht konzentriert. Durch die kontinuierliche Identifizierung neuer Trends, Bedrohungen und verdächtiger Aktivitätsmuster verbessert das Unternehmen die frühzeitige Erkennung von Sicherheitsverletzungen. Die Integration fortschrittlicher Technologie und Expertenwissen gewährleistet eine zeitnahe Identifizierung von Risiken.

- **Prävention.** Spezielle interne Expertenteams, wie das Red Team, suchen aktiv nach digitalen Schwachstellen, um Risiken zu identifizieren und zu mindern, bevor sie ausgenutzt werden können.

- **Erkennung und Reaktion.** Telefónica verfügt über ein Netzwerk von Computer Security Incident Response Teams (CSIRTs), die eine schnelle und effektive Reaktion auf Vorfälle gewährleisten. Diese Teams koordinieren sich, um Sicherheitsvorfälle effizient zu bewältigen und deren Auswirkungen zu minimieren. Sie arbeiten auch mit nationalen und internationalen CSIRTs und CERTs im öffentlichen und privaten Sektor zusammen und stärken so die globale Cybersicherheit.

Die schrittweise Stärkung der Sicherheitskapazitäten und -ressourcen von Telefónica wurde durch die Entscheidung erreicht, intern spezifische Fähigkeiten in den Bereichen Kryptografie, Cyber-Intelligence und Cyber-Verteidigung zu entwickeln.

Das robuste Governance-Modell von Telefónica, das einen Top-down- und Bottom-up-Ansatz kombiniert, stellt sicher, dass Cybersicherheit ein zentraler Bestandteil der Geschäftsstrategie und -abläufe des Unternehmens ist.

Quellen: Telefónica – Global Security Transparency Center https://www.telefonica.com/en/global-transparency-center/security/

KASTEN 4

AUFBAU EINER CYBERSICHERHEITSKULTUR: TELEFÓNICA DEUTSCHLAND

Cybersicherheit wird oft als Domäne von Spezialisten angesehen, die in Silos arbeiten – aber echte Resilienz hängt von jedem einzelnen Mitarbeiter ab[31]. Der Ansatz *„ Stärkung des „schwächsten Glieds"* veranschaulicht, dass selbst die besten Abwehrmaßnahmen versagen können, wenn die täglichen Praktiken im gesamten Unternehmen nicht mit grundlegenden Cyber-Abwehrmaßnahmen und -richtlinien im Einklang stehen.

Bei Telefónica verankern wir eine „Safety-First"-Denkweise im gesamten Unternehmen. Unser Ansatz kombiniert kontinuierliche Sensibilisierung, maßgeschneiderte Schulungen und moderne Engagement-Formate, um allen Mitarbeitern zu helfen, sichere Verhaltensweisen im beruflichen Alltag anzuwenden. Von selbstbestimmtem Lernen über Angebote im Intranet und Wissenszentren bis hin zu interaktiven Präsentationen und Kursangeboten unserer Sicherheitsexperten – wir möchten Cybersicherheit für jeden Matarbeitenden relevant und zugänglich machen.

Um die Mitarbeitenden noch stärker einzubinden, hat Telefónica neue Formate wie **die Security-Arena** eingeführt – eine Vor-Ort-Veranstaltung, die anregende Minispiele mit Diskussionselementen kombiniert – sowie ein browserbasiertes Spiel, das Social-Engineering-Taktiken untersucht. Für das Management helfen Tabletop-Übungen dabei, Prozesse und Verantwortlichkeiten zu testen und zu verfeinern. Menschen bleiben eine unserer wichtigsten Ressourcen. Durch das Angebot vielfältiger Lernformate, die Förderung offener Kommunikation und die Stärkung der gemeinsamen Verantwortung baut Telefónica eine Unternehmenskultur in Bezug auf die Cybersicherheit auf, die die langfristige Widerstandsfähigkeit unterstützt.

Ergänzend zu dieser kulturellen Grundlage hat Telefónica Deutschland Anfang 2024 ein virtuelles, interdisziplinäres **Threat Intelligence Squad** eingerichtet. Das Team analysiert wichtige geopolitische und Cyber-Risiken und veröffentlicht einen Bericht zur sich ständig weiterentwickelnden Bedrohungslandschaft, wie beispielsweise das „Threat Intelligence Radar 2024–2025".

Durch die Konzentration auf Sensibilisierung, Schulung und interne Kommunikation fördert Telefónica Germany erfolgreich eine positive Cybersicherheitskultur, die die Mitarbeiter befähigt, de facto die erste Verteidigungslinie zu bilden.

Quellen: UK National Cybersecurity Centre – Cyber Security Toolkit for Boards | Telefónica Deutschland – Threat Intelligence Radar 2024–2025

KASTEN 5

SCHUTZ VON UNTERSEEKABELN: TELXIUS

Angesichts der wachsenden Zahl hybrider Bedrohungen, darunter die jüngsten Vorfälle in der Ost- und Nordsee, erweisen sich Unterwasserkabel[32] als unverzichtbarer Faktor für die digitale Widerstandsfähigkeit.

Telxius[33] implementiert ein ganzheitliches Sicherheitsmodell, das ein effektives Management durch aktuelle Richtlinien, eine Kombination aus robusten physischen und Cybersicherheitsmaßnahmen, regelmäßige Audits und eine kontinuierliche Bewertung der Sicherheitspraktiken gewährleistet. Die internen Vorschriften sind auf die rechtlichen Rahmenbedingungen und internationalen Standards abgestimmt und werden durch Schulungs- und Sensibilisierungsprogramme für Mitarbeiter unterstützt.

In diesem Zusammenhang gewährleistet Telxius die Widerstandsfähigkeit seiner Anlandestationen für Unterseekabel durch den Betrieb eines Business Continuity Management Systems gemäß den Vorschriften und Richtlinien der Telefónica-Gruppe auf der Grundlage der Norm ISO 22301. Darüber hinaus unterhält das Unternehmen ein aktives integriertes Managementsystem für seine wichtigsten Landestationen, das die Anwendung von Best Practices gemäß ISO 27001 für Informationssicherheitsmanagement, ISO 14001 für Umweltmanagement und ISO 50001 für Energieeffizienz gewährleistet.

Die Geschäftskontinuität wird durch redundante Kabelwege, verbesserte physische Sicherheit, robuste Kontinuitätspläne, regelmäßige Tests und klar definierte Verfahren zur Notfallwiederherstellung (Recovery-Management) gestärkt. Das Krisenmanagement umfasst strukturierte Reaktionspläne, geschultes Personal, etablierte Kommunikationskanäle und Bewertungen nach Krisen („Lessons learned"). Die physische und personelle Sicherheit wird durch Zugangskontrollen, Überwachung, Schutz von Vermögenswerten, Notfallprotokolle und die Förderung einer sicheren Arbeitsumgebung gewährleistet.

Im Bereich Cybersicherheit verfolgt Telxius einen mehrschichtigen Ansatz, der Daten, Anwendungen, Geräte, Netzwerke und Perimeter abdeckt und KI und maschinelles Lernen für die Echtzeit-Erkennung von Bedrohungen nutzt. Zu den Maßnahmen gehören End-to-End-Verschlüsselung, Netzwerksegmentierung, Schutz von Unternehmensgeräten und Schutzmaßnahmen gegen den Diebstahl von Zugangsdaten, um eine sichere Kommunikation, den Schutz von Daten und die Risikominderung zu gewährleisten.

Erhöhung der Resilienz durch verbesserte Koordination

Es besteht ein dringender Bedarf an koordinierten Maßnahmen und einem wirksamen grenzüberschreitenden Dialog, um die wichtige Infrastruktur zu schützen. Der EU-Aktionsplan zur Kabelwegesicherheit enthält einen Rahmen zur weiteren Erhöhung der Widerstandsfähigkeit und Sicherheit von Unterseekabeln[34]. Die aktive Einbindung der Interessengruppen aus der Industrie wird entscheidend sein, um eine umfassende und praktische Reaktion zu gewährleisten.

Ein harmonisierter Ansatz für das Unterwasserkabel-Ökosystem muss Sicherheitsziele mit operativer Machbarkeit, nachhaltigen Geschäftsmodellen und der strategischen Nutzung öffentlicher Mittel in Einklang bringen. Dieser Ansatz muss durch angemessene, risikobasierte Best Practices untermauert werden, die in enger Zusammenarbeit mit Partnern aus der Industrie entwickelt wurden.

Die Fallstudie zeigt, wie wichtig öffentlich-private Partnerschaften für den Schutz kritischer globaler Infrastrukturen wie Seekabel vor einer Vielzahl physischer und digitaler Bedrohungen sind.

Quellen: Telxius, ein weltweit führender Anbieter von Konnektivitätslösungen | Telefónica (Dezember 2024) – Unsichtbare Infrastruktur, die die digitale Welt antreibt: Unterseekabel

B. Nutzung des Know-hows der Telekommunikationsbranche zur Stärkung des Schutzes in allen Sektoren

Der Telekommunikationssektor spielt eine wichtige Rolle bei der Sicherung einer Vielzahl von anderen Wirtschaftssektoren. Der TK-Bereich nutzt seine Erfahrungen, seine qualifizierten Mitarbeiter, seine umfangreichen Partnernetzwerke und seine robusten operativen Fähigkeiten nicht nur zum Schutz seiner eigenen Infrastruktur, sondern auch zur Stärkung der Widerstandsfähigkeit der Gesellschaft, der Unternehmen und der öffentlichen Verwaltung insgesamt. Mit ihrem fundierten technischen Fachwissen und ihrer hohen Einsatzbereitschaft leistet die Branche einen wichtigen Beitrag zur Sicherung von Dienstleistungen in den Bereichen Verteidigung, Bankwesen, Energie, Gesundheitswesen, Finanzen, Verkehr, Fertigung und anderen Schlüsselbranchen.

Der Bereich des Cyberbetrugs hat organisierte kriminelle Gruppen auf den internationalen Markt für Cyberkriminalität gelockt, wo sie schwer aufzuspüren und strafrechtlich zu verfolgen sind. Um Betrug zu bekämpfen, investieren Betreiber erhebliche Ressourcen in die Identifizierung, Filterung und Blockierung betrügerischer Datenströme, doch diese Verbrechen sind oft Teil einer ausgeklügelten und organisierten Kette von Ereignissen – technische Maßnahmen allein reichen daher nicht aus. Trotz aller Bemühungen der Branche haben Kriminelle einen Weg gefunden, in dem sie technische Abwehrmaßnahmen umgehen und mittels „Social Engineering" gezielt menschliches Verhalten für ihre Angriffeszwecke ausnutzen.

KASTEN 6

SICHERHEITSDIENSTE VON TELEFÓNICA FÜR UNTERNEHMEN UND ÖFFENTLICHE VERWALTUNGEN

Telefónica bietet eine umfassende Palette von Cybersicherheitslösungen. Als vertrauenswürdiger Managed Security Service Provider (MSSP) konzentriert sich Telefónica Tech auf Prävention, Erkennung und schnelle, effektive Reaktion, um Cyberangriffe abzuwehren, Unternehmen und öffentliche digitale Dienste zu schützen und die Cyber-Resilienz in allen Branchen und Regionen zu stärken. Das Unternehmen bietet auch spezialisierten Schutz für Operational-Technology-Systeme (OT), die industrielle Prozesse steuern und maßgeschneiderte Cybersicherheitsansätze erfordern, die an ihre spezifischen Architekturen und Einschränkungen angepasst sind. Diese Mission wird von einem multidisziplinären Team hochqualifizierter Cybersicherheitsexperten vorangetrieben, das über umfangreiche Erfahrung in der Erbringung von Dienstleistungen für Dritte verfügt.

Die rund um die Uhr verfügbaren Kapazitäten von Telefónica Tech basieren auf hochmodernen Digital Operations Centern (DOC) und Security Operations Centern (SOC), die strategisch günstig in Europa und Amerika positioniert sind. Telefónica Tech bietet globalen Schutz, der sich auf lokales Fachwissen stützt, und unterstützt Kunden während des gesamten Bedrohungszyklus. Das anpassungsfähige Dienstleistungsportfolio kombiniert proprietäre Technologien mit etablierten Produkten und Lösungen von Drittanbietern und gewährleistet so einen umfassenden und flexiblen Schutz vor sich ständig weiterentwickelnden Bedrohungen.

Die Cybersicherheitsfähigkeiten von Telefónica Tech werden von Kunden aus einer Vielzahl von Branchen geschätzt, durch ein starkes Netzwerk strategischer Partner gestützt und von führenden Branchenanalysten regelmäßig anerkannt. Ergänzend zu seinen Kernsicherheitsdiensten bietet Telefónica auch Cyberversicherungslösungen an, um den Schutz zu verbessern und das Risikomanagement zu unterstützen. Darüber hinaus veröffentlicht das Unternehmen regelmäßig Berichte und Cyber-Intelligence-Analysen, die wertvolle Einblicke in neue Bedrohungen und Trends liefern.

Mit seinem umfassenden Angebot an Sicherheitsdienstleistungen für Unternehmen und öffentliche Verwaltungen ist Telefónica ein wichtiger Partner beim Aufbau eines sicheren und widerstandsfähigen digitalen Ökosystems.

Quellen: Telefónica Tech | Telefónica Tech – Cybersicherheitsdienste | Telefónica Tech – Fallstudien | Telefónica Tech (Juli 2025) – Cybersicherheitsbericht 2025 H1 | Telefónica Tech (2025) – Cyberresilienz in kritischen Infrastrukturen | Telefónica Cyberversicherungsdienste

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

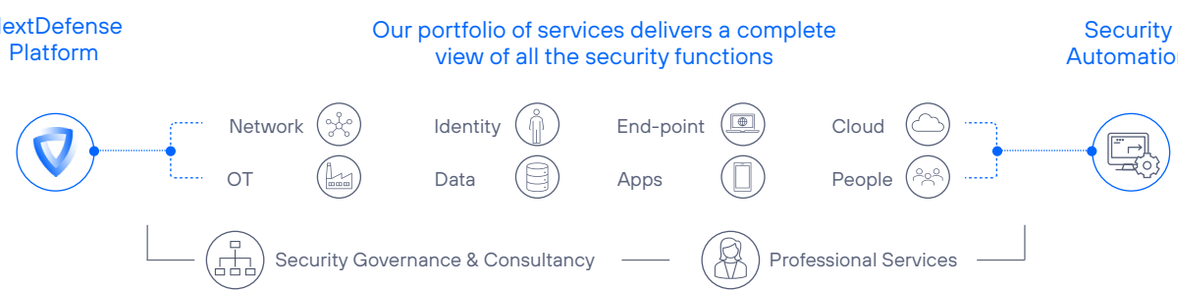
+370k EDR agents deployed

+50k h. Pentesting and Red Team

+4,150 TB Logs ingested into SIEM

HIGHEST LEVEL PARTNERSHIP

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



Quellen: Telefónica Tech | Telefónica Tech – Cybersicherheitsdienste | Telefónica Tech – Fallstudien | Telefónica Tech (Juli 2025) – Cybersicherheitsbericht 2025 H1 | Telefónica Tech (2025) – Cyberresilienz in kritischen Infrastrukturen | Telefónica Cyberversicherungsdienste

KASTEN 7

DIE ROLLE VON TELEFÓNICA BEI DER STÄRKUNG DER TECHNOLOGISCHEN FÄHIGKEITEN DES VERTEIDIGUNGSSEKTORS

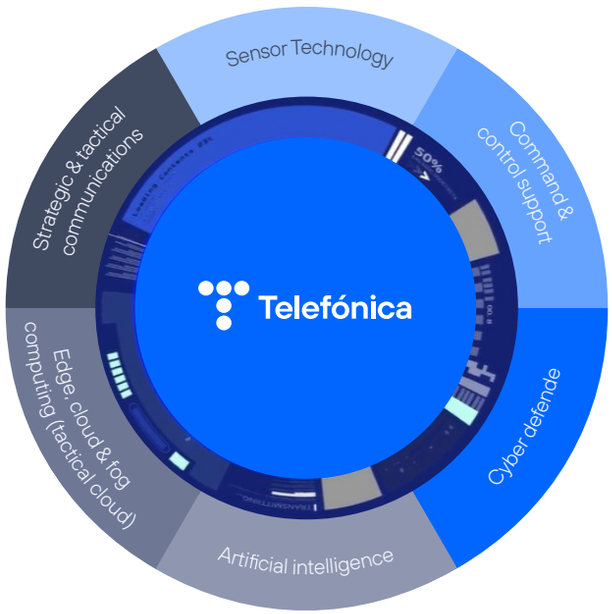
Ohne eine fortschrittliche, widerstandsfähige digitale Infrastruktur und vertrauenswürdige Technologiepartner kann keine Verteidigungsfähigkeit sicher funktionieren. Auf der spanischen Verteidigungs- und Sicherheitsmesse (FEINDEF 2025)[35], stellte Telefónica seine umfassende Technologiestrategie vor, die darauf abzielt, die strategischen, operativen und taktischen Fähigkeiten zu stärken und gleichzeitig die Sicherheit im gesamten Verteidigungssektor zu verbessern. Moderne Verteidigungs- und Militäroperationen erfordern moderne und hocheffektive Kommunikationsmittel und Technologien.

Telefónica bringt sein umfangreiches Fachwissen in die Integration von Verteidigungstechnologien in Schlüsselbereichen wie Hypersensing, strategische und taktische Konnektivität – einschließlich 5G-Taktikblasen[36] und Spektrumdominanz – sowie sicheren Datentransport mit Post-Quanten-Bereitschaft ein. Diese Fähigkeiten werden durch fortschrittliche Cloud-, Edge- und Fog-Computing-Architekturen ergänzt, wobei letztere als dezentrale Schicht zwischen Edge- und Cloud-Umgebungen fungieren. Zusammen ermöglichen sie die effiziente Organisation und Verwaltung missionskritischer Informationen.

In Kombination mit KI-gesteuerter Datenverarbeitung, robuster digitaler Sicherheit, fortschrittlichen Cyberabwehrfähigkeiten und Kommandoposten der nächsten Generation, die mit Extended Reality erweitert wurden, bietet dieses umfassende technologische Ökosystem einen entscheidenden Vorteil sowohl beim Schutz als auch bei der strategischen Nutzung von Informationen.

Auch die Gefahren durch Drohnen sind vielfältig und umfassen Risiken für den Flugverkehr Spionage, Terrorismus sowie Störung kritischer Infrastrukturen. Sie sind [37-38] Parallel dazu fördert Telefónica Innovationen sowohl intern als auch durch offene Innovationsmodelle mit Wayra, seinem Corporate Accelerator. Das Unternehmen hat mehrere Vereinbarungen geschlossen, darunter mit dem Defence Innovation Accelerator for the North Atlantic (DIANA) der NATO, wodurch sechs Telefónica-Labore in das internationale Netzwerk von DIANA integriert wurden. Diese Labore sind auf Spitzenbereiche wie Quantentechnologien, Netzwerke der nächsten Generation, das Internet der Dinge (IoT) und Cybersicherheit spezialisiert.

Integration of technologies for information superiority



Die Zusammenarbeit von Telefónica mit dem Verteidigungssektor verdeutlicht die entscheidende Rolle von Innovationen und technologischem Know-how des privaten Sektors für die Verbesserung der nationalen Sicherheit und Verteidigungsfähigkeiten.

Quellen: Telefónica Defensa y Seguridad | Telefónica (Mai 2025) – Die Verteidigungs- und Sicherheitsmesse FEINDEF: Technologie, Talent und Innovation

KASTEN 8

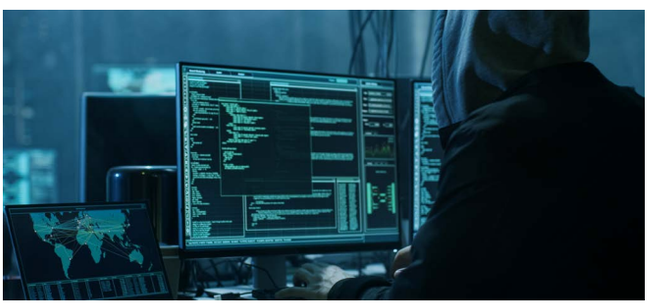
DIE BEKÄMPFUNG VON BETRUG: ANHEBUNG DER STANDARDS UND SENSIBILISIERUNG

Die Zunahme von Betrugsfällen gibt zunehmend Anlass zur Sorge und veranlasst die Akteure im digitalen Ökosystem, ihre Bemühungen zur Bekämpfung dieser Bedrohung zu intensivieren. Kriminelle finden Wege, den menschlichen Faktor durch Social Engineering auszunutzen. Gleichzeitig macht es die Zunahme der grenzüberschreitenden Cyberkriminalität für die Strafverfolgungsbehörden immer schwieriger, Betrug zu bekämpfen.

Telefónica hat den Kampf gegen Betrug mit einer Reihe von Initiativen in verschiedenen Regionen konsequent unterstützt. Hier einige Beispiele (die Liste ist nicht vollständig).

GSMA Open Gateway initiative[39]

Die Betreiber haben verschiedene Netzwerk-APIs (Application Programming Interfaces) eingeführt, die die digitale Sicherheit verbessern und Betrug bekämpfen sollen (z. B. Gerätestatus, Geräteort, SIM-Swap, Betrugssignal ...). Diese APIs ermöglichen es Entwicklern und Partnern, intelligente Ebenen der Kundenauthentifizierung, -verifizierung und -schutz innerhalb mobiler Netzwerke aufzubauen. Diese Innovation hilft Unternehmen – wie Finanzinstituten und Online-Händlern – die Benutzerauthentifizierung zu stärken und Betrug besser zu verhindern.



SPANIEN

Im Februar 2025 verabschiedete die spanische Regierung in breitem Konsens mit der Industrie eine Ministerialverordnung zur Bekämpfung von Betrug bei Sprachanrufen und 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.

in dem Maßnahmen zur Bekämpfung von Identitätsbetrug festgelegt wurden – bei dem die Absendernummer so verändert wird, dass die Empfängernummer eine vertrauenswürdige Nummer, eine bekannte Nummer oder eine Institution anzeigt.

Der Plan umfasst mehrere technische Maßnahmen: Sperrung nicht autorisierter Nummern, z. B. solcher, die keinem Dienst, Betreiber oder Kunden zugewiesen sind; Verhinderung von gefälschten spanischen Nummern, die aus internationalen Anrufen oder Nachrichten stammen, mit Ausnahme von Nutzern, die sich rechtmäßig im Ausland im Roaming befinden; Einrichtung eines nationalen Registers für alphanumerische Absender-IDs, das von der Nationalen Kommission für Märkte und Wettbewerb (CNMC) verwaltet wird, um die Imitation legitimer Einrichtungen wie Banken oder Behörden zu verhindern; und Verbot der Verwendung von Mobilfunknummern für Kundendienstzwecke oder unaufgefordertes Telemarketing, wobei Unternehmen stattdessen geografische Nummern oder 800/900-Leitungen verwenden müssen, die nun für ausgehende Anrufe zugelassen sind.

BRASILIEN

Brasilien setzt zunehmend biometrische Identifizierung in einigen Produkten ein, darunter auch Verhaltensbiometrie, um Betrug in verschiedenen Bereichen wie Sozialversicherung, Bankwesen, Telekommunikation und Behörden zu bekämpfen. Durch die genaue Überprüfung von Identitäten können biometrische Systeme dazu beitragen, Betrug wie Identitätsdiebstahl, Kontoübernahmen und nicht autorisierte Transaktionen aufzudecken und zu verhindern.

Vivo bietet darüber hinaus eine Vielzahl von Produkten und Dienstleistungen zur Bekämpfung von Betrug an. Ein Beispiel dafür ist Vivo Anti-Spam[41]: Dieser kostenlose Dienst für Mobilfunknutzer analysiert das Anrufverhalten im gesamten Netz und blockiert mithilfe intelligenter Algorithmen unerwünschte Anrufe. Oder die Plattform *"Modo Seguro"*[42], über die Vivo-Nutzer ihr Gerät im Falle eines Diebstahls oder Verlusts aus der Ferne sperren und Daten löschen können.

Großbritannien

Virgin Media O2 (VMO2) verfolgt einen proaktiven und vielschichtigen Ansatz zur Bekämpfung von Betrug durch Technologie, Zusammenarbeit innerhalb der Branche und Sensibilisierung der Kunden. Als Mitwirkender an der „Telecoms Fraud Sector Charter" der britischen Regierung unterstützt VMO2 gemeinsame Bemühungen zur Verbesserung der Erkennung von Betrugsanrufen und -SMS, zur Verhinderung von Nummernmissbrauch und zum Datenaustausch mit Strafverfolgungsbehörden. Auf der Verbraucherseite hat das Unternehmen DAISY[43], ins Leben gerufen, eine innovative Sensibilisierungskampagne, bei der simulierte Kundennummern verwendet werden, um betrügerische Anrufe anzulocken und zu untersuchen – damit soll die Wahrscheinlichkeit verringert werden, dass echte Kunden ins Visier genommen werden. In Kombination mit Tools wie KI-basierter SMS-Filterung und verbesserter Anrufüberprüfung spiegeln diese Bemühungen das starke Engagement von VMO2 wider, Nutzer zu schützen und Betrug im gesamten Telekommunikationsbereich zu reduzieren.

Ein ganzheitlicher Ansatz zur Betrugsbekämpfung

Kooperation und ein ganzheitlicher Ansatz sind der Schlüssel zur Betrugsbekämpfung. Um fortschrittliche Tools effektiv einsetzen zu können, benötigen Unternehmen sowohl Flexibilität als auch zeitnahen Zugriff auf relevante Daten – ohne dass übermäßige oder unverhältnismäßige Datenschutzrichtlinien diesen Kampf behindern. Dies erfordert die Berücksichtigung der gesamten Wertschöpfungskette sowie die Priorisierung der Sensibilisierung der Nutzer[44] und der Strafverfolgung[45]. Die sektorübergreifende Zusammenarbeit ist für die Erreichung gemeinsamer Ziele von entscheidender Bedeutung und erfordert einen flexiblen, pragmatischen und zukunftssicheren Ansatz, um der raschen Dynamik von Betrugsfällen entgegenzuwirken.

Der proaktive Ansatz von Telefónica zur Betrugsbekämpfung unter Einsatz fortschrittlicher Technologien und Informationen unterstreicht die Notwendigkeit einer gemeinsamen, öffentlichen und branchenweiten Anstrengung zum Aufbau digitaler Vertrauenswürdigkeit.

Quellen: UK VMO2 (Mai 2025) - Neuer Bericht fordert Überarbeitung der Betrugsbekämpfung, da die Mehrheit der Polizisten der Meinung ist, dass den Beamten die Ressourcen und Fähigkeiten zur Ermittlung dieser Straftaten fehlen | INCIBE. Qué hacer si eres víctima de un fraude | GSMA – GSMA Open Gateway | Regierung von Spanien (Februar 2025)- Spanien plant Maßnahmen zur Bekämpfung von Telefon- und SMS-Betrug | VIVO – Antispam service | Vivo (Mai 2025) - Vivo Seguro | UK VMO2 (November 2024) - O2 stellt Daisy vor, die KI-Oma, die Betrügern Zeit stiehlt

C. Ein wichtiger Innovationssektor im Bereich fortschrittlicher Technologien und Katalysator für deren Einführung

Der Telekommunikationssektor ist ein wichtiger Motor für Innovation und setzt kontinuierlich modernste digitale Technologien und erstklassige Betriebsverfahren ein und integriert diese. Dazu gehören Cloud Computing, künstliche Intelligenz und neue Quantentechnologien – nicht nur, um die eigene Effizienz, Widerstandsfähigkeit und Dienstleistungserbringung zu verbessern, sondern auch, um eine sichere digitale Transformation in allen Branchen und öffentlichen Diensten zu ermöglichen.

> **Technologie wird das Hauptmerkmal des Wettbewerbs im neuen geopolitischen Umfeld sein. Eine Handvoll kritischer und grundlegender Technologien wie KI, Quantenphysik, Biotechnologie, Robotik und Hyperschall sind wichtige Faktoren sowohl für langfristiges Wirtschaftswachstum als auch für militärische Überlegenheit**
>
> *Weißbuch zur europäischen Verteidigungsbereitschaft 2030 – März 2025*

KASTEN 9

DIE ZUKUNFT DER SOCS: ERHÖHUNG DER DIGITALEN SICHERHEIT MIT KI

Telefónica Tech leitet einen bedeutenden Wandel in der Art und Weise ein, wie Unternehmen Herausforderungen im Bereich Cybersicherheit angehen, indem es die Entwicklung des Security Operations Center (SOC) durch den **strategischen Einsatz von künstlicher Intelligenz (KI) und Automatisierung** vorantreibt.

Angesichts einer zunehmend komplexen und feindseligen digitalen Landschaft – geprägt von hybriden Infrastrukturen, einer Kombination aus lokalen Systemen und mehreren öffentlichen und privaten Cloud- -Umgebungen, der Verbreitung vernetzter Geräte und einem kritischen Mangel an Fachkräften – fördert Telefónica Tech eine moderne, effiziente und proaktive SOC-Architektur.

Mit seiner NextDefense-Lösungs[46], tintegriert das Unternehmen fortschrittliche Funktionen wie Verhaltensanalysen, automatisiertes Alarmmanagement und erweiterte Bedrohungsinformationen, wodurch Fehlalarme deutlich reduziert, kritische Vorfälle besser priorisiert und Reaktionszeiten verkürzt werden können.

Dieser Ansatz bietet Unternehmen einen umfassenden Überblick über ihr gesamtes digitales Ökosystem, einschließlich Multi-Cloud- und Operational-Technology-Umgebungen (OT), und ermöglicht so eine frühzeitige Risikoerkennung, kontextbezogene Bedrohungsanalysen und präventive Maßnahmen. Darüber hinaus ergänzt Telefónica Tech seine technologischen Fähigkeiten durch Expertendienstleistungen wie Threat Hunting, Cybersecurity-Bewertungen und strategische Beratung und hilft Unternehmen dabei, maßgeschneiderte Sicherheitsstrategien zu definieren, die Ressourcen optimieren und Betriebskosten senken.

Durch die vollständige Integration von KI in die SOC[47], werden sich wiederholende und wenig wertschöpfende Aufgaben automatisiert, sodass sich Analysten auf wirkungsvollere Maßnahmen konzentrieren können, die Betriebseffizienz gesteigert und die Widerstandsfähigkeit gegenüber immer raffinierteren Cyberbedrohungen aktiv gestärkt wird: Durch die Integration von KI und Automatisierung in die Cybersicherheit können Unternehmen Bedrohungen proaktiv erkennen und neutralisieren, wodurch die Erkennungsgeschwindigkeit und die Reaktionszeiten verbessert werden und ein Übergang von einem reaktiven zu einem präventiven Ansatz erfolgt. KI-Systeme analysieren große Datenmengen, um Anomalien und aufkommende Risiken in Echtzeit zu identifizieren, während die Automatisierung sich wiederholende Aufgaben übernimmt und menschliche Analysten für komplexe Entscheidungen freistellt. Maschinelles Lernen verbessert diese Fähigkeiten, indem es kontinuierlich aus neuen Bedrohungen lernt und die Abwehrmaßnahmen anpassungsfähiger und effizienter macht.

Die Integration von KI in Security Operations Center (SOCs) wird für die Bewältigung des wachsenden Volumens und der zunehmenden Komplexität von Cyberbedrohungen von entscheidender Bedeutung sein und eine effizientere Erkennung und Reaktion ermöglichen

Quellen: Telefónica Tech – Next Defense | Telefónica Tech - Das SOC der Zukunft: Wie KI und Automatisierung die Zukunft neu definieren | Telefónica Tech - Cybersicherheitsautomatisierung mit KI zur Vorhersage und Neutralisierung von Bedrohungen

KASTEN 10

CHANCEN UND BEDROHUNGEN DURCH QUANTENTECHNOLOGIEN

Quantentechnologien ermöglichen bahnbrechende Fortschritte in der Datenverarbeitung und eine extrem sichere Kommunikation. Die Entwicklung des Quantencomputings stellt jedoch eine ernsthafte Bedrohung dar, insbesondere durch Strategien *wie „jetzt speichern, später entschlüsseln"*., Um dieses Risiko zu mindern, ist die Einführung von Post-Quantum-Kryptografie (PQC) oder hybriden kryptografischen Systemen die wirksamste kurzfristige Gegenmaßnahme.

In diesem Zusammenhang forderte die von 18 EU-Mitgliedstaaten unterzeichnete gemeinsame Erklärung von 2024[48] die vorrangige Umsetzung des Übergangs zur Post-Quanten-Kryptografie auf der Grundlage der Empfehlung der Europäischen Kommission[49]. Auf diese Initiativen folgte im Juni 2025 die Veröffentlichung des Fahrplans für den Übergang zur Post-Quanten-Kryptografie[50].

Parallel mit der Erklärung wurden im Jahr 2024 die ersten Standards veröffentlicht. Angesichts der Standardisierungsbemühungen in verschiedenen Regionen gewinnt das Konzept der **Krypto-Agilität**[51] — die Fähigkeit, Sicherheitslösungen dynamisch anzupassen, um neue Standards oder Verschlüsselungsalgorithmen zu integrieren – zunehmend an Bedeutung für die Widerstandsfähigkeit.

Die Rolle von Telefónica im Bereich Quantentechnologie

Telefónica hat ein spezielles Kompetenzzentrum für Quantentechnologien eingerichtet[52]. Das Unternehmen macht bereits große Fortschritte in Richtung quantensicherer Netzwerke[53], indem es eine zusätzliche Schutzebene durch quantenresistente Technologien integriert und traditionelle kryptografische Methoden mit Post-Quanten-Kryptografie (PQC) kombiniert. Über das Labor hinaus treibt Telefónica auch Zukunftstechnologien wie die Quantenschlüsselverteilung (QKD) voran, die bereits aktiv im EuroQCI-Netzwerk[54], eingesetzt werden, um ihre weitere Entwicklung zu beschleunigen. Dies wurde in enger Zusammenarbeit mit führenden akademischen und Forschungseinrichtungen sowie in Partnerschaft mit etablierten Netzwerkausrüstungsherstellern durchgeführt.

Auf der MWC25[55], wurden mehrere Anwendungsfälle vorgestellt, darunter Anwendungen im Gesundheitswesen[56], in der Verteidigung und in der Versorgungswirtschaft sowie umfassendere Bemühungen zum Aufbau eines robusten Quantenökosystems. Dazu gehören Partnerschaften mit Herstellern von Quantencomputern und die Zusammenarbeit mit dem Provinzrat von Biskaya[57].

Die Bedeutung der Finanzierung

Eine intensive Zusammenarbeit verschiedener Expertengruppen und die Bereitstellung von Testumgebungen sind der Schlüssel zur Entwicklung sicherer, innovativer Dienste. Eine verbesserte Widerstandsfähigkeit sollte stets marktorientiert sein und durch den Telekommunikationssektor unterstützt werden. Gezielte öffentliche Fördermittel können Investitionslücken schließen, wo private Anreize nicht ausreichen, während öffentliche Beschaffungen die Einführung strategischer, langfristiger Technologien vorantreiben können.

Durch sein frühzeitiges Engagement im Bereich der Quantentechnologie ist Telefónica führend bei der Vorbereitung auf die Sicherheitsrisiken und neuen Chancen, die das Quantencomputing mit sich bringen wird.

Quellen: EU-Kommission (April 2024) - Empfehlung zur Post-Quanten-Kryptografie | Erklärung der EU-Mitgliedstaaten (Nov. 2024) - Securing tomorrow today: transitioning to Post-Quantum Cryptography. | EU-Kommission (Juni 2025) - Koordinierter Fahrplan für den Übergang zur Post-Quanten-Kryptografie | Telefónica Tech (June 2025) – Strategische Vorbereitung auf die Post-Quanten-Kryptografie | Telefónica (März 2025) - Telefónica eröffnet ein spezielles Kompetenzzentrum für Quantentechnologien | Telefónica - Quantensichere Netzwerke | Telefónica (Oktober 2024) - QKD, kryptografische Schlüssel und Quantennetzwerke |Telefónica (März 2025) - Telefónica antizipiert Quantenherausforderungen mit einer innovativen Demo auf dem MWC |Telefónica (März 2025) - Telefónica und Vithas testen Abschirmung gegen Quantenangriffe in zwei Krankenhäusern |Telefónica (März 2025) - Partner der Regierung von Biskaya bei der Entwicklung ihrer industriellen Strategie für Quantentechnologie

4. *Empfehlungen* für politische Akteure für eine sicherere, innovativere und vertrauenswürdigere Welt

Die EU-Staaten arbeiten daran, die Sicherheit zu verbessern, ihre Abwehrfähigkeiten zu stärken, die Cyberresilienz der gesamten Gesellschaft zu erhöhen, erhebliche Investitionen zu tätigen und strategische Abhängigkeiten zu verringern. In diesem Zusammenhang wird ein robuster und Telekommunikationssektor, der auf vertrauenswürdigen Betreibern basiert und als wichtiger Technologiepartner fungiert, von entscheidender Bedeutung sein.

Aber selbst ein starker Privatsektor in Form von Unternehmen der freien Wirtschaft kann diese Herausforderungen nicht alleine bewältigen. Um das volle Potenzial der digitalen und sicherheitspolitischen Ambitionen auszuschöpfen, sind weitere Maßnahmen erforderlich: unter anderem ein enger, verhältnismäßiger und kohärenter Rechtsrahmen, eine gezielte Unterstützung für die Entwicklung eines wettbewerbsfähigen Ökosystems im Bereich strategischer Netzwerktechnologien, Bereitstellung öffentlicher Finanzmittel für Sicherheit und Resilienz als öffentliches Gut sowie der strategische Einsatz öffentlicher Beschaffungsmaßnahmen. Ebenso wichtig sind die Entwicklung von Cyberkompetenzen, eine bessere Koordinierung und Zusammenarbeit zwischen den Behörden, eine nachhaltige Zusammenarbeit mit dem Privatsektor sowie mehr Ressourcen und internationale Zusammenarbeit zur Bekämpfung von Betrug und Cyberkriminalität.

Strategische Ambitionen müssen durch ein Umfeld unterstützt werden, welches diese fördert. Ein in sich gezielt koordinierter, vereinfachter und hinreichend finanzierter Rahmen ist nicht nur eine Option, sondern eine Voraussetzung für die Erreichung der Ziele in Bezug auf Resilienz und Sicherheit. Im Folgenden finden Sie Empfehlungen zur Förderung einer sichereren und vertrauenswürdigeren digitalen Welt.

> **Eine robuste Vorsorge ist nicht umsonst zu haben. Investitionen in die Vorsorge sind mit Kosten verbunden, die jedoch durch die langfristigen Vorteile in Form von Resilienz, weniger Störungen, geringeren Wiederherstellungskosten und langfristiger Wettbewerbsfähigkeit aufgewogen werden.**
>
> *Strategie der Europäischen Union für Vorsorge – März 2025*[58]

A. Sicherstellung eines robusten und wirtschaftlich nachhaltigen Telekommunikationssektors, der auf vertrauenswürdigen Betreibern basiert und als wichtiger regionaler Technologiepartner fungiert

Der Telekommunikationssektor spielt eine entscheidende Rolle – nicht nur als Wegbereiter für Konnektivität, sondern auch als Hüter der strategischen Autonomie und Souveränität? Die wirtschaftliche Nachhaltigkeit des Telekommunikationssektors ist daher ein Eckpfeiler der allgemeinen digitalen Resilienz der Gesellschaft. Um diese Rolle zu stärken, sind die folgenden politischen Maßnahmen unerlässlich:

- **Anerkennung der strategischen Bedeutung des Telekommunikationssektors** für die Stärkung der Widerstandsfähigkeit aller Branchen.

- **Berücksichtigung der Kosten für die Aufrechterhaltung einer sicheren und widerstandsfähigen Telekommunikationsinfrastruktur**, der operativen Fähigkeiten und der schnellen Reaktion auf Vorfälle in der Strategie über die Zukunft der Konnektivität.

- **Einführung eines modernisierten Rechtsrahmens und einer zukunftsorientierten Wettbewerbspolitik, die die Grundlagen des Sektors stärken.** Dies sollte die Skalierbarkeit und die langfristige Investitionskapazität ermöglichen, die erforderlich sind, um angesichts eskalierender cyberphysischer Bedrohungen Sicherheit und Widerstandsfähigkeit aufrechtzuerhalten.

B. Investitionen in Sicherheit, Widerstandsfähigkeit und Dual-Use-Technologien durch öffentliche Mittel, gezielte steuerliche Anreize und den strategischen Einsatz öffentlicher Beschaffungsmaßnahmen fördern

Der Privatsektor sollte nicht allein für die Bereitstellung öffentlicher Güter oder die Finanzierung von Resilienzmaßnahmen über das wirtschaftlich vertretbare Maß hinaus verantwortlich sein. Die Regierungen müssen sich stärker engagieren, indem sie wirksame industriepolitische Maßnahmen umsetzen, öffentliche Investitionen tätigen und das öffentliche Beschaffungswesen strategisch nutzen.

- **Erhöhung der öffentlichen Mittel und Gewährung** von Steueranreizen zur Unterstützung von Verteidigungs-, Cybersicherheits- und Resilienzmaßnahmen – ähnlich wie in anderen strategischen Sektoren wie dem Energiesektor, um die Investitionslücke zu schließen.

- **Unterstützung des Einsatzes wesentlicher Technologien,** die Innovation und langfristige Resilienz fördern, wie künstliche Intelligenz und quantensichere Lösungen.

- **Stärkung und ggf. Modernisierung des öffentlichen Beschaffungswesens als strategischer Hebel zur Förderung technologischer Innovation und Resilienz** — wobei der Fokus nicht ausschließlich auf den niedrigsten Kosten liegen sollte, sondern Sicherheit und einem Fokus auf die Einführung europäischer Technologien/ Förderung der Diversität und technologischer Souveränitätsowie langfristiger Ziele im Vordergrund stehen sollten..

C. Einführung eines gestrafften, verhältnismäßigen, faktenbasierten, risikobasierten und kohärenten Regelungs- und Normenrahmens für die Sicherheit in enger Zusammenarbeit mit dem privaten Sektor

Die Verringerung der regulatorischen Komplexität, der Abbau bürokratischer Hürden, die Förderung bewährter Verfahren und die Gewährleistung eines kohärenten, verhältnismäßigen und vorhersehbaren Rahmens – gepaart mit einer Haltung, die dem privaten Sektor vertraut und ihn stärkt – werden für einen dauerhaften Erfolg von entscheidender Bedeutung sein. Um dieses Ziel zu unterstützen, sollten die politischen Entscheidungsträger:

- **Bewährte Verfahren im Bereich der Cybersicherheit fördern und gleichzeitig Mindeststandards entwickeln** insbesondere in Regionen, in denen diese fehlen –, unabhängige Aufsichtsbehörden einrichten und mit ausreichenden Ressourcen ausgestattete strategische Rahmenwerke schaffen, die die Umsetzung und Einhaltung der Vorschriften unterstützen.

- **Die fragmentierte Sicherheitslandschaft und die Meldepflichten straffen**, gleiche Wettbewerbsbedingungen in allen Ökosystemen gewährleisten, die Angleichung an internationale Standards priorisieren und die Wechselwirkungen zwischen Regulierungsrahmen und verschiedenen Kontaktstellen bewerten, um eine effektivere Ressourcenzuweisung für sinnvolle Sicherheitsergebnisse zu ermöglichen.

- **Sicherstellen, dass alle regulatorischen Verpflichtungen faktenbasiert, risikobasiert und verhältnismäßig sind**, und dass sie stets von gründlichen Kosten-Nutzen-Analysen und klaren Finanzierungsstrategien begleitet werden.

D. Fördern Sie die Entwicklung von Cybersicherheits- und Technologiekompetenzen und stärken Sie gleichzeitig das öffentliche Bewusstsein und Verständnis für digitale Sicherheit

- In alle Ebenen **der Aus- und Weiterbildung investieren**, um einen starken Nachwuchs an Fachkräften für Cybersicherheit und Technologie aufzubauen.

- **Förderung des lebenslangen Lernens und der Weiterqualifizierung** durch gezielte Initiativen für die derzeitige Belegschaft, insbesondere in kritischen Sektoren

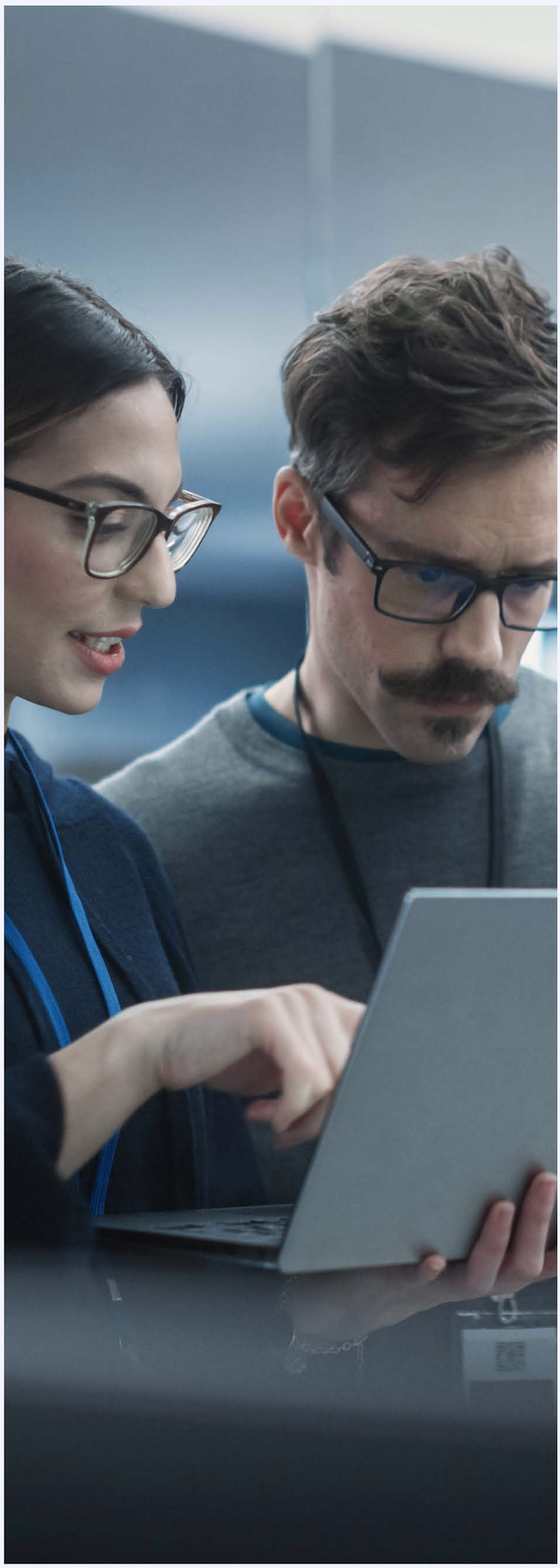
- **Unterstützung von Sensibilisierungskampagnen** zur Aufklärung von Bürgern und Unternehmen – insbesondere KMU – über grundlegende Cyberhygiene, digitale Risiken, Betrug und sichere Praktiken im Internet.

E. Verbesserung der Koordinierung in den Bereichen Cyber-Intelligence, Verteidigung und Abwehr von Cyberkriminalität, unterstützt durch mehr Ressourcen und verstärkte Zusammenarbeit

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. Glossar der wichtigsten begriffe

Cyber-Intelligence bezieht sich im Allgemeinen auf den Prozess des Sammelns, Analysierens und Anwendens von Informationen über Cyber-Bedrohungen, um Entscheidungsfindungen zu unterstützen und die Cybersicherheit zu verbessern.

Eine Cyberbedrohung ist jeder potenzielle Umstand, jedes Ereignis oder jede Handlung, die Netzwerke und Informationssysteme, die Nutzer solcher Systeme und andere Personen schädigen, stören oder anderweitig beeinträchtigen könnte[59].

Cybersicherheit bezeichnet die Maßnahmen, die zum Schutz von Netzwerk- und Informationssystemen, den Nutzern dieser Systeme und anderen von Cyberbedrohungen betroffenen Personen erforderlich sind.

Abschreckung bezeichnet die Maßnahme, eine Handlung oder ein Ereignis durch das Schüren von Zweifeln oder Ängsten vor den Folgen zu verhindern.

Digitale Sicherheit umfasst Informationssicherheit und Cybersicherheit und gilt für die Mittel, Systeme, Technologien und Elemente der Netzwerk- und Informationssysteme.

Ein wesentlicher Dienst ist ein Dienst, der für die Aufrechterhaltung lebenswichtiger gesellschaftlicher Funktionen, wirtschaftlicher Aktivitäten, der öffentlichen Gesundheit und Sicherheit oder der Umwelt von entscheidender Bedeutung ist[60].

Ein Vorfall ist ein Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von gespeicherten, übertragenen oder verarbeiteten Daten oder von Diensten, die von Netz- und Informationssystemen angeboten werden oder über diese zugänglich sind, beeinträchtigt.

Resilienz bezeichnet die Fähigkeit, einen Vorfall zu verhindern, sich davor zu schützen, darauf zu reagieren, ihm zu widerstehen, ihn abzuschwächen, zu absorbieren, sich daran anzupassen und sich davon zu erholen. Im weitesten Sinne ist es die Fähigkeit einer Organisation, einer Ressource oder einer Struktur, einer Reihe bekannter und zukünftiger interner und externer Bedrohungen zu widerstehen, den Auswirkungen eines teilweisen Verlusts oder einer teilweisen Beeinträchtigung der Plattform, des Systems oder des Dienstes standzuhalten, den Dienst mit einem minimalen angemessenen Leistungsverlust

wiederherzustellen und fortzusetzen und aus Vorfällen gewonnene Erkenntnisse zu übernehmen[61]. **Cyber-Resilienz** geht über die traditionelle Cybersicherheit hinaus; sie ist die Fähigkeit einer Organisation, die Auswirkungen bedeutender Cybervorfälle auf ihre primären Geschäftsziele und -vorgaben zu minimieren[62]. In der Erkenntnis, dass 100% ige Sicherheit nicht erreichbar ist, müssen Organisationen adaptive Strategien und eine „*Wann, nicht ob*"-Denkweise verfolgen und anerkennen, dass Vorfälle unvermeidlich sind.

Die Sicherheit von Netz- und Informationssystemen ist die Fähigkeit von Netz- und Informationssystemen, mit einem bestimmten Maß an Zuverlässigkeit allen Ereignissen zu widerstehen, die die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit der gespeicherten, übertragenen oder verarbeiteten Daten oder der von diesen Netz- und Informationssystemen angebotenen oder über diese zugänglichen Dienste beeinträchtigen könnten[63].

Quellen: Definitionen gemäß der Verordnung (EU) 2019/881 über die ENISA; Richtlinie (EU) 2022/2557 über die Widerstandsfähigkeit kritischer Einrichtungen (CER); Richtlinie (EU) 2022/2555 – NIS 2 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union; Definition von „Abschreckung" aus Oxford Languages.

6. Referenzen

1. EU-Kommission (Oktober 2024) – Bericht von Sauli Niinistö – Gemeinsam sicherer: Stärkung der zivilen und militärischen Vorsorge und Bereitschaft Europas

2. Spanische Regierung (2021) – Spanische nationale Sicherheitsstrategie

3. Deutsche Regierung (2022) – Deutsche Nationale Sicherheitsstrategie | Britische Regierung (2022) – Britische Cybersicherheitsstrategie 2022–2030

4. Weltwirtschaftsforum (WEF) (Januar 2025) – Global Risk Report 2025

5. ENISA (September 2024) – ENISA-Bedrohungslage 2024

6. Quellen Abbildung 1: Checkpoint (April 2025) – Globaler Cyberangriffsbericht für das 1. Quartal 2025. Checkpoint – Der Stand der Cybersicherheit | Weltwirtschaftsforum (WEF) (Januar 2025) – Globaler Cybersicherheitsausblick 2025 | GSMA (Februar 2025) – Betrug und Scams: Sicherheit in der mobilen Welt | Internationaler Währungsfonds (IWF) (April 2024) – Kapitel 3 Globaler Finanzstabilitätsbericht, Cyberrisiken: Eine wachsende Sorge für die makrofinanzielle Stabilität

7. Checkpoint (April 2025) – Globaler Cyberangriffsbericht für das 1. Quartal 2025. Checkpoint – Der Stand der Cybersicherheit 2025

8. Weltwirtschaftsforum (WEF) (Januar 2025) – Globaler Cybersicherheitsausblick 2025

9. GSMA (Februar 2025) – Betrug und Scams: Sicherheit in der mobilen Welt

10. ENISA (November 2024) – NIS-Investitionen

11. Internationaler Währungsfonds (IWF) (April 2024) – Kapitel 3 Globaler Finanzstabilitätsbericht, Cyberrisiken: Eine wachsende Sorge für die makrofinanzielle Stabilität.

12. ENISA (Juli 2025) – Sicherheitsvorfälle im Telekommunikationsbereich 2024

13. Quellen Abbildung 2: (1) Weltwirtschaftsforum (WEF) (Januar 2025) – Globaler Cybersicherheitsausblick 2025 | (2) GSMA (Februar 2025) – Betrug und Scams: Sicherheit in der mobilen Welt. | (3) Gartner (Dezember 2024) – IT-Kennzahlen 2025: Analyse der IT-Sicherheitsmaßnahmen; ENISA (November 2024) – NIS-Investitionen | (4) Eurobarometer (Mai 2024) – Umfrage zu Cyber-Kompetenzen | EU Mind the Cyber Skills Gap (August 2023): eine eingehende Untersuchung

14. Ofcom (Februar 2025) – Ausfallsicherheit mobiler RAN-Stromversorgung

15. US-Amt des National Cyber Director (Juni 2024) – Zusammenfassung der Informationsanfrage zur Harmonisierung der Cybersicherheitsvorschriften 2023

16. Telefónica (Januar 2025) – DORA, NIS2 und CRA: Entschlüsselung der europäischen Rechtslandschaft im Bereich Cybersicherheit. Verweise auf NIS2-, DORA-, CRA-, CSA-DSGVO- und CER-Rechtsvorschriften

17. Telefónica (April 2025) – Verteidigung, Sicherheit und Vorsorge: ein Aktionsplan der EU. Referenzen: Niinistö-Bericht über die Vorsorge und Bereitschaft der EU, Oktober 2024; Weißbuch zur europäischen Verteidigungsbereitschaft 2030, März 2025; Europäische Strategie für Vorsorge, März 2025; Protect EU: EU-Strategie für innere Sicherheit, April 2025; ReArm Europe-Haushaltsplan, März 2025; Arbeitsprogramme für den mehrjährigen Rahmen

18. Telefónica (April 2025) – Verteidigung, Sicherheit und Vorsorge: ein EU-Aktionsplan

19. Das EU-Gesetz über Cybersolidarität trat am 4. Februar 2025 in Kraft. Es zielt darauf ab, die Kapazitäten der EU zur Erkennung, Vorbereitung und Reaktion auf bedeutende und groß angelegte Cybersicherheitsbedrohungen und -angriffe zu stärken. Das Gesetz umfasst ein europäisches Cybersicherheitswarnsystem und einen umfassenden Cybersicherheits-Notfallmechanismus zur Verbesserung der Cyberresilienz der EU.

20. ENISA – Europäische Datenbank für Schwachstellen

21. MITRE CVE-Datenbank für Schwachstellen – https://www.cve.org/

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

23. Telefónica (Juni 2024) – Chile: Vorreiter in Sachen Cybersicherheit in Lateinamerika

24. EU-Chile (Juni 2025) – ANCI startet in der chilenischen Patagonien ein Projekt zur Stärkung der Cybersicherheit in Lateinamerika und der Karibik

25. GSMA (Februar 2025) – Sicherheitslage im Bereich der Mobilfunkkommunikation 2025

26. Europäische Kommission – Bericht über die Cybersicherheit und Widerstandsfähigkeit der Kommunikationsinfrastrukturen und -netze der EU; Informelles Treffen der Telekommunikationsminister – Gemeinsamer Aufruf. März 2022

27. NIS-Kooperationsgruppe (Februar 2024) – Cybersicherheit und Widerstandsfähigkeit der europäischen Kommunikationsinfrastrukturen und -netze ; OECD (Mai 2025) – Verbesserung der Widerstandsfähigkeit von Kommunikationsnetzen ; Weltbank (Dezember 2024) – Widerstandsfähige Telekommunikationsinfrastruktur: Ein Leitfaden für Praktiker

28. Internationale Handelskammer (ICC) (Juli 2024) – Schutz der Cybersicherheit kritischer Infrastrukturen und ihrer Lieferketten; ENISA (Juni 2023) – Bewährte Verfahren für die Cybersicherheit in Lieferketten

29. Telefónica (Februar 2025) – Konsolidierter Jahresbericht 2024

30. Telefónica – Globales Zentrum für Sicherheitstransparenz

31. Britisches National Cybersecurity Centre – Cyber Security Toolkit für Vorstände

32. Telefónica (Dezember 2024) – Unsichtbare Infrastruktur, die die digitale Welt antreibt: Unterseekabel

33. Telxius, ein weltweit führender Anbieter von Konnektivitätslösungen – https://telxius.com/en/inicio-en/

34. EU (Februar 2025) – Gemeinsame Mitteilung zur Stärkung der Sicherheit und Widerstandsfähigkeit von Unterseekabeln

35. Telefónica (Mai 2025) – Die Verteidigungs- und Sicherheitsmesse FEINDEF: Technologie, Talent und Innovation

36. Telefónica (Februar 2024) – Taktische 5G-Blasen und Network Slicing in öffentlichen Netzwerken

37. Spanien (Mai 2025) – Jahresbericht zur nationalen Sicherheit

38. Telefónica (März 2025) – Telefónica revolutioniert den Einsatz von Drohnen mit einem umfassenden und sicheren Service

39. GSMA – GSMA Open Gateway

40. Spanische Regierung (Februar 2025) – Spanien plant Maßnahmen zur Bekämpfung von Betrug per Telefon und SMS

41. Vivo (Dezember 2024) – Antispam-Dienst

42. Vivo (Mai 2025) – Vivo Seguro

43. UK VMO2 (November 2024) – O2 stellt Daisy vor, die KI-Oma, die Betrügern Zeit stiehlt

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

45. VMO2 (Mai 2025) – Neuer Bericht fordert Überarbeitung der Betrugsbekämpfung, da die Mehrheit der Polizisten der Meinung ist, dass den Beamten die Ressourcen und Fähigkeiten zur Ermittlung dieser Straftaten fehlen

46. Telefónica Tech – Next Defense

47. Telefónica Tech – Das SOC der Zukunft: Wie KI und Automatisierung die Zukunft neu definieren

48. Erklärung der EU-Mitgliedstaaten (Nov. 2024) – Die Zukunft heute sichern: Übergang zur Post-Quanten-Kryptografie.

49. EU-Kommission (April 2024) – Empfehlung „

50. EU-Kommission (Juni 2025) – Ein koordinierter Fahrplan für den Übergang zur Post-Quanten-Kryptografie

51. Telefónica Tech (Juni 2025) – Strategische Vorbereitung auf die Post-Quanten-Kryptografie

52. Telefónica (März 2025) – Telefónica eröffnet ein spezielles Kompetenzzentrum für Quantentechnologien

53. Telefónica – Quantensichere Netzwerke

54. Telefónica (Oktober 2024) – QKD, kryptografische Schlüssel und Quantennetzwerke

55. Telefónica (März 2025) – Telefónica antizipiert Quantenherausforderungen mit einer innovativen Demo auf dem MWC

56. Telefónica (März 2025) – Telefónica und Vithas testen Abschirmung gegen Quantenangriffe in zwei Krankenhäusern

57. Telefónica (März 2025) – Telefónica ist Partner der Regierung von Biskaya bei der Entwicklung ihrer industriellen Strategie für Quantentechnologie

58. EU (März 2025) – Strategie der Europäischen Union zur Vorsorge

59. EU (2019) – Verordnung (EU) 2019/881 (CSA) über die ENISA und die Zertifizierung der Cybersicherheit von IKT

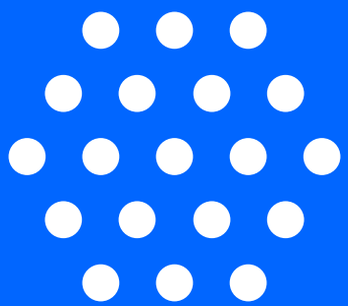
60. EU (2022) – Richtlinie (EU) 2022/2557 über die Widerstandsfähigkeit kritischer Einrichtungen (CER)

61. OFCOM – Erklärung zu Leitlinien für die Widerstandsfähigkeit von Netzen und Diensten

62. Weltwirtschaftsforum (WEF – April 2025) – Der Cyber-Resilienz-Kompass: Wege zur Resilienz.

63. EU (2022) – Richtlinie (EU) 2022/2555 – NIS 2 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union

Digitale Sicherheit:
Widerstandsfähigkeit, Innovation und Vertrauen



Folgen Sie der Diskussion auf:
unserer Web, Linkedin oder
abonnieren Sie unseren Newsletter

Telefónica

Digitale öffentliche Politik, Regulierung und Wettbewerb

2025