European Telecommunications ISAC

Telco Security Landscape 2026

etis TNO

Publisher	ETIS | The community for telecom professionals www.etis.org
Coordinator	Andrija Višić (ETIS Central Office) av@etis.org
Editor	Richard Kerkdijk (TNO) richard.kerkdijk@tno.nl
Release date	April 20th 2026

Contents

Preface 4
Introduction 5
Telco Security Landscape 2026 6
Perspective on landscape evolution 11
Featured: Elisa’s power resilience approach 13
Closing words 14
About 15

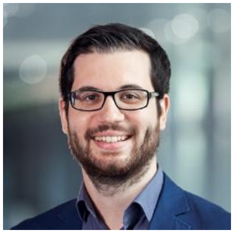
Preface

The telco security environment remains influenced by growing geopolitical tension. Over the past year, these pressures have shown little sign of easing. Across Europe, evolving power dynamics and regional uncertainties continue to affect societies, economies and the resilience of critical infrastructure. This reality highlights the importance of sustained investment in defence, security and reliable civilian communication systems, which are vital in times of crisis.

State-driven threats are still a major concern, yet they represent only one part of a much broader picture. Many telcos depend on technologies and computing resources from regions where tensions are rising, while advances in cloud technology and artificial intelligence are increasingly exposing the limits of long-established security practices. The threat of intentional disruption by both logical and physical means is also on the rise and there is a clear and urgent need for joint resilience planning across sectors and supply chains.

The Telco Security Landscape 2026 reflects the combined insights of ET-ISAC members and aims to inform a broader audience about trends and developments that deserve close attention in the coming year. We thank all contributors for their engagement and hope that this publication inspires European telcos in discussions and decisions towards strengthening their overall security posture.

Rolv. R. Hauge
BCM Manager at
Telenor Norway
and chair of ETIS
Information Security
Working Group



Stefan Kuch
Head of Swisscom
CSIRT and chair of
ETIS CERT-SOC
Telco Network

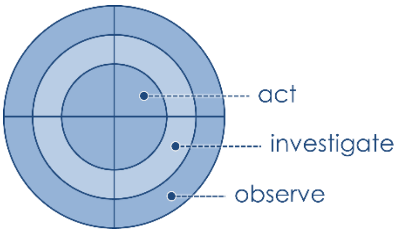
Introduction

The **Telco Security Landscape** depicts key developments that will affect the (cyber) security priorities for European telecommunications providers over the coming years. It is compiled on an annual basis and serves as a strategic guide for the ET-ISAC's activities and meeting agendas. Over the years, it also proved valuable to drive and validate security strategies of individual companies in the ISAC's constituency. Through this public report, the ET-ISAC would like to share insight into its current focus areas and inspire security leaders in other industries to reflect on their relevance as well.

The landscape is visualised in a radar diagram where topics are classified as threats, opportunities or both, as colour coded below:

- = threat
- = opportunity
- = combination of both

In essence, the closer a topic is placed to the center of the radar diagram, the higher ET-ISAC perceives its priority. Here the radar distinguishes three specific action perspectives. The center ring comprises topics that the industry needs to **act** upon in the short term, whereas the middle and outer rings encompass topics that ET-ISAC wishes to **investigate** further or merely **observe** for now.



All topics depicted in the Telco Security Landscape stem from insights provided by security leaders in the European telco industry. In the final quarter of each year, these topics are collected, evaluated and weighted through a series of workshops with ET-ISAC delegates (typically Chief Information Security Officers (CISOs) and representatives thereof). These workshops are indepently facilitated by Dutch knowledge institute TNO who also compile the output report and visualisation.

Telco Security Landscape 2026

This year's Telco Security Landscape is comprised of eight threats, one distinct opportunity and one development that (to some extent) exhibits both characteristics. Combined, they offer a viable perspective on strategic security issues that will affect the telco industry in its entirety and thus warrant a degree of collaboration under the ET-ISAC umbrella. Each landscape topic is briefly described below and the overall radar visualisation is subsequently depicted on page 8-9.

01 **systemic cyber resilience challenges.** The deteriorating geopolitical environment has made telco infrastructure an increasingly attractive target for state sponsored disruption, espionage and prepositioning operations. These threats extend to the critical industries and services that telcos depend on, most notably the energy sector and key SaaS providers. Telcos must recalibrate their resilience strategies to reflect the heightened threat and strengthen collaboration with sectors they rely on to develop jointly aligned resilience plans.

02 **geopolitical sovereignty risks.** Telcos remain heavily dependent on technology and computing resources originating from geopolitically volatile regions. Geopolitical tension or conflict could disrupt access to critical services or resources, as already demonstrated at the ICC in The Hague where sanctions resulted in the loss of e-mail access. The momentum behind Europe's drive for digital sovereignty is accelerating, and telcos have an opportunity to take a leading role in shaping and enabling it.

03 **shortfalls in fundamental security hygiene.** Telco infrastructures consist of highly heterogeneous technology stacks and must support numerous legacy protocols. This complexity makes it inherently difficult to implement consistent security baselines across the entirety of a telco's technical estate, increasing the likelihood of exploitable vulnerabilities.

04 **supply chain dependencies.** Hardware and software supply chains carry systemic risks that require sustained, structural attention. Vulnerabilities in vendor supplied network equipment can expose telcos to a wide range of cybersecurity threats. While initiatives such as GSMA's Network Equipment Security Assurance Scheme (NESAS) framework offer partial mitigation, they do not address all risks or cover all relevant equipment classes. Global supply chains are also threatened by geopolitical instability, creating potential shortages in network

equipment and critical spare components. This reinforces the need for well maintained and appropriately sized replacement stockpiles.

05 **expanding AI exposure surface.** Artificial Intelligence (AI) will become integral to the operation, maintenance and optimization of next generation telco infrastructure, including 6G. Telcos will need to protect the integrity, reliability and security of the underlying models and algorithms. In parallel, Large Language Models (LLM) are now widely used in day to day workflows and increasingly augmented by autonomous AI agents. This heightens the need for robust policies, strong governance and education of staff to prevent the exposure or misuse of sensitive data.

06 **regulatory complexity and misalignment.** Security regulation continues to expand rapidly at both national and European levels. Recent years have seen the introduction of the Cyber Resilience Act, the NIS2 Directive, the CER Directive, the EECC 5G security toolbox and the AI Act. Telcos also inherit requirements from regulation designed for other sectors, for example the Digital Operational Resilience Act (DORA) for financial services. The result is a complex, overlapping and often misaligned regulatory landscape. Greater rationalization and harmonization of security relevant regulation across Europe is necessary to ensure long term viability, clarity and effectiveness.

07 **obsolescence of traditional security models.** Rapid technological change (cloud, AI) and a new reality of politically motivated cyber threats mean that long established security practices are no longer sufficient. Telcos must transition to new security models, with the concept of zero-trust architectures as a promising direction of travel. While 3GPP is embedding this thinking into emerging 5G and 6G standards, future proof security models and practical migration strategies for legacy infrastructure remain limited.

08 **complexity of cloud security configuration.** Telcos are increasingly migrating business and operational support systems into public cloud environments. This offers benefits in terms of speed and automation, allowing telcos to minimize their exposure to new vulnerabilities and threats. At the same time, however, it creates a reliance on generic certifications (e.g. ISO/IEC 27001, ISO/IEC 27017) and on in-house and third party teams to sustain robust cloud security configurations. As cloud platforms and security features expand in scope, configuration management becomes more complex, driving the need for continuous investment in specialist cloud security skills.

expanding AI exposure surface — 05

systemic cyber resilience challenges — 01

shortfalls in fundamental security hygiene — 03

obsolescence of traditional security models — 07

quantum computing — 09

TELCO SECURITY LANDSCAPE 26

02 geopolitical sovereignty risks

04 supply chain dependencies

08 complexity of cloud security configuration

10 AI-enhanced cyber defence

06 regulatory complexity and misalignment

09 **quantum computing.** Many of the cryptographic mechanisms that telcos depend on today — especially public key algorithms — are vulnerable to future quantum enabled cryptanalysis. The urgency to migrate to quantum-safe algorithms and architectures is increasing, particularly given the growing "harvest now, decrypt later" threat.

10 **AI enhanced cyber defence.** The use of AI in cybersecurity has matured significantly. Machine learning for anomaly detection has been in production for more than a decade, and most modern monitoring platforms now embed AI driven predictive capabilities. Looking ahead, the agentic shift creates new opportunities for SOC and CSIRT automation, self-healing network capabilities and AI-enabled red teaming. In parallel, generative AI may accelerate and strengthen DevSecOps workflows, including testing, patching and automated code remediation.

Perspective on landscape evolution

While the telco security landscape transformed significantly over the past year, many of the current topics build on themes established in our earlier reports. As an example, the *systemic cyber resilience challenges* explained in the previous section largely stem from the *nation state attacks on telco infrastructure* that were a focal point in last year's landscape. Recognizing that this challenge demands a cross-sector approach, the topic was broadened to include industries with a similar threat profile that are critical to telco operations. Topics such as *regulatory complexity and misalignment*, the *expanding AI attack surface* and the *complexity of cloud security configurations* emerged from a similar evolution in the ET-ISAC's vision and perspective.

A key addition to this year's landscape is the subject of *digital sovereignty*, which is gaining prominence as global tensions drive demand for cloud and AI infrastructures under European jurisdiction. To keep pace with the rapid evolution of threats and communication technologies, the ISAC members also added *obsolescence of traditional security models* to the radar. Looking beyond the fundamental baselines addressed in landscape topic 03, this item addresses the need to transition towards modernized and future-proof security concepts such as zero trust.

This year's landscape no longer features *scarcity of cyber security talent* and *cloud native infrastructures* as focal themes. As these topics are now well-understood, the ET-ISAC chose to redirect its attention to newer, evolving developments.

Featured: Elisa’s power resilience approach

To enhance its resilience against power outages, Finnish telecom operator Elisa developed a novel battery concept that effectively makes its mobile network double as a virtual power plant. Batteries are a common provision at RAN (Radio Access Network) sites, not least to fulfil regulatory requirements with respect to backup power. Traditionally, such batteries remain idle until there is an actual power outage. Elisa, however, transformed them into a smartly controlled energy resource. To this end, an AI-driven system monitors the electricity market and directs base stations to charge their batteries when energy prices are low and run on self-reliant battery power when the energy production drops or the demand for electricity is high. To enable this, Elisa upgraded its RAN energy storage to lithium-ion batteries that lend themselves well to regular charging and discharging. It also acquired a permit to take part in the energy balancing markt and help stabilize the national electricity grid in case of imbalances, thus creating a new source of income.

Aside from lowering the energy bill and generating new revenue, the advanced battery configuration bolstered Elisa’s resilience against both predictable and unforeseen fluctuations in the electricity grid. Power-related service disruptions were reduced by ~70% while the upgraded battery setup ensured 10-26 hours of service continuity during severe outages, significantly surpassing the mandatory 3-hour backup threshold. Leveraging this proven success, Elisa now also offers the technology as a commercial service to operators and tower companies under the Gridle brand.

Markus Lyyra
Sales Director
at Elisa Industriq

Closing words

As we close this year's edition of the Telco Security Landscape, it is evident that Europe has entered a period marked by rising geopolitical tension and rapid technological change. Much like in our previous reflections, we continue to observe shifts in global dynamics that directly shape the security priorities of European telecommunications providers.

Recent global developments underscore that secure, resilient electronic communication is vital to European stability. In a volatile geopolitical landscape, telecommunications infrastructure has become a primary target for state-sponsored actors. This threat also extends into the critical sectors and cloud-based services upon which telcos depend for their daily operations. Meanwhile, rapid advances in AI and cloud computing offer immense opportunities but also introduce new vulnerabilities. As traditional defences fall behind on this evolving threat landscape, the industry needs to reinforce its security culture and move toward adaptive, modern security models that are capable of withstanding constant change. These developments will affect strategic planning well beyond the current year.

While this overview cannot capture every detail, we hope it offers a practical perspective on issues that deserve the attention of European telcos. Each organisation will have to define its own path forward, but we trust that the insights shared here will help refine priorities for the upcoming year(s). We also value further dialogue with fellow security professionals on the presented topics. If you are interested in such engagement or would like to hear more about the activities that the ET-ISAC is undertaking this year, please reach out to us via isac@etis.org..

The Telco Security Landscape will be reviewed later this year, and we look forward to sharing another updated edition early 2027.

About

ETIS - the Community for Telecom Professionals in Europe, is a partnership-based foundation that drives collaboration and information sharing among European telecommunications providers. Its mission is to provide a trusted collaboration platform that enables parties across the telco ecosystem to reach their strategic objectives and improve their business performance. To this end, ETIS coordinates a great variety of working groups and task forces, all populated with experts and stakeholders from across the European telco industry. These groups include the ETIS Information Security WG (oriented at CISOs and representatives thereof) and the ETIS CERT-SOC Telco Network (focused on intelligence sharing and operational collaboration), that are both also part of the European Telecommunications ISAC (ET-ISAC). ETIS is governed by a total of 35 telecom operators and actively collaborates with bodies such as ENISA, Connect Europe, ITU and GSMA. The ET-ISAC is part of a larger network of vital industry ISACs across Europe. For more information please visit the working group and upcoming events pages on www.etis.org.

TNO - The Netherlands Organisation for Applied Scientific Research, is one of Europe's leading R&D and innovation bodies. Its mission is to strengthen the competitiveness of companies and the welfare of society in a sustainable way. TNO is a non-profit organisation that operates independently and objectively and its many working areas include telecommunications and cybersecurity. TNO is a longstanding partner of ETIS and a core member of the ETIS Information Security WG. Its role includes coordination of the group's annual security landscaping activity, of which this publication is the result. For more information, please visit www.tno.nl/en/.