European Telecommunications ISAC

Telco Security Landscape 2025

Connect Europe 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 7th 2025

Contents

Preface

Last year's Telco Security Landscape was impacted by rising geopolitical tensions. The situation has only worsened, and challenges European countries to an extent few had foreseen. It seems clear that European nations will need to increase defence and security investments.

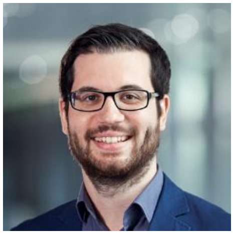
Securing a nation is not merely a diplomatic or military issue, but an all-of-society effort. NATO's Article 3 sets forth seven baseline requirements for resilience and civil preparedness, one of which is "Resilient civil communications systems" – which also underpins the other six. Telecommunications is essential in crisis and conflict – the likelihood of which has increased. This will and must impact European telcos. Still, nation-state attacks are but one of the top ten issues highlighted in this 2025 edition of the ET-ISAC Telco Security Landscape. Many threaten, but some also offer opportunities to improve, the security of European telcos. Issues like cloud native infrastructures, adoption of AI technologies, and security regulations offer both security challenges and opportunities.

The European Telecommunications ISAC (ET-ISAC) forms an arena for security professionals from European telcos to share their security challenges, practices, plans, observations, knowledge, ideas and experience. Our aim is to contribute to an improved security posture for telcos throughout Europe, and thus to the security posture of European nations.

This landscape report is based on the input, deliberations and consensus of the ET-ISAC members. While much of the knowledge sharing within the ET-ISAC is trust-based and confidential, we choose to make this summary public, as food for thought and a call for attention to the highlighted topics among a wider audience.

We would like to thank our colleagues in the ET-ISAC and the ETIS Central Office for their support in preparing this publication and hope you enjoy the read!

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

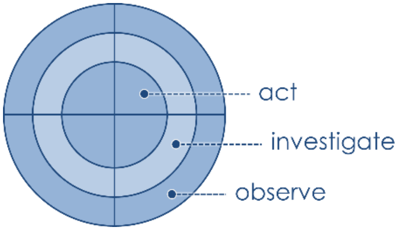
Introduction

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 2025

This year's Telco Security Landscape is comprised of five threats, one distinct opportunity and four developments that (to some extent) exhibit 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 **scarcity of cyber security talent.** There is a structural shortage of a skilled cyber security workforce. Much the same as for companies in other industries, telcos will need to invest in recruitment and optimise conditions to retain staff for a career in cyber security.

02 **deficient execution of security fundamentals.** Telco infrastructures are comprised of heterogeneous technology stacks and need to support a variety of legacy protocols. As a result, it is inherently hard to deploy fundamental security baselines consistently across a telco's technical estate. This raises the likelihood of exploitable vulnerabilities.

03 **cloud native infrastructures.** A telco's internal infrastructure increasingly employs cloud technologies such as Docker and Kubernetes . This requires a fundamental rethinking of security models, architectures and mechanisms, and appropriate attention for emerging issues such as the security of Application Programming Interfaces (APIs). At the same time the agility of cloud technology can also be beneficial to security, e.g. when responding to threats and incidents.

04 **nation state attacks on telco infrastructure.** As a result of the deteriorating geopolitical climate, telco infrastructure is increasingly targeted by state sponsored disruption, espionage and prepositioning campaigns. Recently reported attacks on US communications providers (Salt Typhoon) and undersea cable infrastructure clearly illustrate that telcos need to adjust their resilience strategies to a new reality of threats.

05 **cloud and third party dependency.** While core communications infrastructure is typically maintained on-premise or in private clouds, there is a tendency to move non-primary support systems to public cloud environments. The implication is a reliance on generic certifications and attestations (e.g. an ISO/IEC 27001 or ISO/IEC 27017 certificate) and a

potential susceptibility to geopolitical tensions. In addition, security in telco operations often relies on the capability of vendors to which particular (maintenance) duties have been outsourced. Governing this (and the corresponding access of third party employees to telco owned infrastructure) appropriately can also be challenging.

06 **supply chain integrity concerns.** Hardware and software supply chains come with systemic risks that need structural attention. Initiatives such as GSMA's Network Equipment Security Assurance Scheme (NESAS) address the issue to some extent, but do not cover all associated risks (nor all relevant equipment).

07 **telco adoption of AI technologies.** Artificial Intelligence (AI) will play an even more important role in the maintenance and optimization of future telco infrastructure (among which 6G). Telcos will need to assess how they can protect the underlying algorithms to ensure appropriate reliability. On a more generic level there is also a need to safeguard sensitive data whenever telco employees use public Large Language Models (LLMs). A positive development is that AI may drive fundamental enhancements in cyber defence.

08 **increased security regulation.** Upcoming regulation, both at national and European level, will come with new security obligations and put pressure on CISO teams. Prominent examples include the European Cyber Resilience Act (CRA), the revised Network and Information Security (NIS2) Directive, the Critical Entities Resilience (CER) Directive and the 5G security guidelines under the European Electronic Communications Code (EECC). A potential positive effect is that this offers an incentive to elevate internal security discipline (compliance) and improve the reliability of IT products and services.

09 **quantum computing.** Many cryptographic mechanisms that telcos presently rely on (particularly public key schemes) are vulnerable to cryptanalysis by quantum computers. There is a growing sense of urgency to plan migration towards post-quantum cryptography, not least in view of the well-known "harvest now, decrypt later" threats.

10 **automation and orchestration.** In the monitoring, response and intelligence space, automation may become the game changer that closes (or at least reduces) the present gap between attackers and defenders, not least in terms of speed. The potential of automation also extends to areas such as DevSecOps and third party assurance, and might even contribute to talent retention (topic #01) since it allows security specialists to focus on more fulfilling duties.

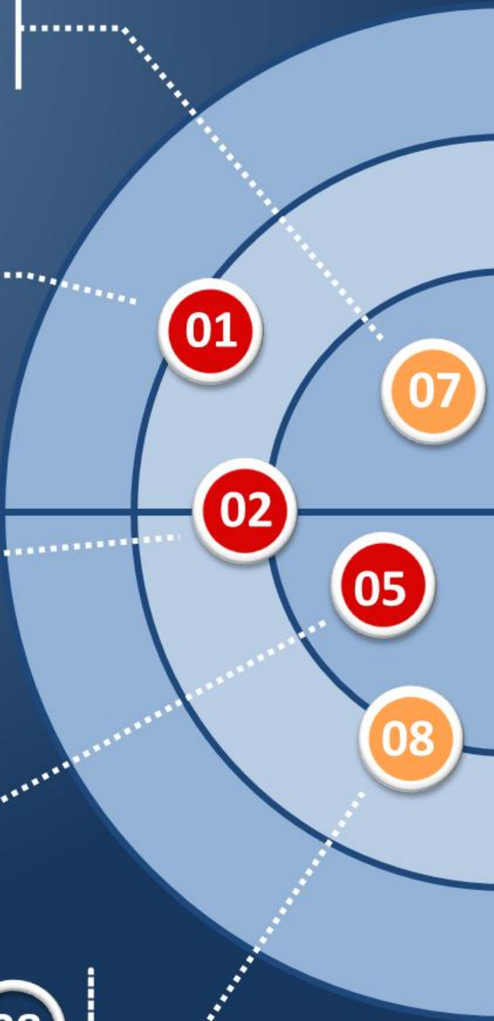
07 telco adoption of AI technologies

01 scarcity of cyber security talent

02 deficient execution of security fundamentals

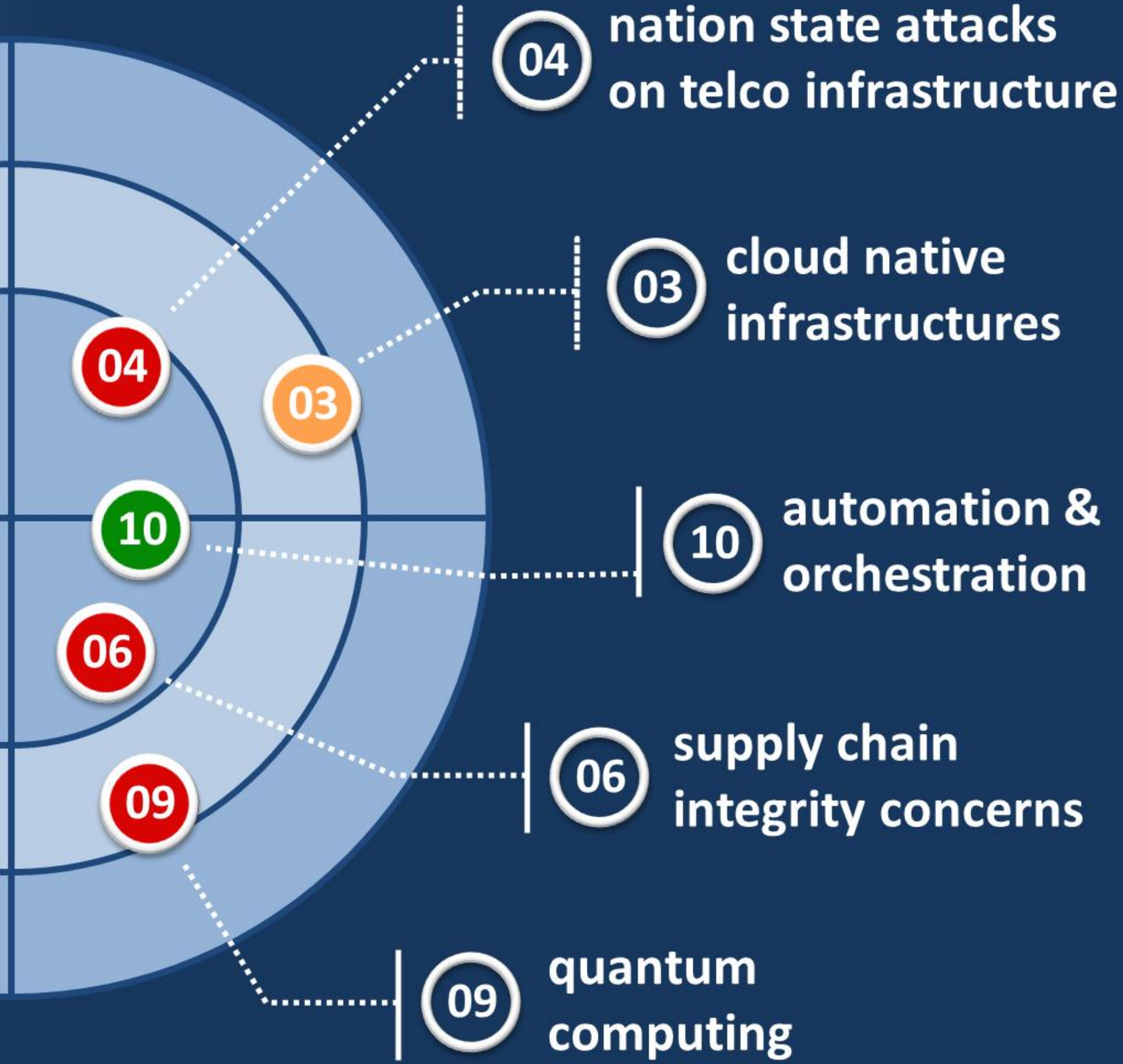
05 cloud and third party dependency

08 increased security regulation



TELCO SECURITY LANDSCAPE 25

etis TNO innovation for life



04 nation state attacks on telco infrastructure

03 cloud native infrastructures

10 automation & orchestration

06 supply chain integrity concerns

09 quantum computing

Featured: KPN's quantum journey

In today's digital age, the security of data transmission is paramount, especially for telecom companies like KPN. Traditional cryptographic methods are increasingly vulnerable to the advancements in quantum computing. Post Quantum Cryptography (PQC) offers a solution by developing cryptographic algorithms that are resistant to quantum attacks. This is crucial for KPN to ensure the confidentiality and integrity of customer data, protect against cyber threats, and maintain trust in their services.

Implementing PQC at KPN involves integrating these new algorithms into the existing infrastructure. This process requires a thorough assessment of current systems and a strategic plan to transition to quantum-resistant algorithms. By adopting PQC, KPN can proactively defend against future quantum threats, ensuring that data remains secure even as quantum computing advances.

KPN is already working on Quantum Key Distribution (QKD) in a lab environment, which could be the next step in quantum resilience in the long term. QKD offers secure exchange of encryption keys based on quantum technology, which is inherently resistant to eavesdropping. This process ensures that any attempt to intercept the keys could be detectable, thus preventing unauthorized access.

Looking to the future, the combined approach of implementing PQC and expanding QKD efforts from the lab to real-world applications will be essential for KPN to navigate the evolving landscape of cybersecurity. As quantum computing continues to advance, the threats to traditional encryption methods will only increase. By proactively adopting these technologies and maintaining the flexibility to adapt, KPN can safeguard its network, protect customer data, and maintain a competitive edge in the telecom industry. Embracing these innovations today will ensure a secure and resilient tomorrow.

Hinko Bastiaanse
Security architect
at KPN

Policy reflections

Connect Europe is glad to collaborate with ETIS and TNO on this edition of the Telco Security Landscape to translate the technical analysis provided by ET-ISAC into actionable policy recommendations that align with Europe's current political and regulatory context. We hope that the integrated landscape can then serve as a key reference point for European decision-makers as they consider the security priorities that need to be addressed through public policy initiatives.

Security and technological sovereignty are now central to Europe's digital policy agenda. Escalating geopolitical tensions and increasingly frequent natural disasters have heightened concerns about the resilience and security of Europe's critical infrastructure. Securing connectivity networks, from the sky to the seabed, has become a political priority.

The deepening interdependence between telecom and other critical sectors like energy, transportation, and government, highlights our industry's vital role in safeguarding customers, as well as the broader economy and society. This means that telecoms must invest significantly and continuously in the security and resilience of their infrastructure and services.

According to the Landscape, operators need to invest in network automation and orchestration, modernise legacy systems, adopt AI and post-quantum cryptography, and attract cybersecurity talent. However, these efforts are hampered by the sector's structural challenges, such as low returns on investment, market fragmentation, heavy regulation, and intense competition from mostly non-European tech giants. Connect Europe's State of Digital Communications 2025 reports a 2% decline in telecom investment in 2023 – the first drop in seven years – signalling a critical turning point. A new policy approach is essential to reverse this trend, promoting sustainable growth, innovation, and investment.

Beyond underinvestment, Europe faces a weak ecosystem in critical connectivity technologies. Telecom networks are increasingly dependent on cloud, AI, and other technologies, most of which are produced outside Europe, while Europe's share of the global ICT market has fallen by 10% in less than a decade. To foster "Made in Europe" innovation, funding mechanisms need strengthening, and public procurement must be better leveraged. A more vibrant telecom ecosystem would support the transition to cloud-native infrastructure, offering a wider choice of trusted solutions while ensuring significant investments on the critical telco infrastructure.

Finally, the EU telecom sector is focused on implementing new regulations like the NIS2 Directive, DORA, the CRA, and national measures from the 5G Security Toolbox. These frameworks address critical issues like supply chain integrity. However, the coexistence of various European risk management and reporting obligations, alongside national requirements, risks undermining legal clarity. Harmonising these regulations across the EU and the broader European region is essential for consistency and legal certainty.

To help our industry meet the challenges outlined in the Landscape, we recommend the following: to policymakers:

- Recognise the sector's crucial role in enhancing resilience across all industries and acknowledge the cost of maintaining secure and resilient telecom infrastructure in the broader debate on the future of connectivity in Europe and the 2030 Digital Decade targets, ensuring these investments are supported through private and public funding.
- Adopt a new regulatory approach for the telecom sector, guided by the upcoming Digital Networks Act (DNA), and a forward-looking competition policy that strengthen the sector's fundamentals and enable scalability to sustain the continuous investment needed to maintain security and resilience amid heightened cyber and physical threats.
- Simplify and harmonise security regulations across markets and streamline reporting obligations to allow operators to allocate resources more effectively to security. This would also enhance cooperation between authorities and operators in fighting large-scale threats.
- Enhance European capabilities by supporting a competitive ecosystem in strategic network technologies, strengthening cooperation against cybercrime, and leveraging funding mechanisms and fiscal incentives to drive public and private investment in cybersecurity and cyber culture.

Paulo Grassia
Senior Director of Policy
and Advocacy at
Connect Europe

Closing words

At the time of publication, we recognise that we have entered a new era of multipolarity. We see a shifting tendency away from liberal democracy towards autocracy in many parts oft he world, and we have seen the start of trade wars from which the global effects have yet to fully materialise. This may very well affect the telecoms industry over the coming year, presenting new issues with significant security impact to be dealt with. Nevertheless, we believe the current edition of the Telco Security Landscape presents a portfolio of issues deserving of the attention of security functions in, and management of, European telcos.

In light of geopolitical tension and a shift in priorities among allies, there seems to be little doubt that continued focus on secure and resilient electronic communication is required in Europe. The collaboration facilitated by the ET-ISAC hopefully contributes to that end. Obviously, the concise overview of strategic developments exhibited through the ET-ISAC's Telco Security Landscape does not capture every nuance or detail. For each topic that was included in the landscape, the most appropriate way forward will often depend on an organisation's particular context and circumstances. Nonetheless we hope this overview will aid both telecoms providers and organisations in other (vital) industries to refine their security priorities for the upcoming year(s). The ET-ISAC would also welcome 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 specific 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 and updated in the fourth quarter of this year and the ET-ISAC will release a new edition early 2026.

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 enable parties across the telco ecosystem to reach their strategic objectives and improve their business performance. To this end, the ETIS Central Office in Brussels 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 jointly also comprise the European Telecommunications ISAC (ET-ISAC). ETIS is entirely governed by a total of 30 telecom operators and actively collaborates with bodies such as ENISA, ETNO, ITU and the GSMA where appropriate. The ET-ISAC is part of a larger network of vital industry ISACs that spreads all 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 cyber security. 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/.

Connect Europe is the voice of the leading providers of connectivity networks and services in Europe. Our members are at the forefront of innovation in the telecom and technology ecosystems, connecting over 270 million Europeans with cutting-edge mobile and fixed networks, such as fibre and 5G. Collectively, they account for more than 70% of total telecom sector investment in Europe. Formerly known as ETNO, we stand for an improved policy and regulatory environment that enables citizens and businesses to benefit from digital connectivity and services. For more information, please visit www.connecteurope.org.