etis TNO

European Telecommunications ISAC

Telco Security Landscape 2024

Publisher	ETIS | The community for telecom professionals www.etis.org
Coordinator	Andrija Višić (ETIS Central Office) av@etis.org
Editor	Richard Kerkdijk (TNO)
Release date	April 29th 2024
Copyright	© 2024 ETIS, all rights reserved

Contents

Preface

Looking back over the past years, there is a stronger realisation than ever before that while the modern digital society is gradually growing ever more dependent on digital communication, the correspondingly ever more critical infrastructure is also in the crosshairs of nations and actors that perceive to be in conflict with "the west", including the liberal democracies of Europe. Meanwhile, telco operators are experiencing unprecedented rates of change to both their business and technology. This comes with new security risks and challenges to be addressed, but also offers opportunities for addressing security and resiliency in new ways and applying emerging technologies to better the efficiency and effectiveness of security measures.

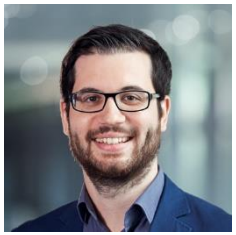
The European Telecommunications ISAC (ET-ISAC) forms an arena for security professionals from European telcos to share their security challenges, practices, plans, observations, knowledge, ideas and experience. Our aim is to contribute to an improved security posture for telcos throughout Europe, and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

After existing as an ETIS-internal deliverable for several years, 2023 marked the first public edition of the ET-ISAC Telco Security Landscape. While much of the knowledge sharing within the ET-ISAC is trust-based and confidential, we chose to make the summary of this landscape public, as food for thought and a call for attention to the highlighted topics among a wider audience. This updated 2024 edition is, as usual, based on the input, deliberations and consensus of the ET-ISAC members.

We would like to thank our colleagues in the ET-ISAC and at the ETIS Central Office in Brussels for their support in preparing this publication. We hope that it will be a useful reference for you, and inspire reflection on your security posture and security program going forward.

Enjoy the read!

Rolv. R. Hauge
Head of security advisory at Telenor and chair of ETIS Information Security Working Group



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

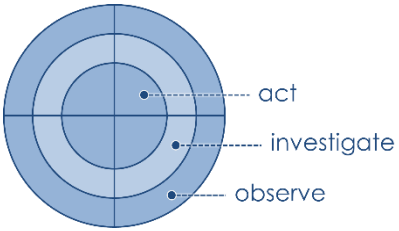
Introduction

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 2024

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 **migration to public cloud.** Driven by cost and efficiency, there is a tendency to move telco systems to public cloud environments. The implication is a reliance on fairly generic certifications and attestations (e.g. an ISO/IEC 27001 or ISO/IEC 27017 certificate) and there is a need to assess more closely under which circumstances this will suffice. Furthermore, the allocation of security relevant responsibilities between telcos and their cloud providers needs to be understood in more detail and appropriately acted upon.

03 **cloud native infrastructures.** Telco internal infrastructures increasingly employ cloud technologies such as Docker and Kubernetes. This requires a fundamental rethinking of traditional security models and architectures, and an appropriate focus on emerging issues such as the security of Application Programming Interfaces (APIs). Many CISO teams will likely need to re-skill to govern and facilitate this appropriately.

04 **geopolitical tension.** Geopolitics can affect the availability of specific equipment and (spare) parts or make the supply of energy less stable, potentially impacting telco service continuity. In addition, some governments may impose restrictions on working with specific vendors or service providers in view of national security concerns.

05 **third party dependency.** Security in core telco operations often relies heavily 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 be challenging and will likely become even more

complex now that telcos are increasingly integrating native software development pipelines with those of their suppliers.

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 important role in the maintenance and optimization of future telco infrastructures (among which 6G). Telcos will need to assess how they can protect the underlying algorithms in order to ensure appropriate reliability. On a more generic level there is a need to safeguard sensitive data whenever telco employees use publicly available Large Language Models (LLMs). A positive development is that AI will 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 new 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" threat. At the same time quantum computing (e.g. QKD) may offer telcos new opportunities for securing their networks and supplying more secure connectivity services.

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.

telco adoption of AI technologies 07

scarcity of cyber security talent 01

migration to public cloud 02

third party dependency 05

increased security regulation 08

TELCO SECURITY LANDSCAPE 24

etis TNO innovation for life

04 geopolitical tension

03 cloud native infrastructures

10 automation & orchestration

06 supply chain integrity concerns

09 quantum computing

Featured: BT's journey in third party security

Third party dependency and **Supply chain integrity concerns** rightly continue to be near-term risks which all telcos need to act upon. In fact, the theme of supply chain security features to a greater or lesser extent in all 10 themes within this year's Telco Security Landscape. The supply chain ecosystems that all telcos operate in will inevitably grow in scale and complexity, to a point where almost any reported security incident, data breach etc. has to be triaged and assessed for potential direct impact.

The risks around supply chain security do not exist in isolation – they reside within a broader landscape of evolving geopolitical tensions, technology developments, and governmental and regulatory interventions. The complexity of these challenges cannot be understated, and requires a response which goes above and beyond traditional supply chain risk management actions.

As providers of critical infrastructure, telcos are now rightly required to operate an enhanced regime to identify and reduce the security risks, including those from their third-party suppliers. In the UK, this enhanced regime is enacted through the Telecommunications (Security) Act 2021, which operators are required by law to comply with.

At BT Group we are transforming and maturing our approach to third party risk management by taking a whole-lifecycle management approach. This will be centralised onto a single platform that will automate our relationship with suppliers, increase visibility, aggregate all risks and issues, and provide actionable data insights, through ingesting automated data feeds that further enrich our capability to assess supply chain security risk. By understanding and effectively managing these risks, we will enable the value of our supply chain to be fully realised and provide assurance to our customers and stakeholders.

Dominic Wood
Security Governance
and Assurance Director
at British Telecom

Closing words

Technological changes, geopolitics and supply chain challenges are underpinning topics to most items highlighted in this year's edition of the Telco Security Landscape. Ever more volatile geopolitics, combined with the exhibited ability and willingness of threat actors of multiple nationalities to not only establish footholds in the critical infrastructures of what they view as geopolitically and ideologically adversarial nations, but also make use of said footholds for conducting disruptive and destructive cyberoperations at varying points of conflict escalation, is a stark reminder of the need for the critical infrastructure operators and industries of Europe to collaborate on security challenges and come together to find effective approaches to ensure security and resilience. The collaboration facilitated by the ET-ISAC hopefully contributes to that end.

Obviously, the concise overview of strategic developments exhibited through the ET-ISAC 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 2025.

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/.

etis TNO