

GSMA Mobile Telecommunications Security Landscape - 2026

Copyright © 2026 GSMA

February 2026

About the GSMA

The GSMA is a global organisation unifying the mobile ecosystem to unlock the full power of connectivity so that people, industry and society thrive.

Led by our members, we represent the interests of over 1,100 operators and businesses in the broader ecosystem. The GSMA also unities the industry at world-leading events, such as MWC (in Barcelona, Kigali, Las Vegas and Shanghai) and the M360 Series.

Unlock the benefits of GSMA membership

As a member of the GSMA, you join a vibrant community of industry leaders and visionaries – helping to shape the future of mobile technology and its transformative impact on societies worldwide.

Our unique position at the heart of the mobile industry means you get exclusive access to our technical experts, data and analysis – as well as unrivalled opportunities for networking, innovation support and skills acceleration.

For more information, please visit: http://www.gsma.com/membership/

Security Classification: Non-confidential

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document is confidential to the Association and is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those permitted under the security classification without the prior written approval of the Association.

Copyright Notice

Copyright © 2026 GSM Association

Disclaimer

The GSM Association ("Association") makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

Antitrust Notice

The information contained herein is in full compliance with the GSM Association's antitrust compliance policy.

Contents

1.	Executive Summary	1
2.	Mobile networks, devices and consumers are under attack	3
2.1	Software Security	5
2.2	Democratisation of Attacks	6
2.3	Successful Pre-Positioning Attacks	7
2.4	Exploiting Weak Cyber Hygiene	8
2.5	Supply Chain Security	9
2.6	The Spectrum: Security, Fraud, Scams	11
3.	Threat Actors	12
4.	Risk Management	15
5.	Coordinated Vulnerability Disclosure	17
6.	Generative and Agentic Artificial Intelligence Security	19
7.	Post Quantum Cryptography	20
8.	Mapping the Global Cybersecurity Regulatory Landscape	22
9.	Final Thoughts	25

1 Executive Summary

This is the GSMA's eighth annual Mobile Telecommunications Security Landscape report. Building on the previous reports[1], it reflects developments during 2025, updated analyses, new and updated content, identifies key trends and provides a look at some of the emerging security topics.

The report highlights first that mobile networks, devices and consumers are experiencing a full spectrum of attacks across the globe. This report analyses these attacks and identifies six key areas for attention:

- Software implementations as a key frontline of attacks
- A democratisation of attacks, whereby there is a lowering of the technical and resource barriers to launch attacks
- Pre-positioning attacks that seek to establish a bridgehead for later attacks
- Exploitation of weak cyber hygiene
- Supply chain attacks
- Scam attacks on mobile consumers

Each of these areas includes a definition, some indicators of compromise and security mitigations to be developed, extended and implemented.

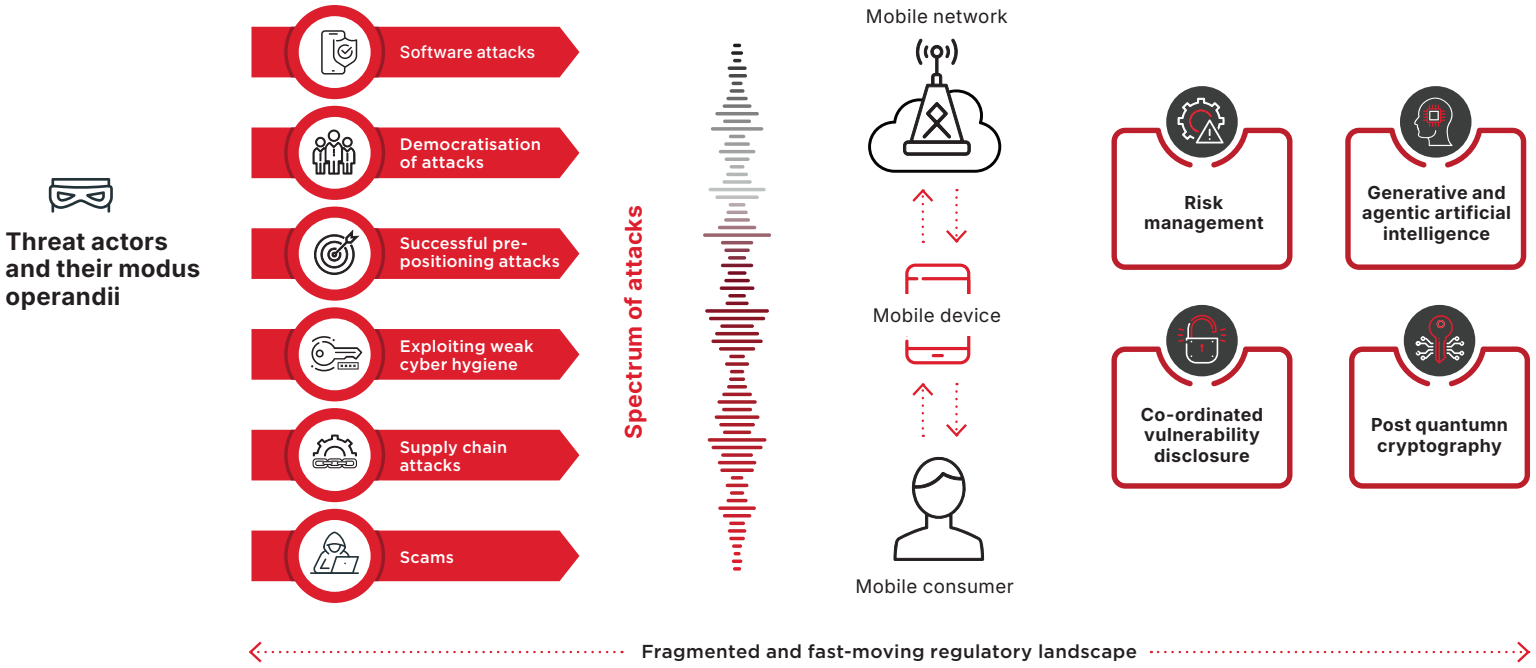


Figure 1, An Overview of topics

[1] https://www.gsma.com/solutions-and-impact/technologies/security/publications/

New for this year, the report includes a threat actor analysis provided from the perspective of the GSMA Telecommunications-Information Sharing and Analysis Center (T-ISAC). Any defensive strategy can benefit from understanding the likely attackers and their attack techniques, hence, the report identifies and discusses four threat actor groups highly relevant to the mobile telecoms industry and provides an analysis of the key attack tactics employed by these threat actors.

The report moves on to consider strategic responses (see also the 2025 report[2] for an in-depth analysis of strategic security responses). A powerful strategic security response to a range of the attack types identified earlier is to utilise risk and threat management to fully design and leverage valuable security investments. The range, velocity and dynamics of the current threat landscape make it challenging to fully address every threat in every dimension and the prioritised impact of security interventions can be maximised through a risk management approach. A second part of the strategic defence approach involves threat and vulnerability sharing (as exemplified by GSMA's T-ISAC service and included in the Threat Actor section). Finally, another GSMA service where the mobile industry continues to strengthen its collective security posture is through structured approaches to vulnerability disclosure via the GSMA Co-ordinated Vulnerability Disclosure scheme.

The report moves on to analyse the emerging security needs associated with generative and agentic artificial intelligence and considerations and migration for post quantum cryptography. In the past few years, effective Generative Artifical Intelligence (AI) technology capabilities and availability have increased significantly enabling a range of new uses for both offensive and defensive purposes with major ramifications for mobile telecoms security. Agentic AI is characterised by autonomy and intent-driven decision-making to leverage workflows that decompose complex goals, iteratively optimise actions, and actively adapt to dynamic environments, positioning itself as the cornerstone of next-generation digital infrastructure.

Post Quantum Cryptography (PQC) is a topic with some uncertainty on timing but with potential for a significant security impact. A Cryptographically Relevant Quantum Computer (CRQC) has the potential to break public key infrastructures which underpin many current security protocols including some key distribution and digital signature regimes. The report illustrates some of the important push and pull factors alongside a set of migration and other practical factors to consider for PQC transition.

The landscape is completed by examining the fast-moving and often fragmented topic of global cybersecurity regulations. To address the evolving threat landscape, national and international policy must adapt. Based on the synthesis of threat intelligence and strategic mapping, a range of recommendations emerge and are described.

Finally, the report identifies ten key security protection priority areas derived from the report content.



[2] https://www.gsma.com/solutions-and-impact/technologies/security/gsma-mobile-telecommunications-security-landscape-2025/

2 Mobile networks, devices and consumers are under attack

The mobile industry has long aimed to develop and deploy robust security measures to protect its assets, customers and services. GSMA continue to see attacks directly on mobile networks, services and devices, including attacks on service delivery, denial of service, the delivery of malware and attacks seeking to exfiltrate data.

In mobile networks, a single breach can disrupt infrastructure, customers, and supply chains. There is a commonality of attack tactics such as credential theft, token abuse, Software-as-a-Service (SaaS) exploitation, and living-off-the-land methods. This highlights the urgent need for tailored operational security, ongoing behavioural monitoring, robust governance and underscores the importance of flexible detection models and sector-specific expertise.

The operational attack surface is wide and complex. Attacks can be launched at many different points externally and from within the network. Mobile Network Operators (MNOs) have been targeted for many years and these attacks continued in 2025[3]. Threat actors use a range of attack techniques to achieve their goals. After an initial phase of reconnaissance[4], the attack may move to establish an initial access bridgehead. This initial access phase may persist for months or years[5], with low levels of activity, occasionally contacting the Command and Control (C2) server, gathering information, exfiltrating low levels of data or waiting for a better time to launch a more destructive or impactful attack. Hence the need for threat hunting[6] activity. The techniques to establish this initial access can utilise simple, well-known attack tools exploiting known vulnerabilities.

To give a sense of scale, UK operator BT reported detecting 2,000 potential attack signals per second across its network, equating to 200 million per day whilst Deutsche Telekom reported 70 million attacks per day[7] on their 'honeypot' systems[8] Virgin Media O2 has blocked 1 billion scam text messages on its mobile network[9]. The attacks go beyond network infrastructure, seeing attacks on mobile devices and directly against our customers. Scam and fraud are escalating at an alarming rate worldwide, $1.4 trillion[10] in global banking fraud losses reported[11]. A massive smishing campaign leveraging a reported[12] 194,000 domains.



[3] https://techcrunch.com/2025/05/08/a-timeline-of-south-korean-telco-giant-skts-data-breach/
[3] https://corporate.orange.be/en/node/57971
[3] https://www.theregister.com/2024/06/21/optus_data_breach_faulty_api/
[3] https://therecord.media/luxembourg-telecom-outage-reported-cyberattack-huawei-tech
[3] https://www.infosecurity-magazine.com/news/bouygues-telecom-breach-customer/
[3] https://www.bleepingcomputer.com/news/security/telefonica-confirms-internal-ticketing-system-breach-after-data-leak/
[3] https://m-en.yna.co.kr/view/AEN20251106006051320
[3] https://techcrunch.com/2025/10/28/lg-uplus-is-latest-south-korean-telco-to-confirm-cybersecurity-incident/
[4] https://www.gsma.com/solutions-and-impact/technologies/security/latest-news/mobile-telecom-security-landscape-blog-october-24/
[5] https://www.reuters.com/business/media-telecom/us-company-with-access-biggest-telecom-firms-uncovers-breach-by-nation-state-2025-10-29/
[6] https://www.gsma.com/solutions-and-impact/technologies/security/latest-news/mobile-telecom-security-landscape-blog-november-24/
[7] https://business.bt.com/content/dam/bt-business/pdfs/insights/cyber-agility/the-cyber-agile-organisation-report-for-uk-market.pdf
[8] https://report.telekom.com/cr-report/2024/governance/cybersecurity-and-data-protection.html
[9] https://news.virginmediao2.co.uk/virgin-media-o2-blocks-1-billion-scam-text-messages-on-its-mobile-network/
[10] https://www.biometricupdate.com/202510/scams-overtake-1-trillion-as-ai-supercharges-global-fraud-networks-biocatch
[11] https://www.gsma.com/solutions-and-impact/technologies/security/scams/gsma_study/airtel-spam-detection-solution/
[12] https://unit42.paloaltonetworks.com/global-smishing-campaign/

GSMA

An analysis of these reported attacks identifies several important areas, that are identified below and expanded upon in later sections:

- The importance of software security
- A democratisation of attack tools
- Successful pre-positioning attacks
- Exploiting weak cyber hygiene
- Supply chain attacks
- A spectrum of attacks: security, fraud and scams

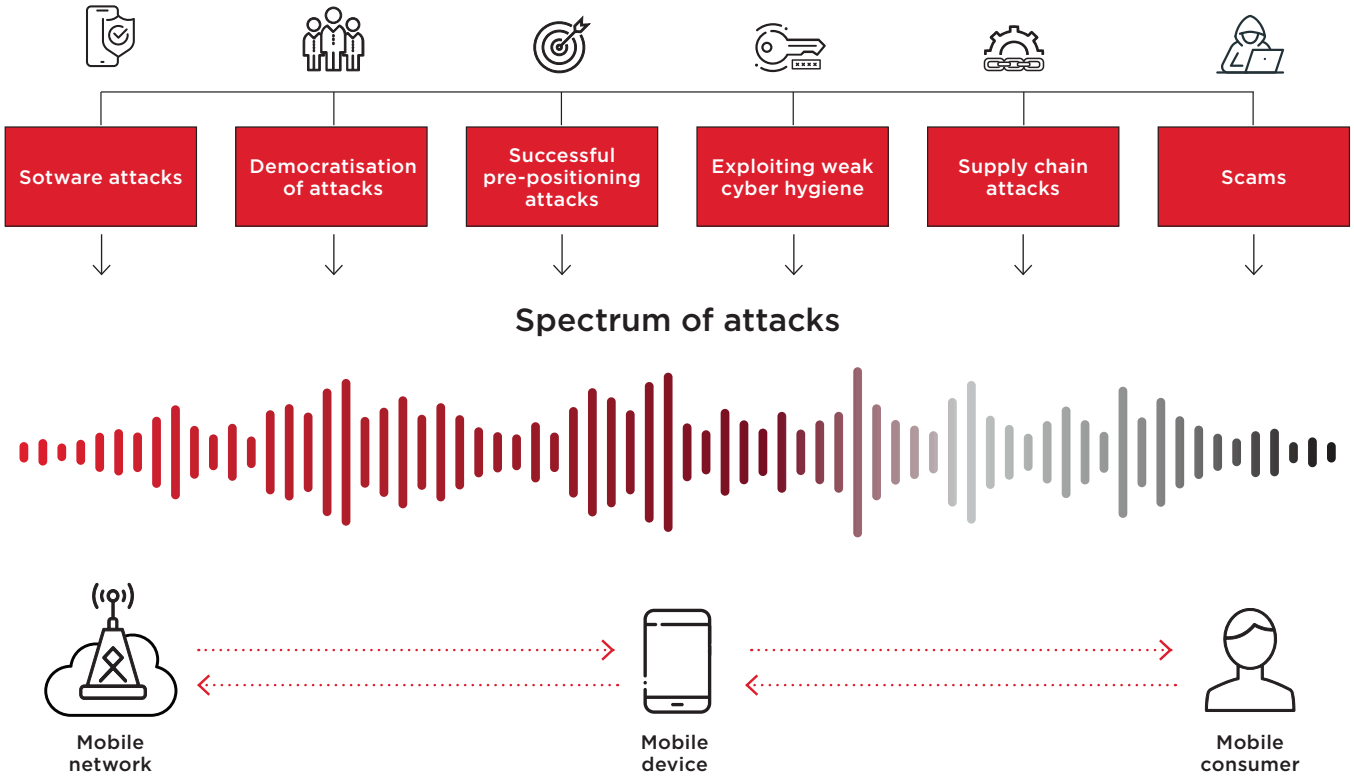


Figure 2, A spectrum of attacks

2.1 Software Attacks



A software attack is a malicious attempt to gain unauthorised access to a computer system or network by exploiting vulnerabilities in code. Deficiencies in coding implementations lead to potential vulnerabilities that attackers may seek to exploit (as demonstrated in the later sections of this report and in this subsection).

A robust software development lifecycle[13] is fundamental to quality code creation and some aspects of this process are susceptible to attack / compromise. Threat actors have been observed abusing legitimate tooling and functions such as software code repositories[14] (including open-source repositories), open-source software attacks[15] and abuse of Application Programming Interfaces (API) (an important set of functionality for telecom networks)[16]. APIs extend the potential attack surface and can provide access to powerful capabilities and data.

There are a number of indicators of software compromise, notably system crashes or degraded performance, audits of code composition and code hashes to verify deployed code, system crashes and API errors / error logs.

Secure-by-design software has been important for many years, and guidance is being refreshed[17] and has identified so-called unforgiveable code vulnerabilities[18]. Secure use of third-party software components is an important area[19] including the protection[20] and tracking of code repositories. A thorough understanding of the composition of deployed code is vital, eg by using a Software Bill of Materials (SBOM) and code equivalence including code signing. Guidance and best practices for API security[21] are also being updated.



SOFTWARE ATTACKS

DEFINITION

- A malicious attempt to gain unauthorised access to a computer system or network by exploiting vulnerabilities in software code

INDICATORS OF COMPROMISE

- Unusual or unauthorised software installations
- API overloads / data leaks
- Unexpected configuration changes
- System crashes or degraded performance
- Unexpected new code libraries or binaries
- Lateral movement activity

MITIGATIONS

- Secure by design code development lifecycle
- Being fully aware of code composition, eg by using an SBOM
- Manage security of code repositories
- Adopt security best practices for API development security
- Use of privileged access workstations and utilising the principle of least privilege.

[13] https://www.gsma.com/solutions-and-impact/technologies/security/supply-chain-toolbox/
[14] https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/ongoing-targeting-of-online-code-repositories
[15] https://unit42.paloaltonetworks.com/npm-supply-chain-attack/
[16] https://www.nccgroup.com/why-api-security-is-now-a-non-negotiable-for-the-telecommunications-sector/
[17] https://www.cisecurity.org/insights/white-papers/secure-by-design
[18] https://www.ncsc.gov.uk/report/a-method-to-assess-forgivable-vs-unforgivable-vulnerabilities
[19] https://safecode.org/wp-content/uploads/2017/05/SAFECode_TPC_Whitepaper.pdf
[20] https://www.ncsc.gov.uk/collection/developers-collection/principles/protect-your-code-repository
[21] https://www.nccgroup.com/why-api-security-is-now-a-non-negotiable-for-the-telecommunications-sector/ & https://www.ncsc.gov.uk/blog-post/new-guidance-on-securing-http-based-apis

2.2 Democratisation of Attacks

Should simple attack tools prove ineffective, threat actors may seek to use more innovative and complex attack techniques. There are a set of barriers to using these more complex capabilities including requiring higher skill levels and experience, higher costs, more resources and can be challenging and expensive to achieve. However, there has been a progressive lowering of skill and resource levels required to launch effective attacks establishing a relatively low-barrier to the use of security attack tools. A range of approaches have been evidenced:

- SMS Blasters[22] - An SMS text blast sends a message to a large group of people simultaneously. However, relatively low-cost, portable and easy-to-use fake mobile base transceiver stations (SMS blasters) can be used for fraudulent use[23] to send a localised smishing 'blast' that can bypass SMS firewall tools. SMS blasters are being increasingly evidenced across the globe[24]
- Ransomware / phishing / cybercrime / malware as-a-service – where as-a-service providers offer attack tools in a commodity fashion, e.g. simplifying the technical aspects of a ransomware attack[25]
- An evolution of smishing[26] including utilising a decentralised Phishing-as-a-Service (PhaaS) model, rapidly rotating domains to attempt to evade detection. This can take differing forms including 'fast flux'[27] and domain generation algorithms[28]
- Botnets-for-hire - access to large networks of compromised computers to launch large-scale attacks like Distributed Denial-of-Service (DDoS) attacks for a fee
- Dark web marketplaces - that operate like legitimate e-commerce sites, offer a wide array of hacking tools, exploit kits, and stolen credentials
- Initial access brokers - threat actors (TAs) who seek to procure access to your network and sell them to other TAs[29]
- Artificial Intelligence (AI)-enabled attack efficiency gains - AI can automate various stages of an attack, such as reconnaissance, vulnerability scanning, and data analysis, which previously required significant human expertise
- AI-generated phishing and social engineering - generative AI can produce convincing and personalised phishing emails, text messages, and social media posts

Mitigation approaches can aim to just make it harder for the attacker by implementing more security best practice capabilities such as those contained in GSMA FS.31 Baseline Controls[30], guidelines in the GSMA Mobile Cybersecurity Knowledge Base[31], implementing threat hunting and a top 20 strategic security approaches[32].

DEMOCRATISATION OF ATTACKS

DEFINITION

- The widespread and relatively low-barrier use of security attack tools

INDICATORS OF COMPROMISE

- Increased use of common security tools
- Rise in attacks using off-the-shelf malware
- More breaches by less sophisticated actors
- Increasing bypass of SMS firewalls
- Customers clicking on known scam links

MITIGATIONS

- Patching
- GSMA FS.31 Baseline controls and
- MCKB
- Threat hunting,
- SMS Blaster guidance FS.67
- A 'top 20' strategic security approaches including know your attack surface, defensive force multipliers, layered defences, supply chain security, resilience-by-design, risk management, use of privileged access workstations and utilising the principle of least privilege.

[22] https://www.gsma.com/newsroom/press-release/gsma-asia-pacific-mobile-industry-taskforce-calls-for-government-and-law-enforcement-support-to-stamp-out-sms-blaster-device-threat/
[23] https://commsrisk.com/criminal-gangs-drive-imsi-catcher-sms-blasters-around-vietnam/
[24] https://news.risky.biz/risky-bulletin-sms-blasting-incidents-are-rising/
[25] https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/
[26] https://www.securityweek.com/massive-china-linked-smishing-campaign-leveraged-194000-domains/
[27] https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-093a
[28] https://www.akamai.com/glossary/what-are-dgas
[29] https://www.cisecurity.org/insights/blog/initial-access-brokers-how-theyre-changing-cybercrime
[30] https://www.gsma.com/solutions-and-impact/technologies/security/gsma_resources/fs-31-gsma-baseline-security-controls/
[31] https://www.gsma.com/solutions-and-impact/technologies/security/cybersecurity-knowledge-base/
[32] https://www.gsma.com/solutions-and-impact/technologies/security/latest-news/mobile-telecom-security-landscape-blog-july-25/

2.3 Successful Pre-Positioning Attacks

Reactive security defences play a huge role in delivering safe and resilient networks. However, the reported attacks include those with a successful launch and utilisation of pre-positioning attacks where an adversary compromises systems now and persists to prepare for a later escalation or undertake ongoing low-level data exfiltration and 'beaconing' to C2 servers[33]. These 'quiet' attacks may have been missed by defence capabilities or may have existed prior to defence upgrades. While reactive security defences can deliver safe and resilient networks, they occasionally miss successful attacks that seek to pre-position a persistent 'bridgehead' from which to assert cyber-attacks in a variety of forms. Ongoing threat actor actions can utilise *'living off the land'* [34] techniques to attempt to evade detection. Other IoCs include unusual traffic flows and / or account usage, unexpected changes in software and unusual account usage / time of usage (eg outside of normal office hours).

Proactive threat hunting[35] plays a role in uncovering these long-term attacks. Threat hunting activity searches for signs of an attacker's lateral movement through the network, identifies unauthorised privilege escalation, access rights abuse, and other threats.

Some regulations are pushing operators to establish the principle of 'assumed compromise' whereby operators should normally assume network oversight functions to be subject to high-end attacks, which may not have been detected, and implement business practices that make it harder for an attacker to maintain covert access. Mitigation activities include:

- Threat hunting
- Implement trusted boot capabilities and secure roots of trust with periodic rebooting of systems
- The GSMA Telecommunication Information Sharing and Analysis Center[37] (T-ISAC) is the central hub of information threat sharing for the Telecommunication Industry. Information threat sharing is essential for the protection of the mobile ecosystem
- Proactive penetration testing can be an additional tool with which to identify potential initial attack vectors and existing weaknesses

PRE-POSITIONING ATTACKS

DEFINITION

- An adversary compromises systems now and persists there to prepare for a later escalation or low-level data exfiltration and 'beaconing'

INDICATORS OF COMPROMISE

- Unusual traffic flows and account usage
- Unusual persistent accounts or tasks
- Unexplained network traffic such as low-level outgoing beaconing, sometimes over a protracted period
- Unexplained changes in software

MITIGATIONS

- Threat hunting
- Secure roots of trust with periodic rebooting of systems
- Threat intel sharing
- Proactive penetration testing

[33] https://media.defense.gov/2025/Apr/02/2003681172/-1/-1/0/CSA-FAST-FLUX.PDF
[34] https://securityboulevard.com/2025/05/living-off-the-land-lotl-attacks-how-your-tools-are-used-against-you
[35] https://www.gsma.com/solutions-and-impact/technologies/security/latest-news/mobile-telecom-security-landscape-blog-november-24/
[36] https://api.gcforum.org/api/files/public/upload/aa4aad66-74f7-4490-a4e6-f6d3f1e327bf_Enhancing-Protection.pdf
[37] https://www.gsma.com/solutions-and-impact/technologies/security/t-isac/

2.4 Exploiting Weak Cyber Hygiene



Threat actors will use a range of attack tools, often starting by using the most basic and readily available toolsets that seek to exploit well-known vulnerabilities[38] and these have been shown to be effective in recent successful attacks. When these attack techniques fail, the adversary is forced to utilise more resources, expertise and effort to launch more sophisticated attacks. The role of the defender is to make attacks progressively harder to launch and achieve success. This defensive strategy begins with effective baseline security controls[39].

Indicators of compromise relating to poor cyber hygiene include unusual account activity, unexpected new account accesses, unauthorised software packages and configuration changes, suspicious network traffic including data exfiltration (including low-level flows) and data flows of unencrypted data.

Recent attacks illustrate some areas where cyber hygiene can be improved in areas such as:

- Improving user and administrator account security including enabling a multi-factor authentication (MFA) arrangement and password storage mechanisms
- Patching systems more frequently or adding additional mitigating controls to combat known vulnerabilities
- Monitoring and analysis of logging data and data flows to spot suspicious traffic flows and ongoing/previous attacks
- Improving network and system segmentation to make it harder for attackers to move laterally, re-use credentials and limit the impact of the attack
- Encrypt stored encryption keys and sensitive data
- Undertake a complete asset inventory to understand the full attack surface[40]
- Understand the details of the supply chain (including third-party remote system access arrangements). See also, the later Supply Chain section in this report
- Implement a strong baseline set of controls[41]
- build in multilayer defences for strength and depth[42]



CYBER HYGIENE

DEFINITION

- A practice of taking steps to protect devices, networks, and data from cyber threats

INDICATORS OF COMPROMISE

- Unusual account activity
- Unauthorised software
- Unexpected configuration changes
- Suspicious network traffic

MITIGATIONS

- Patching or adding additional security controls
- Improving user and administrator account security
- Monitoring and analysis of logging data and data flows
- Improving network and system segmentation
- Encrypting key data
- GSMA FS.31 Baseline controls and GSMA MCKB
- GSMA Supply Chain Toolkit
- Multilayer defences

[38] https://www.cve.org/
[39,40] https://www.gsma.com/solutions-and-impact/technologies/security/gsma_resources/fs-31-gsma-baseline-security-controls/
[41] https://www.gsma.com/solutions-and-impact/technologies/security/gsma_resources/fs-31-gsma-baseline-security-controls/
[42] https://www.rg-cs.co.uk/security-stop-press-cyber-criminals-exploit-trusted-platforms-in-lots-attacks/

2.5 Supply Chain Attacks

Supply chain attacks continue at pace[43]. The opportunity for indirect attacks through supplier or third-party tooling and services should not be underestimated and requires vigilance about which third-party tools are in use, as well as awareness of the security posture of the various third parties. Perhaps a less obvious supply chain attack is *'Living Off Trusted Sites'* [44](LOTS). Where threat actors extend their stealth techniques into the cloud, using trusted sites and legitimate services to avoid detection and disguising C2 as ordinary traffic or innocuous messages on platforms as such Slack and Telegram. Other indicators of compromise can include abnormal login times (especially on administrator accounts), unusual privilege escalation (including on Active Directory), unexplained software and firmware updates and increases in database read volumes that might indicate exfiltration attempts.

There are a range of mitigating approaches including utilising the GSMA's updated and re-issued GSMA Supply Chain Toolbox[45] that uses a lifecycle model to describe a number of guidelines ('tools' in the 'toolbox').

The concept of 'know your traffic' is a powerful one whereby monitoring and understanding all network traffic is undertaken to identify, mitigate, and prevent security threats and fraud.

Supply chain interventions throughout the lifecycle can:

- Inform of the strength of development processes
- Understand the adequacy of in-built security controls and assurances
- Be clear on the security of in-life security maintenance arrangements
- Improve the speed of response to mitigate new security vulnerabilities
- Ensure de-commissioning is undertaken in a controlled and secure manner
- Understand the depth[46] of supply chains

As part of supply chain assurance, GSMA Network Equipment Security Assessment Scheme (NESAS)[47] exists to facilitate improvements in network equipment security levels, across the mobile industry by providing an underpinning security assurance. The purpose of the scheme is to audit and test network equipment vendors, and their products, against a security baseline, so they can demonstrate to network operators (or regulators) that they are conforming to the desired standard. The scheme has been defined by industry experts through GSMA, 3GPP, ETSI and wider entities. GSMA NESAS only plays one part of the security strategy. NESAS only tests products and processes at a point in time. It is important to guarantee that the actual deployed code is the same code that was tested through NESAS (so called binary equivalence) and that secure configurations are used. Additional layers of security are required to deliver a robust deployment for in-service use.

To perform their contracted activities, a managed service provider (MSP) must administer their systems and services and without proper controls, this high level of privileged access, can leave a system vulnerable to attack.

SUPPLY CHAIN ATTACKS

DEFINITION

- A type of cyber or operational attack where an attacker compromises telecommunications systems or services by exploiting weaknesses in the suppliers, vendors, or partners involved in building, maintaining, or operating telecom networks

INDICATORS OF COMPROMISE

- Disguised C2 traffic
- Abnormal Routing Protocol Changes
- Spikes in DNS Query Volume
- Privilege Escalation in Active Directory
- Abnormal Login Times
- Unplanned software/ firmware updates
- Unauthorised Management Software
- Unexplained increases in database read volumes

MITIGATIONS

- Adopt a lifecycle approach to improve the whole chain of supply and operation
- Know your traffic- logging and monitoring of all traffic types
- Use industry security assurance schemes to provide a security underpinning
- Fully understand the depth of the supply chain and the security processes of each vendor
- Actively manage code deployments and update to ensure correct code versioning and binary equivalence
- Strictly control remote access arrangements

[43] https://unit42.paloaltonetworks.com/npm-supply-chain-attack/
[44] https://www.rg-cs.co.uk/security-stop-press-cyber-criminals-exploit-trusted-platforms-in-lots-attacks/
[45] https://www.gsma.com/solutions-and-impact/technologies/security/supply-chain-toolbox/
[46] https://datatracker.ietf.org/doc/draft-ietf-scitt-architecture/
[47] https://www.gsma.com/solutions-and-impact/industry-services/assurance-services/network-equipment-security-assurance-scheme-nesas/

It is important to identify which systems each MSP can access and what the secure access mechanisms are. These accesses should only allow activities that are within the contracted scope of service provider activity. Segmentation (to limit the scope for lateral movement), least privilege (to decrease the impact a malicious access account may have), use of secure 'jump' boxes, use of dedicated work stations, privileged access management, multi-factor authentication, attributable accounts and' just in time' principles and limited duration access for privileged accounts can all be effective controls. The secure separation of privileged access workstations[47] used by systems administrators is a key area of supply chain security.

As architectures continue to move towards disaggregated components, leverage cloud and virtualisation architectures as well as increase in third party tools for monitoring, management and security, it is clear that the available supply chain 'surface area' for an attacker to exploit is becoming broader. Active and in-depth knowledge of direct, indirect and open-source supply routes are all needed. The force multiplier effect for an attacker of a single successful attack providing access across all the target supplier's customers makes using a compromised vendor an attractive proposition[48]. The potential attack force-multiplier enabled through a supply chain attack means building skills, processes, tools and experience will present an enduring benefit – supply chain security will remain a key security area.

As architectures continue to move towards disaggregated components, leverage cloud and virtualisation architectures as well as increase in third party tools for monitoring, management and security, it is clear that the available supply chain 'surface area' for an attacker to exploit is becoming broader.



[47] https://www.gsma.com/solutions-and-impact/technologies/security/latest-news/mobile-telecom-security-landscape-blog-june-25/
[48] https://tuxcare.com/blog/xz-compromise/

2.6 The Spectrum: Security, Fraud, Scams

Scams fall into a spectrum of differing attack types, including those focussed on attacking network infrastructure and services, those seeking to defraud operators by abusing services and accounts, and those seeking to scam mobile users directly. The scam economy has grown rapidly over the last five years, surpassing the illegal drug trade and costing victims $1 trillion worldwide[49].

Users of mobile technologies are targeted by a variety of actors – whether it be low-level fraud via phishing, smishing, or through social engineering against them, or call centres. Scams and fraud can take many forms, and some of these exploit mobile devices themselves and their supporting service as an attack channel. These include attacks such as service fraud (e.g. identity fraud or mobile money fraud), mobile spam and, increasingly scams or "social engineering" fraud, which trick victims into revealing sensitive information about themselves and the services they consume, without realising they have compromised their own security. GSMA are working closely to test innovative concepts, including Open Verified Calling, and implement new solutions, like the Scam Signal API[50], that directly target scams.

The importance of mobile operators taking scam prevention seriously is clear. For example, Bharti Airtel's network-based AI-powered Spam detection solution[51] has resulted in a reduction in financial losses for its customers of nearly 70% - a 14.3% drop in overall cybercrime incidents on the Airtel network (also rolled rolled out to Nigeria, Uganda,Tanzani and Rwanda). TPG Telecom[52] partnered with Apate.ai to pilot a proactive, intelligence-driven defence against scam calls. The program was designed not just to block malicious calls, but to divert them into a secure environment where valuable threat data could be gathered and used to strengthen protection. The collaboration delivered its goal resulting in 280,000+ scam calls successfully diverted from the TPG Telecom network and $7.6 million+ in estimated scam losses prevented. Anti-scam measures are increasingly being provided on-device[53] as well as within the network. The range of new operating system capabilities is extensive, including the ability to disable 2G connectivity (a route for smishing attacks).

The mobile industry is taking comprehensive steps to combat the rising number of scams that affect individuals and society, and to improve trust in global mobile networking. Additional information can also be found in the GSMA scams content hub[54] that shares a wide range of scam prevention resources to provide the industry guidance, intelligence and education tools and the document *Fraud and Scams: Staying Safe in the Mobile World*[55]. Only by uniting and working together can the global mobile industry and the wider ecosystem collectively tackle this issue to safeguard consumers and ensure a secure future for all.



*Sources: 1 – link; 2 – link; 3 – link; 4 – link; 5 – link; 6 – Global State of Scams 2025 Report, Global Anti Scam Alliance; 7 – UK Home Office; 8 – link; 9 – link; 10– link; 11 – link

[49] https://www.biometricupdate.com/202510/scams-overtake-1-trillion-as-ai-supercharges-global-fraud-networks-biocatch
[50] https://www.gsma.com/solutions-and-impact/gsma-open-gateway/gsma_study/vodafone-implements-scam-signal-api-to-combat-fraud/
[51] https://www.gsma.com/solutions-and-impact/technologies/security/scams/gsma_study/airtel-spam-detection-solution/
[52] https://www.gsma.com/solutions-and-impact/technologies/security/scams/gsma_study/apate-ai-powered-scam-detection-diversion-and-real-time-threat-intelligence/
[53] https://safety.google/intl/en-GB_ALL/safety/scams-fraud/
[53] https://www.huaweicentral.com/android-16-will-modify-call-settings-to-safeguard-you-from-scammers/,
[53] https://www.samsung.com/us/support/answer/ANS10003438/ & https://support.apple.com/en-gb/guide/iphone/iphe4b3f7823/ios
[54] https://www.gsma.com/solutions-and-impact/technologies/security/scams/
[55] https://www.gsma.com/solutions-and-impact/connectivity-for-good/public-policy/gsma_resources/fraud-and-scams-staying-safe-in-a-digital-world/

3 Threat Actors

In today's digital landscape, organisations and individuals encounter ongoing risks from threat actors. Gaining a comprehensive understanding of these actors, the specific threats they present, and identifying which threat actors are most relevant to the mobile industry is crucial for enhancing cybersecurity defences. GSMA's Telecommunications Information Sharing and Analysis Center has been tracking a range of threat actors, and some are described below, along with an analysis of their attack techniques.

What is a Threat Actor?

Any person, group, or entity[56] that intentionally uses computers, networks, or systems to cause harm to others. This is often achieved by exploiting vulnerabilities to steal data, disrupt services, or achieve financial, political, or ideological goals. These actors are also known as malicious actors or bad actors and can range from individual cybercriminals and hacktivists to state-sponsored organizations and even insiders within an organisation. It is crucial for the telecommunications industry to be aware of the threat actors referenced in this report. They exemplify the most advanced, persistent, and impactful cyber threats targeting telecommunications globally, each with distinct motives and tactics that have dramatically shaped the threat landscape in recent years.

Salt Typhoon

Salt Typhoon AKA UNC2286 has been active from at least 2019, the group has conducted extensive cyber-espionage campaigns, particularly targeting telecommunications infrastructure, energy networks and government systems worldwide. The analysis from a CISA report[57] on Salt Typhoon confirms the group exploits known vulnerabilities in backbone, customer edge and provider-edge routers to gain access, create privileged accounts, and maintain persistent network access, allowing interception of communications and manipulation of network configurations. All this is achieved by leveraging zero-day exploits, lateral movement and living on the land[58] to stay undetected for extended periods of time[59].

While much of the public reporting has focused on U.S. targets, Salt Typhoon's operations have extended into Canada, Europe, the Middle East, and Africa (EMEA) where it has targeted telecoms, government entities, and technology firms[60].

LightBasin

The threat actor LightBasin, also known as UNC1945 + UNC281 is a cyber espionage group. They focus on targeting telecommunications, finance, retail and hospitality and health care industries. Their primary focus is targeting Linux and Solaris based systems using various tactics by leveraging their in-depth knowledge of the telco network architecture.

The adversary implements operations security (OPSEC) measures to hide these connections from investigators by tampering with legitimate binaries on target systems. Once they gain access to a network, they establish multiple redundant remote access mechanisms using a combination of custom backdoors and publicly available proxy tools configured to relay traffic to adversary-controlled remote infrastructure[61]. Since 2016[62], they have contributed to malware that has affected 13 different telecommunication businesses across the globe[63].

[56] https://www.cisa.gov/sites/default/files/2025-09/CSA_COUNTERING_CHINA_STATE_ACTORS_COMPROMISE_OF_NETWORKS.pdf
[57] https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-239a
[58] https://blog.talosintelligence.com/salt-typhoon-analysis/
[59] https://docbox.etsi.org/Workshop/2025/10_SECURITY_CONFERENCE/9OCTOBER/GEOPOLITICS/BLUEHOUR_Holtmanns.pdf
[60] https://www.darktrace.com/blog/salty-much-darktraces-view-on-a-recent-salt-typhoon-intrusion
[61] https://www.crowdstrike.com/en-us/blog/an-analysis-of-lightbasin-telecommunications-attacks/
[62] https://www.techtarget.com/searchsecurity/news/252508413/LightBasin-hackers-spent-5-years-hiding-on-telco-networks
[63] https://www.bleepingcomputer.com/news/security/lightbasin-hacking-group-breaches-13-global-telecoms-in-two-years/

Scattered Spider

Scattered Spider, (also known as UNC3944 & Octo Tempest) is a financially motivated cybercriminal group. Unlike many other threat groups, Scattered Spider is believed to be composed of relatively young, English-speaking members based in Western countries. They engage in data extortion by leveraging personal information gathered through open-source intelligence (OSINT) or prior breaches. The adversary uses multiple social engineering techniques SIM Swap attacks to obtain to obtain credentials, install remote access tools, and/or bypass MFA. Scattered Spider use social engineering to convince support staff to reset passwords or enrol new MFA devices, effectively bypassing security controls. Additionally, they have used SIM swapping to hijack victims' phone numbers and intercept MFA codes. They have also employed MFA fatigue attacks, repeatedly sending push notifications to users in they hope that they'll eventually approve the request out of frustration or confusion. Scattered Spider has targeted the Retail, Hospitality, Banking Sector and Telecommunications Industries.

ShinyHunters

ShinyHunters, is another financially motivated group that are linked to the threat actor cluster UNC6040 by Google.[64] The name is inspired by the Pokémon community term for rare "shiny" creatures, reflecting the group's pursuit of high-value data.[65] This group specialises in data theft, extortion, and the leaking of sensitive information. In their most recent attacks, they gained access through credential theft, phishing, or exploiting misconfigured cloud services like exposed S3 buckets or unsecured GitHub repositories. Since they are English speaking individuals, they have successfully adopted vishing (voice phishing) as a social engineering technique. ShinyHunters also impersonate IT Support/help desk and trick employees into authorising malicious connected apps in platforms like Salesforce, giving them direct access to customer data via APIs.

Since they are English speaking individuals, they have successfully adopted vishing (voice phishing) as a social engineering technique.



[64] https://cloud.google.com/blog/topics/threat-intelligence/unc6040-proactive-hardening-recommendations
[65] https://cloud.google.com/blog/topics/threat-intelligence/voice-phishing-data-extortion

Modus Operandi of the Threat Actors

Salt Typhoon, Scattered Spider, ShinyHunters, and LightBasin are prominent modern cyber adversaries with overlapping advanced TTP's (tactics, techniques and procedures).

- Abuse of valid accounts and the identity plane across enterprise, telecom, and cloud/SaaS environments, preferring logins with stolen or purchased credentials over exploit heavy intrusion paths.
- Bypassing strong authentication through MFA gaps and session/token reuse, including opportunistic social engineering where feasible to regain access quickly.
- Living off the land with native admin tools and builtin platform functionality (PowerShell, WMI, RMM, SQL queries/exports) to blend with normal IT operations and reduce malware footprints.
- Systematic discovery to map networks, services, and cloud metadata, identifying high value datasets and accessible routes before deeper actions.
- Largescale data theft using native export mechanisms and web services, especially from cloud data warehouses and SaaS platforms where controls are weaker or misconfigured.
- Operational security with commercial VPNs, proxies, and commodity cloud/Virtual Private Server (VPS) infrastructure to obscure operator location and infrastructure lineage throughout campaigns.
- Persistence primarily via valid accounts, longlived sessions, and legitimate services or scheduled tasks rather than heavy custom implants.

Figure 3: Shows the tactics used by the Threat Actor using the MITRE ATT&CK® adversary tactics framework[66].

Mobile operators can prioritise strong identity controls, have clear asset visibility, well-rehearsed incident responses, ensure multi-factor authentication is enforced for all privileged and remote accesses, that passwords are never stored in plaintext, and privileged accounts are audited regularly. Network segmentation and continuous monitoring of logs can be used to detect lateral movement early and ensure there are clear processes for change management and supplier oversight. GSMA's T-ISAC community enables the mobile industry to share new IoCs in near real-time. This intelligence sharing can also include details of detection methods and feedback on effective defensive controls. In this way, many operators can share from the learning of a few operators or even a single operator. This defensive force-multiplier can be delivered by promptly sharing knowledge and information that can benefit the wider range of stakeholders.

	Threat Actors			
	LightBasin	Salt Typhoon	Scattered Spider	ShinyHunters/ UNC5537
Impact			✓	
Exfiltration	✓	✓	✓	✓
Command & Control	✓	✓	✓	
Lateral Movement	✓	✓	✓	
Discovery	✓	✓	✓	✓
Credential Access		✓	✓	
Defense Evasion	✓	✓	✓	✓
Privilege Escalation		✓	✓	
Persistence	✓	✓	✓	✓
Execution		✓	✓	
Initial Access	✓	✓	✓	✓

Figure 3, Tactics used by the Threat Actors

[66] https://attack.mitre.org/tactics/enterprise/

4 Risk Management

A powerful strategic security response to a range of the attack types identified earlier is to utilise risk and threat management to fully design and leverage security investments. The range, velocity and dynamics of the current threat landscape make it challenging to fully address every threat in every dimension and the prioritised impact of security interventions can be maximised through a risk management approach.

Threat and risk assessment allows identification of the most likely and impactful risks considering the technical security threats to which the business may be exposed given its architectural design, legacy network estate, supplier selection, enabling technologies, operation and support arrangements, and software builds, etc. By focusing on the areas of threat/risk, a business can examine the gross risk likelihood and impact. Then, considering the effect of existing controls and mitigations, a net risk position can be determined. A review of this net risk position can assess whether the risk profile is within the company risk tolerance or whether additional controls and mitigation activity is required to further reduce the net risk position.

Threat intelligence-informed modelling focuses specifically on security threats (that might compromise confidentiality, integrity and / or availability (CIA)) to a system or application. Threat modelling aims to identify and mitigate security vulnerabilities.

There are many different risk and threat modelling approaches used within a telco environment including:

- Attack Trees[67]
- GSMA risk identification reports such as GSMA documents GSMA PQTN PQ.02 - Guidelines for Quantum Risk Management for Telco[68] and member-only documents such as FS.30 Security Manual & FS.39 5G Fraud Risks
- NIST Artificial Intelligence Risk Management Framework (AI RMF 1.0)[69]
- NIST Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations[70]

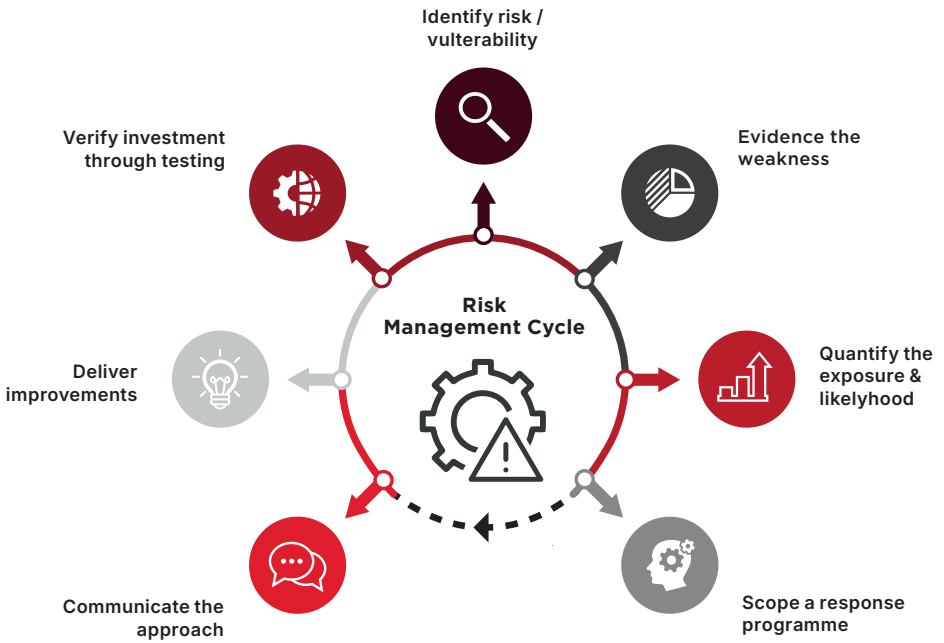


[67] https://2t-security.com/why-should-i-use-attack-trees/
[68] https://www.gsma.com/get-involved/working-groups/wp-content/uploads/2023/09/Guidelines-for-Quantum-Risk-Management-for-Telco-v1.0.pdf
[69] https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf
[70] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1-upd1.pdf

UK's NCSC has published a report[71] examining the systematic analysis of a telecoms network from an attack tree perspective. The idea being to identify possible attack approaches from an attacker perspective and then break these down into different categories of attack type which can then be considered against the effects of existing controls. The approach began by drawing upon existing threat and attack data, global attacks on telecoms systems, practical industry security practitioner input and international security standards. From this data, a series of attacks was pulled together into 'attack trees'. Each attack tree was considered for their relative risk of success and likelihood. From this analysis, the most important risks can be listed. Security controls and mitigations can then be considered in order that the net risk position is at an acceptable level for the business.

A related topic explored in the 2025 mobile security landscape report[72] is resilience-by-design. This plays to the categories of risk that have high impact, but potentially are less likely; so called 'black swan' events. This philosophy requires changing some design and planning assumptions and then developing and deploying networks in accordance with these revised assumptions. With far-sighted design assumptions, network and service designs and implementations can enable better preparation and delivery response to possible step changes in the threat landscape.

Undertaking a comprehensive threat and risk assessment can improve security through focusing on the most impactful risk areas, maximising returns on security investments, identifying duplicate controls and identifying new risk areas. Consider developing in-depth expertise, tools and expertise in a risk / threat framework that works for your environment. The aim is to apply knowledge from risk insights to provide impactful multi-layered defensive technologies. The GSMA Mobile Cybersecurity Knowledge Base[73] (MCKB) has been updated to add links to additional security guidance and now features a section dedicated to risk management.



Some risk treatment options are:

- Accept the net risk position
- Sharing the risk through a new delivery arrangement
- Avoid the risk, e.g. by closing a platform, system or access
- Transfer the risk to another party, perhaps through a revised supply arrangement
- Risk education through implementing additional security controls/architectural re-design to limit the impact and/or reduce the likelihood of a successful attack

Figure 4, A Risk Management Cycle

[71] https://www.ncsc.gov.uk/files/Summary%20of%20the%20NCSCs%20security%20analysis%20for%20the%20UK%20telecoms%20sector.pdf
[72] See p11 of https://www.gsma.com/solutions-and-impact/technologies/security/gsma_resources/gsma-mobile-telecommunications-security-landscape-2024/
[73] https://www.gsma.com/solutions-and-impact/technologies/security/cybersecurity-knowledge-base/

5 Coordinated Vulnerability Disclosure

Another part of the strategic defence approach involves threat and vulnerability sharing (as exemplified by GSMA's T-ISAC service (see earlier Threat Actors section). Another service whereby the mobile industry continues to strengthen its collective security posture through structured approaches to vulnerability disclosure.

The GSMA's Coordinated Vulnerability Disclosure (CVD) Programme provides a trusted framework for security researchers, vendors, and operators to report and remediate vulnerabilities. GSMA's CVD programme primarily assesses vulnerabilities that relate to telecoms standards functionality rather than IT level or vendor specific issues. By acting as a neutral coordination body, the GSMA helps ensure that discovered weaknesses are responsibly disclosed, assessed, and addressed before they can be exploited, thereby reducing risk across the entire mobile ecosystem. This is made possible by 25 volunteers from GSMA MNO and vendor members, who form the expert panel supporting the programme

The GSMA CVD programme, established in 2017, has handled over one hundred disclosures to date. In 2025 alone, GSMA received 15 CVD cases, covering areas such as 5G Standalone (SA), Access Control, and eSIM. Mobile security researchers to submit their vulnerability disclosures to the programme[74].

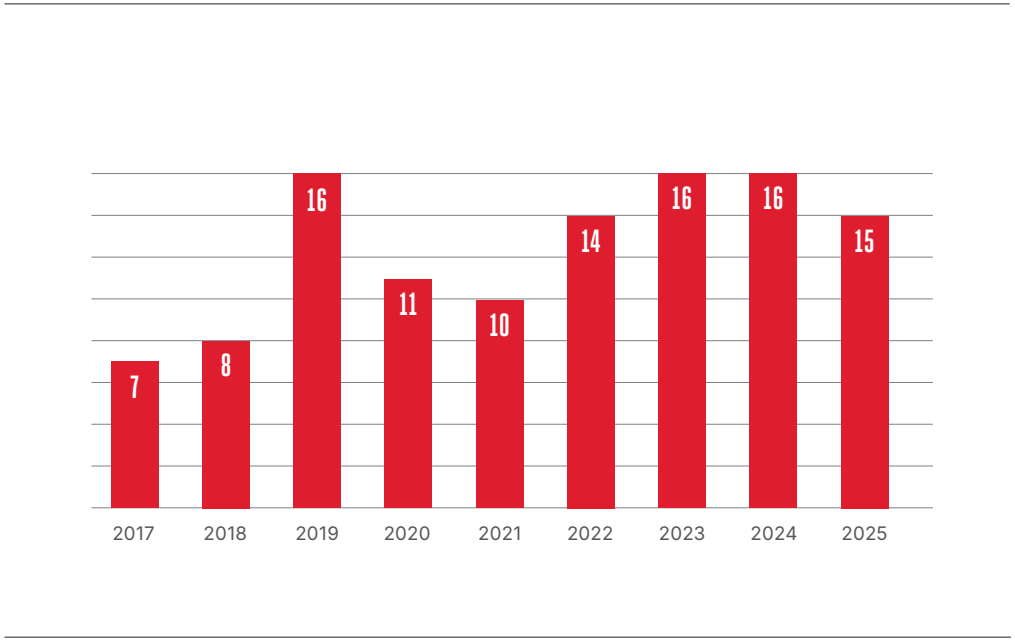


Figure 5, Number of GSMA CVD Disclousers per year

[74] https://www.gsma.com/solutions-and-impact/technologies/security/cvd-submit-a-vulnerability/

In addition to the GSMA initiative, other industry-driven disclosure frameworks play an important role in raising security maturity. For example:

- CERTs and national disclosure programmes provide structured channels for vulnerability reporting that span multiple sectors, including mobile.
- Standards and specifications organisation programmes such as ETSI and 3GPP provide an avenue for researchers to report vulnerabilities affecting their relevant standards or specifications.
- Device and platform providers maintain robust vulnerability reward programmes and bug bounty schemes, incentivising proactive researcher participation.
- Telecom operators and equipment vendors increasingly run their own disclosure channels, often aligned with international best practices, to ensure that issues identified in their infrastructure or services are resolved swiftly.

The diagram opposite provides a breakdown of % cases in a variety of network component areas. Radio Access Networks (RAN) are a key area due to their reliance on less secure legacy technologies and the complexity of RAN protocols can increase the risk of insecure implementations.

Taken together, these initiatives reflect a growing culture of transparency and collaboration in the mobile industry. By embedding coordinated disclosure practices at both the industry-wide and individual company levels, stakeholders are better positioned to respond to emerging threats, safeguard users, and build trust in mobile technologies.

Breakdown of cases across network areas

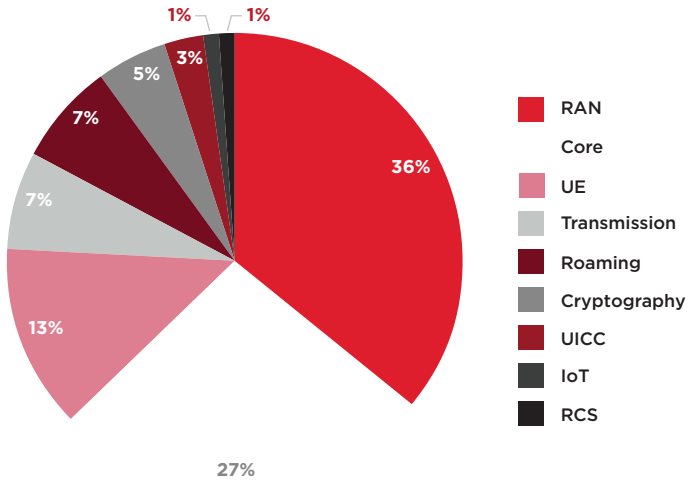


Figure 6, Breakdown of cases in different network areas

6 Generative and Agentic Artificial Intelligence Security

In the past few years, effective generative AI technology capabilities and availability have increased significantly enabling a range of new uses for both offensive[75] and defensive purposes with major ramifications for mobile telecoms security.

AI/ML has the potential to lower the technical barriers to attack methods that may have previously been unavailable to less sophisticated threat actors including:

- Enhancing the efficiency and effectiveness of social engineering attack types, such as smishing, vishing and phishing.
- Scams empowered by generative AI
- Identification of new attack types through use of AI
- Synthetic identity fraud (such as deepfakes)
- Enabling efficiencies for attackers and lowering the attacker skill base

Defensive AI-enabled solutions are also emerging such as the MITRE ATLAS™ (Adversarial Threat Landscape for Artificial-Intelligence Systems[76]) that aims to provide a knowledge base of adversary tactics and techniques based on real-world attack observations. NIST has released guidance such as *Artificial Intelligence Risk Management Framework* [77].

With the rapid evolution of generative AI, artificial intelligence is now transitioning into the era of agentic AI characterised by autonomy and intent driven decision-making. Unlike traditional AI limited to predefined tasks, Agentic AI leverages workflows that decompose complex goals, iteratively optimise actions, and actively adapt to dynamic environments, positioning itself as the cornerstone of next-generation digital infrastructure.

Whilst the area is still in its relative infancy, protecting new AI systems, data[78] and algorithms has many similar requirements to the introduction of other new solutions. Whilst AI is providing efficiency enablers for attackers, the security defensive controls require many of the same security controls and cyber hygiene to establish a security baseline of extant deployed networks, systems and service. Beyond baseline security, autonomous agent collaboration demands enhanced security. Anyone adopting agentic systems into any workflow must adopt the concept of the threat actor as internal to the workflow, rather than as an external party interacting with it. Consider[79],

1. Boundary Collapse, where an agentic model's output is executed by tooling that treats the model as authoritative;
2. Supply Chain Substitution, tampered dependencies, images, or model weights;
3. Privilege Misconfiguration, overly permissive service accounts that let an agent or user facing tool modify the model scheduler itself, or any sensitive data crossing a boundary from deterministic permissions to probabilistic.

AI system security is maturing. There are security challenges with some emerging tools[80] that need to be built to reflect existing best practices to defend against known attack types[81]. The broader hand over between governance and security is also being explored. GSMA launched the first industry-wide Responsible AI (RAI) Maturity Roadmap[82] to provide telecoms operators with the tools and guidance to test and assess their responsible use of the technology.

AI Is Not Enough: Why Cyber Hygiene and Standards Still Matter in Telecom Security[83].

Samantha Kight - Head of Industry Security, GSMA

[75] https://www.darktrace.com/news/new-report-finds-that-78-of-chief-information-security-officers-globally-are-seeing-a-significant-impact-from-ai-powered-cyber-threats
[76] https://atlas.mitre.org/
[77] https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf
[78] https://www.cyber.gov.au/sites/default/files/2025-05/CSI_AI_Data_Security.pdf
[79] https://www.gsma.com/solutions-and-impact/technologies/artificial-intelligence/agentic-ai-for-telecom-charting-the-course-for-an-intelligent-future/ and the broader document for a wider discourse
[80] https://www.axios.com/2025/10/28/atlas-chatgpt-openai-web-browser-security-privacy
[81] https://mellea.ai
[82] https://www.gsma.com/newsroom/press-release/gsma-launches-maturity-roadmap-as-telecoms-industry-leads-the-way-in-the-deployment-of-responsible-ai/
[83] https://insight.scmagazineuk.com/ai-is-not-enough-why-cyber-hygiene-and-standards-still-matter-in-telecom-security

GSMA

7 Post Quantum Cryptography

Post Quantum Cryptography is a topic with some uncertainty on timing but with potential for a significant security impact. A Cryptographically Relevant Quantum Computer (CRQC) has the potential to break public key infrastructures which underpin many current security protocols including some key distribution and digital signature regimes. It is a complex area with significant uncertainty. For telecoms, GSMA's Post Quantum Telco Networks (PQTN) Task Force[84] has been active for several years in developing guidelines focused on telco preparedness for quantum safe security.

There was much debate about the timescales for *transition* to PQC, so this is explored further here. In large part this is impacted on by the timescales within which a CRQC will become available. The security of commonly employed cryptographic algorithms, such as RSA- and elliptic curve-based public key encryption and digital signature schemes, is reliant upon the hardness of solving certain underlying mathematical problems. Security of these asymmetric protocols is founded on the assumption that a compute- or time- bounded attacker is unable to efficiently compute the prime factors of large integers or solve the discrete log problem. The advent of a CRQC fundamentally changes our assumptions regarding the compute powers available to bad actors. Shor's algorithm, for example, enables the efficient factorisation of large integers and allows attackers to efficiently solve the discrete log problem. Importantly, Shor's algorithm can achieve an exponential speedup, relative to known classical methods, rendering it infeasible to simply increase key sizes. Consequently, a sufficiently large fault tolerant quantum computer poses a threat to systems and protocols that utilise public key cryptography and/or digital signatures, and large-scale changes are required to retain present-day security assurances in the face of this quantum threat (the CRQC 'pull' factor).

Whilst there is uncertainty on the timing for the availability of a CRQC, the recent NIST announcements[85] with the intention to deprecate some important and widely used algorithms provides a clear 'push' priority to effect change. There is a lot of additional information on specific algorithms and key lengths, and an analysis of the impact will be valuable as part on ongoing PQC transition planning. There has been significant activity to prepare for QSC including at NIST[86], ETSI[87] and IETF[88] and significant national and regional activity (take a look at some of the conference presentations to get an update). NIST has released three PQC standards to start the transition to post-quantum cryptography: the Module-Lattice-Based Key-Encapsulation Mechanism [FIPS203], the Module-Lattice-Based Digital Signature Algorithm [FIPS204], and the Stateless Hash-Based Signature Algorithm [FIPS205]. There are real-world implementations of these algorithms (including open-source code) beginning to be made available.



[84] https://www.gsma.com/solutions-and-impact/technologies/security/post-quantum/
[84] PQ.01 https://www.gsma.com/solutions-and-impact/technologies/security/gsma_resources/post-quantum-telco-network-impact-assessment-whitepaper-pq-01
[84] PQ.02 https://www.gsma.com/solutions-and-impact/technologies/security/gsma_resources/guidelines-for-quantum-risk-management-for-telco-pq-02/
[84] PQ.03 https://www.gsma.com/newsroom/gsma_resources/pq-03-post-quantum-cryptography-guidelines-for-telecom-use-cases/
[84] PQ.04 https://www.gsma.com/solutions-and-impact/technologies/security/gsma_resources/pq-04-post-quantum-cryptography-in-iot-ecosystem/
[84] PQ.05 https://www.gsma.com/solutions-and-impact/technologies/security/gsma_resources/pq-05-post-quantum-cryptography-for-5g-roaming-use-case/
[85] https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf
[86] https://csrc.nist.gov/projects/post-quantum-cryptography
[87] https://www.etsi.org/technologies/quantum-safe-cryptography
[88] https://datatracker.ietf.org/wg/pquip/about/

The diagram illustrates some of the important push and pull factors alongside a set of migration and other factors to consider for PQC.

Most existing QSC migration advice sensibly points to establishing an inventory of encryption protocols in use. Other early steps include identifying critical systems and then identifying their supporting protocols, risk analysis and prioritisation, developing the transition plan and delivering it. Practical complementary approaches can focus beyond today's implementations and look at the planned future state of networks and systems. This can include understanding planned technology refresh, vendor product roadmaps and transformation projects. There may be little point planning a transition for a system that is due to be phased out soon. Cryptographic agility is an important system design and standardisation feature allowing rapid transition of cryptographic algorithm.

More QSC detailed approaches are identified in the PQTN Task Force documentation[89] which is actively being developed with more guidance.

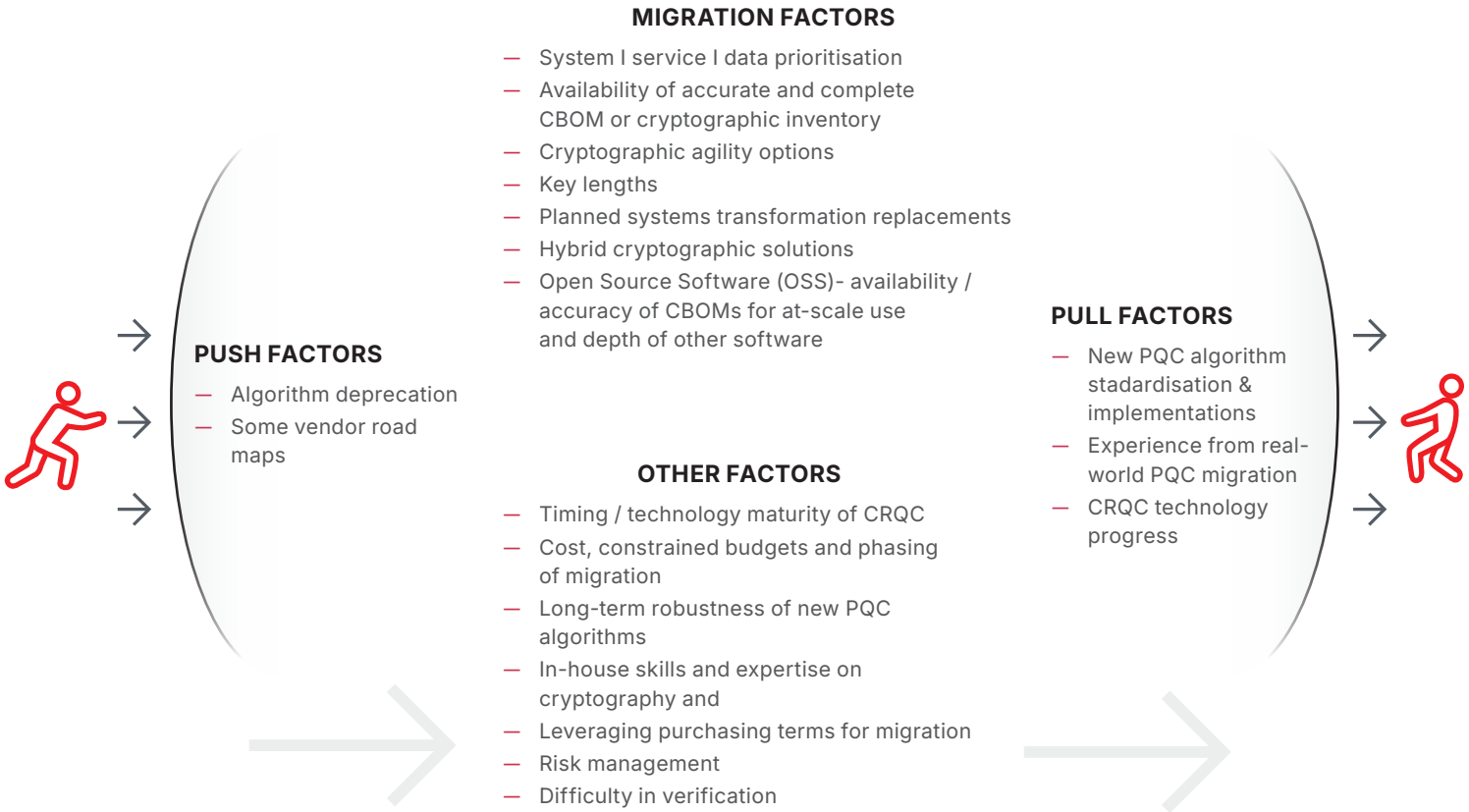


Figure 7, A range of factors affecting PQC

[89] https://www.gsma.com/solutions-and-impact/technologies/security/post-quantum-telco-network-task-force/

8 Mapping the Global Cybersecurity Regulatory Landscape

Cybersecurity regulation is now a defining factor in the resilience of mobile networks. A GSMA report[90] highlights that fragmented, misaligned, or overly prescriptive regulation imposes unnecessary costs, diverts resources from genuine risk mitigation, and in some cases increases exposure to cyber threats.

A Fragmented and Fast-Moving Landscape

Cybersecurity regulation is no longer the domain of a few national strategies or voluntary frameworks. Today, it spans mandatory product security laws, sector-specific obligations, certification schemes, and cross-border data governance regimes. From the EU's Cyber Resilience Act (CRA) to the UK's Telecoms Security Act (TSA) and China's cybersecurity review measures, the regulatory patchwork is expanding rapidly.

For mobile operators, this fragmentation results in overlapping or contradictory obligations from multiple authorities, duplicated reporting requirements, and administrative burdens that deliver limited security benefit.

Rapidly Expanding Patchwork

Cybersecurity regulation now spans:

- Mandatory product security laws (e.g., EU's Cyber Resilience Act, UK's PSTI Act)
- Sector-specific obligations (e.g., UK's Telecoms Security Act)
- Certification schemes (e.g., EU Cybersecurity Act, Japan's JC-Star, ISMAP)
- Standards agencies (ITU, UNECE, ETSI, NIST, ISO, ENISA, APEC)
- Cross-border data governance (e.g., China's Cybersecurity Review)

The following map shows how cybersecurity regulation and standards vary across regions, highlighting where countries converge and where their approaches begin to diverge. Countries are included because they have established cybersecurity laws, national strategies, or sectorspecific obligations that create real, enforceable requirements for mobile operators. Others are not shown because their frameworks remain voluntary, highlevel, or still in draft.

Strategic Governance and Resilience

The persistence of ransomware and the targeting of critical sectors call for a renewed focus on strategic governance. National Cyber Security Strategies (NCSS) must evolve to reflect the changing threat environment. ENISA's *Interactive Map of NCSS*[91] provides a valuable overview of how EU Member States are structuring their approaches, from governance models to implementation measures. It also highlights good practices that can be adapted across borders.

A key takeaway from ENISA's mapping is the importance of resilience, including the ability to recover quickly and maintain continuity across critical sectors. The ability to recover quickly from cyber incidents is now as critical as prevention. This includes not only technical recovery but also reputational and operational continuity. Strategies must therefore embed resilience across sectors, with tailored approaches for high-risk domains like energy, healthcare, and manufacturing.

[90] https://www.gsma.com/solutions-and-impact/connectivity-for-good/public-policy/gsma_resources/the-impact-of-cybersecurity-regulation-on-mobile-operators
[91] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map

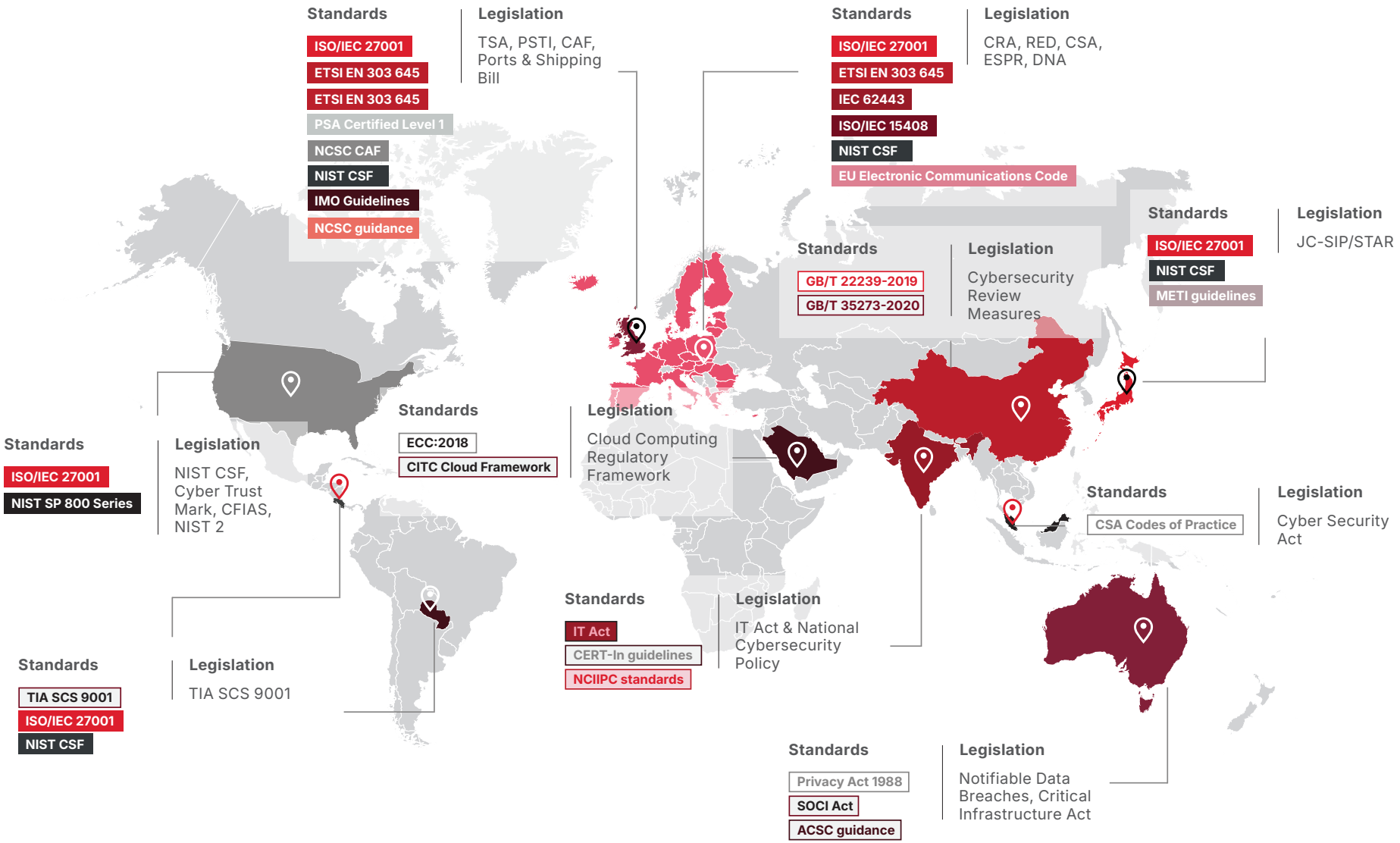


Figure 9, Mapping the global cybersecurity regulatory landscape

Looking Ahead: Strategic Recommendations

To address the evolving threat landscape, national and international policy must adapt. Based on the synthesis of threat intelligence and strategic mapping, the following recommendations emerge.

- **Harmonisation:** Align cybersecurity policy with international standards wherever possible, to reduce regulatory fragmentation and inconsistency.
- **Consistency:** Ensure new policies and frameworks are consistent with existing policy to avoid duplication or conflict.
- **Risk- and outcome-based:** Adopt risk-based and outcome-based approaches in the design and implementation of cybersecurity regulation, giving operators flexibility to innovate and deploy effective solutions.
- **Collaboration:** Promote a collaborative regulatory culture with industry, supported by secure threat intelligence sharing to strengthen resilience, increase awareness of cyber threats, enable constructive enforcement, and foster a joint approach to combating cybercrime.
- **Security-by-design:** Encourage a proactive, security-by-design approach to mitigating cyber risks.
- **Capacity-building:** Strengthen the institutional capacity of cybersecurity authorities to ensure a whole-of-government approach and effective application of policy and regulation.

The cyber threat landscape is increasingly complex, with ransomware, geopolitical tensions, and resilient threat actors shaping the strategic environment. National regulatory strategies must evolve to meet these challenges, embedding resilience, risk management, intelligence, and collaboration at their core.

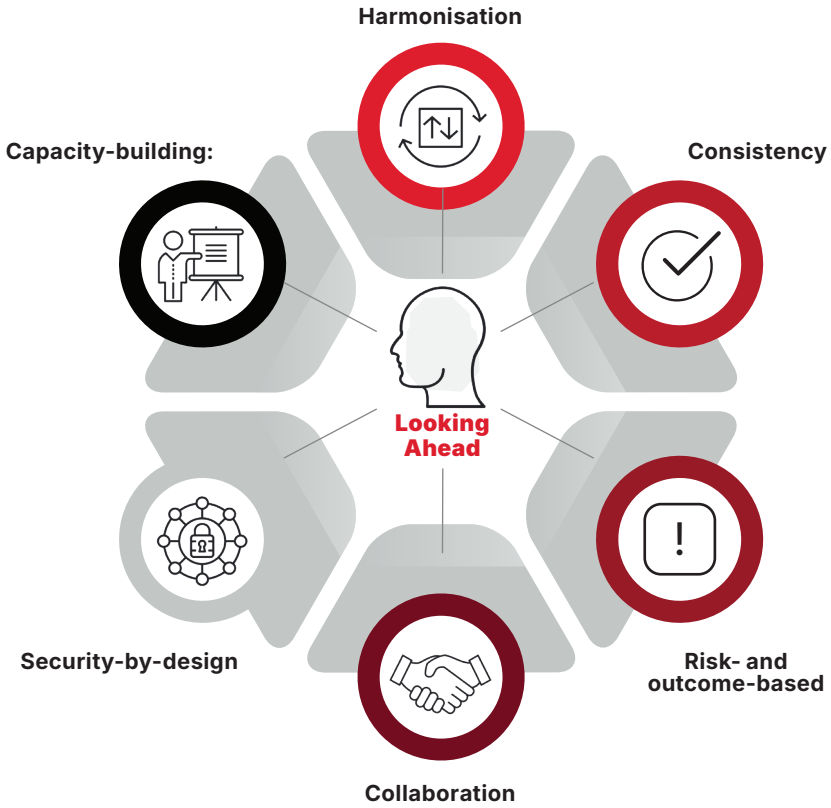


Figure 8, Significant factors to consider for regulation

9 Final Thoughts

The GSMA Mobile Security Landscape Report 2026 provides an overview of the security landscape for the mobile industry in the context of current threats facing mobile network operators, their customers and the wider ecosystem.

The report has identified a range of key security protection areas including:

1. Strengthen cyber hygiene and baseline controls including MFA, encrypting sensitive data, network segmentation and regular patching
2. Know your traffic including enhanced threat detection and incident response including threat hunting
3. Secure the software attack vector including more secure code, API security and third-party risk management
4. More broadly, strengthen the entire supply chain security by applying security controls throughout the product or service lifecycle
5. Combat scams and social engineering
6. Adopt and support industry schemes, for example GSMA's CVD & T-ISAC
7. Adopt a risk-based security approach including risk assessments, layered defences and updating defences against the latest threats
8. Prepare for emerging technologies such as AI and PQC
9. Engage with industry collaboration standards such as GSMA's fraud and security groups[92]
10. Promote a security-first culture with executive engagement and continuous improvement

Over the coming year, the GSMA will continue to support its members on security matters by providing security best practices, services and events that convene the industry - engagement by all stakeholders is strongly encouraged.

To get in touch, or to get more closely involved, please email **security@gsma.com.**

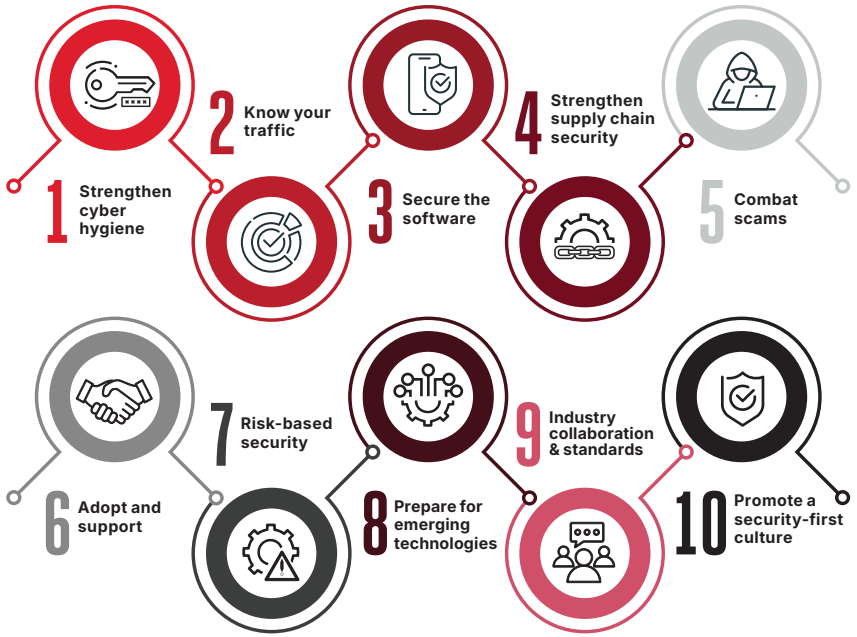


Figure 10, A range of key security protection areas

[92] https://www.gsma.com/solutions-and-impact/technologies/security/gsma_resources/security-assurance-andcertification/

GSMA Head Office
1 Angel Lane
London
EC4R 3AB
UK

Email: security@gsma.com

