# GSMA Mobile Telecommunications Security Landscape - 2026



February 2026

# 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.

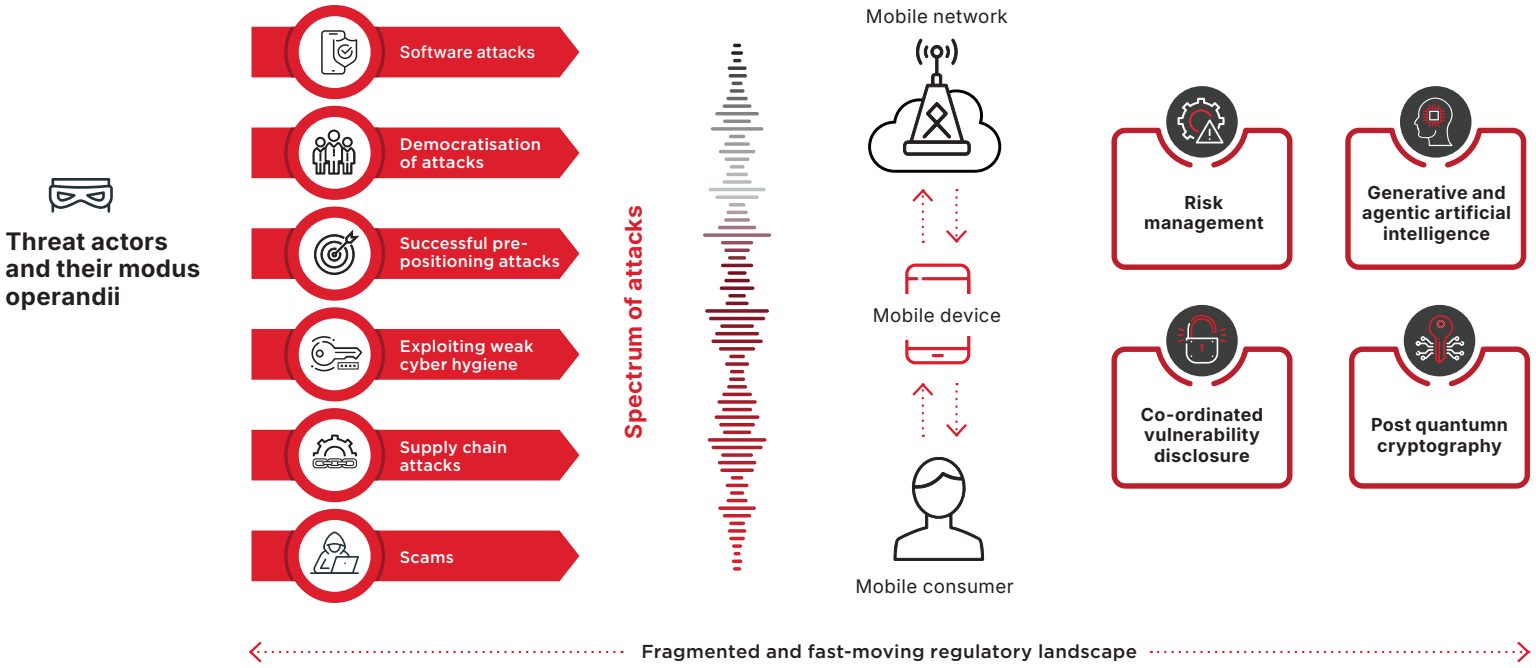


**Figure 1,** An Overview of topics

[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/

**GSMA Head Office**
1 Angel Lane
London
EC4R 3AB
UK

Email: security@gsma.com