

WWRF Huddle 2026

Session 3: Many Disciplines, One Trust Framework

Alex Leadbeater CEng MIET
(Technical Security Director, GSMA)
(ETSI Fellow, Chair ETSI CYBER & 3GPP SA3-LI)
16/09/26

We are the world's leading Member Organisation for the mobile ecosystem

Connectivity for good

Engaging members, governments & society to advance policy, facilitate digital innovation and reduce inequalities

Industry solutions

Supporting the technology that makes mobile work through projects, working groups and other collaborative activities

Convening

Bringing the mobile ecosystem and its customer sectors together through the world's largest and most influential connectivity events

- Founded over 25 years ago; not-for-profit global trade body
- Over 1,000 company members across the global connectivity ecosystem; >10,000 individuals
- Industry Working Groups and Permanent Reference Documents
- Host of MWC Barcelona, the world's largest and most influential connectivity event, and numerous other global gatherings

Context of Security Regulation and Standards



What is the purpose of National, EU or Global Security Regulation?

- Protect National, European or Global Citizens from defined threat, which the regulation aims to mitigate?
- We must not lose sight of the fundamental purpose of security regulation.

What is the purpose of Security Standards?

- Define a common minimum baseline level to address defined Security Threats / Risks.
- Security bar must be achievable, while adding value (current product security vs “needed” security delta).
- Must be possible to move the bar over time.

Security is a cost?

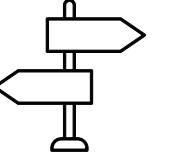
- Effective targeted Security Standards, Certification and Regulation reduce cost (e.g. financial or privacy).
- Security certification that does not mitigate intended threat / risk increases cost for little benefit.
- Multiple overlapping security mechanisms, requirements and certification obligations are inefficient.
 - End user, manufacturer or service provider rarely benefit.
 - Market agility and innovation reduced.

Overly prescriptive Regulation and Standards?

- Reduce end product market competition and security innovation?
- Barrier to market entry (including access to standards and standards creation).
- Inflexible regulation and standards are vulnerable to market or security threat landscape change.

Ultimately if the end service / product user does not receive the intended security or privacy benefit, then both regulation and security certification have failed.

Agenda



Security Landscape

Emerging Security Context

Future Context

Overview

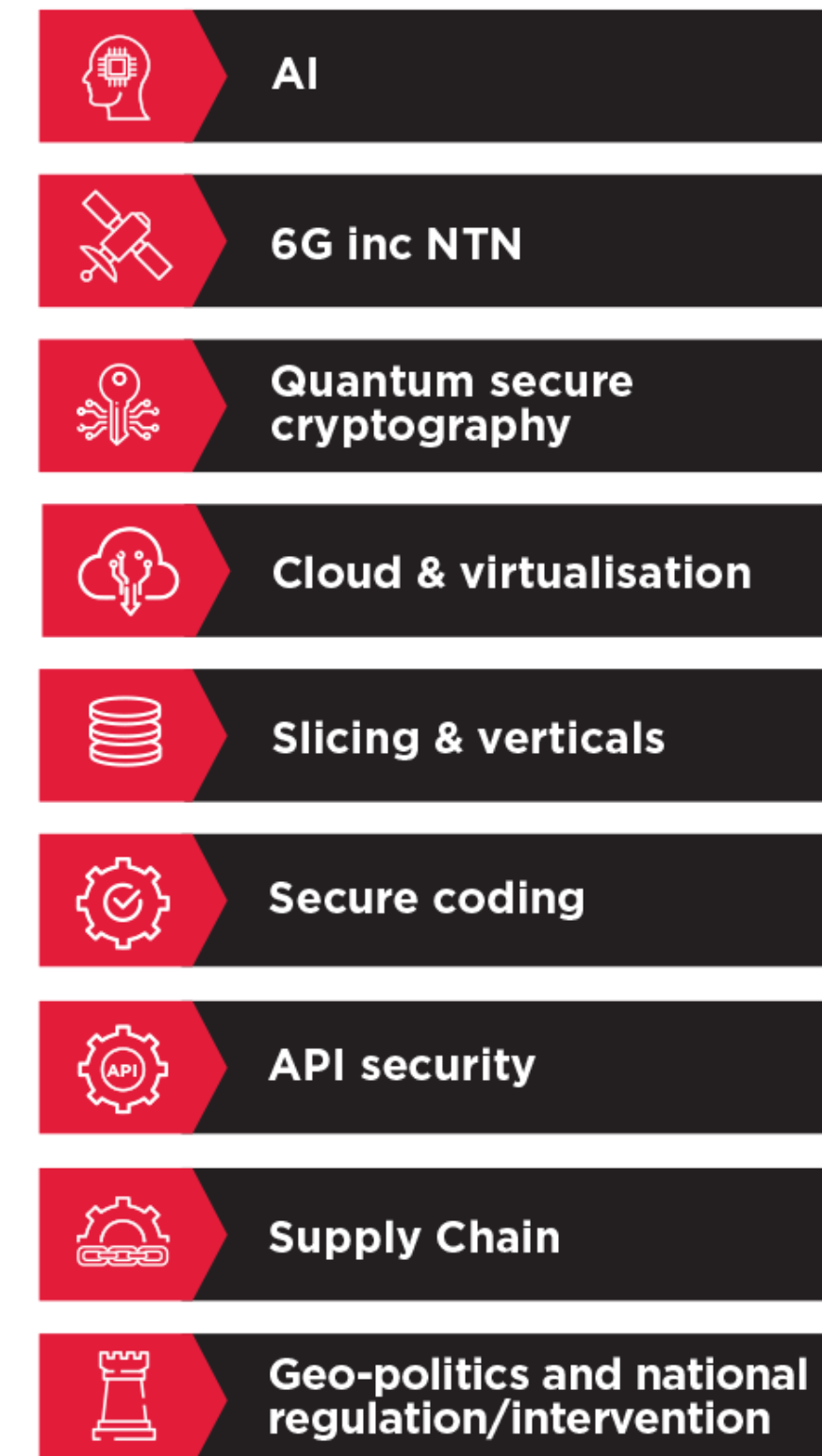
Strategic Security



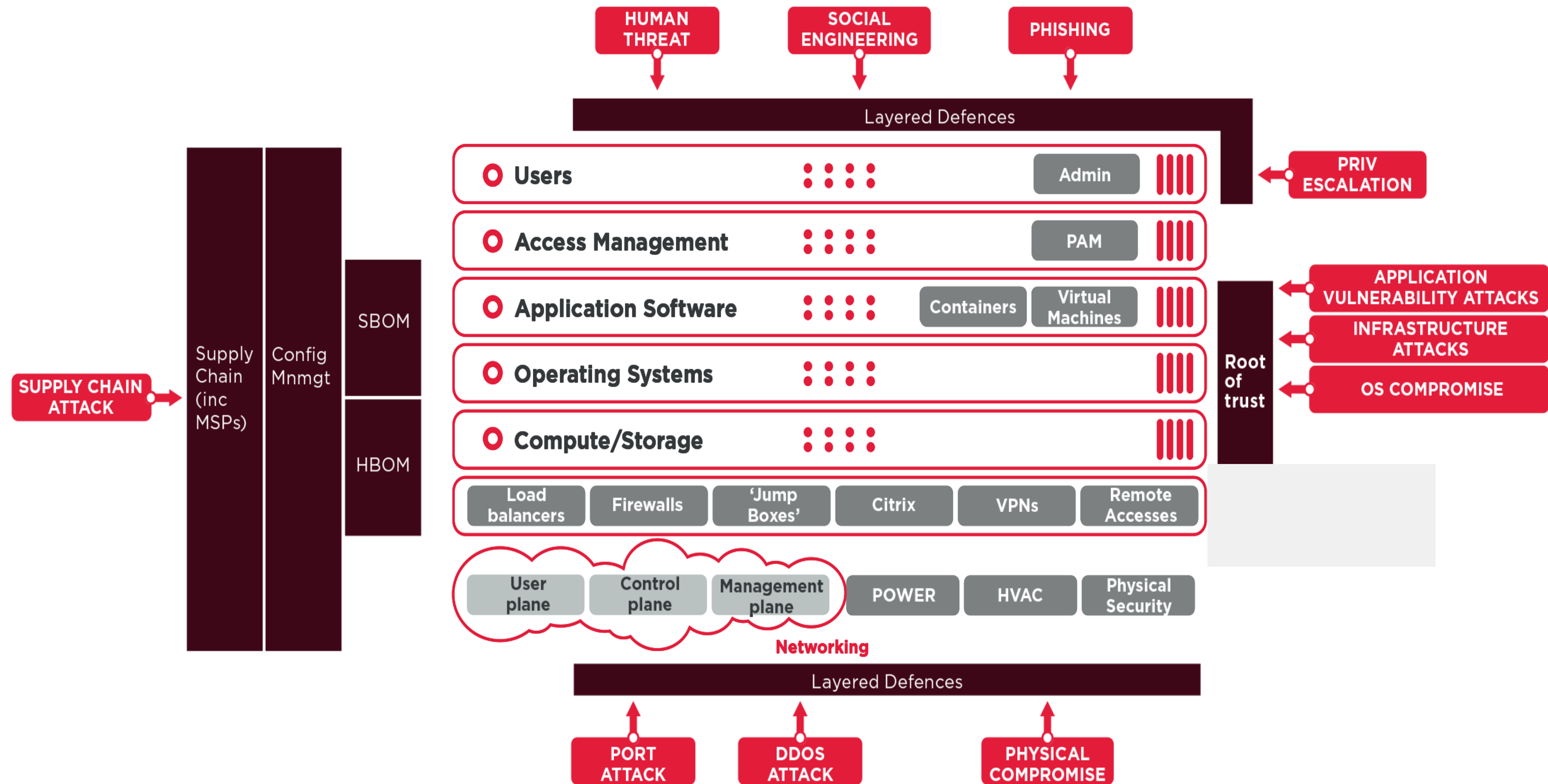
Technical Security



The Emerging Security Context

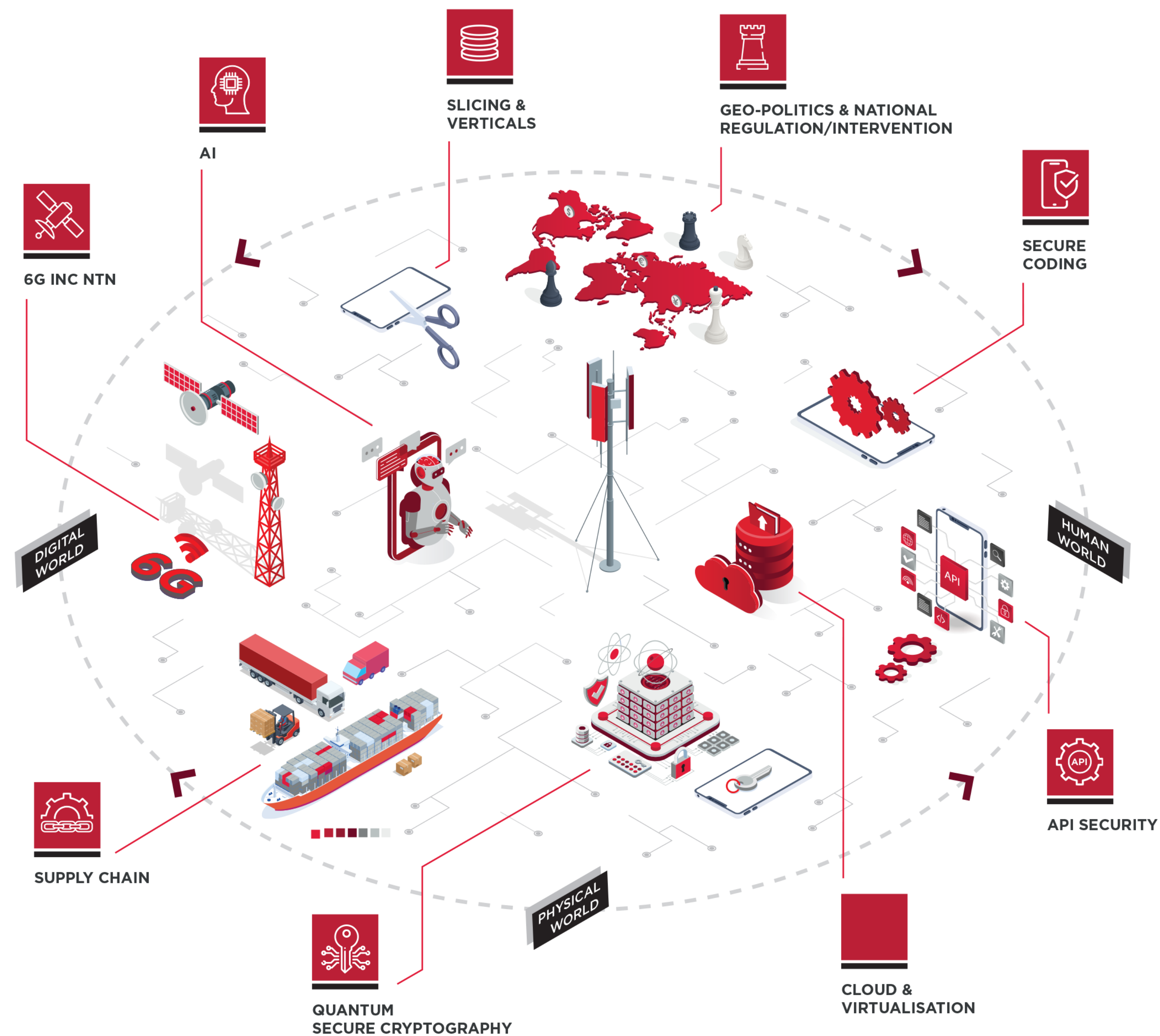


The attack surface



Emerging and 6G Perspectives

The Emerging Security Context



6G Security Evolution not Revolution factors

9

3GPP TR 33.801-01 – (6G is a 2026 to 2028 Technology).

How to deal with Legacy is one of the biggest challenges.

- Network, Services and Handset.

3GPP focussing on Key Security areas;

- Core Security Architecture** – e.g. Where to place trust anchors and relationship between them.
- RAN Security** – e.g. Selective risk based protection of MAC Control Elements (CEs).
- Roaming and Interconnect** – Overcoming limitations of 5G roaming design.
- Subscription and Authentication** – Quantum safe by default.
- Privacy Enhancements** – e.g User Authorisation
- Security Monitoring**
- Sensing (ISAC)**

AI, Quantum Safe, Secure by Design, NTN and Zero Trust concepts, native part of design.

Balance between Privacy Vs Network Operation / Fraud Reduction / Resilience.

GSMA Security Landscape 2026 / 6G Cyber Security Highlights

Encourage industry to following existing controls and best practice.

- Most recent breaches are examples where GSMA best practice would have significantly reduced impact.

T-ISAC (GSMA Telecoms Information Sharing and Analysis Centre)

- One Organisation’s detection is another’s prevention.

Focus areas including; API Security, SBOM, Handset Security, AI.

Telco for AI & AI for Telco.

Increased focus on Scam reduction

- SS7 Misuse
- SMS Blasters
- Identity Verification
- GSMA Foundry OVC

FASG 6G Security subgroup.

Preparing industry for Post Quantum.

- PQTN Taskforce, Crypto Inventory, Threat from Store and Future decrypt.
- Algorithm agility is not new or a quantum only challenge.

Digital Sovereignty causing significant uncertainty.

Customer Terminal



Device Anti-Theft (FS.25)

IoT Security (FS.60)

Software Updates (FS.25) / Mobile Malware (SG.19)

(e)UICC Profiles (FS.27)

IMEI Security

Cryptographic Algorithms (FS.35)

Operator Network



Voicemail Services (SG.20)

Voice Calling VoLTE (FS.22)

Exchange of Subscriber Credentials (FS.28) / Credentials Storage

Network Function Virtualization (FS.33) / Inter-NF Communication

Network Partner



SIM Box Fraud (FS.01) / SMS Fraud (FF.09) / Binary SMS (FS.42)

SS7 (FS.07, FS.11, FS.52)

Diameter (FS.19)

GTP-C (FS.20)

GTP-U (FS.37)

5G (FS.36)

SIP (FS.38)

Key Management (FS.34)

Interconnect Signalling (FS.21) / Interconnect Testing (FS.26)



Risk Management

ATT&CK Framework (FS.57/xx)

Controls Testing Methodology

Baseline Controls (FS.31)

5G Fraud (FS.39)

5G Security (FS.40)

Fraud Manual (FF.21)

Security Manual (FS.30)

Vulnerability Disclosure (FS.23)

Post Quantum Crypto (PQ.1, PQ.2)



Private IP Network

DNS Encryption (IG.10)

IP Exchange Network (IR.34, IR.77)

Key FASG Permanent Reference Documents

Impacts & Opportunities of AI & Frontier Models 11

The democratisation of vulnerability identification and exploit?.

- Code vulnerabilities
- Config vulnerabilities
- Doesn't change fundamental security principles.
- LLMs and Agentic as force multiplier.
- Standards vulnerabilities.

Eventual establishment in CI CD pipeline?

AI as a barrier or enabler to market entry?

- Cost, Skill availability.

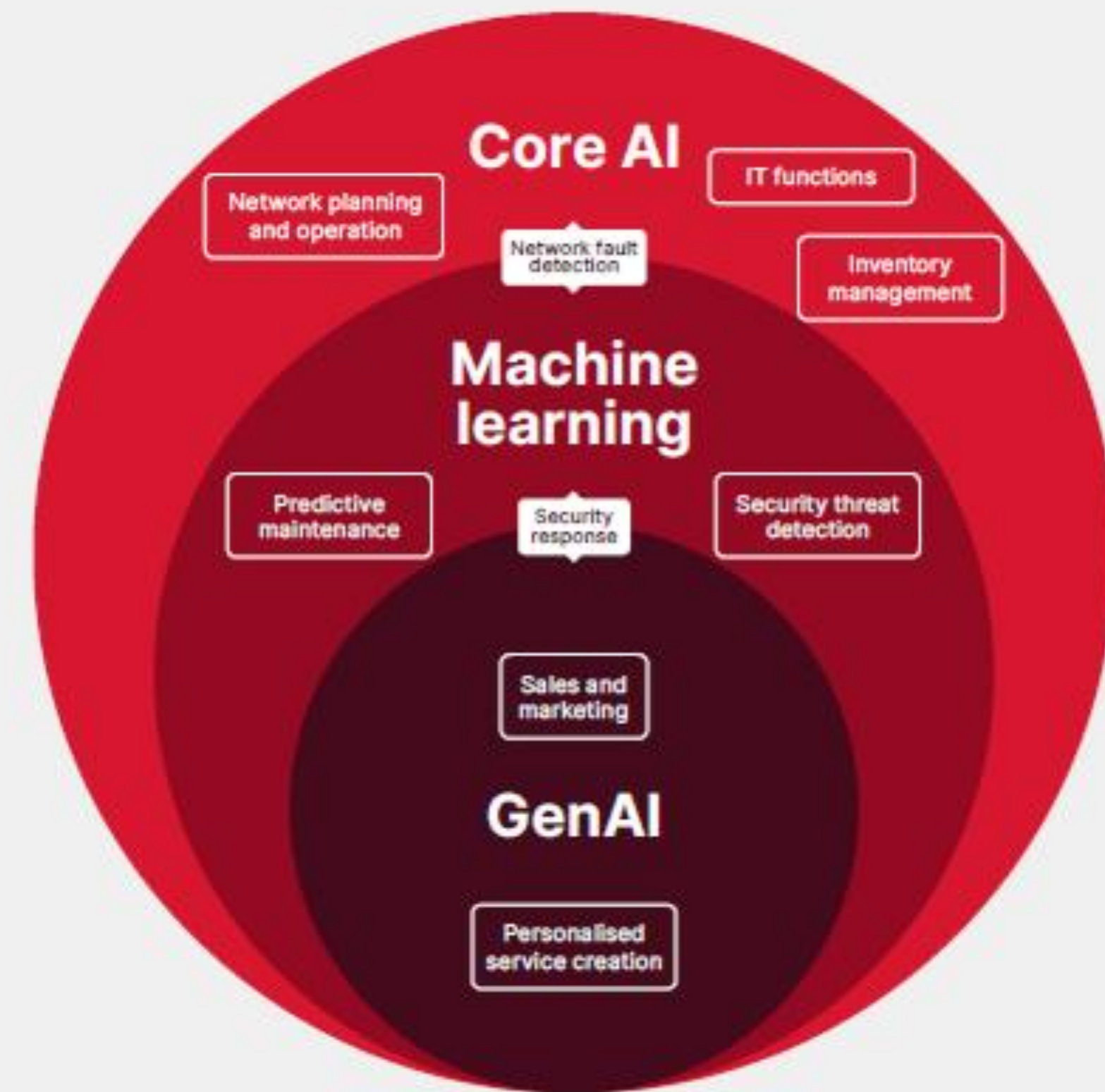
Security and Privacy Best Practice still very much evolving.

- Best Practice evolves with failure.

Rate of AI evolution outpacing standards?

Rate of AI evolution outpacing regulation!

Figure 17
Examples of telco-specific use cases with AI



Source: GSMA Intelligence

Further Information

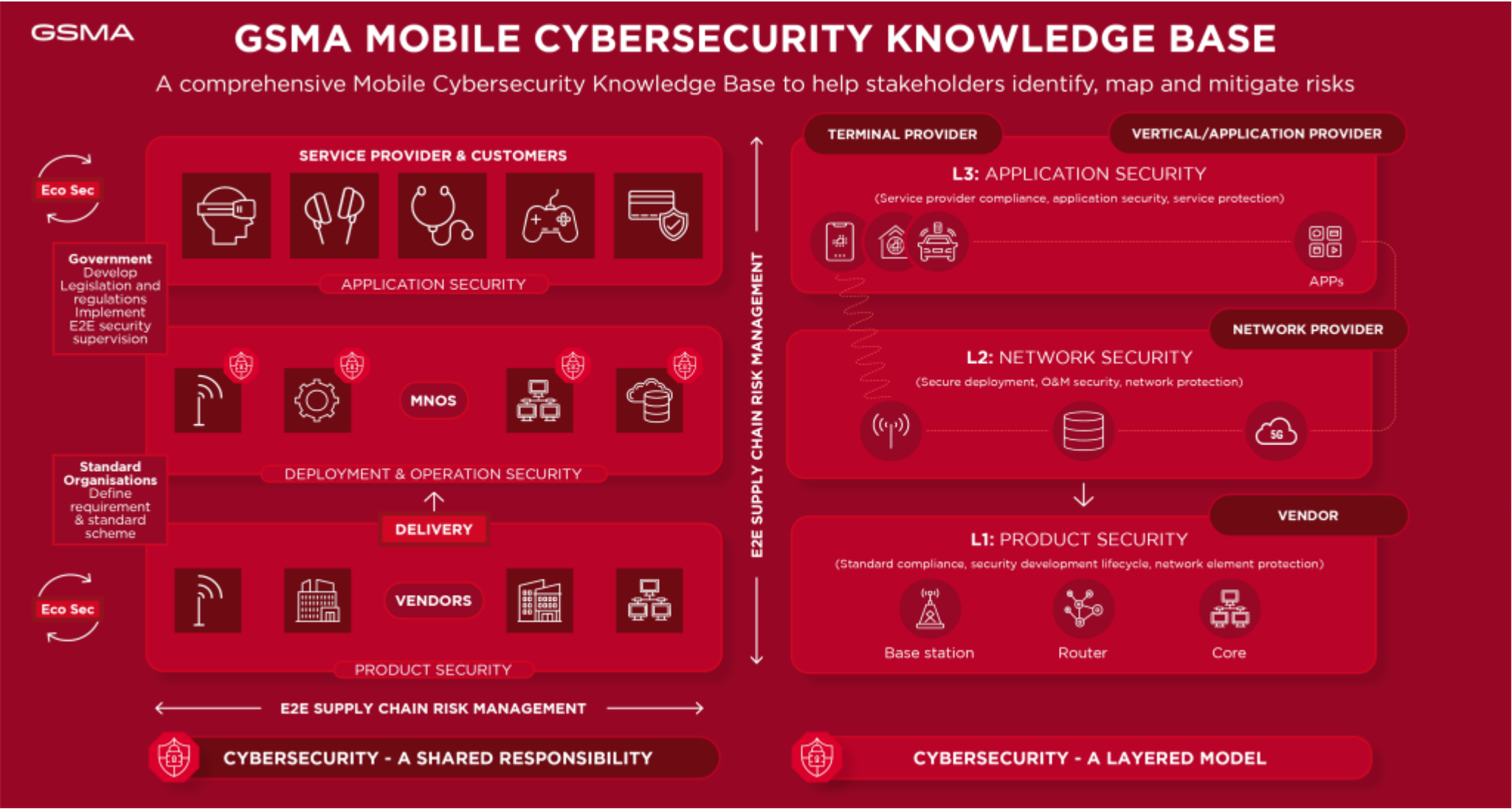
Further GSMA / 3GPP Cyber Security Information

GSMA Security Landscape

<https://www.gsma.com/solutions-and-impact/technologies/security/gsma-mobile-telecommunications-security-landscape-2026/>

GSMA MCKB

<https://www.gsma.com/solutions-and-impact/technologies/security/cybersecurity-knowledge-base/>



3GPP SA3

<https://www.3gpp.org/3gpp-groups/service-system-aspects-sa/sa-wg3>

Thank You