

Whitepaper

# **Mobilfunk-Cybersicherheit in der Schweiz – eine Übersicht**

---

Bern im Mai 2026

## Inhaltsverzeichnis

1. Einleitung.....	2
2. Ausgangslage.....	3
3. Zusätzliche Sicherheitsfunktionen in 5G-Netzen.....	6
4. Rechtliche Grundlagen in der Schweiz .....	8
5. Organisationen, welche die Mobilfunk-Sicherheit voranbringen.....	8
6. Standards, Normen, Empfehlungen zur Mobilfunk-Sicherheit.....	10
7. Massnahmen für die Mobilfunk-Sicherheit .....	14
8. Exkurs: Sicherheit im Internet der Dinge (IoT) .....	16
9. Cybersicherheit ist eine gemeinsame Verantwortung .....	17
10. Zusammenfassung über Mobilfunk-Netze in der Schweiz.....	17
Anhang GSMA Mobile Cyber Security Knowledge Base .....	19

## 1. Einleitung

Seit über 25 Jahren sind in der Schweiz drei Mobilfunknetze in Betrieb und die neuste Mobilfunkgeneration 5G hat den kommerziellen Betrieb im Jahr 2019 aufgenommen. Die Mobilfunkabdeckung erreicht über 99% der Schweizer Bevölkerung und ermöglicht den Zugang zu mobilem Internet. Mit höherer Datengeschwindigkeit, grösserer Kapazität sowie geringerer Latenzzeiten leistet 5G einen wichtigen Beitrag zur Digitalisierung der Schweiz und hat die Art und Weise, wie Menschen kommunizieren, arbeiten und ihre Freizeit verbringen, verändert.

Gleichzeitig können Unternehmen und staatliche Organisationen ihre Prozesse und Dienstleistungen verbessern, indem sie die neuen Funktionen sowie verbesserte Sicherheitsmassnahmen und Best Practices nutzen. Dazu gehören auch vernetzte Geräte und Anlagen (Internet der Dinge, IoT) sowie basierend darauf intelligente Anwendungen und Automatisierung. Beispiele für die Nutzung mobiler Datenverbindungen sind neue Anwendungen wie teilautonomes Fahren, smarte Fabriken und digitalisierte Gesundheitsversorgung. Es überrascht daher nicht, dass der Bundesrat die mobile Kommunikation und damit auch die 5G-Netze zur kritischen Infrastruktur der Schweiz zählt.

Durch die neuen technologischen Möglichkeiten entstehen jedoch auch neue Bedrohungsvektoren für böswillige Akteure, organisierte Kriminalität oder staatliche Akteure. In Kombination mit der stetigen Weiterentwicklung von Hackerangriffen, die teilweise durch Künstliche Intelligenz (KI) oder professionelle Angriffe als Service (DDoSaaS, RaaS etc.) unterstützt werden, wird das digitale Ökosystem neuen Risiken ausgesetzt.

Das Bundesamt für Cybersicherheit (BACS) verzeichnete im vergangenen Jahr 64'733 freiwillige Meldungen zu möglichen Cybervorfällen. Das ist eine leichte Zunahme von 3% gegenüber 2024 und entspricht einer Meldung rund alle 8 Minuten<sup>1</sup>. Zudem müssen seit dem Inkrafttreten des Informationssicherheitsgesetzes am 1. April 2025 Cybervorfälle bei kritischen Infrastrukturen dem BACS zwingend gemeldet werden. 2025 waren dies insgesamt 222 Cybervorfälle.

<sup>1</sup> BACS (2026): Jahresbericht 2025. Bundesamt für Cybersicherheit BACS. Bern.

Diese Zahlen zeigen die Problematik und die Bedeutung von wirksamen Cybersicherheits-Massnahmen deutlich auf. Dazu trägt auch die Technologieentwicklung bei und neue Mobilfunkgenerationen wie 5G beinhalten neben den Leistungssteigerungen auch verbesserte Sicherheitsfunktionen. Die Bedenken hinsichtlich der Cybersicherheit von Mobilfunk und insbesondere 5G haben in den vergangenen Jahren dazu geführt, dass die Technologie durch unabhängige Testinstitute geprüft und gemäss verschiedenen internationalen Sicherheitsregelwerken zertifiziert wurde (u. a. NESAS, SCAS, EU Common Criteria). Branchenverbände wie die GSMA haben zudem eine umfassende Cybersicherheits-Wissensbasis entwickelt, welche die Mobilfunknetzbetreiber dabei unterstützt, die Cyberresilienz ihrer Netze zu verbessern. Basierend darauf kann die Cybersicherheit heute faktenbasiert bewertet werden.

Bereits 2021 hatte der Schweizerische Verband der Telekommunikation (asut) einen Bericht zu «5G-Cybersicherheit in der Schweiz» erstellt und veröffentlicht. Für die vorliegende Aktualisierung konsultierte asut Sicherheitsexperten ihrer Mitglieder. Dabei wird dem aktuellen Stand der Technik und insbesondere der Betriebsprozesse Rechnung getragen. Der Bericht beleuchtet verschiedene Aspekte der Cybersecurity der Schweizer Mobilfunkinfrastruktur. Mobilfunknetzbetreiber und Zulieferer bilden die zentralen Säulen für Cybersicherheit, doch das gesamte Ökosystem bzw. Geschäftsumfeld erfordert gleichermassen Aufmerksamkeit: Welche Best Practices gibt es? Welche Rolle spielen Standards und Branchenempfehlungen? Wie lässt sich der Wert international anerkannter Zertifizierungen einordnen? Und was ist wesentlich für die Schaffung sinnvoller und effizienter regulatorischer Rahmenbedingungen?

Der Bericht gibt einen breiten Überblick über den Stand der Cybersicherheit im Mobilfunk, möglicher Bedrohungen und insbesondere Massnahmen, welche Mobilfunknetzbetreiber und ihre Lieferanten zur Stärkung der Cybersecurity ergreifen können. Die vorliegende Übersicht wurden von Praktikern aus der Cybersicherheit erstellt. Es ist keine wissenschaftliche Studie und hat auch nicht den Anspruch auf Vollständigkeit. Der Bericht gibt jedoch einen umfassenden Überblick über die Cybersicherheitspraxis in der Schweizer Telekombranche und richtet sich damit an ein interessiertes und technisch versiertes Fachpublikum.

## 2. Ausgangslage

### Sicherheit im Betrieb

Die Gewährleistung der Sicherheit in Telekommunikationsnetzen ist die zentrale Aufgabe der Netzbetreiber. Grundlage dieser Sicherheits- und Datenschutz-Kultur ist das Fernmeldegeheimnis, das in der Bundesverfassung verankert ist und im Fernmelderecht konkretisiert wird. Mit der fortlaufenden Weiterentwicklung der Kommunikationstechnologien wurden Vorkehrungen und Massnahmen jeweils an die neuen Gegebenheiten angepasst. Dies gilt auch für 5G und dessen Weiterentwicklung 5G Advanced sowie für zukünftige Mobilfunkgenerationen.

Einige zentrale Sicherheitsanforderungen sind in der Schweiz rechtlich vorgeschrieben. Diese finden sich im Informationssicherheitsgesetz, im Datenschutzgesetz, im Fernmeldegesetz und in den Verordnungen zum Fernmelderecht. In Kombination mit global etablierten Best-Practices haben sich diese Regularien aus Sicht der Telekommunikationsbranche bewährt. Sie erlauben eine der Unternehmenssituation angepasste Umsetzung von Security-Massnahmen und verhindern eine innovationshemmende Überregulierung.

Um Privat- und Geschäftskunden sowie die Telekommunikationsinfrastruktur und die interne IT-Infrastruktur zu schützen, haben sich die Betreiber weitere strikte Sicherheitsregimes auferlegt und interne, spezialisierte Sicherheitsorganisationen aufgebaut. Zu den wichtigsten Massnahmen gehören etwa:

- Der Betrieb eines Informations-Sicherheits-Managementsystems (ISMS) nach ISO 27001
- Der Betrieb eines Security Operation Centers (SOC) oder einer vergleichbaren Instanz, also einer zentralen Organisation, welche die Sicherheit im Netz ständig überwacht, Bedrohungen analysiert, Massnahmen ergreift respektive veranlasst und damit Angriffe abwehrt.
- Das Pflegen eines Business Continuity Managements (BCM) nach ISO 22301, um den Betrieb systemkritischer Prozesse zu schützen und im Krisenfall aufrecht zu erhalten.
- Regelmässige Penetrationstests (Pentests), mit welchen untersucht wird, ob Angreifer mit bekannten Methoden unautorisiert in das Netz eindringen könnten.
- Leakage Prevention, also die Verhinderung respektive Detektion von nicht-autorisierten Datenabflüssen.
- Ein System zur Verwaltung personenbezogener Daten (PIMS) gemäss ISO 27701 und den geltenden Datenschutzgesetzen
- Umfassende Sicherheitsframeworks, die verschiedene organisatorische und technische Massnahmen beinhalten. Beispiele für deren Implementierung sind: EDR, SOAR/SIEM und Authentifizierungsmanagementsysteme.
- Die stetige Sensibilisierung und Schulung der eigenen Mitarbeitenden zum Thema Cyber-Sicherheit und Datenschutz.

Die Cybersicherheit liegt in der Verantwortung jedes einzelnen Netzbetreibers. Es kann daher keine Einheitslösung geben und je nach Ausgangslage und Rahmenbedingungen wird auf die geeigneten Massnahmen, Standards und Best-Practice-Empfehlungen zurückgegriffen. Die jeweiligen Sicherheitskonzepte richten sich nach den angebotenen Diensten, den Eigenheiten der Netze und Infrastrukturen, den technischen Rahmenbedingungen, der jeweiligen Bedrohungslage und auch immer nach den Bedürfnissen der Kundinnen sowie Kunden.

## Sicherheit in der Lieferkette

IT-Systeme und Kommunikationsnetze bestehen aus einer Vielzahl von Komponenten und Applikationen unterschiedlicher Hersteller und Lieferanten. Dazu gehören nicht nur die eigene IT im Unternehmen, sondern beispielsweise auch Clouddienste in externen Rechenzentren. Die Sicherheit der Lieferkette ist daher ein zentrales Thema in der Cybersecurity. Sie betrifft alle Branchen und ist kein spezifisches Kommunikations- oder Mobilfunkthema.

Im Bereich der Kommunikationsnetze wird die Sicherheit in der Lieferkette von den Betreibern und von den Herstellern der Telekommunikations-Systeme konsequent berücksichtigt. Dabei umfassen die Lieferanten nicht nur den direkten Technologiepartner der Netzbetreiber, sondern letztlich die ganze Lieferkette für die Herstellung aller Komponenten. Angesichts der Bedeutung von Mobilfunk und insbesondere 5G erhält die Frage der Sicherheit in der Lieferkette zusätzliches Gewicht. Daher sollen die unterschiedlichen Bedrohungsarten im Folgenden detailliert aufgezeigt werden:

**Produktintegrität und Qualität:** Die hohe Komplexität von 5G-Netzen und die damit einhergehende stärkere Abhängigkeit der Netzbetreiber von internationalen Hardware- und Softwareanbietern sowie teilweise auch von Drittanbieter-Software und -Diensten erhöhen ganz grundsätzlich das Risiko von Sicherheitslücken, Produktmanipulationen in der Lieferkette oder fehlerhaften Produkten sowie Software-Updates. Dies kann zu Störungen im Netzwerkbetrieb, schwerwiegenden Ausfällen oder gar zu koordinierten Angriffen führen. Beispiele dafür aus dem IT-Bereich sind die Kompromittierung von SolarWinds im Jahr 2020, was zur

Verteilung von schadhafte Softwareupdates führte, oder die ungetesteten Sicherheitspatches von CrowdStrike, die 2024 zu einem weltweiten Ausfall von Windows-Betriebssystemen führte.

Die Ursache für Softwareschwächen liegt meist in mangelhafter Programmierung, der Verwendung ungeprüfter Open-Source-Codes und fehlendem Qualitätsmanagement in der Entwicklungsphase. Notwendig wären mehrschichtige Verteidigungsmechanismen und Funktionstests, gefolgt von unabhängigen Tests, um diese Softwareschwächen zu vermeiden.

Eine geringere Produktqualität kann auch entstehen, wenn relevante Standards nicht in die Fertigungsprozesse integriert oder standardisierte Sicherheitsfunktionen nicht implementiert wurden. Eine weitere Ursache sind absichtlich installierte Sicherheitslücken (z. B. Malware) in einer nicht durchgängig überwachten und kontrollierten Lieferkette oder wenn Software von nicht vertrauenswürdigen oder sicheren Plattformen verwendet wird. Diese können beispielsweise zur Manipulation eines Netzwerks oder Teilen davon missbraucht werden. Solche Manipulationen können von einzelnen Angreifern, der organisierten Kriminalität oder auch im Auftrag einer staatlichen Organisation durchgeführt werden.

Hinsichtlich der Sicherheit der Lieferkette setzen Schweizer Betreiber geeignete und bewährte Instrumente ein. Dazu gehören unter anderem internationale Standards und Normen wie ISO 28000. Ein ordnungsgemässes Lieferketten-Risikomanagement umfasst zudem die Bewertung und Prüfung des Lieferkettenmanagements und der Vertrauenswürdigkeit der Lieferanten, die Sicherstellung, dass Hard- und Software bei der Auslieferung einer binären Äquivalenzprüfung (Manipulationssicherheit) unterzogen werden, sowie Labortests vor der Integration in Live-Netzwerkumgebungen.

**Abhängigkeit von einem einzelnen Lieferanten:** Nicht nur im Bereich der Cybersicherheit stellen einseitige Abhängigkeiten von einzelnen Schlüssellieferanten ein Betriebsrisiko dar. Dies haben beispielsweise die Lieferengpässe während der Corona-Pandemie eindrücklich gezeigt, als diverse Komponenten nur mit langer Lieferfrist verfügbar waren. Auch politisch motivierte Handelskonflikte mit entsprechenden Sanktionen sowie generell Knappheit von Schlüsselprodukten oder -rohstoffen können zur Schwächung der Cybersicherheit führen.

Der Telekommarkt in der Schweiz ist durch einen starken Infrastrukturwettbewerb geprägt. Die drei Mobilfunknetzbetreiber arbeiten dabei mit unterschiedlichen Lieferanten zusammen und verfügen zudem über ein ausgereiftes Risiko- und über ein Business Continuity Management, was die Resilienz der gesamten Versorgung erhöht und damit das Risiko für die Schweiz reduziert.

**Einsicht in Datenströme und Infrastrukturen durch Lieferanten und Dienstleister:** Beim Betrieb komplexer IT- und Netzwerksysteme haben Lieferanten und Dienstleister wenn erforderlich Zugang und Einblick in ausgewählte Daten. Dies ist notwendig, da diese Unternehmen mit ihrer oftmals globalen Expertise den Netzbetreiber unterstützen. Der unbefugte Zugriff sowie Manipulation oder Verlust kritischer Daten stellt jedoch ein wesentliches Risiko dar. Dieses muss durch technische, organisatorische und prozessuale Sicherheitsmassnahmen durch den Netzbetreiber kontrolliert sowie minimiert werden.

Grundlage ist eine Risikobewertung basierend auf Vertraulichkeit, Integrität und Verfügbarkeit, wodurch die notwendigen Schutzstandards insbesondere für kritische Infrastrukturen und Daten festgelegt werden. Daten in IT- und Telekommunikationssystemen werden durch strikte Zugriffsrechte und eindeutige Klassifizierungen geschützt. Technische und organisatorische Massnahmen wie Zugriffsbeschränkungen, Protokollierung und definierte Rollen lassen Manipulationen erkennen und bekämpfen. Für externe Dienstleister gelten verbindliche Sicherheitsprüfungen und sie müssen – und dies gilt auch für Lieferanten – konkreten Compliance-Richtlinien folgen.

Zusätzliche Massnahmen wie die Härtung der Systeme, Multi-Faktor-Authentifizierung und erhöhte Überwachung stärken die Cyberresilienz zusätzlich und blockieren potenzielle unrechtmässige Zugriffswege. Durch Zertifizierungen wie ISO 27001 werden entsprechende Vorkehrungen regelmässig durch externe Auditoren überprüft.

**Schwachstellen-Management:** Schwachstellen lassen sich nie vollständig vermeiden und sind in diesem Sinne auch keine Produktfehler. Das kontinuierliche Überprüfen und Testen von Produkten, die Analyse und Nachverfolgung von Schwachstellen sowie die koordinierte Offenlegung und Behebung von Sicherheitslücken, zählen deshalb zu den wichtigsten Aktivitäten im Bereich der Cybersicherheit. Dazu gehören auch Bug-Bounty-Programme, die von einzelnen Netzbetreibern durchgeführt werden. Eine gute Cybersicherheits-Praxis misst dabei dem Schwachstellenmanagement über den gesamten Produktlebenszyklus aller Netzkomponenten hinweg eine hohe Bedeutung bei. Dabei gilt das Schwachstellenmanagement als gemeinsame Verantwortung der Netzbetreiber und Lieferanten.

Lieferanten müssen regelmässig nach möglichen Schwachstellen bei der eigenen Forschung und Entwicklung, bei Open-Source-Bestandteilen sowie bei Komponenten von Drittanbietern suchen. Robuste Prozesse (z. B. gemäss ISO 30111) sind zu etablieren, um Produkte mit Schwachstellen unverzüglich zu identifizieren und Massnahmen zu ergreifen. Die Massnahmen sollen im Rahmen eines koordinierten Offenlegungsverfahrens verbunden mit Security Notices und Security Advisories erfolgen (z. B. gemäss ISO 29147).

Eine wichtige Rolle im Schwachstellen-Management übernehmen die Betreiber von Geräten oder Netzkomponenten. Sie müssen ein Asset- und Lifecycle-Management-System implementiert haben, regelmässige Software-Updates und Sicherheits-Patches durchführen und die Anweisungen der Lieferanten zur Behandlung identifizierter Schwachstellen beachten.

### 3. Zusätzliche Sicherheitsfunktionen in 5G-Netzen

Technisch gesehen bietet der 5G-Standard deutlich mehr Sicherheit als die Vorgänger-Technologien. Zu den neuen Eigenschaften und Funktionalitäten im Vergleich zu 3G/4G gehören insbesondere:

- Der striktere Authentifizierungsprozess beim Anmelden am Funknetz.
- Die Möglichkeit stärkerer Verschlüsselung der Daten.
- Die Sicherung und Trennung der Komponenten im Netz mit neuen kryptografischen Lösungen. Sollten einzelne Komponenten angegriffen werden, ist der Schutz anderer Komponenten weiterhin gewährleistet.
- Die verschlüsselte Übertragung der Langzeitidentität der Teilnehmer (IMSI), wodurch Man-in-the-Middle-Attacken mit Hilfe von IMSI-Catchern nahezu verunmöglicht werden.
- Die Authentication Confirmation beim Roaming; dabei sendet das Gerät eines Nutzers einen kryptografischen Beweis über die Identität des Mobilfunkbetreibers, in dessen Netzwerk sich das Gerät eingewählt hat, zurück an den heimischen Mobilfunkbetreiber. Dieser verifiziert die Identität des Geräts und des ausländischen Netzes.
- End-to-End-Signalisierungssicherheit nach dem Prinzip «Security by Design» zwischen den 5G-Kernnetzen verschiedener Betreiber.

Diese und weitere Mechanismen tragen dazu bei, dass 5G-Netze deutlich sicherer sind als frühere Mobilfunkgenerationen. Zudem wurden zusätzliche Sicherheitsprotokolle implementiert, um neue Bedrohungen wie «Fake Base Stations» oder «Netzdowngrade-Angriffe» auf Endgeräte der Kundinnen und Kunden zu verhindern. Aktuell haben Schweizer Betreiber neben 5G auch 5G-Stand-Alone (5G SA) in Betrieb genommen. 5G SA funktioniert vollständig unabhängig von der 4G-Infrastruktur und insbesondere auf den zentralen Betriebssystemen

(sogenanntes Core-Netz). Neben weiteren Qualitätssteigerungen in der Versorgung bietet 5G SA auch weitere Sicherheitsverbesserungen.

Neben den erweiterten Funktionalitäten von 5G und 5G SA sind folgende Aspekte und technologische Entwicklungen für die Cybersicherheit der Mobilfunknetze sowie grundsätzlich von Kommunikationsnetzen von Bedeutung:

**Cloud-native** ist ein Software-Entwicklungsansatz, bei welchem die Nutzung von Cloud-Computing-Umgebungen in eigenen oder externen Rechenzentren im Zentrum steht. Cloud-native Software nutzt bewährte Verfahren wie Microservices, Container und Continuous Deployment. Die Vorteile liegen in der hohen Effizienz und Innovationsgeschwindigkeit im Betrieb der Netze. Sie ermöglicht die Skalierung von Funktionen, die schnelle Einführung neuer Funktionalitäten und eine verstärkte Automatisierung. Dies stärkt die Wettbewerbsfähigkeit der Unternehmen, ist jedoch gleichzeitig auch die Voraussetzung für die wirkungsvolle Bekämpfung von Cyberangriffen.

Auch moderne Netzwerkarchitekturen sind Cloud-native konzipiert und standardisiert. Für die Sicherheit sind diese neuen Möglichkeiten und Netzwerkarchitekturen vorteilhaft, etwa weil Schwachstellen durch Softwareaktualisierungen rasch und automatisiert behoben werden können und nicht in die Hardware eingegriffen werden muss. Gleichzeitig steigt damit aber auch die Bedeutung von Drittanbietern, die Updates in der notwendigen Kadenz und Qualität bereitstellen müssen.

**Künstliche Intelligenz (KI):** Die Verfügbarkeit und Nutzung von künstlicher Intelligenz stellt eine fundamentale Herausforderung für die Cybersicherheit dar. Dies gilt nicht nur für die Kommunikationsinfrastrukturen, sondern grundsätzlich für alle IT-basierten Systeme und Anwendungen. KI-basierte Tools ermöglichen das rasche Aufspüren von Schwachstellen, die dann für Cyberangriffe ausgenutzt werden können. Ziel dieser Angriffe ist potenziell jedes vernetzte System oder Gerät, da mit Hilfe von KI-Anwendungen auch eine schrittweise Infiltration – im Vergleich mit menschlichen Akteuren – rasch möglich ist.

Die Mobilfunknetzbetreiber sind dieser Entwicklung jedoch nicht schutzlos ausgeliefert. Die Cybersicherheit wird durch spezialisierte Teams und Organisationen aktiv und laufend überwacht. Dabei steht nicht nur der Schutz der Mobilfunknetze im Zentrum, sondern auch der Endgeräte der Nutzerinnen und Nutzer. Dabei können Netzbetreiber zunehmend selbst auf KI-Tools zur Überwachung der Datenströme in ihren Netzen zurückgreifen und damit rasch und automatisiert Auffälligkeiten oder Angriffe erkennen, bewerten und bekämpfen.

Das bedeutet jedoch auch, dass die in den Netzen verwendeten KI-Komponenten den Sicherheits- und Datenschutzanforderungen entsprechen müssen. Um den Nutzen von KI zu erhöhen, sollte die Zusammenarbeit zwischen privaten und öffentlichen Akteuren gefördert werden. Sie ist der vielversprechendste Weg, die Cyberabwehr zu stärken und so die Sicherheit der Nutzerinnen und Nutzer sowie die Stabilität der Mobilfunknetze zu gewährleisten.

**Internet-Technik:** Moderne Kommunikationsnetze wie 5G basieren weitgehend auf den Internet-Protokollen und weniger auf telekommunikationsspezifischen Protokollen. Aus Perspektive der Sicherheit hat dies einerseits den Nachteil, dass Angreifer das breite Spektrum an internetbasierten Angriffsmethoden zur Verfügung steht. Sie müssen sich also nicht zuerst mit den Eigenheiten von Kommunikationsnetzen auseinandersetzen. Andererseits sind diese Angriffsmethoden besser bekannt und es gibt bewährte Konzepte und Protokolle (beispielsweise Verschlüsselung wie TLS), mit welchen man ihnen begegnen kann.

**Network Slicing:** Diese Technik ermöglicht das Bereitstellen von verschiedenen virtuellen Netzen auf einer gemeinsamen physischen Netzwerkinfrastruktur. Die einzelnen Slices erfüllen die Anforderungen an Übertragungsraten, Latenzzeiten, Reichweiten, Verfügbarkeiten oder maximale Gerätedichte der verschiedenen Anwendungsfälle. So stellen etwa Multimediaanwendungen andere Netzwerkanforderungen als Endgeräte des Internets der Dinge

(IoT). Die Eigenschaften lassen sich ohne Eingriff in die Hardware anpassen. Network Slicing kann auch dazu genutzt werden, system- oder unternehmenskritische Anwendungen vom übrigen Netz abzukoppeln und speziell abzusichern.

**Dezentralisierung:** 5G verfügt über eine dezentralere Architektur als frühere Mobilfunkgenerationen und verlagert Funktionen sowie Datenverarbeitung gezielt an den Rand des Netzes. Durch Mobile Edge Computing (MEC) wird Intelligenz näher zu den Nutzenden gebracht, was eine lokale, kontrollierte und ressourcenschonende Datenverarbeitung ermöglicht. Aus Cybersecurity-Sicht unterstützt diese Architektur eine verbesserte Sicherheitsarchitektur, da sicherheitsrelevante Funktionen näher an den Entstehungsort der Daten umgesetzt, Netzsegmente stärker isoliert und zentrale Abhängigkeiten reduziert werden können. Wenngleich sich die Angriffsfläche bei einer Dezentralisierung praktisch erhöht, so stärkt diese bei geeigneter Umsetzung dennoch die Resilienz und die Abwehrfähigkeit der Infrastruktur.

## 4. Rechtliche Grundlagen in der Schweiz

Die in der Schweiz gültigen rechtlichen Grundlagen zur Sicherheit von Telekommunikationsnetzen sind für alle Mobilfunkgenerationen sowie auch für zukünftige Generationen anwendbar. Relevant sind in erster Linie:

- Das Fernmeldegesetz (FMG) – es regelt insbesondere die zuverlässige Versorgung der Schweiz mit Fernmeldediensten, die Grundversorgung, den störungsfreien Betrieb, die Persönlichkeitsrechte und den Wettbewerb.
- Die Verordnung über Fernmeldedienste (FDV) – sie legt die Rahmenbedingungen für die Erbringung von Telekommunikationsdiensten in der Schweiz fest, einschliesslich, aber nicht beschränkt auf Regelungen zum Telekommunikationsgeheimnis. Sie enthält ausserdem Sicherheitsanforderungen, die für Betreiber von Telekommunikationsnetzen gegen die „unbefugte Manipulation von Telekommunikationssystemen“ gelten. Dazu gehören insbesondere der Betrieb eines Informationssicherheitsystems (ISMS) und eines Business-Continuity-Managementsystems (BCM).
- Das Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG) – es bezweckt den Schutz der Persönlichkeit und der Grundrechte von Personen, deren Personendaten verarbeitet werden. Die überarbeitete Fassung, die im September 2023 in Kraft trat, ist auch auf die europäischen DSGVO-Grundsätze abgestimmt.
- Die Nationale Cybersicherheitsstrategie (NCS 2023) – sie zeigt auf, mit welchen Zielen und Massnahmen der Bund und die Kantone gemeinsam mit der Wirtschaft und den Hochschulen den Cyberbedrohungen begegnen wollen.
- Das Informationssicherheitsgesetz (ISG) – es verpflichtet Betreiber kritischer Infrastrukturen sowie Regierungs- und Verwaltungsstellen zur Aufrechterhaltung eines angemessenen Risikomanagements und eines Informationssicherheitsmanagementsystems (ISMS), sowie zur Meldung von Cybersicherheitsvorfällen an das Nationale Zentrum für Cybersicherheit (BACS).

## 5. Organisationen, welche die Mobilfunk-Sicherheit voranbringen

### International

Auf internationaler Ebene entwickeln und pflegen verschiedene Organisationen Empfehlungen, Standards und Instrumente für die Mobilfunk-Sicherheit. Sie berücksichtigen dabei die Weiterentwicklung technologischer Standards sowie die laufend entstehenden neuen Bedrohungslandschaften. Zu wichtigen Organisationen gehören:

- Die Europäische Union, unter anderem via ihre Agentur für Cybersicherheit ENISA (European Network and Information Security Agency)
- Das Europäische Institut für Telekommunikationsnormen ETSI (European Telecommunications Standards Institute) ist eine der drei grossen Normungsorganisationen in Europa und verfolgt das Ziel, weltweit anwendbare Standards für die Informations- und Kommunikationstechnik zu schaffen.
- Die International Organization for Standardization (ISO) ist der weltweite Zusammenschluss nationaler Normungsorganisationen und veröffentlicht internationale Standards in nahezu allen Bereichen, mit Ausnahme der Elektro- und Elektroniktechnik (dieser Bereich wird primär durch die IEC abgedeckt). Für die Mobilfunkindustrie sind insbesondere jene ISO-Standards relevant, die Qualitätsmanagement, Sicherheits- und Datenschutzprozesse sowie das Business-Continuity-Management betreffen. Diese Standards unterstützen Unternehmen dabei, sichere, robuste und regelkonforme Sicherheitsprozesse über den gesamten Lebenszyklus von Mobilfunknetzen hinweg zu gewährleisten.
- Das 3rd Generation Partnership Project (3GPP) ist eine weltweite Kooperation von Standardisierungsgremien für die Standardisierung im Mobilfunk; konkret für GSM, UMTS, LTE und 5G/NR. Ihr Ziel ist es, technische Spezifikationen, Protokolle und Schnittstellenstandards zu entwickeln, die alle Aspekte der Mobilfunktechnik so präzise beschreiben, dass die Mobilgeräte aller Lieferanten in allen Mobilfunknetzen fehlerfrei funktionieren und Netzwerkelemente verschiedener Lieferanten miteinander kommunizieren können. Dazu gehört auch die Informationssicherheit.
- Die GSM Association (GSMA) ist die weltweite Industrievereinigung der Mobilfunkindustrie, Lieferanten sowie weiterer Akteure aus der Telekommunikationsbranche. Zusammen mit 3GPP hat sie das Network Equipment Security Assurance Scheme (NESAS) entwickelt. Diese Initiative bietet einen Rahmen für die Förderung der Sicherheit in der gesamten Mobilfunkbranche und steht allen Anbietern von Netzwerkausrüstungen offen, die von 3GPP definierte Funktionen unterstützen. Zudem hat die GSMA das weltweit umfassendste und international am weitesten anerkannte Cybersicherheits-Framework entwickelt und betreibt dieses in der sogenannten Mobile Cybersecurity Knowledge Base (MCKB). Sie dient als zentrale Informationsplattform, die Mobilfunknetzbetreiber, Ausrüster und Regulierungsbehörden dabei unterstützt, Cybersicherheitsbedrohungen zu adressieren und die Sicherheit von Mobilfunknetzen und -diensten zu stärken. Angesichts ihrer Bedeutung für Netzbetreiber sind weiterführende Informationen zur MCKB im Anhang zu finden.
- Das National Institute of Standards and Technology (NIST) ist eine Bundesbehörde der Vereinigten Staaten. Es ist unter anderem für Standardisierungsprozesse verantwortlich, einschliesslich solcher im Bereich der Cybersicherheit, wozu insbesondere das weit verbreitete Cybersecurity Framework (CSF) gehört. Darüber hinaus widmet NIST dem Thema 5G-Sicherheit besondere Aufmerksamkeit und behandelt dieses ausführlich in seiner Special Publication zur 5G-Cybersicherheit (SP 1800-33B).
- Die Internationale Fernmeldeunion (englisch International Telecommunication Union, ITU) ist eine Sonderorganisation der Vereinten Nationen und die einzige völkerrechtlich verankerte Organisation, die sich weltweit mit technischen Aspekten der Telekommunikation beschäftigt. Sie ist Veranstalterin der Weltfunkkonferenz (World Radiocommunication Conference, WRC), welche die Vollzugsordnung für den Funkdienst (Radio Regulations, RR) fortschreibt, sowie der Weltweiten Konferenz für internationale Fernmeldedienste (World Conference on International Telecommunications, WCIT), die die Vollzugsordnung für internationale Fernmeldedienste (International Telecommunication Regulations, ITR) fortschreibt.

- Die Transported Assets Protection Association (TAPA) gibt Standards zur Sicherheit von Betriebsstätten und von Transporten heraus. Diese decken einen Teil der Risiken in der Lieferkette ab.
- Die Digital Geneva Convention steht unter der Schirmherrschaft des NIST Cybersecurity Framework und hat sich zum Ziel gesetzt, Zivilpersonen vor staatlich geförderten Cyberangriffen zu schützen. Das Eidgenössische Departement für auswärtige Angelegenheiten (EDA) nimmt hier eine führende Rolle ein und kofinanziert das Projekt.

## National

Das neu geschaffene Bundesamt für Cybersicherheit (BACS) ist das Kompetenzzentrum des Bundes für Cybersicherheit und für die koordinierte Umsetzung der Nationalen Cyberstrategie (NCS) zuständig. Neben Lagebeurteilung und technischer Expertise unterstützt das BACS insbesondere die kritischen Infrastrukturen bei Cybervorfällen. Dazu gehören gemäss Informationssicherheitsgesetz auch die Telekommunikationsnetze. Damit unterliegen die Telekomanbieter auch der Meldepflicht für Cybervorfälle.

Das Fernmeldegesetz verpflichtet die Telekomanbieter, die unbefugte Manipulation von Fernmeldeanlagen durch fernmeldetechnische Übertragung zu bekämpfen. Dazu gehören insbesondere auch Cyberangriffe auf die Telekominfrastruktur. Zur Stärkung der Cybersicherheit bestehen auf Verordnungsstufe Vorgaben zu Sicherheitsmanagementsystemen sowie zum Betrieb sicherheitskritischer Fernmeldeanlagen. Das Bundesamt für Kommunikation überwacht den Vollzug dieser Auflagen und kann zusätzliche Vorschriften zur Konkretisierung von Gesetz und Verordnung erlassen.

Das Nationale Testinstitut für Cybersicherheit (NTC) in Zug wurde im November 2020 gegründet. Als unabhängige Schweizer Organisation führt es seit 2022 Cybersecurity-Tests für Käufer und Betreiber von vernetzten Komponenten durch. Partner und Unterstützter des NTC sind unter anderen der Kanton Zug sowie das Bundesamt für Cybersicherheit (BACS).

## 6. Standards, Normen, Empfehlungen zur Mobilfunk-Sicherheit

Die oben erwähnten Organisationen geben die für die Branche relevanten Standards, Normen und Empfehlungen bezüglich Sicherheit heraus. Einige davon betreffen spezifisch 5G, andere sind allgemein in den Informations- und Kommunikationstechnologien (IKT) anwendbar und weitere gelten allgemein für die Wirtschaft. Diese Werkzeuge bieten umfassende Orientierung und ermöglichen den Schweizer Betreibern, eine eigene Strategie zu entwickeln und umzusetzen. Zu den wichtigsten Standards, Normen und Empfehlungen gehören:

		Wirkungsebene	
Instrument	Beschreibung	Betreiber	Lieferant
<b>Norm ISO 27001</b> (Information security management)	<p>Legt die Anforderungen für Herstellung, Einführung, Betrieb, Überwachung, Wartung und Verbesserung eines dokumentierten Informations-Sicherheits-Managementsystems (ISMS) fest. Um Datenschutz und Informationssicherheit ganzheitlich gewährleisten zu können, werden auch individuelle IT-Risiken innerhalb der gesamten Organisation berücksichtigt. Alle Schweizer Betreiber pflegen ein ISMS.</p> <p>Die Norm ist umfassend, breit anerkannt, und zertifizierbar. Sie gilt generell für Datennetze und wird in der Schweiz von vielen Telekomgrosskunden angewendet.</p> <p>Mit der Richtlinie ISO 27001/2 liegt auch eine Beschreibung der Best-Practice für die Umsetzung vor.</p>	X	X
<b>Standard ISO 27701</b> (Privacy Information Management System)	<p>Diese Norm bietet einen Rahmen für ein Privacy Information Management System (PIMS) und stellt eine Datenschutz-Erweiterung zu ISO 27001 dar. Sie gibt konkrete Empfehlungen zum Umgang mit personenbezogenen Daten. Dies ist insbesondere relevant für den Betrieb und die Verwaltung sensibler Netzdaten unter Einhaltung der geltenden gesetzlichen Vorgaben, wie dem Datenschutzgesetz (DSG) und der dazugehörigen Datenschutzverordnung (FDV).</p>	X	X
<b>EU-Toolbox für 5G-Sicherheit</b>	<p>Ihr Kern ist ein risikobasierter Massnahmenkatalog zur 5G-Sicherheit. Die Toolbox deckt alle in der EU in 5G-Netzen eingesetzten Produkte ab (sowohl reine 5G-Komponenten, als auch sonstige Komponenten der IKT) und gilt für alle Betreiber respektive deren 5G-Netze in der EU.</p>	X	X
<b>Norm ISO 22301</b> (Security and resilience - Business continuity management systems)	<p>Ziel der Norm ist es, unabhängig von der Branche sicherzustellen, dass Organisationen über ein Managementsystem verfügen, das es ihnen ermöglicht, ihre wichtigsten Geschäftsaktivitäten auch bei Störungen jeglicher Art fortzuführen, etwa bei Cyberangriffen, Naturkatastrophen oder Unterbrechungen der Lieferkette. Die Norm richtet sich an die gesamte ICT-Branche und ist zertifizierbar.</p>	X	

		Wirkungsebene	
Instrument	Beschreibung	Betreiber	Lieferant
<b>Norm ISO 20243</b> (Open Trusted Technology Provider Standard (O-TTPS) - Mitigating maliciously tainted and counterfeit products)	Liefert eine Reihe von Richtlinien, Anforderungen und Empfehlungen, die spezifische Bedrohungen der Integrität von Hard- und Software während des gesamten Produktlebenszyklus betreffen. Insbesondere behandelt sie auch Bedrohungen im Zusammenhang mit böswillig manipulierten Produkten. Die Norm ist praxistauglich ausgelegt und zertifizierbar.		X
<b>GSMA MCKB</b> (Mobile Cybersecurity Knowledge Base)	<p>Die MCKB erleichtert und fördert die Zusammenarbeit, um Netzwerke und Dienste vor Störungen und unbefugtem Zugriff zu schützen, sowie Risiken zu verhindern und zu mindern. Auf operativer Ebene bietet die MCKB klare, schrittweise Anleitungen, um Sicherheitsnachweise zu schaffen und dabei das gesamte Risikospektrum von Ende-zu-Ende-Mobilfunknetzen zu berücksichtigen.</p> <p>Mit dem branchenweit fortschrittlichsten und umfassendsten Set an Sicherheitsmassnahmen und Regelwerken, fungiert die MCKB als Brücke zwischen den Anforderungen der Aufsichts- und Compliance-Verpflichtungen der Betreiber, der Verbesserung der Sicherheitsresilienz sowie der Ermöglichung von Anwendungssicherheit. Darüber hinaus unterstützt sie beim Aufbau von Sicherheitsfähigkeiten für die Planung, den Betrieb und die Wartung von Mobilfunknetzen.</p>	X	X
<b>NESAS-Schema</b> (Network Equipment Security Assurance Scheme)  <b>SCAS</b> (Security Assurance Specification)	Ein von 3GPP und GSMA definiertes Konzept, das die Sicherheit in der gesamten Mobilfunkbranche adressiert. Es definiert Anforderungen und einen Bewertungsrahmen für die sichere Produktentwicklung und einen sicheren Produktlebenszyklus. Insbesondere empfiehlt es den Einsatz von Sicherheitstest von Netzkomponenten gemäss den Vorgaben der 3GPP. In der aktuellen Fassung basiert NESAS noch auf Selbstdeklaration, in der nächsten Version wird es zertifizierbar sein. Die grossen Netzkaufrüster haben eine Bewertung ihrer Produktentwicklungs- und Lifecycle-Management-Prozesse mit NESAS erfolgreich abgeschlossen. Das NESAS-Schema ist spezifisch auf Mobilfunknetze ausgerichtet. Unternehmen können sich nach ihm auditieren lassen und die Audit Reports sind bei GSMA öffentlich einsehbar <a href="http://www.gsma.com/">http://www.gsma.com/</a> . Das NESAS-Schema wird auch eine Rolle bei der von der		X

		Wirkungsebene	
Instrument	Beschreibung	Betreiber	Lieferant
	<p>EU angestossenen Sicherheitszertifizierung für 5G spielen.</p> <p>GSMA SCAS beschreibt Sicherheitsanforderungen und Testfälle, um die Sicherheit von Mobilfunk-Netzwerkprodukten im Rahmen des NESAS-Verfahrens zu bewerten.</p>		
<p><b>Norm ISO/IEC 15408 Common Criteria (CC)</b></p> <p>und <b>European CC (EUCC)</b></p>	<p>Der international anerkannte Standard zur Bewertung der Sicherheit von Informationstechnologie-Produkten. Er bietet einen Rahmen, um Sicherheitsmerkmale standardisiert zu spezifizieren, umzusetzen und zu evaluieren.</p> <p>EUCC, das European Cybersecurity Certification Scheme, ist ein neues Rahmenwerk der Europäischen Union zur Zertifizierung der Cybersicherheit von IKT-Produkten, -Dienstleistungen und -Prozessen. Das Schema baut auf dem Common-Criteria-Standard sowie der Common Evaluation Methodology (ISO/IEC 18045) auf und stellt sicher, dass IKT-Produkte hohe Sicherheitsanforderungen durch einen strukturierten Prüf- und Bewertungsprozess erfüllen.</p>		X
<p><b>ETSI-Spezifikation TS 133.501 / 3GPP TS 33.501</b></p> <p>(Security architecture and procedures for 5G System)</p>	<p>Spezifikation zur Sicherheitsarchitektur, also zu den Sicherheitsfunktionen und den Sicherheitsmechanismen für 5G-Netze. Abgedeckt werden auch die Sicherheitsverfahren, die innerhalb des 5G-Systems einschliesslich des 5G-Kernnetzes und des 5G-New-Radios durchgeführt werden. Die Spezifikation ist zertifizierbar und ihr zu folgen ist Pflicht, sowohl für Betreiber als auch für Lieferanten.</p>	X	X
<b>NIST-Standards</b>	<p>Diverse IKT-Sicherheitsstandards des US-amerikanischen National Institute of Standards and Technology (NIST). Sie sind auf die Rahmenbedingungen in den USA zugeschnitten und nicht generell auf die Schweiz übertragbar. Die Standards sind zertifizierbar und haben inhaltliche Überschneidungen mit ISO 27001.</p>	X	X
<p><b>C-TPAT</b></p> <p>(Customs-Trade Partnership Against Terrorism)</p>	<p>Ein in öffentlich-privater Partnerschaft erarbeitetes Programm unter Leitung der Zoll- und Grenzschutzbehörde der USA für den erhöhten Schutz der Lieferkette privater Unternehmen zum Schutz vor Terroranschlägen. Dies erhöht auch den Schutz von IKT-Equipment vor Manipulationen während dem Transport. Nach C-TPAT kann zertifiziert werden. Auch</p>		X

		Wirkungsebene	
Instrument	Beschreibung	Betreiber	Lieferant
	wenn es sich dabei um ein US-amerikanisches Regelwerk handelt, bietet es praktische Ansätze zum Verbessern der Produktsicherheit.		
<b>TAPA-Standards</b> (Transported Assets Protected Association)	Standards für Sicherheit in Betriebsstätten (Facility Security Requirements, FSR) und für den Transport (Trucking Security Requirements). TAPA sind weltweit akzeptierter Industriestandards und als solche zertifizierbar.		X
<b>Norm ISO 28000</b> (Specification for security management systems for the supply chain)	Bietet eine umfassende Grundlage für das Sicherheitsmanagement in Lieferketten (Supply Chains). Insbesondere ermöglicht sie es, ein vollständiges System für die Sicherheit in der Lieferkette aufzubauen. Die Norm ist spezifisch auf die Sicherheit in der Logistik ausgerichtet und kann zertifiziert werden. Sie ergänzt insofern die ISO 27000, die sich mit Produktsicherheit befasst.		X
<b>Norm ISO 29147</b> (Vulnerability Disclosure)	Diese Norm legt Richtlinien und Anforderungen für die Meldung von Schwachstellen in Produkten und Dienstleistungen fest. Sie beschreibt, wie Hersteller mit Berichten über potenzielle Sicherheitslücken umgehen sollen.		X
<b>Norm ISO 30111</b> (Vulnerability Management)	Dies ist eine international anerkannte Leitlinie und Empfehlung zur Etablierung robuster Prozesse für den Umgang mit potenziellen Schwachstellen in Produkten und Dienstleistungen.		X
<b>Geneva Manual</b>	Das Manual ist ein praxisorientierter Leitfaden, um die Sicherheit und Stabilität im digitalen Raum zu fördern. Es dient als Referenzwerk für Unternehmen und andere nicht-staatliche Akteure, um abstrakte internationale Cybersicherheits-Normen in konkrete Handlungen umzusetzen.	X	X

## 7. Massnahmen für die Mobilfunk-Sicherheit

### Bei den Mobilfunknetzbetreibern

Massnahmen, Prozesse und Organisationen der Mobilfunknetzbetreiber im Bereich der Cybersicherheit haben sich grundsätzlich bewährt und werden fortgeführt. Sie müssen jedoch laufend an neue Bedrohungslagen sowie an die Weiterentwicklung der Mobilfunktechnologie angepasst werden.

Gesetzliche Rahmenbedingungen bilden dabei die Grundlage, während die Branche zusätzliche Sicherheitsmassnahmen einsetzt – getrieben durch Kundenanforderungen, bewährte

Industriestandards und eigene Sicherheitsinteressen. Dazu gehört insbesondere, dass die Betreiber die Kontrolle über die zentralen Systeme, den Kommunikationsverkehr sowie die Kundendaten haben. Lieferanten oder Dienstleister können nur mit dem Einverständnis der Betreiber und kontrolliert durch diese darauf zugreifen. Zudem stützt sich die Branche auf technik- und herstellerneutrale internationale Standards, Normen und Empfehlungen. Dies hat auch den Vorteil, dass rascher auf neue Entwicklungen, Anforderungen und Risiken reagiert werden kann, als dies im Rahmen des Gesetzgebungsprozess möglich wäre.

Für die Informationssicherheit nimmt der Standard ISO 27001 (Information Security Management System) eine zentrale Funktion ein, ergänzt durch die detaillierten Vorgaben aus ISO 27002. Zu seinen wichtigsten Vorteilen gehören:

- Er ist universell, international anerkannt und wird von einem neutralen Gremium herausgegeben. Die Anwendung des Standards kann zertifiziert werden.
- Er wird verbreitet angewendet und hat sich auch in anderen Branchen bewährt. So referenziert etwa der Verband Schweizerischer Elektrizitätsunternehmen VSE in seinem Handbuch zur Umsetzung von OT-Sicherheit in kritischen Infrastrukturen der Schweiz auf diesen Standard.
- Auch die Geschäftskunden der Telekommunikationsunternehmen nutzen den weit verbreiteten Standard. Grosse Geschäftskunden verlangen zunehmend eine entsprechende Zertifizierung als Grundvoraussetzung für die Zusammenarbeit mit Anbietern.
- Er berücksichtigt auch die individuellen IT-Risiken innerhalb einer Organisation und hilft, Datenschutz und Informationssicherheit ganzheitlich zu gewährleisten
- Er wird von den Schweizer Telekomanbietern angewendet.

Als spezialisierte und branchenweit unterstützte Sicherheitslösung bieten die in der GSMA MCKB definierten technischen Massnahmen einen umfassenden Ansatz zur Minderung gezielter Risiken und werden voraussichtlich in naher Zukunft zertifizierbar sein.

## In der Lieferkette

Wie bereits erwähnt führt der Infrastrukturwettbewerb mit drei unabhängigen Mobilfunknetzen zu einer Stärkung der Resilienz bei dieser kritischen Infrastruktur. Der Grund liegt unter anderem darin, dass die drei Netzbetreiber neben dem Risikomanagement auch unterschiedliche Lieferanten für die Ausrüstung der verschiedenen Netzwerklayer beziehen. Der Ausfall eines Netzes oder Lieferschwierigkeiten eines Lieferanten können daher kompensiert werden. Damit ist die Schweizer Mobilfunkinfrastruktur in sich bereits resilient.

Zur Sicherheit der Mobilfunknetze trägt weiter bei, dass die Lieferanten ihrerseits ständig daran arbeiten, die Qualität ihrer eigenen Lieferkette zu sichern. Als Basis hierfür dient ihnen die Norm ISO 28000. Die relevanten Transport- und Logistikunternehmen sowie Lieferanten von wichtigen Netzkomponenten sind nach ihr zertifiziert, was bereits für eine Grundsicherheit sorgt. Zur Behandlung von spezifischen Risiken werden beispielsweise folgende weitere Standards herbeigezogen:

- ISO 20243 (Produktintegrität)
- TAPA-Standards FSR (Facility Security Requirements,) und TSR (Trucking Security Requirements).
- C-TPAT (Schutz vor terroristischen Aktionen im Rahmen der Lieferkette)

Aus Sicht der Branche steht damit auch für die Sicherheit in der Lieferkette ein bewährtes Instrumentarium zur Verfügung. Die Mobilfunknetzbetreiber fordern von ihren Lieferanten die entsprechenden Zertifikate und Nachweise ein.

Die von ausländischen Staaten oder hochspezialisierten Organisationen ausgehende Bedrohungen können durch die Anwendung relevanter Normen und Standards reduziert, jedoch nicht vollständig ausgeschlossen werden. Wenn ein Staat entschlossen ist, Netzkomponenten zu kompromittieren, wird er in der Regel einen Weg finden. Das zeigt sich im Ukraine-Krieg, in dem staatlich unterstützte Gruppen gezielt Netzwerkinfrastrukturen angegriffen und erfolgreich kompromittiert haben.

Ein aktueller Ansatz zur Erhöhung der Produktsicherheit ist das National Test Center for Cyber Security (NTC), das 2022 gegründet wurde und vom Kanton Zug sowie vom Nationalen Zentrum für Cybersicherheit (NCSC) unterstützt wird. Dort können vernetzte Komponenten systematisch auf Schwachstellen getestet werden.

Ein wichtiger, jedoch langfristig ausgelegter Ansatz ist die Initiative «Digital Geneva Convention» unter dem Patronat des UNHCR. Sie hat sich zum Ziel gesetzt, ähnlich wie die Menschenrechtskonvention, eine internationale Übereinkunft zur Sicherheit in der IKT zu etablieren. Damit zielt sie vor allem auf Staaten, welche die Cybersicherheit durch Manipulationen an Geräten und Komponenten gefährden.

## 8. Exkurs: Sicherheit im Internet der Dinge (IoT)

Neben den Sicherheitsrisiken im Zusammenhang mit dem Betrieb der Mobilfunknetze und der Lieferkette entstehen auch auf der Anwendungsseite neue Risiken. So sind verschiedene Kommunikationstechnologien in der Lage, eine grosse Anzahl von Geräten mit dem Internet zu verbinden (Internet der Dinge). Hier gilt es insbesondere, die Konfiguration und den Betrieb von IoT-Geräten abzusichern. Dies ist vor allem wegen der stark steigenden Anzahl von verbundenen Geräten wichtig. Aktuell ist 5G noch nicht die wichtigste Zugangstechnologie für IoT; das wird sich aber ändern.

Prinzipiell bietet 5G die Möglichkeit, den Datenverkehr von IoT-Geräten in separaten Network-Slices abzuwickeln. Dadurch lassen sich andere Anwendungen im Netz vor Bedrohungen durch kompromittierte IoT schützen. Doch viele dieser IoT-Endgeräte sind ab Werk nicht auf Sicherheit ausgelegt und entsprechend vorkonfiguriert (Security by Design):

- Viele Geräte ab Werk verwenden unsichere Standard-Passwörter. Die Nutzer werden beim Setzen von eigenen, sicheren Passwörtern ungenügend angeleitet.
- Oft stehen nicht benötigte Schnittstellen und Ports offen, ohne dass die Nutzer darauf hingewiesen werden.
- Die Firmware der Geräte wird nicht, zu spät oder nicht über die ganze Nutzungsdauer mit Sicherheits-Updates versorgt.

Solche Risiken entziehen sich weitgehend dem Einfluss der Netzbetreiber, weil die meisten IoT-Endgeräte nicht von ihnen geliefert, betrieben oder geprüft werden können. In der Regel werden diese IoT-Geräte von den Nutzern selbst auf dem freien Markt beschafft und in eigener Verantwortung betrieben. Die dadurch entstehenden Risiken sind in der Summe relevant, weil jedes unsicher konfigurierte Endgerät ein Angriffsvektor ist und ihre Anzahl stark steigen wird.

Wie mächtig kompromittierte Endgeräte als Angriffswaffe sein können, zeigte bereits ein Vorfall von 2016 beim Internetdienstleister Dyn. Dabei wurden Hunderttausende kompromittierter Endgeräte zu einem Botnetz zusammengefügt und für eine DDoS-Attacke orchestriert. Als Folge waren die betroffenen Online-Dienste (unter anderem Twitter, Pinterest, Reddit) zeitweise gestört. Ursache war der ungenügende Schutz von Endgeräten wie Router und Überwachungskameras.

## 9. Cybersicherheit ist eine gemeinsame Verantwortung

Neue Technologien, die rasante Digitalisierung, der Bedarf an höheren Bandbreiten, schnelleren Datenübertragungsraten, geringeren Latenzen und Serviceinnovationen sind nur einige der Merkmale, die von aktuellen Mobilfunkgenerationen wie 5G und 5G Advanced abgedeckt werden. In einer sich ständig weiterentwickelnden Ära der Digitalisierung und zunehmend komplexer Netzwerke ist eine enge Zusammenarbeit zwischen Industrie, Normierungsinstitutionen, Netzbetreibern, Regulierungsbehörden sowie Nutzern unerlässlich. Nur durch diese Kooperation kann ein Gleichgewicht geschaffen werden, um maximale Cyber-Resilienz gegenüber sich stetig weiterentwickelnden Bedrohungen zu erreichen, den Innovationswettbewerb zu fördern und den Fortschritt der Digitalisierung nicht zu behindern.

## 10. Zusammenfassung Mobilfunk-Cybersicherheit in der Schweiz

In der Schweizer Mobilfunkbranche werden bewährte Verfahren angewendet, wie beispielsweise das bereits erwähnte NIST Cyber Security Framework und seine Sonderveröffentlichung für 5G-Cybersicherheit oder die noch häufiger genutzte GSMA 5G Security Knowledge Base. Darüber hinaus referenzieren Netzbetreiber teilweise auch auf die EU-Toolbox für 5G-Sicherheit, welche jedoch nur kleineren Teil der technischen Massnahmen aus der GSMA Knowledge Base enthält.

Während diese Rahmenwerke Orientierung bieten, um Netzarchitekturen sicher zu gestalten, Sicherheitskonfigurationen zu härten und Abweichungen vom Standard zu überwachen, prüfen die Netzbetreiber zusätzlich, ob Hard und Software ihrer Lieferanten von unabhängigen Stellen zertifiziert wurden. Zu nennen ist insbesondere das Network Equipment Security Assurance Scheme (NESAS), das weltweit Anerkennung findet und branchenweit als Zertifizierungsstandard für Netzwerkausrüster genutzt wird. Auch die Common Criteria Zertifizierungsstandards bieten eine unabhängige Grundlage zur Bestätigung der Konformität.

Durch die freiwillige Übernahme von EU-Konformitätserklärungen und Zertifizierungsschemata – die international an Bedeutung gewinnen und mit dem Cyber Resilience Act (CRA), sowie den neuen EU Common Criteria Vorschriften (EUCC) einheitliche Prüf- und Zertifizierungsstandards verankern werden – können Organisationen sicherstellen, dass sie den sich weiterentwickelnden regulatorischen Anforderungen entsprechen.

Informationssicherheits-, Datenschutz- und Geschäftskontinuitäts-Managementsysteme gemäss diverser ISO-Normen sind weit verbreitet, sowohl bei Netzbetreibern als auch bei Lieferanten. Diese werden teilweise sogar im Rahmen einer gemeinsamen ISO-Zertifizierung zwischen Netzbetreiber und Lieferanten angewendet, was den Vorteil von klaren Definitionen und Verantwortlichkeiten bei sämtlichen Beteiligten und ihrer gemeinsamen Aufgaben mit sich bringt.

In den vergangenen Jahren haben Schweizer Mobilfunknetzbetreiber dem Cybersicherheits-Risikomanagement eine wesentlich höhere Priorität zugewiesen, nicht nur in technischer, sondern auch in organisatorischer Hinsicht. Die Sicherheitsteams und -kompetenzen wurden fortlaufend ausgebaut, neue Prozesse und Richtlinien eingeführt und Sensibilisierungsprogramme gestartet.

Ein weiterer wichtiger Faktor, den Schweizer Betreiber in der Risikolandschaft identifiziert haben, sind Schwachstellen. Diese können nie ausgeschlossen werden und erfordern deshalb ein effektives und zeitnahes Management. Hierzu etablierten die Betreiber, direkte Verbindungen zwischen den CERT-Teams (Cyber Emergency Response Teams) und den Product Security Incident Response Teams (PSIRT) ihrer Lieferanten. Dies ermöglicht eine direkte und sichere Offenlegung bekannt gewordener Schwachstellen mit sofortigen Sicherheitswarnungen und Hinweisen, die den Betreibern Hilfestellung zur zeitnahen Behebung der

Schwachstellen oder zur Minderung der Risiken bieten. Auch das BACS (Bundesamt für Cybersicherheit) befasst sich im Rahmen des neuen Informationssicherheitsgesetzes mit diesem Risiko für alle Betreiber kritischer Infrastrukturen.

Selbst bei der Umsetzung etablierter Cybersicherheits-Best-Practices können Netzunterbrüche oder kurzfristige Dienstbeeinträchtigungen auftreten. Medienberichte der letzten zeigen, dass die Hauptursachen für Vorfälle in fehlerhaften Geräten, Software-Bugs, Interoperabilitätsproblemen in Multi-Vendor-Umgebungen sowie menschlichen Fehlern bei Wartungsarbeiten im Netzbetrieb liegen.

Um die Netzsicherheit weiter zu erhöhen und Vorfälle zu minimieren, ist es wesentlich, die Produktqualität zu verbessern, insbesondere durch die Reduktion von Hardwaredefekten und Softwarefehlern. Zudem kann die Optimierung des Change-Managements im Netzbetrieb sowie die kontinuierliche Weiterqualifizierung des technischen Personals dazu beitragen, betriebsbedingte Vorfälle wirksam zu verhindern.

Zuletzt profitieren die Netzbetreiber und die Cybersicherheit von einem innovativen und wettbewerbsorientierten Wirtschaftsstandort. Dies führt nicht nur zu einer raschen Digitalisierung mit umfangreichen, neuen und innovativen Lösungen, sondern auch zu einer stetigen und rasanten Weiterentwicklung der Cybersicherheit. Cybersicherheit ist damit mehr als nur ein «Compliance Thema» und entwickelt sich zu einem Wettbewerbsfaktor. Dies kann den Netzbetreibern auch Möglichkeiten hinsichtlich Dienstleistungen im Bereich Cyber-Security für Endkunden eröffnen.

## Anhang GSMA Mobile Cyber Security Knowledge Base

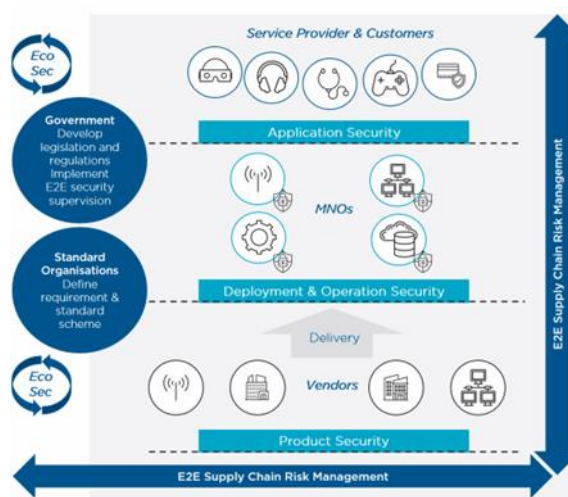
Die GSM Association (GSMA) ist der globale Branchenverband der Mobilfunknetzbetreiber, der über 750 Betreiber und 400 Unternehmen des Mobilfunk-Ökosystems weltweit vertritt. Sie fördert Innovationen (5G, IoT) und Sicherheit. Die GSMA Mobile Cyber Security Knowledge Base ist eine umfassende Ressourcensammlung zur Risikominimierung, die Best Practices, Dokumente und Sicherheitsleitfäden für Netzbetreiber und Anbieter bereitstellt.

Im Nachfolgenden wird der Grundgedanke, der Aufbau und das 3-schichtige Modell der MCKB grob zusammengefasst.

### Mehrschichtiger Sicherheitsansatz und geteilte Verantwortung

Die GSMA, der globale Branchenverband der Mobilfunknetzbetreiber, ist der Auffassung, dass sich Sicherheitsrisiken in 5G-Netzen durch die Implementierung koordiniert abgestimmter und überprüfbarer Sicherheitsmassnahmen wirksam adressieren lassen – insbesondere dann, wenn diese Massnahmen auf gemeinsam anerkannten Standards basieren. Diese Standards bilden ein solides Sicherheitsfundament, müssen jedoch kontinuierlich überprüft und aktualisiert werden, um den neuesten Erkenntnissen aus der Sicherheitsforschung und neu identifizierten Angriffsvektoren Rechnung zu tragen.

Darüber hinaus müssen Mobilfunknetzbetreiber ihre individuellen Risiken fortlaufend bewerten und ihre Schutzmassnahmen entsprechend anpassen – unter Berücksichtigung der aktuellen Empfehlungen zur Risikominderung sowie ihrer spezifischen betrieblichen Anforderungen.



Quelle: <https://www.gsma.com/security/5g-Cyber-Security-knowledge-base/>

Die GSMA hat eine dreistufige Architektur und ein Managementmodell entwickelt, das als industrieweite Methodik zur Sicherstellung der 5G-Cybersicherheit dient.

Das 5G-Sicherheitsmodell umfasst drei zentrale Ebenen:

1. **Product Security Layer:** Sicherstellung der Sicherheit von Netzwerkequipment und Geräten durch Hersteller anhand global anerkannter Standards
2. **Deployment & Operation Security:** Schutz der Netzarchitektur, Netzfunktionen und Datenebenen durch technische und organisatorische Massnahmen

### 3. **Application Security Layer:** Schutz der Anwendungen, Dienste und Endnutzer über den MNO-Verantwortungsbereich hinaus

Diese drei Ebenen bilden gemeinsam einen ganzheitlichen, schichtweisen Sicherheitsansatz, der die Rollen und Verantwortlichkeiten aller beteiligten Akteure klar strukturiert und eine durchgängige Sicherheitsarchitektur für 5G-Netze ermöglicht.

**Product Security Layer:** Die Produktsicherheit liegt in der Verantwortung der Hersteller, wie Geräteanbieter oder Netzwerkausrüster. Die Sicherheitsbewertung von Netzwerkelementen ist dabei ein zentrales Instrument: Sie bildet die Grundlage, um zu prüfen, ob Netzgeräte und -komponenten gemäss definierten Sicherheitsanforderungen entwickelt und implementiert wurden. Sicherheitszertifizierungsprogramme sollten sich an global anerkannten und einheitlichen Standards orientieren, um einen kosteneffizienten und nachhaltig handhabbaren Betrieb innerhalb des gesamten Ökosystems sicherzustellen.

Ein Beispiel hierfür ist das Network Equipment Security Assurance Scheme (NESAS), das gemeinsam von 3GPP und GSMA entwickelt wurde. NESAS stellt ein industrieübergreifendes Sicherheits-Framework bereit, das Verbesserungen des Sicherheitsniveaus in der gesamten Mobilfunkbranche erleichtert. Es definiert Sicherheitsanforderungen und einen Bewertungsrahmen für sichere Produktentwicklung und Produktlebenszyklusprozesse. Zudem kommen von 3GPP definierte Sicherheitstestfälle zur Evaluierung von Netzwerkausrüstung zum Einsatz.

**Deployment & Operation Security:** Die Netzsicherheitsebene wird in der Regel vom Mobilfunknetzbetreiber (MNO) verwaltet, gesteuert und betrieben, wobei bestimmte Elemente auch an spezialisierte Dienstleister ausgelagert werden können. Bereits in der Netzplanungsphase führen MNOs eine umfassende und kontinuierliche Risikobewertung durch, welche die eingesetzten Netzkomponenten, die von Herstellern bereitgestellten Netzfunktionen sowie die gesamte Netzwerkarchitektur berücksichtigt, um Sicherheitsbedrohungen wirksam zu managen.

Innerhalb der Signalisierungs-, Management- und Datenebene sollten automatisierte Sicherheitsmechanismen zur Echtzeit-Erkennung und -Kontrolle von Bedrohungen implementiert sein. Ein Beispiel hierfür sind die in den GTP-U-Sicherheitsempfehlungen der GSMA (FS.37) beschriebenen Verfahren. Diese zeigen, wie sowohl eingehende als auch ausgehende böartige Aktivitäten auf der Datenebene erkannt und kontrolliert werden können. Zu solchen Bedrohungen zählen unter anderem Malware, die Ausnutzung von Netzwerkdiensten, Command-and-Control-Verbindungen sowie Angriffe auf der Applikationsebene und weitere Angriffsformen.

**Application Security Layer:** Der Anwendungs-Sicherheitslayer umfasst sowohl die Nutzer von mobilen Endgeräten (User Equipment, UEs) als auch die vertikalen Branchen, die eine Vielzahl von Anwendungen bereitstellen und nutzen. Die Sicherheit auf dieser Ebene erfordert eine enge Zusammenarbeit zwischen Mobilfunknetzbetreibern (MNOs), Geräteherstellern, Anwendungsentwicklern und Diensteanbietern, um die Sicherheit der 5G-Netze sowie der darin betriebenen Dienste und Nutzer sicherzustellen.

Die Anwendungssicherheit reicht über den Verantwortungsbereich der MNOs hinaus. Vertikale Branchen müssen daher selbst Verantwortung für die Sicherheit ihrer Lösungen übernehmen. Sie sind gefordert, über die von den MNOs bereitgestellten integrierten Sicherheitsfunktionen hinaus zusätzliche Mechanismen zu implementieren, um Vertraulichkeit, Integrität und Verfügbarkeit weiter zu schützen und damit das gesamte Sicherheitsniveau zu erhöhen.

Den vertikalen Branchen obliegt es sicherzustellen, dass die Anwendungsschicht zentrale Werte vor Schäden durch Cyberangriffe schützt, Sicherheitsbedrohungen frühzeitig erkannt werden können und essenzielle Dienste im Störfall rasch wiederhergestellt werden. Die Inter-

aktion zwischen vertikalen Branchen und den MNOs, die die Konnektivität bereitstellen, erfordert eine enge Abstimmung, um optimale Filter, Autorisierungs- und Authentifizierungsmechanismen zu gewährleisten. Diese Aspekte werden üblicherweise in Service Level Agreements (SLAs) geregelt, welche die beteiligten Parteien vor Datenlecks schützen sollen.

In ähnlicher Weise müssen auch die Sicherheitsmassnahmen zwischen miteinander verbundenen Mobilfunknetzbetreibern gestaltet und umgesetzt werden, um Betrug, unbefugten Datenzugriff sowie Identitätsmissbrauch zu verhindern. All diese Aktivitäten erfordern eine koordinierte Zusammenarbeit aller Partner im Interconnection Ökosystem.

### **Ein wirkungsvolles Schema für das Netzwerk-Sicherheitsmanagement in der Telekommunikationsbranche:**

Im Mai 2021 veröffentlichte die GSMA die Mobile Cyber Security Knowledge Base (MCKB). Ziel dieser Wissensbasis ist es, den verschiedenen Akteuren im 5G-Ökosystem dabei zu helfen, Sicherheitsrisiken effektiv zu identifizieren, zu bewerten und zu steuern.

Die Veröffentlichung erfolgte vor dem Hintergrund zahlreicher europäischer Publikationen der letzten Jahre zur Sicherheit von 5G-Netzen. Dazu zählen unter anderem:

- die NIS-Richtlinie,
- der EU Cyber Security Act,
- die EU-weit koordinierte Risikoanalyse zur Cybersicherheit von 5G-Netzen,
- das ENISA Threat Landscape for 5G Networks,
- das Network Equipment Security Assurance Scheme (NESAS),
- die EU Toolbox für 5G-Sicherheit,

sowie weitere sicherheitsrelevante Rahmenwerke und Empfehlungen.

Da die GSMA-Mitglieder parallel daran arbeiten, die Vielzahl dieser Sicherheitsanforderungen und Empfehlungen umzusetzen, wurde die GSMA Mobile Cyber Security Knowledge Base entwickelt, um als Leitfaden zu dienen, der diese Dokumente in einen gemeinsamen Kontext setzt und die Gesamtsicht erleichtert.

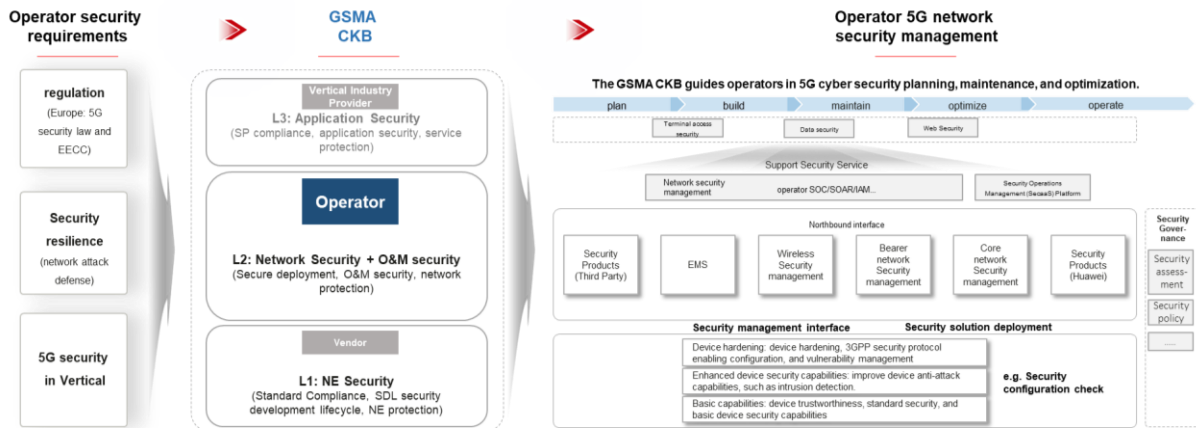
Neben NESAS existieren weitere relevante Initiativen wie das Konzept der EU-Toolbox für 5G-Sicherheit und andere sicherheitsbezogene Programme. Da GSMA-Mitglieder an der Umsetzung unterschiedlichster Sicherheitsanforderungen und Empfehlungen arbeiten, wurde die GSMA Mobile Cyber Security Knowledge Base (MCKB) entwickelt. Sie dient als Leitfaden, um diese Dokumente im Gesamtzusammenhang zu betrachten.

5G-Netze stehen vor neuen Sicherheitsbedrohungen und Herausforderungen. Das objektive, schnelle und wirksame Verständnis, Mapping und die Eindämmung bestehender und aufkommender Bedrohungen sind daher essenziell geworden. Die GSMA hat hierfür eine umfassende Bedrohungsanalyse durchgeführt, an der Experten aus dem gesamten Ökosystem beteiligt waren – darunter Mobilfunknetzbetreiber (MNOs), Hersteller, Dienstleister und Regulierungsbehörden. Zusätzlich wurden Beiträge aus öffentlichen Quellen wie 3GPP, ENISA und NIST integriert, und die identifizierten Bedrohungen geeigneten und wirksamen Sicherheitskontrollen zugeordnet. Die MCKB ist eine branchenweite Initiative. Sie bietet wesentliche Einblicke für die Risikomanagementstrategien aller relevanten Stakeholder und stellt Leitlinien zu Best Practices sowie Massnahmen zur Risikominderung bereit.

## MCKB unterstützt Stakeholder bei der Identifikation, Abbildung und Minderung von Risiken

Die Mobile Cyber Security Knowledge Base (MCKB) erleichtert und fördert die Zusammenarbeit zwischen allen Beteiligten, um Netze und Dienste vor Störungen, unbefugtem Zugriff sowie anderen Risiken zu schützen und diese wirksam zu verhindern bzw. zu mindern. Auf operativer Ebene bietet die MCKB klare Anleitungen und Schritt-für-Schritt Vorgehensweisen, um Sicherheitszusicherungen aufzubauen und dabei das gesamte Spektrum der Risiken in End-to-End-5G-Netzen zu berücksichtigen.

Die MCKB fungiert als Brücke zwischen den Anforderungen hinsichtlich Aufsicht und Compliance der Betreiber, der Verbesserung der Sicherheitsresilienz sowie der Absicherung von 5G-Anwendungen. Gleichzeitig unterstützt sie beim Aufbau der notwendigen Sicherheitsfähigkeiten für Planung, Betrieb und Wartung von 5G-Netzen.



## Die MCKB bietet Mobilfunknetzbetreibern praktische Leitlinien für das Management der 5G-Netzicherheit

- **End-to-End-Sicherheit:** NESAS stellt die Sicherheit für 5G-Netzwerkelemente sicher, während die 5G-Security-Knowledge-Base die Sicherheit in der Planung, dem Aufbau, der Wartung, der Optimierung und dem Betrieb von Carrier-Netzen unterstützt.
- **Praxisleitfaden:** Betreiber können die 5G-Security-Knowledge-Base als zentrale Referenz und Grundlage nutzen, um ihre Sicherheitszusicherungen im 5G-Bereich zu verbessern.
- **Zusammenarbeit aller Akteure:** Betreiber können mit Ausrüstungsanbietern, Applikationsanbietern und Regulierungsbehörden zusammenarbeiten, um die in der Knowledge Base definierten Sicherheitsanforderungen einzuhalten.
- **Sicherheitsbewertung:** Betreiber können die in der Knowledge-Base definierten Sicherheitskontrollen implementieren und Bewertungen gemäss dem GSMA-Sicherheitsreifeegradmodell durchführen.

**Comprehensive and structured threat analysis for mobile networks**

Fields	Threats	Fields	Threats
Application	Malicious Applications	Core Network	DoS attack against core network
	UE Compromising		Voice call eavesdropping
	Theft of Personal Data		Mobile communication monitoring
UE	UICC based web browser compromise	Cloud	NF API Exploitation
	UICC credential theft		SMS Eavesdropping
	IMSI Catching		CDR Harvesting
RAN	DoS Against Terminal Device	Interconnect	Virtual Machine Abuse
	5G/4G/3G to 2G Downgrade		DDoS attacks against MEC
	DoS Attack Against the Network		Abuse of MEC APIs
	SMS Spam	Network O&M	Unauthorized Access to the Slice Management Plane
	Passive Eavesdropping		Network Slice Resource Pre-emption
	Impersonating Calls and Texts		Network Slice Data Theft and Tampering
	Active Eavesdropping	Network O&M	Spoofing Attack for Roaming Interconnections
	Radio Jamming		Location Data Breach
	Breaking LTE on Layer 2		Eavesdropping/Tampering the Data on Roaming Interconnections
	FBS enabled LTE billing compromise	Network O&M	HLR Outage
	Privacy Attacks using Side Channel Information		A2P SMS Re-routing
	5G authentication		S57 RCE and Tunneling
	LTE Inspector	Network O&M	Identity Theft or Fraud
	IMP4GT, IMPersonation Attacks in 4G NeTworks		Exploitation of network configuration data weakness
	REVOLTE		Log Tampering
	Stealthy Location Identification Attack		
	GPRS Cryptanalysis Security		
Hijacking TCP Connection under LTE/5G Network			

**Detailed attack methods and impact description**

CORE-T1: DoS Attack against Core Network	
<b>Threat Description</b>	An attacker initiates (D)DoS attack against the core network through UEs, roaming interfaces, 3rd applications, the internet, base stations, and transport devices that consume network resources and make services unavailable.
<b>Attack Methodology</b>	In a distributed denial-of-service attack (DDoS attack), the incoming traffic flooding the victim network originates from many different sources. DDoS messages can be crafted on a laptop connected to the core network of the victim operator and sent over the N1/N32/N9/N6/N2/N3 interfaces. The attacker can send a large amount of signaling and user data messages towards network nodes in a short period of time. These messages can trigger traffic that exceeds the processing capability of network devices. As a result, too many network resources are occupied and unavailable for normal service.
<b>Potential Impact</b>	Normal core network services unavailability is a critical incident that prevents customers accessing or using services at home or while roaming. Impacted customers may contact customer service who could get overwhelmed. In addition, such attacks cause severe reputational loss for networks operator.

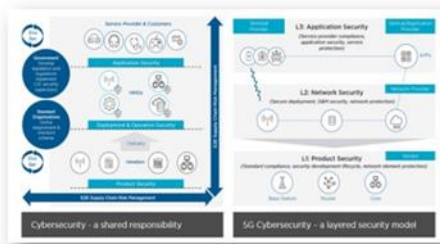
<https://www.gsma.com/security/5g-cybersecurity-knowledge-base/>

**Definition der Verantwortlichkeiten der Stakeholder bei der Risikominderung**

Die Cybersicherheit in 5G-Netzen ist eine geteilte Verantwortung, an der verschiedene zentrale Akteure beteiligt sind – darunter Mobilfunknetzbetreiber (MNOs), Hersteller, Dienstanbieter, Kunden, Behörden sowie Entwickler.

Ein Beispiel hierfür ist das Szenario CoreT1: DoS- Angriff auf das Core-Netz, das in der 5G-Cybersecurity Knowledge-Base beschrieben wird. Dort werden die entsprechenden Massnahmen zur Risikominderung ausgewiesen. Dabei zeigt sich klar, dass drei unterschiedliche Stakeholdergruppen in die Eindämmung dieses Risikos eingebunden sind, wobei jeder Stakeholder genau definierte Verantwortlichkeiten trägt, um die sichere Einführung und den sicheren Betrieb von 5G-Systemen zu gewährleisten.

**GSMA CKB responsibility sharing model**



From GSMA website CKB landing page

GSMA CKB points out that 5G cybersecurity is a shared responsibility that involves key stakeholders

- ✓ **Application Security** main responsibility of application developers and service providers
- ✓ **Network Security** commonly managed, controlled and operated by the MNO, but some elements might also be outsourced to specialized service providers.
- ✓ **Product Security** main responsibility of vendors

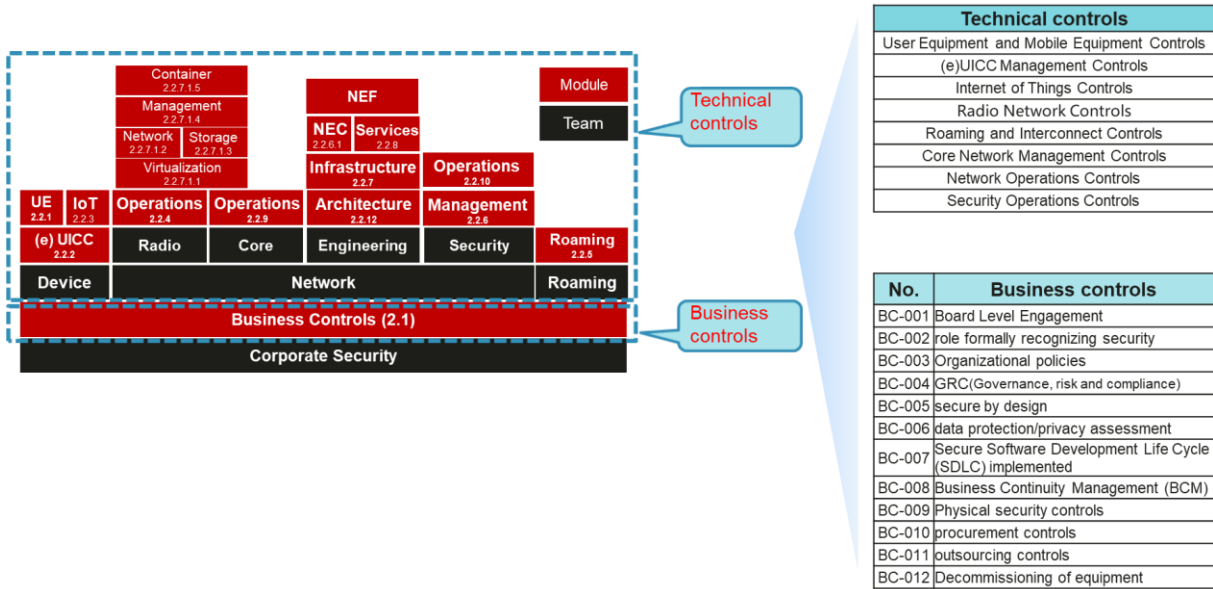
**Mitigation measures recommended to stakeholders**

CORE-T1: DoS Attack against Core Network		
Mitigation Measures	<b>Service Provider</b>	Ensure the security of apps and monitor application server behaviours to prevent hackers from controlling the apps to start DDoS attacks.
	<b>Operator</b> ( FS.31 BC-014, RI-001, NO-007, NO-012, NO-013, NO-015, NO-016)	Request NESAS compliance to ensure equipment has a baseline level of security prior to equipment delivery. Deploy anti-DDoS devices between gNodeBs and the core network, and between the core network and the internet. Deploy security edge protection proxies (SEPPs) and signalling firewalls on the control plane of the core network to filter out attack signalling packets from roaming networks. Enable flow control and DDoS attack pattern packet filtering mechanisms within core network devices.
	<b>Vendor</b>	Provide flow control and DDoS attack pattern packet filtering mechanisms within core network devices and/or anti-DDoS devices. Provide the SEPP function based on 3GPP specifications to filter out abnormal signalling over roaming interfaces.
References	Reuters Staff "Vodafone hit by three-hour mobile network outage in Germany" Reuters. 23 Nov 2020. 3GPP 33.821.	

**Bereitstellung eines Baseline-Sicherheitskontrollsatzes, den Mobilfunknetzbetreiber einsetzen können**

Die Mobile Cyber Security Knowledge Base (MCKB) definiert Baseline Sicherheitskontrollen für Referenzimplementierungen von Mobilfunknetzen. Diese Kontrollen werden in technologische und betriebliche (Business) Kontrollen unterteilt.

Mobilfunknetzbetreiber können diese Controls nutzen, um die aufgeführten Massnahmen mit ihren bestehenden internen Sicherheitskontrollen zu vergleichen, potenzielle Lücken zu identifizieren und zu bewerten sowie anschliessend entsprechende Massnahmen zur Schliessung dieser Lücken innerhalb ihrer Organisation einzuleiten.



Technical controls
User Equipment and Mobile Equipment Controls
(e)UICC Management Controls
Internet of Things Controls
Radio Network Controls
Roaming and Interconnect Controls
Core Network Management Controls
Network Operations Controls
Security Operations Controls

No.	Business controls
BC-001	Board Level Engagement
BC-002	role formally recognizing security
BC-003	Organizational policies
BC-004	GRC(Governance, risk and compliance)
BC-005	secure by design
BC-006	data protection/privacy assessment
BC-007	Secure Software Development Life Cycle (SDLC) implemented
BC-008	Business Continuity Management (BCM)
BC-009	Physical security controls
BC-010	procurement controls
BC-011	outsourcing controls
BC-012	Decommissioning of equipment