UNOFFICIAL MACHINE TRANSLATION

Grant Thornton

MINISTERSTVO PRŮMYSLU A OBCHODU

Financováno Evropskou unií
NextGenerationEU

Analysis of cyber risks associated with the operation of 5G networks for private (closed) networks and the provision of public services, including the impact of Open RAN and Open Core approaches on the security of 5G networks

Prepared for the Ministry of Industry and Trade

[August 2024]

Národní plán obnovy

Contents

List of abbreviations and explanations

3GPP	Third Generation Partnership Project (3GPP)
AES	Advanced Encryption Standard
AI	Artificial Intelligence
API	Application Programming Interface
CA	Certification Authority
CU	Centralised Units
DDoS	Distributed Denial of Service
DDS	Dynamic Spectrum Sharing
DoS	Denial of Service
DRP	Disaster Recovery Plan
DTLS	Datagram Transport Layer Security
DU	Distributed Units
E2EE	End-to-End Encryption
EAP-AKA	Extensible Authentication Protocol – Authentication and Key Agreement
EDR	Endpoint Detection and Response
ENISA	European Union Agency for Cybersecurity (European Network and Information Security Agency)
FCC	Federal Communications Commission
GDPR	General Data Protection Regulation
IAM	Identity and Access Management
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
IP	Internet Protocol
IPSec	Internet Protocol Security
IRT	Incident Response Team
ISACs	Information Sharing and Analysis Centres
ITU	International Telecommunication Union
MFA	Multi-Factor Authentication
ML	Machine Learning
NFV	Network Functions Virtualisation
Open Core	Open network core / Open backbone network
Open RAN	Open Radio Access Network
PFCP	Packet Forwarding Control Protocol
PKI	Public Key Infrastructure
QoS	Quality of Service
RAN	Radio Access Network
RBAC	Role-based access control
SDN	Software-Defined Networking

SSH	Secure Shell – a cryptographic network protocol for secure access to network services
STIX	Structured Threat Information eXpression
TLS	Transport Layer Security
UDP	User Datagram Protocol
UIM	Unified Identity Management
VPN	Virtual Private Network

Executive Summary

5G technology represents a revolutionary leap in the world of telecommunications, bringing not only faster and more reliable connectivity, but also entirely new possibilities for industrial applications and public services. The roll-out of 5G networks is a key factor in realising the concept of the 'Internet of Things' (IoT), which enables the interconnection of millions of devices, from smart homes to autonomous vehicles and smart infrastructure. 5G networks promise improvements in several key areas, such as higher data transfer speeds, which allow for the instant downloading and streaming of high-definition content; significantly lower response times (latency), which is crucial for real-time applications such as autonomous vehicles, industrial automation and telemedicine; and support for a much greater number of devices per unit area, which is essential for the development of smart cities and IoT applications. Despite these benefits, 5G technology also faces new cyber threats and security challenges. The complex architecture of 5G networks, which encompasses a large number of different devices and systems, potentially increases the scope of attacks and broadens the range of vulnerabilities.

Key cyber risks of 5G networks

1. **Network complexity**: The greater complexity and heterogeneity of devices and systems increases the likelihood of vulnerabilities and attacks.
2. **Nature of 5G architecture**: The distributed architecture of 5G networks increases the potential scope of an attack, which can lead to a breach of service integrity and availability.
3. **Supply chain**: Dependence on various hardware and software suppliers can pose security risks associated with insufficient control over the entire chain (operators, device manufacturers, software developers, suppliers)
4. **Privacy and data protection**: The increased volume of data and its dissemination across different parts of the network heightens the risk of privacy breaches and leaks of sensitive information.
5. **Signal jamming and attacks**: 5G technology may be vulnerable to physical attacks, such as signal jamming and eavesdropping.

The main benefits and risks of using Open RAN and Open Core can be summarised as follows:

1. **Open RAN**
   - **Benefits**: Enables flexibility and interoperability between devices from different vendors, which can lead to cost reductions and innovation.
2. **Open Core**
   - **Benefits**: Open Core also improves network interoperability and flexibility. Furthermore, it enables faster and more efficient deployment of new services.
   - **Risks**:
     - The introduction of standardised open interfaces may increase the risk of cyber attacks if they are not adequately secured.
     - Furthermore, reliance on third-party software solutions may increase or lead to new types of vulnerabilities.

In light of the identified risks associated with Open RAN/Open Core approaches, at least the following recommended security measures must be applied:

1. **Strengthening security standards and controls**: Implementing robust security measures and standards for all parts of the 5G network.
2. **Monitoring and anomaly detection**: Implementation of advanced systems for monitoring and detecting unusual activity on the network.
3. **Supplier security audit**: Thorough vetting and auditing of all suppliers involved in the construction and operation of 5G networks.
4. **Data and privacy protection**: Deployment of strong encryption mechanisms and strict data protection rules.
5. **Training and awareness**: Regular staff training and raising awareness of current threats and security measures.

Conclusion

Open RAN and Open Core approaches offer flexibility and interoperability, but at the same time increase potential security risks due to open interfaces and reliance on third-party software solutions. For the successful and secure deployment of 5G technologies, it is essential to adopt comprehensive security measures, such as strengthening standards, network monitoring, supplier audits, data protection and regular staff training. Overall, a carefully balanced approach to security will enable the full potential of 5G networks to be realised whilst minimising associated cyber risks.

1 Introduction

5G networks expand the possibilities for transmitting information, including sensitive data. It is therefore necessary to analyse the cyber resilience and potential vulnerabilities of these networks with regard to approaches such as Open RAN or Open Core.

To this end, the study should:

- Identify and analyse potential vulnerabilities in 5G networks related to Open RAN and Open Core approaches and assess their potential impact on the overall security of the mobile network in question.
- Assess potential and possible types of cyber attacks that may compromise the integrity, confidentiality and availability of data within both private and public 5G networks built in an Open RAN environment.
- To analyse the opportunities and risks associated with identity and access management within such 5G networks and to assess potential vulnerabilities in authentication and authorisation systems.
- To assess the risks and security aspects associated with the implementation of Open RAN and Open Core architectures in 5G networks from the perspective of the risk of data transmission integrity breaches in such 5G networks, and to propose a method to ensure that data remains intact and unaltered during transmission.
- Examine and evaluate measures to protect such 5G networks from potential unauthorised communication with foreign servers (e.g. sending data or receiving commands and instructions from abroad) and propose a possible method for detecting such negative phenomena.
- To examine and evaluate the ability of 5G networks built in an Open RAN environment to withstand distributed denial-of-service (DDoS) attacks, and to propose a method for ensuring network availability even under high load.
- Propose a system for the regular auditing and monitoring of security measures in such 5G networks and propose a method for ensuring an immediate response to potential security incidents.
- To verify that data backup and recovery in such 5G networks are not compromised.
- Create a framework overview of how the use of Open RAN and Open Core equipment is managed in other technologically advanced countries and recommend the application of any best practices.

1.1 Disclaimer and statement by the author

The author makes no representations and accepts no liability regarding the authenticity, correctness, accuracy or completeness of any information obtained from public sources.

The study (hereinafter referred to as the “study”) was prepared to the extent and with the relevance applicable as at the date of its preparation, i.e. the date stated in the study’s header. The author is not responsible for any changes to relevant facts and regulations that have occurred after that date. The study or any part thereof may not be copied or altered in any way, nor may it be made available to third parties or otherwise disposed of without the express prior written consent of the author. Any such action will be considered unauthorised. Interpretations, assessments, opinions and conclusions are valid only within the overall context of the study.

1.2 List of sources

1.2.1 EU sources

- Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the 'European Union Agency for Cybersecurity'), on the certification of the cybersecurity of information and communication technologies, and repealing Regulation (EU) No 526/2013 ('Cybersecurity Act')
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
- Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union
- European Commission Recommendation on the cybersecurity of 5G networks of 26 March 2019
- European Parliament resolution of 12 March 2019 on security threats related to China's growing technological presence in the EU and on possible measures at EU level to mitigate them (2019/2575 (RSP))
- Communication from the Commission to the European Parliament, the Council (EU), the European Economic and Social Committee and the Committee of the Regions – Secure deployment of 5G networks in the EU – Implementation of the EU package of measures of 29 January 2020
- Report by EU Member States on the coordinated assessment of EU cybersecurity risks in 5G networks of 9 October 2019
- EU Toolbox for the cybersecurity of 5G networks
- Secure deployment of 5G in the EU: Implementation of the EU Toolbox – Communication from the European Commission of 29 January 2020
- ENISA document: Threat Assessment for Fifth Generation Mobile Telecommunications Networks (5G) of November 2019

1.2.2 Czech Republic sources

- Constitutional Act No. 1/199 Coll., the Constitution of the Czech Republic, as amended (hereinafter referred to as the “Constitution”)
- Constitutional Act No. 110/1998 Coll., on the Security of the Czech Republic, as amended (hereinafter referred to as the “Act on the Security of the Czech Republic”)
- Act No. 110/2019 Coll., on the processing of personal data (hereinafter referred to as the “Data Protection Act”)
- Act No. 127/2005 Coll., on Electronic Communications and on Amendments to Certain Related Acts (the Electronic Communications Act)
- Act No. 134/2016 Coll., on Public Procurement, as amended (hereinafter referred to as the “Public Procurement Act”)
- Act No. 181/2014 Coll., on cyber security and amending related acts, as amended (hereinafter referred to as the “ZKB”)
- Act No. 89/2012 Coll., the Civil Code, as amended (hereinafter referred to as the “Civil Code”)
- Act No. 418/2011 Coll., on the criminal liability of legal persons and proceedings against them, as amended (hereinafter referred to as “ZTOPO”)
- Act No. 349/1999 Coll., on the Public Defender of Rights, as amended (hereinafter referred to as “ZVOP”)
- Government Regulation No. 432/2010 Coll., on criteria for determining elements of critical infrastructure, as amended
- Decree No. 82/2018 Coll., on cyber security, as amended (hereinafter referred to as “VKB”)
- Decree No. 437/2017 Coll., on criteria for determining operators of essential services
- Decree No. 317/2014 Coll., on significant information systems and the criteria for their designation, as amended

1.2.3 Online resources

- The state is reviving Cell Broadcast to send hazard warnings to mobile phones https://www.lupa.cz/clanky/stat-znovu-krisi-cell-broadcast-pro-rozesilani-vystrah-pred-nebezpecim-do-mobilu/
- https://www.lupa.cz/market-voice/pripojit-k-5g-cestujici-nestaci-budoucnost-zeleznice-se-jmenuje-frmcs/
- https://op.europa.eu/en/publication-detail/-/publication/8c6755a1-4f55-11ed-92ed-01aa75ed71a1/language-en/format-PDF/source-search
- Roll-out of 5G networks in the EU: deployment is facing delays and security issues remain unresolved (https://op.europa.eu/webpub/eca/special-reports/security-5g-networks-03-2022/cs/index.html)
- ENISA threat landscape for 5G networks (https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks/@@download/fullReport)
- Recommendations for assessing the trustworthiness of technology suppliers for 5G networks in the Czech Republic (National Cyber and Information Security Agency – Recommendations for assessing the trustworthiness of technology suppliers for 5G networks in the Czech Republic (gov.cz))

2 Identification and analysis of potential vulnerabilities in 5G networks related to Open RAN and Open Core approaches

The Open RAN architecture comprises various components, such as distributed units (DU), centralised units (CU) and base units (BU). Base units play a key role within the radio access network (RAN) by providing the physical layer for communication between user devices and the network.

This chapter focuses on the main components of 5G networks, such as:

- Interfaces between Open RAN units,
- Open RAN network control and management,
- The Open RAN supply chain
- SDN and virtualisation of network element functions
- Open Core interoperability and integration
- Open Core updates and patch management

and identifies associated potential vulnerabilities and security challenges.

2.1 Interfaces between Open RAN units

The interface between base units (BU), distributed units (DU) and centralised units (CU) in the Open RAN architecture is a key element enabling flexibility and interoperability in the radio access network. This open interface, known as OPEN RAN, supports communication and coordination between different parts of the network, enabling operators to combine and customise technologies from different manufacturers. However, it is precisely this openness and complexity that can increase security risks. The text goes on to provide an overview of potential vulnerabilities relating to the interfaces.

2.1.1 Eavesdropping and data manipulation

The interfaces between the BU, DU and CU also transmit sensitive information, including user data and control signals. If communication between these units is not properly encrypted and secured, attackers may eavesdrop on this information or even manipulate the transmitted data. Such a situation would then result in the leakage of sensitive information, disruption of services, or enable attackers to carry out fraudulent activities.

Eavesdropping and data manipulation within the Open RAN architecture, particularly between base units (BU), distributed units (DU) and centralised units (CU), can lead to various types of fraudulent activities. Here are some specific examples of fraudulent activities that could occur:

1. Cloning attacks
   If an attacker manages to eavesdrop on and obtain sensitive information from communications, they can use it to create device clones. These cloned devices can then connect to the network, thereby allowing the attacker unauthorised access to the network and its services. This can lead to unauthorised use of services, the transmission of malicious content, or other harmful activities.
2. Spoofing
   Data manipulation can allow an attacker to insert fake messages into communications. For example, an attacker may spoof messages that appear to come from a trusted source to trick network components into performing unwanted actions, such as redirecting traffic, disabling certain functions, or disrupting services.
3. Man-in-the-Middle (MitM) attacks

In a MitM attack, an attacker eavesdrops on and potentially alters communication between two parties without their knowledge. In the context of Open RAN, an attacker can intercept and modify transmitted data. This can lead to a breach of data confidentiality and integrity, and enable the attacker to obtain sensitive information or influence further network behaviour.

4. Billing attacks and service abuse
   Attackers can manipulate data, alter billing and, in particular, payments for services, or create false records of service usage. For example, they can modify invoice details and completely alter payments for services. Such actions then cause financial losses for service providers and undermine customer trust.
5. Malware distribution and phishing
   Data manipulation can also take the form of inserting malicious software or phishing links into communications. An attacker can then trick users or network components into downloading and executing malicious code, leading to further compromise of the network and systems, data theft or disruption of services.

For example, a fake software update might be carried out as follows:

1. Eavesdropping and identifying a vulnerability: The attacker eavesdrops on communications between the BU and DU and discovers that a software update is planned.
2. Falsifying a message: The attacker sends a fake software update message that appears to come from a trusted source.
3. Distribution of malicious code: The fake update contains malicious code, which is installed on the base units (BU).
4. Attack: The malicious code allows the attacker to gain control of the BUs, monitor communications, collect sensitive data, or disrupt network functionality.

2.1.2 Unreliable authentication and authorisation

Another vulnerability in network components may lie in the reliability of verifying the identity of other elements in the network and in verifying the permissions of other elements to communicate within the network. Weaknesses in authentication and authorisation mechanisms may allow unauthorised entities to access network functions or perform operations that should only be permitted to trusted components.

2.1.3 Lack of standardisation and unmanaged implementation

Standardisation and implementation are key elements in ensuring security within the Open RAN architecture. Although the O-RAN Alliance provides standards and specifications for securing communication between various components, such as base units (BU), distributed units (DU) and centralised units (CU), **there are various vulnerabilities** that can compromise this architecture.

- Incorrect implementation of standards
  - Description: Although there are clear standards for securing communication between the DU and the CU, not all manufacturers and operators are able to implement these standards correctly or comply with them
  - Example of vulnerability: Errors in the implementation of encryption protocols may allow data to be intercepted or manipulated.
- Insufficient compatibility
  - Description: Different vendors may implement O-RAN standards in different ways, which can lead to compatibility issues. These issues may cause certain security features to fail to function correctly.
  - Example of a vulnerability: If a single component does not support a particular security feature, this may compromise the overall security architecture of the network.
- Failure to apply updates and patches
  - Description: Standards evolve and new security threats require regular updates and patches. Vulnerabilities may arise if updates are not applied in a timely manner or are not available for all network components.
  - Example of a vulnerability: Known vulnerabilities in older software versions that have not been patched can be exploited by attackers.
- Sub-interfaces as a weak link
  - Description: Communication between the DU and CU involves several interfaces that must be securely implemented. If certain interfaces are not sufficiently secure, they can be exploited for attacks.
  - Example of a vulnerability: Man-in-the-middle (MitM) attacks on unsecured interfaces may allow attackers to eavesdrop on or manipulate communications.
- Limited security testing
  - Description: Security testing is critical for identifying vulnerabilities before deployment to a production environment. Insufficient testing may mean that some vulnerabilities remain undetected.
  - Example of a vulnerability: Protocol exposure in the test environment and production deployment may be exploited after the system is deployed.
- Insecure key and certificate management
  - Description: The management of cryptographic keys and certificates is crucial for ensuring secure communication. Weaknesses in this process can lead to the leakage or misuse of keys.
  - Example of a vulnerability: If keys are stored insecurely or if certificates are managed without sufficient controls, they may be compromised, leading to a system breach.

Potential interface vulnerabilities in 5G networks **are primarily mitigated through security measures at the network architecture level, at the protocol level, through the application of standardisation, and through controlled implementation**. Protection against vulnerabilities involves the continuous and regular performance of activities such as:

- Conducting regular security audits and testing – regular penetration tests and configuration audits can help identify and rectify vulnerabilities.
- Compliance with standards and testing compatibility between different components from different suppliers.
- Regular software updates, i.e. keeping all components up to date with the latest patches and security updates.
- Implementing robust key and certificate management, i.e. ensuring the secure generation, storage and management of cryptographic keys and certificates.
- Education and training, i.e. ensuring that people within the organisation are familiar with security procedures and that ICT specialists are able to implement and maintain security measures in accordance with O-RAN Alliance standards.

- **Network infrastructure security**

In addition to software security, the physical infrastructure of the BU, DU and CU must also be secured. This includes protection against physical intrusion, ensuring the secure location and access to the units, and protection against risks such as sabotage or theft of equipment

- **Protocol-level security**

As Open RAN supports a wide range of protocols for communication between the BU, DU and CU, it is essential to ensure that all these protocols are robustly secured against various types of attacks, such as DoS (Denial of Service) attacks, attacks via replication, or the injection of malicious data into communications.

In this area, robust authentication protocols are employed, the importance of which lies primarily in the following benefits:

1. Identity assurance: Strong authentication protocols ensure that every component in the network can reliably verify the identity of the other components with which it communicates. This is key to preventing identity spoofing and other forms of attack where an attacker pretends to be a legitimate entity.
2. Protection against unauthorised access: Strong authentication mechanisms prevent unauthorised entities from accessing network resources and data. This is essential for protecting sensitive information and ensuring that only authorised entities can communicate and perform operations on the network.
3. Data integrity and confidentiality: In addition to identity verification, authentication protocols provide mechanisms to ensure data integrity and confidentiality. This means that data transmitted between components cannot be altered or intercepted without detection.

Today's authentication elements work with various types of robust authentication protocols, such as:

1. Public Key Infrastructure (PKI): PKI uses a pair of public and private keys for identity verification. Each entity has a certificate issued by a trusted certification authority (CA), which is used to verify identity during every communication.
    - Example: When establishing a connection between the BU and the DU, certificates are used for mutual authentication, where each party verifies the other's identity using the public key contained in the certificate.
2. Kerberos: Kerberos is an authentication protocol that uses tickets for authentication. It is based on symmetric cryptography and a trusted third party, known as the Key Distribution Centre (KDC).
    - Example: When communicating between the DU and the CU, Kerberos can provide tickets that verify that both parties are authorised to communicate without the need to repeatedly enter passwords.
3. EAP (Extensible Authentication Protocol): EAP acts as an authentication framework that supports various authentication methods, such as EAP-TLS (Transport Layer Security) or EAP-AKA (Authentication and Key Agreement).
    - Example: EAP-TLS can be used to secure wireless communication between the BU and user devices, where authentication is performed using certificates.

- **Standardisation and implementation**

Although the OPEN RAN Alliance standards define the security of communications between the BU, DU and CU, it is up to manufacturers and operators to implement these standards. Shortcomings in implementation or failure to adhere to best practices can lead to vulnerabilities.

It is essential that comprehensive security measures are adopted, including strong encryption, robust authentication protocols, regular security testing, regular updates, and staff training on security risks and procedures. This will significantly reduce the risk of attacks and ensure safer operation in Open RAN networks.

Minimum standards for interfaces between Open RAN units are established by the Open RAN Alliance, specifically:

1. **O-RAN Architecture Description (O-RAN.WG1.O-RAN-Architecture-Description-v02.00)**: This document provides an overview of the Open RAN architecture, including communication between the DU and CU and the relevant security aspects.
2. **O-RAN Security Focus Group (O-RAN-SFG)**: A group of experts focused on security standards and recommendations for Open RAN, which issues specifications and guidelines regarding the security of various components of the Open RAN architecture.
3. **O-RAN Fronthaul Interface Specifications (O-RAN.WG4.CUS.0-v01.00)**: This document specifies the interface between the DU and CU and sets out security measures to ensure secure communication.

2.2 Open RAN Network Control and Management

Network control and management activities in the context of Open RAN are essential for the effective operation and optimisation of the radio access network. These aspects are particularly important given the distributed architecture of Open RAN, where different components and functions may be provided by different suppliers.

Vulnerabilities and security challenges in Open RAN network management and administration primarily relate to automation and intelligent control, information sharing and overall coordination.

2.2.1 Automation and intelligent control

Open RAN supports advanced automation and the use of artificial intelligence (AI) and machine learning (ML) for dynamic network management and optimisation. Whilst these technologies enable more efficient resource management, improved service quality and reduced costs, they are also associated **with potential vulnerabilities, such as**:

- Exploitation of automation scripts and algorithms: Attackers may attempt to manipulate automation processes or inputs to AI/ML models to disrupt network operations or gain unauthorised access.
    - Vulnerabilities in algorithms and their implementation – AI/ML algorithms may contain errors or be poorly implemented, which can lead to incorrect decisions or exploitation by attackers.
        - Code errors: Bugs or errors in the implementation of AI/ML algorithms can lead to incorrect results or system crashes.
        - Insufficient robustness: Algorithms that are not sufficiently robust may be sensitive to small changes in data or may be easily deceived by specially crafted inputs.
    - Vulnerabilities due to incorrect configuration of automated decision-making systems and the limitations of decision-making systems – automated decision-making systems can significantly streamline network management, but if they are not properly designed or configured, they can cause serious problems.
        - False positive/negative results: AI/ML models can generate false positive or negative results, which can lead to undesirable actions, such as blocking legitimate users or allowing malicious traffic.
        - System overload: Automated systems may perform actions that lead to network overload or instability if they are not properly calibrated or monitored

- Data security breaches for AI/ML: The quality and security of the data used to train AI/ML models is crucial. Malicious or biased data can lead to incorrect decisions or vulnerabilities.
    - Training data manipulation: Attackers can deliberately inject malicious or biased data into the training set, leading to the creation of models that make incorrect predictions or decisions.
    - Poisoning attacks: In poisoning attacks, training data is deliberately corrupted so that models generate predetermined errors or vulnerabilities.

Potential vulnerabilities in AI/ML **are primarily eliminated by implementing the following measures:**

- High-quality and secure training data – ensuring that training data is clean, relevant and free from malicious patterns by:
    - Data validation and filtering: Implement processes for validating and filtering training data to ensure its quality and integrity.
    - Monitoring and auditing of data sources: Regularly monitor and audit training data sources to prevent the infiltration of malicious or biased data.
- Robust algorithms and implementation – by developing and implementing robust AI/ML algorithms that are resilient to various types of attacks and errors, applied at least through:
    - Testing and validation of algorithms: Conduct thorough testing and validation of AI/ML algorithms prior to deployment in a production environment.
    - Red teaming and penetration testing: Use red teaming and penetration testing to identify and rectify potential vulnerabilities in AI/ML systems.
- Monitoring and management of automated systems – ensuring continuous monitoring and management of automated systems so that any issues are identified and resolved in a timely manner. This primarily involves the following measures:
    - Continuous performance monitoring: Implement tools for the continuous monitoring of the performance and behaviour of AI/ML models and automated systems.
    - Alerting and incident response: Establish an alerting system and an incident response plan to ensure a rapid response to any anomalies or incorrect decisions generated by automated systems.

2.2.2 Information sharing and coordination

Open RAN operates on the basis of information sharing between different networks and with different suppliers, which translates into increased requirements for coordination and optimisation. Sharing must be carefully secured to prevent **information leaks**, **including those involving sensitive data**, and to ensure that only authorised entities gain access to relevant data.

Protection in the area of information sharing and coordination is achieved through access and identity management, the application of security protocols and standards, and the monitoring of incidents and timely response to them.

- **Access and identity management**

Securing access to control and administrative functions involves, in particular, the following measures:

- Strong user authentication and authorisation: Ensuring that only authorised persons can make changes to the network configuration or access sensitive data.
- Role-based access control (RBAC): By defining access rights based on users' roles within the organisation, this ensures that everyone has access only to the data and operations necessary for their role.

- **Implementation of security protocols and standards**

The implementation of strong security protocols and adherence to industry standards are key to securing communication and data transfers between different network components. This is achieved through:

- Encryption: Ensuring the secure transmission of data between different parts of the network.
- Data integrity verification and authentication of data origin: Verifying the authenticity and integrity of transmitted data.

- **Incident monitoring and response**

Continuous network monitoring and rapid response to security incidents are essential for identifying and addressing potential threats. This primarily involves:

- Detection of anomalies and breaches: Using AI/ML to identify unusual activities that may indicate security threats.
- Planning and standardising incident response: Preparedness and the ability to respond quickly to security incidents minimise potential damage.

2.3 The Open RAN supply chain

The supply chain in the context of Open RAN architecture presents **challenges and vulnerabilities** due to its inherently diverse and distributed nature. In Open RAN, traditional, monolithic supply models are replaced by more open and modular approaches, enabling operators to combine solutions from different manufacturers. Whilst this brings significant benefits in terms of flexibility and transparency, innovation and potentially cost, the vulnerabilities and security challenges outlined below must be taken into account.

2.3.1 Security risks of multiple suppliers

The Open RAN architecture enables the integration of components from different suppliers. This reduces dependence on a single manufacturer and can lead to innovation and cost reductions. However, the supply chain also brings **specific security risks**, particularly if it involves high-risk suppliers.

- Compatibility and integration vulnerabilities – Components from different suppliers may not work together seamlessly and securely. Different security standards and implementations can cause compatibility issues.
    - Incompatible security measures: Differing implementations of security protocols can lead to security gaps that attackers can exploit.
    - Weak points in integration: Incorrectly integrated systems can create vulnerabilities that may be targeted by attacks.
- Vulnerabilities in the quality and security of individual components - The quality and security of software and hardware from different suppliers can vary significantly. Low-quality or inadequately secured components can compromise the entire network.
    - Poor software/hardware quality: Components with inadequate security measures can be easily exploited.
    - Unsecured updates and patches: If suppliers do not provide regular and secure updates, components may remain vulnerable to new threats.
- Vulnerabilities at the access control and identity management level - Managing access rights and identity verification between components from different suppliers can be complex.
    - Weak authentication mechanisms: If a supplier uses weak authentication protocols, this may allow unauthorised access to the network.
    - Inadequate access control: Missing or poorly configured control mechanisms can lead to unauthorised access to network resources.
- Vulnerabilities associated with high-risk suppliers – Suppliers from certain regions may pose an increased risk due to geopolitical tensions, sanctions or legislation that may require cooperation with government agencies.
    - Politically motivated attacks: Suppliers may be forced to cooperate with governments on surveillance or attacks against foreign networks.
    - Sanctions and restrictions: Suppliers may face sanctions that affect their ability to provide secure and up-to-date products.
- Vulnerabilities associated with untrusted suppliers: Some suppliers may have a history of security incidents, inadequate security practices, or may be directly involved in malicious activities.
    - Delivery of malicious components: Suppliers may, intentionally or through negligence, distribute components containing malicious software or vulnerabilities.
    - Inadequate incident response: Untrustworthy suppliers may respond inadequately to security incidents or fail to inform their customers of vulnerabilities.
- Vulnerabilities associated with supply chain attacks – Attackers may target the supply chain to inject vulnerabilities or malicious software into components before they are delivered.
    - Compromise during manufacturing: Components may be compromised during manufacturing or transport.
    - Manipulation of updates: Attackers may manipulate update processes to introduce malicious code.

By implementing these measures, organisations can better protect their Open RAN networks from security threats associated with multiple suppliers and high-risk suppliers, thereby contributing to the overall resilience and security of the telecommunications infrastructure:

- Thorough vendor assessment and selection – Carefully select vendors based on their security practices, track record and geopolitical risks. This can be ensured, for example, through:
    - Security audits and certification: Require suppliers to undergo regular security audits and certification.
    - Risk assessment: Conduct regular risk assessments associated with individual suppliers.
- Setting clear requirements and contractual terms – Defining clear security requirements and contractual terms that suppliers must meet.
    - Security requirements: Clearly define security requirements in contracts, including regular updates and patches, access control and data protection.
    - Penalties for non-compliance: Establish penalties for non-compliance with security requirements to ensure that suppliers are incentivised to adhere to agreed standards.
- Monitoring of supplier performance: Introduce a system for the ongoing monitoring of supplier performance, including monitoring compliance with SLAs (Service Level Agreements) and security standards.
- Implementation of strong security protocols - Introduce and enforce strong security standards and authentication protocols across all network components through the following measures:
    - Strong authentication protocols: Implement robust authentication mechanisms, such as PKI or Kerberos.
    - Data encryption and integrity: Ensure that all data transmitted between components is encrypted and verified for integrity.
- Through continuous monitoring and updating – Continuously monitor and update all network components to ensure they are secure against new threats. Threats can be prevented by the following measures:
    - Automated updates: Implement systems for automated and secure software and hardware updates.
    - Security monitoring: Introduce tools for continuous network monitoring and the detection of anomalies or potential attacks.

- Implement robust supply chain management and transparency – Introduce robust supply chain management and transparency, and apply governance through:
    - Supply chain tracking: Use tools and technologies to track the origin and integrity of components throughout their entire lifecycle.
    - Inspections and audits: Conduct regular audits and inspections of the supply chain to ensure its security.

2.3.2 Integration and Compatibility, including Interoperability in Open RAN

Integration and compatibility are key factors for the successful deployment of an Open RAN architecture that utilises components from different suppliers. Interoperability refers to the ability of these components to work together seamlessly, which is essential for achieving an efficient and secure network. However, integration and interoperability **introduce several vulnerabilities and security challenges** that must be carefully managed.

- Incompatibility between different vendors – Components from different vendors must be able to work together seamlessly. Different security standards and implementations can cause compatibility issues. Specifically:
    - Incompatible security measures: Different implementations of security protocols can lead to security gaps that attackers may exploit.
    - Weak points in integration: Incorrectly integrated systems can create vulnerabilities that may be targeted by attacks.

- Failed interoperability between components – Interoperability refers to the ability of different systems and components to work together effectively and securely. Failed interoperability occurs in both hardware and software and is mainly associated with:
    - Incorrect configuration: Incorrect configuration can result in components being unable to communicate properly with one another, which may cause outages or security issues.
    - Inconsistent implementation of standards: Suppliers may implement standards in different ways, which can lead to incompatibility and potential security gaps.

- Insufficient/incomplete testing and validation: Thorough testing and validation of all components may not be ensured prior to deployment in a production environment.
    - Insufficient testing: If testing is not thorough enough, bugs or vulnerabilities may remain undetected and could be exploited later.
    - Errors in test scenarios: Incorrect or incomplete test scenarios can lead to a false sense of security and functionality.

- Missing updates and patches – incomplete updates and missing patches compromise the security and functionality of the network. Compatibility and interoperability may not be maintained after updates are applied.
    - Incomplete updates: Updates may be incomplete or incorrectly implemented, which can lead to new security issues.
    - Compatibility issues after updates: After an update is applied, compatibility issues may arise between different components.

- Third-party dependencies – Increased reliance on third parties for critical network components means that network security may be compromised if one of these third parties faces a security incident.

Potential vulnerabilities in integration and compatibility, including interoperability in Open RAN, **can be avoided by implementing the following measures:**

- Standardisation and certification – Adherence to industry standards and certification helps ensure that components from different suppliers are compatible and interoperable. This can be reinforced in particular by specific measures:
    - Protocol standardisation: Implement and adhere to standardised protocols and security measures defined by organisations such as the O-RAN Alliance.
    - Component certification: Require all components to undergo a certification process that verifies their compatibility and security.
- Thorough testing and validation: Before deployment in a production environment, thorough testing of all components must be carried out to ensure their compatibility and interoperability. Effective measures include:
    - Comprehensive test scenarios: Create and execute comprehensive test scenarios that cover all possible interactions between components.
    - Validation of security measures: Include the validation of all security measures and protocols in the testing.
- Dynamic security policy management – The implementation of dynamic tools for security policy management enables rapid adaptation to new threats and changes in the network. This is applied in the form of:
    - Centralised policy management: Use centralised tools for managing security policies that enable changes to be deployed quickly and efficiently.
    - Automation of security updates: Implement systems for the automated application of security updates and patches.

- Cooperation and information sharing – Cooperation between operators, suppliers and security organisations can help identify and address security threats more effectively. This is facilitated by the following measures:
  - Threat intelligence sharing: Establish mechanisms for sharing information on security threats amongst all stakeholders.
  - Joint security exercises: Conduct joint security exercises and tests involving all stakeholders to improve preparedness for security incidents.
- Key and certificate management: Effective management of cryptographic keys and certificates is essential to ensure secure communication between components.
  - Secure key generation and storage: Implement robust systems for generating and storing cryptographic keys.
  - Automated certificate management: Use tools for automated certificate management, including renewal and revocation.
- Transparency and verification – Ensuring transparency and verifying the security and origin of components and software within a complex supply chain is crucial. This includes a thorough security assessment of suppliers and their products prior to integration into the network, monitoring and auditing of software and hardware, and protection against exploitation, such as the insertion of malicious code or hidden backdoors.
- Implementation of a centralised patch and update management system – System patches and updates are essential for addressing vulnerabilities. In an Open RAN environment, where components come from different suppliers, coordinating and applying these updates can be more complex, thereby increasing the risk that some components remain unpatched and vulnerable.
- Reducing reliance on third parties – Robust risk management that covers all levels of the supply chain and the consistent enforcement of incident management measures across all suppliers will enable an effective and timely response to security incidents.

2.4 Software-Defined Networking (SDN) and Network Functions Virtualisation (NFV) Open Core

One of the key elements of Open Core is the use of Software-Defined Networking (SDN) and Network Functions Virtualisation (NFV) technologies. These technologies enable the separation of hardware infrastructure from software. In the context of 5G networks, Open Core refers to the use of open software and standards at the core of the network, which enable greater flexibility, easier integration of new technologies and potentially lower costs, but which also bring with them **specific vulnerabilities and security challenges**.

In this section, we will focus on vulnerabilities at the software level, at the hardware virtualisation level, and in relation to Open Core interoperability and integration.

2.4.1 Software-Defined Networking (SDN)

SDN enables operators to efficiently manage network traffic through a centralised software system. This separation of the control plane (control logic) from the data plane (data forwarding) allows for dynamic network management. **Security challenges include:**

- Vulnerabilities in the control plane: As the SDN control plane can manage the entire network, its compromise can have serious consequences, including the ability to reroute or block network traffic.
- Attacks on the interface between the control and data planes: This interface is critical to the proper functioning of SDN. Attackers may attempt to inject malicious code or eavesdrop on communications.
- Centralisation as a single point of failure: A centralised control plane increases the risk of a ‘single point of failure’, where a compromise of the central system can affect the entire network.

2.4.2 Network Functions Virtualisation (NFV)

NFV enables the deployment of network services as software instances on standard hardware, reducing the need for dedicated network hardware. **Security challenges include:**

- Vulnerabilities in the virtualisation layer: Hypervisors and other components used for virtualisation may contain vulnerabilities that allow attackers to escape from a virtual machine and affect the host system or other virtual machines.
- Vulnerabilities in the management and isolation of virtual network functions (VNFs): Incorrect configuration or management of VNFs can lead to security vulnerabilities, including insufficient segmentation between VNFs, which may allow attacks to propagate across the network.

- Vulnerabilities in access and identity management: In an NFV environment, it may not be ensured that only authorised entities can manage and access VNFs, and robust access control and authentication systems may not be in place, which can make it easier for attackers to compromise the network.

Security in Open Core architecture, particularly in the context of SDN and NFV, requires a comprehensive approach that includes careful planning, implementation and ongoing monitoring. It is important to take measures to secure the control plane, ensure secure communication between the control and data planes, protect the virtualisation infrastructure, and implement effective access and identity management. This requires not only technological solutions but also careful management and staff training to ensure they are aware of potential threats and best practices for mitigating them.

2.5 Interoperability and Integration in Open Core

Interoperability in Open Core 5G networks means that components and systems from different suppliers must work together reliably and securely. This collaboration can cover various aspects of the network, from hardware to software applications. It is key to reaping the benefits of open architecture and modular, efficient, and agile core networks. Accelerating innovation in the context of Open Core also brings **unique vulnerabilities and security challenges** that require increased attention from a security perspective.

- Interoperability-related vulnerabilities:
    - Inconsistency in security standards and implementations: Different security practices and technologies can lead to vulnerabilities in the network where different systems intersect.
    - Security protocol compatibility: Ensuring that all network components use compatible and up-to-date security protocols is essential for preventing data leaks and attacks.
    - Cryptographic key management: The secure exchange and management of cryptographic keys between different systems requires robust solutions that support interoperability.

- Vulnerabilities associated with the integration of heterogeneous systems:
    - Configuration and update errors: Incorrect configuration or delayed application of updates and patches can open up new security gaps in integrated systems.
    - Network design complexity: Greater complexity can make it harder to identify and address security threats. Effective network management and monitoring tools are essential for visibility and security.
    - API and interface security: Integration often relies on APIs and programmable interfaces, which must be carefully secured against unauthorised access and attacks.

To address interoperability and integration challenges in Open Core 5G networks, it is important **to implement several key security measures:**

- Dynamic security policy management: The use of centralised tools for dynamic security policy management enables the creation of an adaptive and proactive security architecture in Open RAN networks. In the context of ever-changing threats and a heterogeneous environment where components come from different vendors, it is essential that the security policy is not only robust but also flexible and capable of responding quickly to new security challenges

- Standardisation and certification: Supporting and adhering to standardised protocols and security rules helps ensure compatibility and security. Certification from reputable organisations can provide confidence in suppliers' security practices.

- Thorough testing: Before deployment to a production environment, thorough interoperability and security testing must be carried out, including simulated attacks and penetration testing.

- Careful management of keys and certificates: Securing cryptographic algorithms, including the management of keys and certificates, is essential for ensuring the confidentiality and integrity of communications.

- Cooperation and threat intelligence sharing: Cooperation between operators, suppliers and security organisations can help identify and address security threats more effectively.

We will focus on the main pillar of security measures – dynamic security policy management – and, in greater detail, we will outline not only the individual benefits but also the key elements of dynamic management.

1. Adaptability to changing threats – Dynamic management enables rapid adaptation to new security threats and vulnerabilities. Management involves updating rules and policies in real time so that it is possible to respond immediately to new types of attacks or newly discovered vulnerabilities. Key elements that deliver these benefits:
    - Centralised management of security policies – Simplifies the management process and ensures consistency across the entire network. Centralisation also provides a better overview and control over the entire security infrastructure.

- Automation of security processes – Dynamic management involves the automation of key security processes, such as incident detection and response, patch and update management, and the implementation of security rules. Automation increases efficiency and reduces the risk of human error.

2. Speed and continuity of collaboration between key components of dynamic security policy management
   - Real-time monitoring and analysis – Implementation of tools for continuous monitoring of network traffic and anomaly detection. Real-time analysis enables the rapid identification of suspicious activities and potential security incidents.
   - Security policy orchestration – Use of orchestration tools that enable the dynamic deployment and updating of security policies across various network components. This ensures that all parts of the network are synchronised and comply with current security standards.
   - Intelligent incident response – Utilising artificial intelligence (AI) and machine learning (ML) for intelligent detection and response to security incidents. These technologies can identify attack patterns, predict future threats and automatically deploy countermeasures.
3. Simple and predictable implementation steps for dynamic security policy management
   - Deployment of centralised management – Implementation of a centralised security policy management system that enables easy deployment and updating of rules and policies from a single location.
   - Integration of automation tools – Use of tools for automating security processes, such as patch management, update management and incident detection tools. Automation should include the ability to automatically respond to identified threats.
   - Regular updates and testing – Regular updates to security policies and rules, based on the latest threat intelligence. Implementation of a process for regularly testing and auditing these policies to ensure their effectiveness.
   - Staff training and education – Ensuring that staff are regularly trained and familiar with dynamic security policies and tools. This includes training on identifying and responding to security incidents and using automation tools.

2.6 Open Core updates and patch management

Updates and patch management are key security aspects for any software, including those that form the core of 5G networks using Open Core architecture. In an Open Core environment, where a greater degree of software-based solutions and virtualisation forms the foundation, it is important to effectively manage updates and patches for various software components. Even so, the process of updating and managing Open Core patches is subject to **vulnerabilities and security challenges**, as outlined below.

- Patch release speed: As security threats are constantly evolving, software vendors must respond quickly by releasing patches. Organisations must implement these patches just as quickly, which can be logistically challenging. Logistically challenging means that the process of releasing, distributing and applying patches requires complex coordination and resources to be carried out effectively and without disrupting network operations.
  - Incomplete coverage: Teams are not coordinated or synchronised, and patching is not planned or communicated.
  - Multiple vendors: Each vendor may have different procedures and timeframes for releasing patches.
  - Geographical dispersion: Deploying patches across different geographical locations adds another layer of complexity, as different regions may have varying requirements and time zones.
  - Service disruption: Patching does not take place with minimal impact on customer services.
- Compatibility and dependencies: In a multi-vendor environment, updates from one vendor may affect the functionality or security of components from other vendors. Managing dependencies and compatibility is key to maintaining a stable and secure network.
- Automation versus manual intervention: Whilst automation can help streamline the patching process, some updates may require manual intervention or configuration, which increases management complexity.

To illustrate the logistical challenges involved in the patching process, we will use the example of a telecommunications company with an Open Core architecture to describe the procedure an organisation must follow to ensure that any new security patches are deployed as soon as possible after their release.

1. Identification of the vulnerability – The company's security team identifies a new vulnerability in one of the components from Supplier A. Supplier A quickly releases a patch for this vulnerability.
2. Patch distribution – The patch must be distributed to all locations where the component from Supplier A is deployed. This includes several data centres and hundreds of base stations.
3. Patch testing – Before deploying the patch in the production environment, it must be thoroughly tested to ensure it does not cause further issues or incompatibilities with other components. This step involves testing in laboratory conditions and simulating real-world scenarios.
4. Coordination between teams – Deploying the patch requires coordination between several teams, namely the security team, the infrastructure management team and the operations teams at various data centres. Each team must be synchronised and ready to apply the patch within the same timeframe to minimise disruption to operations.

5. Patch deployment – The patch must be applied during a pre-scheduled maintenance window to minimise the impact on customer services. As the company provides services across different time zones, patching must be carefully planned to avoid peak operating hours.
6. Post-deployment monitoring – Once the patch has been deployed, continuous monitoring of the network is required to ensure that no unintended side effects have occurred. This includes monitoring network performance, incident reporting and customer feedback.

Effective management of updates and patches is essential for maintaining the security and stability of Open Core 5G networks. **By implementing these recommended measures,** organisations can better protect their infrastructure against ever-changing security threats.

- Regular inventory and assessment: Maintain an up-to-date overview of all software components and their versions within the network. Regularly assessing and categorising software components according to their security risk and importance to the network infrastructure facilitates a rapid response.

- Automated monitoring and patching: Using tools for automated monitoring of security vulnerabilities and patch application helps to reduce the time window and minimise the risk of human error during which the network may be exposed to known threats.

- Pre-deployment testing: Before applying patches or updates in a production environment, it is important to carry out testing in an isolated environment. This helps to identify potential compatibility issues or negative impacts on performance before they affect critical infrastructure.

- Emergency patching procedures: Develop and maintain procedures for rapid patching in the event of critical security vulnerabilities requiring an immediate response. This includes the ability to perform emergency updates outside the regular update cycle.

- Staff training and awareness: Ensure that staff responsible for network management and security are regularly trained and informed about best practices for managing patches and updates, as well as potential threats and how to address them.

- Coordination with suppliers: Maintain close cooperation and communication with suppliers to enable a rapid response to new threats and ensure the prompt release and application of patches.

3 Assessment of potential impacts on the overall security of the mobile network

Assessing the potential impacts on the overall security of 5G mobile networks involves analysing various aspects, ranging from technological to operational and strategic. As the successor to 4G, 5G networks bring significant improvements in speed, capacity and responsiveness, but this also brings new security challenges.

The **main potential impacts** described below relate to the network's inherent characteristics – open architecture, automation/innovation, software, virtualisation and the supply chain.

3.1 Expansion of attack entry points and vectors

The expansion of attack entry points[1] and vectors[2] in 5G networks requires a more detailed look at how 5G technology expands the possibilities for potential attackers and what specific challenges this poses for security teams.

3.1.1 Expansion of physical accessibility within the distributed architecture of 5G networks

5G networks are designed with a highly distributed architecture that integrates many small cells to provide high speeds and low latency. These small cells are deployed in public spaces, including urban areas, which increases physical accessibility and the potential risk of attacks.

3.1.2 Additional attack vectors via IoT devices

With the rise of 5G, the number of connected IoT devices becoming part of the network is growing exponentially. Many of these devices have inadequate security, providing attackers with new avenues to infiltrate networks and carry out attacks.

3.1.3 Exploiting weaker security in edge computing

5G networks utilise edge computing to process data closer to the source, reducing latency. However, edge servers may be vulnerable to attacks as they are located in less secure locations and may contain sensitive data.

3.1.4 Inadequate identification and authentication for a growing number of devices

Ensuring that every device connected to the network is legitimate and has not been compromised is crucial. This requires robust identification and authentication mechanisms capable of handling the vast number of devices in 5G networks.

---

[1] Definition of Expansion of attack entry points: The expansion of attack entry points refers to the overall scope and number of potential entry points (vulnerabilities) into the system that attackers can exploit to carry out an attack.

[2]

Definition of Broader Attack Vector: A broader attack vector focuses on the various ways and methods that attackers can use to penetrate a system. This includes various techniques and tactics that can be used to attack the system.

3.1.5 Logistically demanding deployment of updates andmanaging a growing number of devices

Device software management and regular updates are essential for maintaining their security. In a 5G network environment, this presents a logistical challenge given the vast number of devices.

3.1.6 Partial network compromises affecting the entire network infrastructure

To minimise the risks associated with the proliferation of entry points and attack vectors, it is important to implement segmentation[3] and isolation[4] within the 5G network. This ensures that a compromise of one part of the network does not affect the entire network infrastructure.

Securing 5G networks in the context of the proliferation of entry points and attack vectors requires a comprehensive and layered approach. It is essential to invest in advanced technologies for threat detection and response, as well as in user education and awareness regarding security risks. Cooperation between operators, equipment manufacturers, software developers and government agencies is key to creating a resilient and secure 5G network infrastructure.

3.2 Impact on security the network due dependence on software and virtualisation

The dependence of 5G networks on software and virtualisation brings with it specific security challenges. This dependence enables the rapid deployment of new services and innovations, but at the same time increases the risk of software errors and vulnerabilities that attackers can exploit.

- Software-Defined Networking (SDN) and Network Functions Virtualisation (NFV): - 5G networks make significant use of SDN and NFV for the flexible management and configuration of network functions. However, this flexibility also increases the potential for malicious software and virtualisation errors to be introduced into the network infrastructure.

- Dynamic Update and Configuration: - The ability to dynamically update and configure network functions means that software components can be frequently updated or changed. Conversely, frequent changes can accelerate and contribute to the introduction of new vulnerabilities or instability into the system.

- Widespread software vulnerabilities - The reliance of 5G networks on software means that any software vulnerability can have far-reaching implications for the security of the entire network. Attackers can exploit these vulnerabilities to gain unauthorised access, spread malware, or carry out denial-of-service (DoS) attacks.

3.2.1 Increased demands on software component updates and patch speeds

It is crucial to ensure that all software components are regularly updated and secured against known vulnerabilities. This requires careful monitoring of security advisories and the rapid application of patches.

3.2.2 Increased demands on the creation of security zones and control points

Applying the principles of segmentation and isolation to virtual network functions can help limit the scope of potential attacks. Creating security zones and control points between virtual functions and services can prevent attacks from spreading within the network.

3.2.3 Increased demands on security testing and verification

Intensive security testing and verification of software prior to deployment is essential. This includes the use of static and dynamic code analysis, penetration testing and security audits to identify and eliminate vulnerabilities.

---

[3] Network segmentation: Network segmentation is the process of dividing a single physical network into several smaller, logical networks that are separated and managed according to specific security policies and requirements. It focuses on dividing a single physical network into smaller, logical segments to improve the management and security of communication between different parts of the network.

[4] Network isolation: Network isolation is the process of ensuring that certain parts of the network or specific devices cannot communicate directly with other parts of the network or devices unless explicitly permitted. It focuses on preventing or restricting direct communication between specific parts of the network to ensure the protection of critical systems and data.

3.2.4 The wider impact of insider threats

Given that the management and maintenance of 5G networks require a high level of access to software and configuration tools, it is important to implement measures against insider threats, including access rights and activity monitoring.

Securing 5G networks, **given their reliance on software and virtualisation**, **requires** not only technical measures but also careful procedural and organisational approaches. Companies and organisations must invest in training their teams, developing security policies and procedures, and, last but not least, implementing advanced security tools and technologies to protect against ever-evolving threats.

3.3 A complex and extensive supply chain

5G networks rely on an extensive and complex supply chain that includes hardware manufacturers, software providers, and telecommunications infrastructure service providers. Each of these suppliers can pose a potential security risk if their products or services contain vulnerabilities.

3.3.1 Greater security and product verification

Ensuring that all components and software used in 5G networks are secure and do not contain hidden vulnerabilities or backdoors is extremely challenging. Vulnerabilities may be present in products intentionally or unintentionally, increasing the risk of espionage, sabotage or other cyberattacks.

3.3.2 Difficulties in selecting and excluding suppliers

The selection of suppliers may also be influenced by geopolitical factors, where certain countries or regions may pose a higher risk in terms of espionage or influence. This risk may lead to the exclusion of certain suppliers on national security grounds.

Geopolitical risk in the context of 5G networks refers to security challenges and risks associated with political and economic factors between different countries and regions. This risk can influence the selection of suppliers, the trustworthiness of technological solutions, and the overall security of telecommunications infrastructure. **The following points outline the main impacts of geopolitical risk:**

- International sanctions and restrictions:- Sanctions and restrictions imposed on certain countries may affect the supply of technologies and components needed to build and operate 5G networks. For example, US sanctions against China have affected the ability of Chinese manufacturers such as Huawei to supply technology to other countries.
- Political instability: - Political instability in certain regions can lead to uncertainty and disruption of supply chains. Investment in infrastructure in these areas can be risky, which may affect global supply chains.
- Concerns about cyber espionage: - There are concerns that certain countries may use technology companies to carry out cyber espionage. For example, allegations that Chinese firms such as Huawei may be used by the Chinese government for espionage purposes have led to these firms being excluded from building 5G networks in several countries.
- Critical Infrastructure: - 5G networks are considered critical infrastructure, meaning that their security is key to national security. The selection of suppliers must therefore be carried out with regard to trustworthiness and risks associated with national security.
- Trade Wars - Trade wars and economic conflicts between countries can affect the availability and price of technologies and components for 5G networks. For example, trade conflicts between the US and China have led to price increases for certain technological products.
- Technological dependence – Dependence on technologies and components from a single country may pose a risk. Should political conflicts or sanctions arise, this could significantly affect the availability of necessary technologies. Diversifying supply chains is therefore important to minimise this risk.

3.3.3 Dependence on key suppliers

Heavy reliance on a small number of key suppliers can pose a high risk should their products, services or supply chains be compromised. Diversifying suppliers can help mitigate this risk, but may be logistically and financially demanding.

3.3.4 Increased demands for supplier vetting

The vetting and certification[5]of suppliers against security standards is a fundamental step in ensuring security. This includes assessing suppliers' security procedures, their compliance with industry standards, and their methods of protection against cyber threats.

3.3.5 Increased requirements for contract compliance checks and auditing

Contractual measures[6] and auditing[7] are key strategies for ensuring the security and trustworthiness of the supply chain, particularly in the context of 5G networks. These procedures include formal contractual agreements that set out specific security requirements, and regular audits that verify that suppliers are complying with these requirements. Checks on contractual measures and auditing can minimise risks and ensure that suppliers provide secure and reliable services.

The main components of contractual measures and auditing are outlined below to illustrate specific requirements and changes within the scope of checks/audits:

1. Specification of security requirements – Contracts contain specific requirements for security measures that the supplier must implement. This may include data encryption, access control, staff security training and regular software updates.
2. Compliance with standards – Suppliers are required to comply with specific security standards and regulations (e.g. ISO 27001, GDPR), which ensure that their processes and systems meet the required level of security.
3. Rights and obligations – Contracts clearly define the rights and obligations of both parties, including the obligations of suppliers in the event of a security incident, liability for damages, and penalties for non-compliance with contractual terms.
4. Security audits – Contracts may include provisions for regular security audits to ensure that suppliers consistently meet the specified security requirements.
5. Regular audits – Organisations conduct regular audits of suppliers to verify compliance with contractual terms and security standards. Audits may be scheduled or unannounced.
6. External and internal audits: - Audits may be carried out internally by the organisation's staff or by external certified auditors who provide an independent assessment of suppliers' security measures.
7. Vulnerability assessments – Audits involve identifying and assessing vulnerabilities in suppliers' systems and processes. This may include penetration testing, checking compliance with security policies, and analysing security incidents.
8. Corrective actions – If audits reveal deficiencies or vulnerabilities, suppliers are required to implement corrective actions and improvements. Organisations may set deadlines for the implementation of these measures and monitor their fulfilment.

3.3.6 Pressure to diversify suppliers

Diversifying suppliers and ensuring there is no excessive reliance on a single supplier can increase resilience against risks associated with the supply chain. This includes seeking alternative suppliers for key components and services.

3.3.7 Increased demands on communication

Cooperation and information sharing between operators, suppliers and government bodies can help to identify and address security threats and vulnerabilities within the supply chain.

Securing the supply chain in the 5G ecosystem is complex and requires a proactive and coordinated approach. Effective strategies involve a combination of technical, organisational and policy measures to ensure the integrity and trustworthiness of all aspects of 5G infrastructure and services.

[5] Supplier vetting and certification is a process by which organisations systematically assess and verify the capabilities and security standards of their suppliers prior to their inclusion in the supply chain. This process typically involves formal audits, inspections and certification procedures, which are carried out on the basis of predefined criteria and standards.

.

[6] Contractual measures include the terms and conditions in contracts between an organisation and its suppliers that set out security requirements, standards and expectations.

[7] Auditing is the process of systematically reviewing and evaluating suppliers' security procedures and measures to ensure they comply with contractual measures.

3.4 Network scaling and automation with implications for system decision-making

Network scaling and automation are key to the effective management and optimisation of large-scale and complex 5G networks.

3.4.1 Reliance on automation

5G networks are designed to be highly dynamic and flexible, enabling operators to rapidly scale capacity and services according to current demand. This scaling is heavily reliant on automation, which allows networks to adapt to changes in real time.

3.4.2 More difficult to detect data manipulation

Artificial intelligence (AI) and machine learning (ML) are frequently used for network automation and optimisation. These technologies assist in predicting network load, detecting and responding to security threats, and optimising network traffic. However, reliance on AI and ML also brings potential risks, such as data manipulation, which could influence the system's decision-making.

3.4.3 Greater demands on fault tracing in automation processes

Automation also plays a key role in network configuration and management, which includes deploying network functions, security, and software updates. Whilst automation can significantly increase efficiency and reduce human error, it also increases vulnerability should the automation processes be compromised.

3.4.4 AI/ML could enable manipulation of network operations and the spread of malware

It is essential to ensure that AI and ML algorithms cannot be exploited by attackers to manipulate network operations or spread malware. This requires robust security for the datasets used to train the algorithms, and protection against attacks that could influence their behaviour.

3.4.5 Greater demands on automated incident response controls

Systems for automated incident response must be carefully designed to respond quickly and effectively to potential threats without disrupting network operations or causing false alarms.

3.4.6 Higher security requirements for automation

The security and integrity of the tools used for network automation are critical. This includes ensuring that these tools are not vulnerable to cyber attacks and that their operation is protected against unauthorised access.

3.5 The complexity of international standards and regulations

Standards and regulations play a vital role in establishing a common foundation for the development, implementation and security practices within 5G technologies, ensuring that networks from different operators and in different countries can interoperate securely and efficiently.

3.5.1 Differences in regulations and standardisation

Differences in national regulations and approaches to standardisation can complicate the global deployment of 5G technologies. Whilst some countries may adopt standards quickly, others may lag behind or adopt different regulations, which can lead to fragmentation and interoperability issues.

3.5.2 Security implications

Uniform international standards and regulations are essential to ensure a high level of security in 5G networks. This includes security protocols for encryption, authentication, privacy and data integrity. A lack of coordination and consistency in standardisation can open the door to potential security vulnerabilities.

3.5.3 Pressure for global cooperation

Strengthening global cooperation between countries, regulators and industry stakeholders is key to establishing and maintaining uniform international standards. This includes sharing best practices, joint research and development, and policy coordination.

3.5.4 Greater demands on monitoring and updating standards

Given the rapid pace of technological development, it is important that standardisation bodies regularly update and adapt standards to reflect the latest findings and technological innovations.

3.5.5 Greater demands on education and awareness

Informing and educating stakeholders about the significance and implications of international standards and regulations can support their faster and more effective implementation.

3.6 Increased volume of personal and sensitive data on the network

Privacy protection is a fundamental aspect of 5G network security. With the advent of 5G technology and its ability to support exponential growth in connected devices and applications, the volume of personal and sensitive data generated and transmitted over the network is increasing significantly.

Privacy protection in 5G networks is a multifaceted challenge that requires coordinated efforts between technology innovators, regulators and users. The transition to 5G emphasises the need for robust privacy protection and security measures to ensure that the technology serves the public interest and protects individual rights.

3.6.1 Massive deployment of IoT devices and increased privacy risks

5G networks enable the massive connectivity of IoT (Internet of Things) devices, ranging from smart home appliances to vehicles and industrial sensors. These devices collect and share vast amounts of data, often including personal information, raising concerns regarding surveillance, identification and data misuse.

3.6.2 Increased risk of data breaches

As the number of connected devices and the complexity of networks increase, so does the risk of data breaches. This can include both accidental leaks resulting from configuration errors or vulnerabilities, and deliberate attacks aimed at stealing personal data.

3.6.3 The need for stronger encryption and anonymisation

To ensure privacy protection in 5G networks, it is essential to use advanced methods of data encryption and anonymisation. These techniques help to ensure that, even if an attacker gains access to the data, the information remains protected and unreadable.

3.6.4 The need for regulation of data collection and fair use

Businesses and organisations using 5G networks should adhere to the principles of data minimisation and fair use. This means collecting only the data that is strictly necessary to provide the service and using the data only in accordance with the purpose for which it was collected.

3.6.5 Increased demands on data protection and privacy assessments

Organisations should regularly conduct data protection and privacy risk assessments and ensure that their procedures and technologies comply with applicable regulations, such as the GDPR in the European Union.

3.6.6 Future pressure to adopt data protection and privacy technologies

The development and implementation of privacy-focused technologies, such as homomorphic encryption or differential privacy techniques, can provide a high level of data protection whilst maintaining application functionality.

3.6.7 Greater demands on user education

User education and raising awareness of risks and best practices for personal data protection are key to strengthening overall security and privacy in the 5G ecosystem.

4 Assessment of potential and possible types of cyberattacks on Open RAN

Open RAN offers an innovative approach to the construction of telecommunications networks by promoting greater interoperability and flexibility between components from different manufacturers. However, this also requires an innovative approach to assessing potential and possible types of cyber attacks.

This section identifies attacks on the main components of Open RAN, namely data, data sources and the overall Open RAN architecture, and outlines possible countermeasures for each.

4.1 Attacks on data confidentiality

Data confidentiality is a key component of cybersecurity, encompassing the protection of information against unauthorised access and disclosure. With attacks on data confidentiality in 5G and Open RAN networks, a deeper understanding is required of how data may be compromised and what strategies can be employed to protect it. In the context of 5G and Open RAN networks, there are **specific cyber attacks:**

4.1.1 Eavesdropping

Eavesdropping refers to the unauthorised listening in on communications between devices or within a network. In a 5G/Open RAN environment, calls can be eavesdropped on, text messages monitored, application data intercepted, and even communications between network nodes monitored.

Countermeasures:

- Encryption: Implementing strong encryption at all levels of communication (from endpoints to network segments) can prevent attackers from decrypting intercepted data.
- Secure tunnelling: The use of VPNs (Virtual Private Networks) and protocols such as IPSec to secure data transmitted over public networks.

4.1.2 Man-in-the-Middle (MitM) attacks

MitM attacks allow an attacker to insert themselves into the communication between two parties, thereby enabling them to eavesdrop, modify or insert messages without the parties' knowledge. In 5G/Open RAN, this can be particularly problematic given the dynamic nature of network traffic and communication.

Countermeasures:

- Mutual authentication: Ensuring that both communicating parties can authenticate each other before exchanging any data, which helps prevent attackers from successfully carrying out MitM attacks.
- Network segmentation: Limiting an attacker's ability to move within the network and carry out MitM attacks through careful design of the network topology and isolation of critical systems.

4.1.3 Supply chain trust attacks

Given that Open RAN promotes greater openness and interoperability between different manufacturers and components, this may entail an increased risk of attacks on data confidentiality.

Countermeasures:

- Ensuring data confidentiality in 5G and Open RAN networks requires a comprehensive approach, including strong encryption, rigorous authentication, network segmentation, and the implementation of zero-trust principles. These measures help protect sensitive information and ensure that networks remain resilient against unauthorised access attempts or attacks.

4.2 Attacks on data integrity

Data integrity attacks in 5G and Open RAN networks are attacks aimed at damaging, manipulating or compromising the trustworthiness of information. Ensuring data integrity is essential for the functionality and security of the entire telecommunications ecosystem.

4.2.1 Injection attacks

Injection attacks occur when an attacker inserts or 'injects' malicious data into a system with the aim of performing unauthorised operations. In the context of 5G/Open RAN, this may involve inserting malicious code into network communications or manipulating data flows, leading to service disruption or the spread of malware.

Countermeasures:

- Input validation: Careful checking and restriction of all incoming data to permitted types and formats can prevent injection attacks from succeeding.

- Security protocols and encryption: The use of security protocols and encryption for communication between nodes and devices protects the integrity of transmitted data.

4.2.2 Identity spoofing

Spoofing attacks involve impersonating another entity or device on the network with the aim of gaining unauthorised access to data or services. In 5G and Open RAN environments, attackers can use spoofing to obtain sensitive information or disrupt network communications.

Countermeasures:

- Authentication and authorisation: Ensuring that every entity on the network can be uniquely identified and authenticated before communication begins helps prevent spoofing attacks.

- Network policies and monitoring: Establishing and enforcing strict network policies, alongside continuous monitoring of network traffic, enables rapid detection and response to spoofing attempts.

4.2.3 Supply chain integrity attacks

Given that Open RAN supports greater flexibility and the integration of various technological components from different suppliers, specific challenges may arise regarding data integrity protection.

Countermeasures:

- Security certifications and standards: Ensuring that all components and devices used in the Open RAN network meet robust security standards and have undergone security certification.

- Extended Detection and Response (EDR): Implementing EDR solutions at key network nodes can help with the rapid detection of and response to attempts to manipulate data or other attacks on integrity.

4.3 Attacks on data availability

These attacks are designed to disrupt or completely prevent access to legitimate services and data, which can have serious consequences for users and service providers. In 5G and Open RAN environments, where high levels of connectivity and reliability are expected, attacks on availability are particularly critical.

4.3.1 DDoS (Distributed Denial of Service) attacks

DDoS attacks are one of the best-known forms of availability attack, in which attackers overwhelm network resources (e.g. servers, network infrastructure) with a massive volume of illegitimate traffic, thereby preventing access for legitimate users.

Countermeasures:

- Load balancing and redundancy: Creating multiple copies of critical components and distributing traffic can help absorb the impact of DDoS attacks.
- DDoS protection services: Utilising specialised DDoS protection services that can detect and mitigate attacks before they cause damage.
- Rate limiting and traffic filtering: Implementing rate limiting rules and filtering suspicious traffic at network boundaries can help minimise the impact of DDoS attacks.

4.3.2 Attacks on power sources

The deliberate depletion or disruption of power supplies to network devices, such as transmitters or servers, can lead to service outages. These attacks can be carried out physically or via software (e.g. by causing a device to overload, resulting in excessive power consumption).

Countermeasures:

- Monitoring and management of power resources: Continuous monitoring of energy consumption and forecasting needs based on data analysis can help identify unusual consumption patterns in good time.
- Energy efficiency and redundancy: Improving the energy efficiency of equipment and ensuring redundancy of power sources can help mitigate attempts to drain power.

4.3.3 Attacks exploiting the complexity of the Open RAN architecture

The Open RAN architecture supports a diversity of vendors and components, which can make it difficult to implement a unified solution to protect against availability attacks. Greater complexity and the need to integrate diverse technologies can also mean more potential vulnerabilities.

Countermeasures:

- Advanced monitoring and analysis: The use of advanced tools for monitoring network traffic and device behaviour can help to quickly identify and respond to attacks.
- Cooperation and information sharing: Collaboration between operators, suppliers and security organisations in sharing information on threats and best practices can strengthen defences against availability attacks.

4.4 Some other types of attacks on Open RAN

Open RAN also presents specific security challenges that require comprehensive, multi-layered security strategies.

4.4.1 Side-channel attacks

These attacks exploit information gleaned from side channels, such as power consumption, electromagnetic emissions or even acoustic signals, to uncover sensitive information about network equipment or ongoing operations. Open RAN can be particularly vulnerable if hardware components are not carefully secured.

Countermeasures:

- Physical security: Protecting physical devices from unauthorised access.
- Isolation and encryption: Use of task isolation and data encryption to make it more difficult to obtain useful information via side-channel analysis.

4.4.2 Attacks on interfaces between individual RAN components

Open RAN with different manufacturers and components may pose an increased risk of attacks targeting the interfaces and APIs between these components.

Countermeasures:

- Strong API security protocols: Implement robust security controls and authentication mechanisms for all communication between components.
- Regular security audits: Continuous monitoring and updating of security measures at the interfaces.

4.4.3 Attacks on SDN and NFV

As Open RAN often utilises SDN and NFV to increase network flexibility and efficiency, these technologies become targets for attacks, i.e. attackers manipulate virtual network functions or attack SDN controllers.

Countermeasures:

- Securing the virtualised layer: Ensuring that all virtual network functions are well isolated and protected.
- Strong authentication and encryption: Protecting communication between SDN components and NFV instances.

4.4.4 Insider attacks

Insider attacks pose a threat from internal personnel with legitimate access to the network infrastructure, who may abuse their privileges to carry out malicious actions. These include the following examples of specific types of attacks:

- Theft of sensitive information – An employee with access to confidential information, such as user login credentials, financial data or technical specifications, may copy this information and sell it to third parties or use it for personal gain.
- Manipulation of network configuration – An administrator with access to network configuration may deliberately alter the settings of network components to cause service outages, reduce performance, or expose the network to external attackers.
- Malware installation – An attacker from within the organisation may install malware onto systems or devices on the network, which may lead to gaining access to sensitive data, monitoring network traffic, or even taking complete control of the network.
- Sabotage – A disgruntled employee may deliberately damage hardware, delete critical files or cause other forms of physical or logical sabotage, which can result in serious service outages or data loss.
- Unauthorised changes to software – A developer or technician with access to development or operational systems may make unauthorised changes to software code or settings, which can lead to security vulnerabilities or other issues.
- Creating backdoors – An attacker from within the organisation may create backdoors in software or network components, allowing unauthorised access to the system for themselves or for other attackers.
- Abuse of access rights – An employee with high-level privileges may abuse their rights to access systems or data to which they would not normally have access, and use this information for personal gain or to harm the organisation.

Countermeasures:

- Regular security audits: Checking access rights and monitoring employee activities.
- Least privilege principle: Restricting access to only the information and systems that are strictly necessary.
- Security training: Regular training of employees on security procedures and the identification of potential threats.
- Monitoring and logging: Implementation of systems to monitor and log all network access and activity.
- Incident response: Development and testing of plans for responding to security incidents.

5 Analysis of opportunities and risks related to identity and access management in 5G networks

The transition to 5G technology is bringing about significant changes in network architecture and operation, presenting both new challenges and opportunities for Identity and Access Management (IAM) systems. The analysis of opportunities and risks associated with identity and access management covers several key areas, including security, privacy, interoperability, and scalability.

First, we will outline the possibilities and benefits of identity and access management, which we will then weigh *against the associated risks.*

5.1 Enhanced security

Enhanced security within 5G networks, based on the IAM technology and principles that networks use to protect data and communications, allows users and devices to use the network with confidence that their information and privacy are protected.

5.1.1 Advanced encryption protocols

5G networks utilise the latest and most secure encryption standards, such as AES (Advanced Encryption Standard), to encrypt data transmitted over the network. These protocols ensure that data is protected against unauthorised access during transmission.

5.1.2 Robust authentication techniques

5G networks are introducing advanced authentication methods that go beyond traditional passwords and PIN codes. This includes the use of biometric data, such as fingerprints, facial recognition or voice verification, as well as two-factor authentication (2FA) or multi-factor authentication (MFA) to enhance security when accessing network services.

5.1.3 Security protocols for integrity and authentication

5G implements specific security protocols designed to protect data integrity and authentication. These protocols help ensure that data has not been tampered with during transmission and that communication takes place between authenticated parties.

5.1.4 Network isolation and segmentation

5G technology enables advanced network segmentation, meaning that different parts of the network can be isolated for specific purposes or applications. This allows for better access control and enhances security by minimising the risk of potential threats spreading across the entire network.

5.1.5 Real-time threat detection and response

Thanks to the high throughput and low latency of 5G networks, security systems can effectively monitor network traffic and respond quickly to anomalies or potential security threats. This includes automated systems for detecting attacks and vulnerabilities, which can immediately flag issues and automatically implement countermeasures.

Improved security in 5G networks is therefore not just about stronger encryption algorithms and more robust authentication methods; it encompasses a comprehensive set of technologies and protocols designed to protect the network and its users from a wide range of cyber threats. These security features form the basis for the trusted use of 5G technologies in a variety of applications, from smart homes and IoT devices to critical infrastructure and enterprise networks.

5.2 High scalability

High scalability is one of the key attributes that 5G networks bring to the world of telecommunications, and this has a significant impact on identity and access management (IAM). This feature enables the network to support a vast number of connected devices.

5.2.1 Support for massive IoT and mobile devices

One of the main goals of 5G technology is to enable massive IoT, ranging from smartphones and tablets to a wide spectrum of IoT devices such as sensors, smart home devices, autonomous vehicles and industrial machinery, which means supporting tens of thousands of devices connected to the network per square kilometre. This requires a scalable IAM solution that can effectively manage identity and access rights for a vast number of devices, whilst ensuring security and privacy.

5.2.2 Dynamic management

The high scalability of 5G enables dynamic management of network resources and services, meaning that IAM systems can be adaptive and flexible. This includes the ability to quickly add, update or remove device and user identifiers in real time, which is essential for ensuring security.

5.2.3 Effective segmentation and access policies

Thanks to the network's advanced capabilities, it is possible to effectively segment the network and apply granular access policies based on user or device identities. This segmentation enables the creation of virtual private networks (VPNs) for different types of devices or user groups, which enhances security by isolating sensitive data and operations from other parts of the network.

5.2.4 Automation and AI

With the growing number of devices, the use of automation and artificial intelligence (AI) for IAM management is becoming essential. Highly scalable 5G networks enable the deployment of AI and machine learning to automate identification, authentication and authorisation processes. This not only streamlines management but also helps to predict and respond to security threats in real time.

5.2.5 Enhanced interoperability

The high scalability of 5G networks also supports better interoperability between different networks and services, which is key to managing identities and access across different platforms and providers. This includes the ability to manage identity and access for users and devices that interact with many different network services and applications, simplifying management and improving the user experience.

The high scalability of 5G networks therefore opens up new horizons for IAM solutions, enabling the efficient management of a vast number of devices and users, whilst enhancing security, efficiency and flexibility in a dynamic and interconnected digital world.

5.3 Reduced latency

The reduced latency offered by 5G networks has a significant impact on authentication and authorisation processes. Latency, or delay time, is the time that elapses between sending a request from one point in the network and receiving a response. 5G networks are designed to minimise this delay, often to a few milliseconds or less, which has a significant impact on a range of applications and services and support within identity and access management.

5.3.1 Faster authentication and authorisation

Reduced latency means that authentication and authorisation processes can take place much more quickly. This is particularly important in situations where access speed is critical, such as when accessing secure services, carrying out financial transactions, or using services that require an immediate response.

5.3.2 Improved user experience

Faster system response to user requests improves the overall user experience. Users expect fast and seamless access to digital services and applications, and 5G's reduced latency makes this possible. This is particularly significant for applications such as video streaming, cloud gaming, or virtual and augmented reality, where speed and instant response are essential for a high-quality experience.

5.3.3 Enhanced real-time security

Reduced latency enables the implementation of real-time security measures, such as the immediate detection of and response to security threats through the rapid identification and blocking of unauthorised access attempts.

5.3.4 Support for critical applications

Many critical applications and services, such as autonomous vehicles, remotely controlled operations, or emergency response systems, require very low latency for safe and efficient operation. The reduced latency of 5G networks enables the reliable real-time communication that is essential for these applications.

5.3.5 Integration with Edge Computing

The reduced latency of 5G is key to the effective use of edge computing, where data processing and computational tasks are moved closer to end users. This arrangement enables faster processing and response times, which is essential for applications requiring immediate data processing, such as real-time video analysis or interactive applications.

5.4 Edge Computing

Edge computing refers to a distributed computing architecture in which data processing and computational tasks are performed at the edge of the network, i.e. as close as possible to the data source or the end user. This arrangement offers a number of benefits that positively impact the efficiency, speed and security of IAM systems in a 5G environment.

5.4.1 Localisation of data processing

By moving data processing closer to end users or edge computing devices, latency is reduced and system response times are improved. In the context of IAM, this means faster authentication and authorisation of users and devices, which is essential for applications requiring immediate processing or real-time access control.

5.4.2 Enhanced security and privacy

Edge computing enables a large portion of data to be processed locally without having to be transferred via central servers or to the cloud. This minimises the risk of data leaks during transmission and allows for better control over and protection of data. Within IAM, this means that sensitive information, such as biometric data for authentication, can be processed locally, reducing the risk of compromise.

5.4.3 Scalability and flexibility

Thanks to its ability to process data across many different locations, edge computing enables organisations to scale their operations. It also allows IAM systems to adapt quickly to a growing number of users and devices, whilst ensuring that performance and security requirements are consistently met.

5.4.4 Support for IoT and mobile devices

Edge computing is essential for the effective management and security of IoT devices, which are often dispersed and generate large volumes of data. The integration of edge computing with 5G networks enables rapid data processing and analysis directly on-site, facilitating device authentication and authorisation whilst minimising latency and network load.

5.4.5 Real-time response to threats

The combination of edge computing with the low latency of 5G networks enables an unprecedented ability to detect and respond to security threats in real time. Systems can immediately identify suspicious activity and take measures to thwart it, thereby improving overall system and data protection.

The above-mentioned capabilities related to identity and access management in 5G networks open up new avenues for the development of safer, faster and smarter digital services and infrastructure that can better respond to the needs of a modern, digitally connected society.

5.5 Network complexity

Network complexity is **a significant risk** associated with 5G technologies, which can have far-reaching consequences for network security, management and performance. This risk is particularly relevant in the context of identity and access management (IAM).

5.5.1 Increased number of entry points for attackers

5G networks support a massive number of connected devices, including IoT devices, which means an increase in potential entry points for cyber attackers. With every connected device comes a potential vulnerability that can be exploited. Identity and access management must therefore be extremely robust and capable of monitoring and managing security risks across a vast number of devices.

5.5.2 Complexity of configuration and management

With the transition to 5G, network complexity is increasing not only due to the greater number of devices, but also because of new technologies and architectures such as Network Functions Virtualisation (NFV) and Software-Defined Networking (SDN). In this sense, these technologies can complicate configuration, management and monitoring, which may lead to human error or the overlooking of security vulnerabilities.

5.5.3 Independent components and ensuring interoperability and compatibility

Integrating 5G with existing systems and technologies requires ensuring interoperability and compatibility between different network components and services. This effort to ensure seamless interconnection can reveal new security vulnerabilities, as systems and protocols that were originally designed independently must now work together.

5.5.4 The complexity of end-to-end security

5G networks are designed with the aim of providing end-to-end security, which involves protecting data transmitted between devices and networks. The complexity of such a requirement demands comprehensive security measures at various levels of the network, from the physical layer right up to the application layer. The effective implementation and management of these security measures is challenging and requires thorough planning and coordination.

5.5.5 Challenging management of security updates and patches

Given the rapid development of 5G technologies and applications, new security threats and vulnerabilities are emerging, requiring ongoing updates and patches. Managing these updates and keeping systems up to date and secure within such a complex and dynamically changing network infrastructure is a challenge.

Overall, the complexity of 5G networks presents significant challenges for IAM systems, requiring advanced solutions and strategies to ensure security, management and performance in these complex environments.

5.6 Expansion of entry points and attack vectors

The expansion of the attack surface **is a significant risk** associated with the implementation and operation of 5G networks. An attack refers to all the various points in the system that an attacker could potentially exploit to gain unauthorised access or carry out malicious activities. In the context of 5G networks and IAM systems, this expansion is linked to several key aspects.

5.6.1 Increased number of connected devices

5G networks enable an exponential increase in connected devices, particularly in the IoT sector. Every device, from smart home appliances to industrial sensors, can represent a potential point of attack. Identity and access management for such a vast and diverse set of devices is complex and requires robust security solutions.

5.6.2 More complex network infrastructure

5G technology introduces new architectural components, such as Network Functions Virtualisation (NFV) and Software-Defined Networking (SDN), which add further layers to the network infrastructure. These components may contain inherent vulnerabilities or may be misconfigured, thereby expanding the attack surface

5.6.3 Network diversity and heterogeneity

5G networks integrate various types of networks and technologies, including LTE, Wi-Fi and new radio access networks. This heterogeneity makes it difficult to provide uniform protection and manage security policies, increasing the complexity of monitoring and responding to threats.

5.6.4 Increased user and device mobility

5G networks support greater user and device mobility with faster connections and lower latency. This enables new types of applications and services, but also complicates the tracking and securing of mobile devices and data flows across different networks and geographical areas.

5.6.5 Widespread threats and more sophisticated attacks

As the capabilities of 5G networks grow, so does the sophistication of potential cyberattacks. Attackers can use advanced methods, including AI and machine learning, to identify and exploit vulnerabilities in the network. 5G networks are thus facing a wide range of attacks, from distributed denial-of-service (DDoS) attacks to advanced persistent threats (APTs).

5.7 Interoperability issues

Interoperability issues pose **a significant risk** that can impact authentication and authorisation systems. Interoperability refers to the ability of different systems, devices and applications to communicate with one another and work together effectively, which is essential for the smooth and secure operation of large-scale, heterogeneous 5G networks.

5.7.1 Compatibility between different technologies and standards

5G networks support technologies including older mobile networks (e.g. 4G LTE), Wi-Fi, new radio access technologies and IoT technologies. Ensuring compatibility and interoperability between these different systems and standards is complex and can lead to authentication and authorisation issues if not properly configured.

5.7.2 The complexity of identity and access management

Given the diversity of devices and services in 5G networks, identity and access management (IAM) presents a challenge. Interoperability issues can complicate the management of user identities, permissions and access policies, particularly when systems from different vendors or services running on different platforms need to be integrated.

5.7.3 Ongoing expansion or integration with existing networks

5G networks are designed to work in conjunction with existing telecommunications infrastructures and networks. This requires IAM systems to be capable of supporting the various authentication and authorisation mechanisms used in these networks, which can cause interoperability and compatibility issues.

5.7.4 Challenges in standardisation and regulation

Uniform standardisation and regulation are key to ensuring interoperability in 5G networks. There is a potential for inconsistencies or delays in the development and implementation of standards, which affect the security and functionality of networks.

5.7.5 Security risks associated with interoperability

New security vulnerabilities may arise, as the integration of different systems and technologies often requires compromises in security. For example, if two systems use different security protocols, their integration may result in weaker security.

Addressing these issues requires close collaboration between equipment manufacturers, network providers, standardisation bodies and regulatory authorities. Furthermore, it is important to invest in the development of flexible and modular IAM systems that can be easily adapted to different technology platforms and standards, thereby minimising the impact of interoperability issues on the security and performance of 5G networks.

5.8 Privacy concerns

Privacy is **a key concern** in the context of 5G networks, which can also be affected by the way identity and access are managed. The volume of personal data generated and processed is increasing. Privacy breaches occur in the following areas listed below.

5.8.1 Massive data collection

5G networks enable the collection, transmission and analysis of vast amounts of data from a wide variety of devices in real time. This data collection includes not only personal and sensitive information, but also data on users' location and behaviour. If data is not properly protected, this can lead to serious privacy breaches.

5.8.2 Data security risks

The increased number of devices and the complexity of the network expand potential points of attack, increasing the risk of data leaks or misuse. Insufficiently secured devices or communication channels may be vulnerable to cyberattacks, threatening users' privacy.

5.8.3 Inadequate encryption and data protection

Despite the advanced encryption capabilities offered by 5G, the implementation of encryption may be inconsistent across different devices and services. This can lead to situations where data is transmitted or stored without adequate protection, thereby increasing the risk of its misuse.

5.8.4 Issues with data control and management

Users may have limited control over how their data is collected, processed and shared within 5G networks. This complicates the management of privacy and consent, particularly in the context of international and multi-party networks and differences in legal and regulatory data protection requirements.

5.8.5 Technically complex anonymisation and data minimisation

Even when attempting to anonymise or pseudonymise data, the data sets collected within 5G networks can be so detailed and extensive that anonymisation becomes technically complex or ineffective. This increases the risk of individuals being identified even from large and seemingly anonymous data sets.

5.9 Inadequate authentication and authorisation mechanisms

Inadequate authentication and authorisation in the context of 5G networks pose **a significant risk** that can lead to various security incidents, including unauthorised access, data leaks, or misuse of services. Within 5G networks, which promise higher speeds, massive connectivity and low latency for a wide range of applications from IoT to critical infrastructure, robust authentication and authorisation systems are essential for ensuring security and trust.

5.9.1 Unauthorised access to network resources and services

Weak or compromised authentication mechanisms allow attackers to gain access to sensitive resources or services, which can lead to data breaches, service abuse or sabotage of operations.

5.9.2 Man-in-the-middle (MitM) attacks

Inadequate authentication protocols increase the risk of MitM attacks, in which an attacker eavesdrops on or manipulates communications between two parties without their knowledge. This can lead to the theft of sensitive information, including personal data and login credentials.

5.9.3 Identity spoofing

Weak or ineffective authentication and authorisation methods can make it easier for attackers to impersonate legitimate users or devices and carry out malicious activities, such as spreading malware, phishing attacks or service abuse.

5.9.4 Replay attacks

Without adequate security measures, such as one-time tokens or timestamps, authentication requests can be intercepted and reused by an attacker to regain unauthorised access.

5.9.5 Increased management burden and complexity

In an environment with a diverse range of devices and applications, such as that offered by 5G networks, the management of authentication and authorisation requires advanced identity and access rights management. An inadequate solution can increase the administrative burden and lead to management errors that open up new security gaps.

Mitigating these risks requires a comprehensive approach to security, utilising strong authentication methods (multi-factor authentication (MFA), encryption, secure tokens) and other advanced techniques to ensure that only authorised users and devices have access to network resources and services. In addition, it is important to continuously monitor and review security policies and procedures to ensure they remain up to date.

6 Risks associated with the implementation of Open RAN and Open Core

Open RAN and Open Core enable a more flexible and innovative approach to the development and management of telecommunications networks. The implementation of Open RAN and Open Core architectures in 5G networks presents security challenges and risks, particularly those related to the integrity of data transmission.

6.1 Unclear boundaries in the division of security responsibilities

The division of security responsibilities in the context of implementing these architectures is a key risk that negatively impacts the security and integrity of data transmissions in 5G networks. The risk relates to ambiguities and potential gaps in protection that may arise due to the multi-layered and distributed nature of these architectures.

6.1.1 Increased demands on coordination within the supply chain

The list of differences below serves to explain where risk needs to be monitored and managed:

- Modular and distributed nature: Open RAN and Open Core architectures enable telecommunications operators and service providers to combine and integrate components and systems from different manufacturers. This flexibility leads to greater complexity in coordinating security policies and measures across different suppliers and systems.
- Diversity of suppliers and technologies: With a multitude of suppliers and technologies, the risk of inconsistency in security standards and practices increases. Not all suppliers may have the same level of security, which can create weak points in the overall security architecture.
- Comprehensive management and updates: Managing security and implementing updates in such a diverse and dynamic environment requires coordinated and ongoing effort. Ambiguity regarding responsibility for security patch updates and responding to security incidents can lead to neglect or delays in implementing critical security fixes.

6.1.2 Specific threats associated with the incorrect allocation of security responsibilities

- Security gaps: If it is not clearly defined who is responsible for protecting specific aspects of the network infrastructure, a particular area may be left unmanaged, and attackers can exploit this.
- Incident response coordination: In the event of a security incident, a rapid and effective response may be hampered by uncertainty over who is responsible for handling the incident. Such delays can exacerbate the impact of the incident.

Countermeasures:

- Establishing clear contractual agreements: Contracts and agreements between operators and suppliers should clearly specify the division of security responsibilities and requirements for security standards.
- Standardisation and certification: Promoting and adhering to standardised security protocols and rules, including the certification of components and systems, can help ensure a consistent level of security across the entire ecosystem.
- Cooperation and information sharing: Building partnerships and collaborative networks between operators, suppliers and security institutions to share information on threats, vulnerabilities and best practices in the field of security.

6.2 Expansion access access and attack of in the context of Open RAN and Open Core implementation

6.2.1 Exploitation of the openness and dynamism of Open RAN and Open Core

We face **the exploitation of the openness and dynamism of Open RAN and Open Core** in relation to the main strengths of these architectures, namely flexibility and adaptability. The points below specify its specific aspects.

- Integration of components from different manufacturers: Open RAN and Open Core allow operators to combine hardware and software components from different suppliers. This diversity can make it difficult to ensure consistent security across all network elements, as each manufacturer may have different security procedures and standards.

- Greater system openness: Architectures supporting open standards and interfaces are naturally more susceptible to exploitation if not properly secured. Openness facilitates interoperability and innovation, but it also allows attackers to better understand the system's internal mechanisms and potentially find ways to compromise them.

- Complex network configuration: The dynamic and flexible network configurations enabled by Open RAN and Open Core can lead to difficulties in monitoring and protecting against security threats. Proper configuration and maintenance of security policies require advanced tools and expertise.

6.2.2 Specific threats associated with the exploitation of the openness and dynamism of Open architectures

- Unauthorised access to network segments: Attempts to access network segments that should not be accessible to a given user or device, or unusual login patterns to sensitive areas of the network.

- Unusual network traffic between segments: Unusually high volumes of data transferred between network segments that do not normally communicate, and attempts to communicate between segments that should be isolated.

- Anomalies in virtual machines and containers: Unusual changes in the configuration or status of virtual machines (VMs) or containers, and attempts to access or manipulate the hypervisor or virtualisation management.

- Hidden networks (tunnelling): Detection of traffic tunnelling that may bypass security policies or network segmentation. Use of unknown or unauthorised protocols to conceal communication.

- Unusual configuration changes: Unplanned or unexpected changes to the configuration of the network or virtualisation environment. Changes to firewall or routing rules that are not approved or documented.

- Attempts to escalate privileges: Activities aimed at obtaining higher privileges than those assigned to a user or device. Exploitation of vulnerabilities to gain administrator or root access.

- Malware and unknown software: Detection of the installation or execution of unknown or suspicious software on virtual machines or host systems. Activity associated with malware, such as attempts to spread across network segments or data exfiltration.

- Unusual monitoring and debugging activities: Use of monitoring or debugging tools not commonly used in a given network segment or environment. Unauthorised attempts to monitor network traffic or system logs.

- Easier targeting by attackers: A greater number of interfaces and components means more potential entry points for attackers. Any vulnerability in one of these points can be exploited to compromise the integrity of data transmission or to gain unauthorised access to network resources.

- More complex detection and resolution of security incidents: A larger and more complex network infrastructure can make it harder to detect security incidents in a timely manner and slow down the response to them, increasing the risk of damage caused by attackers.

Countermeasures:

- Strengthening security protocols (e.g. SSH, TLS): Implementing advanced security protocols and regular security updates for all network components, including end-point devices and network infrastructure. Ensuring that all management of network devices and applications takes place via secure channels prevents attackers from obtaining sensitive information.

- Encryption of data at rest and in transit: The use of strong encryption algorithms to protect data stored on systems and transmitted over the network safeguards against eavesdropping and data leaks.

- Advanced monitoring and detection tools: The use of sophisticated tools for network monitoring and the detection of anomalies that may indicate security threats, including attempts to compromise data integrity. Continuous monitoring of network traffic and detection of anomalies.
- Automation of incident response: Implementation of automated incident response systems capable of responding immediately to detected threats, for example by isolating affected segments or shutting down compromised VMs.
- Isolation of critical networks and functions, network segmentation: Creating security zones and using virtualisation to separate critical network functions and services from other parts of the network reduces the risk of attacks spreading.
- Deployment of firewalls and intrusion prevention systems (IPS): Protects the boundaries between network segments and monitors traffic for suspicious activity.
- Training and awareness: Ensuring that all stakeholders are informed about potential security risks and best practices for minimising them.
- Regular audits and testing: Conducting regular audits and penetration tests to ensure that segmentation and virtualisation are correctly configured and do not contain vulnerabilities.

6.3 Incompatibility and configuration errors

Compatibility and configuration present significant challenges in the context of implementing Open RAN and Open Core architectures in 5G networks. These relate to the integration and effective operation of diverse components and systems from many different suppliers. Not only must these systems work together reliably, but they must also meet strict security requirements to protect data transmission and the overall integrity of the network.

6.3.1 Problematic configuration and management

The complexity of implementation and subsequent management is characterised by the following key issues:

- Integration of heterogeneous systems: Network components and systems in Open RAN and Open Core architectures may come from many different vendors, each with their own specifications and protocols. Ensuring their seamless integration and interoperability can be complex and challenging.
- Configuration complexity: With a greater number of configurable components and parameters, the complexity of network management and optimisation increases. Correct configuration is key to network security, performance and reliability, but it also presents greater scope for human error and configuration flaws.
- Updates and maintenance: Regular software and firmware updates are essential for security and functionality, but coordinating these updates across diverse systems and vendors can be a challenge. Inadequate maintenance or incorrect updates can cause security vulnerabilities or service outages.

6.3.2 Specific threats associated with configuration and management issues

- Security weaknesses: Incorrect configuration or incompatibility between system components can create security gaps that attackers can exploit to gain access to network resources or compromise the integrity of data transmission.
- Outages and reduced performance: Compatibility and configuration issues can lead to network instability, service outages and reduced performance, affecting end users and potentially undermining trust in the operator.

Countermeasures:

- Thorough testing and validation: Rigorous compatibility and performance testing prior to deployment in a live environment can identify and resolve potential compatibility and configuration issues.
- Automation and configuration management tools: The use of advanced tools for configuration automation and change management can help minimise human error and simplify the management of complex networks.
- Collaboration and standardisation: Close collaboration between operators, suppliers and standardisation bodies can support the creation of and adherence to standards and protocols that facilitate interoperability and the secure integration of components.
- Continuous education and training: Investment in the education and training of technical teams raises awareness of best practices in configuration and security, contributing to a more robust and secure network infrastructure.

Overcoming the challenges associated with compatibility and configuration requires a combination of technological, process-related and human factors. The key to success lies in detailed planning, thorough testing and the continuous improvement of processes and skills.

6.4 Unauthorised access, unreliable authentication

Access control and authentication are critical security **aspects** in the context of implementing Open RAN and Open Core architectures in 5G networks. They are essential for protecting against unauthorised access and ensuring that only authorised users and devices can communicate over the network and access sensitive data. Weaknesses in access control and authentication mechanisms can significantly increase the risk of data transmission integrity breaches and compromise of the entire network.

6.4.1 Issues related to access control and authentication

The challenges associated with access control and authentication are best summarised by the key factors below:

- Complexity of identity management: In large-scale, heterogeneous networks, such as those utilising Open RAN and Open Core, the management of user and device identities is highly complex. It must be ensured that each entity is assigned the correct permissions and that these permissions are correctly applied across various systems and services.

- Risk of weak authentication protocols: The use of outdated or weak authentication methods can make it easier for attackers to gain unauthorised access. In the dynamic environment of 5G networks, it is essential to use strong, multi-factor authentication methods.

- Inconsistencies in access policies: In multi-layered and modular architectures, ensuring consistency in security policies and access rules across different components and vendors can be a challenge.

6.4.2 Specific threats associated with unauthorised access or unreliable authentication

- Data and service compromise: Weaknesses in authentication and access control can allow attackers to access sensitive data or misuse network services, leading to a breach of data integrity and confidentiality.

- Widespread security incidents: Once unauthorised access is gained, it may allow attackers to spread across the network, complicating the detection and remediation of security incidents.

Countermeasures:

- Implementation of strong authentication mechanisms: The use of multi-factor authentication (MFA) and advanced encryption technologies enhances security when accessing network resources and services.

- Use of strong password and key policies: Implementing robust policies for the creation and management of passwords and encryption keys protects against brute-force attacks and other methods of bypassing authentication.

- Centralised identity and access management: The use of centralised identity management (IDM) and access management (IAM) systems enables more effective control over who has access, to which resources, and under what conditions.

- Consistent access policies and rules: Developing and maintaining consistent security policies and access rules across all network components and suppliers ensures that all aspects of the network are adequately protected.

- Regular review and audit of access rights: Periodic checks and audits of access rights ensure that permissions remain up to date and align with user needs and security requirements.

Effective access management and authentication require constant attention and updating to reflect changing security threats and technological developments.

6.5 Supply chain risks

Supply chain risks represent a significant area of concern in the context of implementing Open RAN and Open Core architectures in 5G networks. These risks stem from an increased reliance on a broad network of suppliers providing hardware components, software applications and services. As Open RAN and Open Core promote greater openness and interoperability, the network may become more susceptible to vulnerabilities introduced via the supply chain, encompassing both intentional and unintentional security threats. Representative risks and their descriptions are set out below.

- Vulnerabilities and backdoors: Components and software from suppliers may contain hidden vulnerabilities or intentionally inserted backdoors that enable unauthorised access or malicious activities. These risks are particularly concerning if the sources of these components are unclear or untrustworthy.
    - Malware-infected updates: A scenario where a supplier accidentally or intentionally releases a software update containing malware, which can then be distributed across the entire network, compromising data and services.
    - Compromised components: Physical components, such as chips or modules, may contain hidden vulnerabilities or malicious elements that were introduced during the manufacturing process by subcontractors.
- Non-compliance with security standards: Not all suppliers may adhere to the same security standards or maintain the same level of security, which can lead to inconsistencies in security practices and weaken the overall security of the network.
    - Inadequate maintenance and support: A supplier that does not offer regular updates and patches for its products may be a source of vulnerabilities that can be exploited by attackers.
- Risk of supply chain disruption: Attacks on the supply chain, where attackers compromise software products or update mechanisms at some point in the supply chain, can have a devastating impact on a large number of users and networks.
- Reliance on a single supplier: Heavy reliance on a specific supplier can increase risk if that supplier encounters security issues, bankruptcy or geopolitical risks that could affect supply or support.

Countermeasures:

- Thorough supplier checks and audits: Regular security audits and quality checks on suppliers and their subcontractors to verify that they adhere to strict security standards.
- Supplier diversification: Reducing reliance on individual suppliers by utilising products and services from multiple suppliers, thereby increasing resilience to failure.
- Ongoing monitoring and updates: Implementing processes for the ongoing monitoring of the security status of components in use and the rapid application of security updates and patches are key to maintaining a high level of security.
- Strong contractual terms: Setting out clear security requirements in contracts with suppliers and introducing penalties for non-compliance.
- Encryption and authentication: Use encryption and strong authentication mechanisms to protect data transmitted between different components and services provided by various suppliers.
- Compliance with standards and certification: Selecting suppliers who comply with internationally recognised security standards and hold certifications provides a certain guarantee of the quality and security of their products and services.
- Incident planning and response: Developing and testing plans for responding to supply chain-related incidents ensures that the organisation can respond effectively to security threats and minimise their impact.

7 Proposal for securing data in 5G networks

Ensuring the integrity and protection of data during transmission in 5G networks is key to their secure and reliable use. There are **several ways to ensure that data remains intact and unaltered during transmission.**

7.1 Data encryption

Encryption protects data during transmission. We will now look in more detail at how data encryption is used in 5G networks, and the methods and standards employed.

Data encryption is a process in which the original readable data (known as plaintext) is converted into an encoded form (known as ciphertext), which is unreadable to anyone who does not have the appropriate key required for decryption. This process ensures that even if data is intercepted during transmission, it cannot be read or misused without the key.

7.1.1 Basic types of encryption used in 5G networks

- Symmetric encryption: This method uses the same key for both encrypting and decrypting data. It is fast and efficient for transmitting large volumes of data. In 5G networks, it is often used to encrypt the data stream between the user's device and the network. An example of a symmetric encryption algorithm is AES (Advanced Encryption Standard).

- Asymmetric encryption: This method uses a key pair – a public key for encryption and a private key for decryption. Asymmetric encryption is typically used for secure key exchange, authentication and digital signatures. RSA (Rivest-Shamir-Adleman) is one of the best-known asymmetric encryption algorithms.

7.1.2 Implementation of encryption in 5G

Encryption can be implemented at various levels; examples are summarised below:

- End-to-end encryption: This method encrypts data on the source device and decrypts it only on the destination device, thereby minimising the risk of unauthorised access to data during transmission across various network segments.

- Transport layer encryption: Protocols such as TLS (Transport Layer Security) are used to ensure encrypted communication between the client and server in 5G networks. TLS forms the basis for a secure web and is widely used for encrypting HTTP connections.

- Network layer encryption: The IPsec (Internet Protocol Security) protocol is most commonly used to ensure security at the network layer when communicating over IP networks. IPsec is relevant for securing data transmitted between 5G devices and network elements.

The main areas affected by the implementation of encryption are key management, addressing network performance and latency, and the deployment of protocols and relevant practices in accordance with the network architecture.

- Key management: Effective key management is essential for securing encrypted communications. In 5G networks, it is necessary to ensure that encryption keys are securely distributed and rotated to prevent their compromise.

- Performance and latency: Whilst encryption enhances security, it can also cause increased latency and reduced network performance. It is important to strike the right balance between security and performance to ensure that security does not compromise the user experience.

- Standardisation and interoperability: Given the diversity of devices and technologies used in 5G networks, standardisation of encryption protocols and practices is essential to ensure their interoperability and effective security.

By employing these encryption methods and addressing the challenges associated with encryption, 5G networks can provide robust protection for data transmitted between devices and network elements, thereby ensuring that data remains intact and unaltered during transmission.

7.2 Integrity Check

Another way of ensuring data integrity is through **integrity checks**. These offer a more detailed insight into how to ensure that data has not been altered during transmission. Integrity checks are crucial for maintaining trust and security in a digital environment, particularly in the context of the fast and large-scale data transfers typical of 5G networks.

Integrity checking is the process of verifying that data has not been altered since it was created, sent or stored. This is usually done using cryptographic hash functions and digital signatures, which enable the authenticity and integrity of the data to be verified. Below, we list the individual options along with their descriptions.

7.2.1 Cryptographic hash functions

- How it works: A hash function takes input data of any length and generates a fixed, unique hash (also known as a fingerprint) from it. If any change occurs in the data, even a very small one, the resulting hash will be completely different. This allows for easy verification of data integrity.

In 5G networks, hash functions can be used to verify the integrity of data shared between devices and network components, preventing data tampering during transmission.

7.2.2 Digital signatures

- How it works: A digital signature combines a hash function-generated data fingerprint with asymmetric encryption. The sender creates a fingerprint of the data, which they then encrypt using their private key, thereby creating a digital signature. The recipient can use the sender's public key to decrypt the signature and compare the fingerprint with the hash they generate themselves from the received data.

Digital signatures can be applied in 5G networks to ensure the authenticity and integrity of messages between network nodes and end devices. This is essential for secure communication protocols and services.

7.2.3 Implementation of integrity checks

The implementation of integrity checks must also focus on specific network characteristics and prioritise their appropriate configuration and application:

- Selection of strong hash functions: It is important to select hash functions that are collision-resistant (i.e. two different sets of data do not generate the same hash). SHA-256 is an example of a strong hash function that is frequently used for integrity checking.

- Effective key management: In the context of digital signatures, effective management of cryptographic keys is crucial to prevent their compromise. Secure key distribution and recovery are essential.

- Performance and latency: Ensuring data integrity can increase computational demands and potentially affect network performance and latency, which is critical in 5G networks. A balance must be struck between security and performance.

- Standardisation and compatibility: In the 5G landscape, it is essential to ensure that integrity checking methods are standardised and compatible across different devices and networks, facilitating interoperability and security.

By implementing these integrity control methods, data in 5G networks can be effectively protected against unauthorised tampering and its integrity ensured during transmission. These procedures, together with other security measures, create a robust defence mechanism for protecting data in the dynamic and diverse environment of 5G technology.

7.3 Mutual authentication

Mutual authentication contributes to secure communication and prevents various attacks, including man-in-the-middle (MITM) attacks. Mutual authentication is a process whereby both parties communicating over a network are able to verify the other party's identity before commencing data exchange. This process is key to ensuring trust and security in digital communication channels.

Mutual authentication is implemented using various methods and protocols that allow both parties to verify that their communication partner is indeed who they claim to be. This is usually done using cryptographic keys, certificates, or one-time passwords.

7.3.1 Mutual authentication methods in 5G networks

We distinguish between three main methods of mutual authentication that can be used in 5G networks:

- Asymmetric cryptography: One of the main methods of mutual authentication is the use of asymmetric cryptography, where each party has a pair of keys (a public and a private key). The public key is shared and is used to encrypt messages, which can only be decrypted with the corresponding private key. The authentication process involves the exchange and verification of digital signatures, which are created using private keys and can be verified using public keys.

- Certificates and PKI (Public Key Infrastructure): Mutual authentication can also be based on the use of digital certificates, which are issued and signed by trusted certification authorities (CAs). These certificates verify the ownership of public keys and enable both parties to verify the other party's identity.

- Authentication and key agreement protocols: 5G networks utilise sophisticated authentication protocols, such as EAP-AKA (Extensible Authentication Protocol-Authentication and Key Agreement), which enable secure mutual authentication between the user device and network elements. Both parties can then securely generate and share encryption keys, which are used to protect communications.

7.3.2 Implementation of mutual authentication

The implementation of mutual authentication in 5G networks can significantly enhance security and data protection. This process is the cornerstone for building trust between communicating parties and is essential for protection against advanced cyber threats. The deployment of mutual authentication is determined by the following areas:

- Key management and distribution: Effective key management is essential for the successful implementation of mutual authentication. This includes the secure storage, renewal and revocation of keys and certificates.

- Protection against attacks: Mutual authentication must be designed to withstand attempts at MITM attacks and other attempts to circumvent authentication mechanisms.

- Compatibility and interoperability: It is important to ensure that authentication methods are compatible with various devices and networks within the 5G ecosystem and support interoperability between different operators and services.

7.4 Network slicing

The concept of 'network slicing' in 5G networks is a key feature that enables the creation of multiple virtual networks on a single physical network infrastructure. Each such "slice" can be tailored to the specific requirements of applications, services or users, including different levels of security. This flexibility is particularly important as 5G networks serve a diverse range of applications, from IoT through to autonomous vehicles and critical communications

Network slicing is the process by which a physical network is divided into several virtual networks (slices), with each slice being independent and capable of being customised according to the specific needs of an application or service. This technology enables operators to optimise and make efficient use of their network resources.

7.4.1 Implementation of network slicing

Network slicing is implemented for various purposes in line with an organisation's security priorities:

- Data flow isolation: Network slicing allows the data flows of different users or services to be separated, preventing mutual interference and potential security risks. For example, data from critical applications can be isolated from normal internet traffic.

- Specific security requirements: Each slice can be configured with its own security policies and mechanisms, tailored to its specific needs. This allows for the implementation of different levels of security depending on the sensitivity and data protection requirements of a particular application or service.

- Dynamic security management: Network slicing enables operators to dynamically adjust security policies and settings in response to changing threats and security requirements, with the ability to respond quickly to incidents, isolate affected network segments and implement specific security measures.

- Optimisation of performance and security: It enables a balance between performance and security by using slices specific to low-latency applications, whilst other slices can be optimised for maximum security, for example for the transmission of sensitive information.

The implementation of network slicing in 5G networks requires careful planning, management and monitoring to ensure that all slices meet their specified requirements whilst providing robust data protection. As with other methods
data security in 5G networks, our approach to network slicing implementation focuses on correct configuration and meeting the prerequisites for successful deployment:

- Management and orchestration: Effective management and orchestration of slices are key to ensuring that each slice meets its security and performance requirements. This requires sophisticated systems for network monitoring and control.

- Standardisation and interoperability: For the effective deployment of network slicing, standardisation of protocols and interfaces is essential to ensure that different technologies and devices can work together reliably and securely.

- Security risks: Whilst slicing provides isolation and can enhance security, it also presents new challenges, such as the need to secure communication between slices and to configure security policies correctly for each slice.

7.5 Security protocols and techniques

Securing data during transmission via security protocols and techniques provides significant protection against unauthorised access, information leakage and data manipulation. The implementation of security protocols and techniques is fundamental to ensuring the confidentiality, integrity and availability of data in 5G networks. **Among the security protocols and techniques, we can choose from:**

- IPsec (Internet Protocol Security): IPsec is a set of protocols for securing Internet Protocol (IP) communication through encryption and authentication at the network layer. In 5G networks, IPsec can be used to secure data between network elements, for example between 5G base stations and the network core, ensuring that data cannot be eavesdropped on or tampered with during transmission.

- TLS (Transport Layer Security): TLS is widely used to secure communication at the transport layer, protecting data transmitted between applications and servers on the internet. In the context of 5G networks, TLS can be used to secure communication between network components or to secure services accessing the network, such as web applications and APIs.

- DTLS (Datagram Transport Layer Security): DTLS provides a similar level of security to TLS, but is designed for use with datagram-based protocols such as UDP. It is suitable for 5G applications requiring low latency, such as voice services or IoT, where communication needs to be secured without a significant impact on performance.

- PFCP (Packet Forwarding Control Protocol): In 5G networks, PFCP is used to establish and manage user data flows within the network core. Although it is primarily used for flow management, the protocol's security aspects, such as the authentication and authorisation of control messages, are important for protecting the network infrastructure.

7.5.1 Implementation of security protocols and techniques

By implementing and correctly configuring these security protocols and techniques, 5G networks can provide robust security for data transmitted between devices and network components, which is key to protection against unauthorised access and attacks. In particular, the text below summarises the dynamic factors of 5G networks that must be taken into account during their implementation:

- Key and certificate management: Effective key and certificate management is essential for the secure implementation of protocols such as TLS and IPsec. The challenge is to keep key management secure whilst remaining sufficiently agile to respond to changes and key renewal.

- Performance and scalability: Security must be implemented in a way that minimises the impact on network performance and latency. This is particularly important in 5G, where the emphasis is on supporting applications requiring low latency and high data transfer rates.

- Interoperability: Given the diversity of devices and technologies in the 5G ecosystem, ensuring interoperability between different security protocols and mechanisms is key. Standardisation and adherence to industry standards are essential to ensure compatibility and secure communication.

- Continuous development and updates: Security protocols and technologies must be constantly updated and adapted to withstand emerging threats and vulnerabilities. This requires operators and device manufacturers to actively monitor the security landscape and rapidly implement necessary updates and patches.

7.6 Incident detection and response

The final method of ensuring data security in a 5G network mentioned in this chapter is **incident detection and response** (enforcement of security policies). Incident detection and response focuses on updating and managing security policies and procedures as a key element in ensuring that data in 5G networks remains intact and unaltered during transmission.

In the dynamic cybersecurity landscape, where threats are constantly evolving and changing, monitoring and responding to incidents, as well as regularly reviewing and updating security protocols, software and hardware, is essential for maintaining a robust defence.

- Incident monitoring and response:

- Proactive monitoring: Continuous monitoring of network traffic and system logs enables the rapid identification of suspicious activity or security incidents. This allows operators to respond quickly and minimise potential damage.
- Incident response plans: Having prepared and regularly updated plans for responding to security incidents is key to resolving issues quickly and effectively. Plans should include procedures for isolating affected systems, investigating incidents, and restoring compromised data or services.

- Regular software and hardware updates:
  - Patching vulnerabilities: Updating software and device firmware in 5G networks is crucial for fixing vulnerabilities that could be exploited by attackers. Regular patching prevents the exploitation of known weaknesses.
  - Security feature updates: Technological advances and new security techniques can provide better protection or more effective performance. Updates may include new encryption algorithms, improved authentication mechanisms, and other advanced security features.

- Compliance with standards and regulations: Ensuring that network operations and security measures comply with international standards and legal regulations is essential for protecting data and maintaining user trust. This includes standards such as ISO/IEC 27001, GDPR and other specific standards for telecommunications and cybersecurity.

- Security policy management:
  - Review and update of security policies: Regular review of security policies and procedures ensures they reflect current threats and best practices. This includes updates to access policies, data encryption policies, monitoring policies and incident response policies.
  - Staff training: Training staff and users of the network infrastructure is essential to ensure they are aware of current threats and security procedures. Training can reduce the risk of security incidents caused by human error.

7.6.1 Implementation

By implementing these measures, organisations and 5G network operators can effectively protect data against ever-changing threats and ensure that security measures remain up to date and effective in combating potential attacks. Implementation must therefore be responsive in this regard, i.e. it must, in particular, consider the adaptability of the proposed measures and assess implementation in the context of complexity:

- Adaptability: The network environment and threats are constantly evolving, which requires flexibility and adaptability in security strategies and procedures.

- Management complexity: Large-scale and dynamic 5G networks present challenges in terms of security management complexity, requiring advanced security management and automation tools.

8 Review and assessment Measures to protect 5G networks from unauthorised communication

Measures to protect 5G networks from unauthorised communication with foreign servers/networks are crucial for ensuring the security and integrity of telecommunications infrastructure. These measures may include a wide range of techniques and procedures, from sophisticated detection and prevention systems to physical hardware security.

8.1 Advanced threat detection and prevention systems

Advanced threat detection and prevention systems form the basis for protecting 5G networks against unauthorised communication with foreign servers and other security threats. These systems combine several technologies and methodologies **to identify, analyse and respond to potential security incidents in real time.**

8.1.1 Intrusion Detection and Prevention Systems (IDS/IPS)

Intrusion Detection Systems (IDS) are designed to passively monitor network traffic and identify suspicious activity or known attack patterns. If an IDS detects a potential threat, it triggers an alert for further analysis.

Intrusion Prevention Systems (IPS) go a step further; not only do they detect potential threats, but they are also capable of actively intervening to block malicious traffic or isolate compromised devices from the rest of the network, thereby preventing the attack from spreading.

The potential threats targeted by detection systems, which indicate unauthorised or unwanted communication with foreign servers, are geopolitically specific and primarily include:

1. Unusual network traffic:
    - Anomalous bandwidth: Extremely high or low bandwidth usage that is not typical of normal traffic.
    - Unusual data volume: An unexpectedly large amount of data transferred, which may indicate data exfiltration or a DDoS attack.
2. Scanning and reconnaissance activities:
    - Port scanning: Attempts to scan ports in order to find open ports and vulnerable services.
    - Network mapping: Attempts to map the network in order to obtain information about the network infrastructure and devices.
3. Suspicious login activity:
    - Brute-force attacks: Repeated failed login attempts, which may indicate attempts to guess passwords.
    - Unusual login locations: Attempts to log in from geographical locations that are not typical for the user in question.
4. Changes in network topology:
    - New devices on the network: Unexpected connection of a new device, which may be potentially malicious.
    - Unauthorised configuration changes: Changes to network device settings that have not been approved or documented.
5. Malicious network traffic:
    - Malware communication: Data transfers between internal devices and known malicious IP addresses or domains.
    - Command and Control (C2) communication: Attempts to communicate with C2 servers used by attackers to control compromised devices.
6. Anomalies in traffic patterns:
    - DoS attacks: An increase in specific types of traffic that may indicate a Denial-of-Service attack.
    - Recurring patterns: Unusual or recurring traffic patterns that deviate from normal operational behaviour.
7. Unauthorised access and privilege escalation:
    - Privilege abuse: Attempts to access sensitive data or systems without the appropriate permissions.

- Privilege escalation: Attempts to obtain higher levels of privilege than those assigned.

8. Suspicious activity at the application level:
   - SQL injection: Attempts to inject malicious SQL code into databases.
   - Cross-site scripting (XSS): Attempts to inject malicious code into web pages, which can be exploited to attack users.

IDSs can generate alerts for suspicious activity and provide details for further analysis. When combined with Intrusion Prevention Systems (IPS), they can not only detect but also actively block malicious traffic and isolate compromised devices. Network administrators can then use this information to conduct in-depth analysis, confirm incidents, and implement appropriate measures to resolve them.

8.1.2 Advanced analytics

The benefits of IDS and IPS systems are enhanced by **advanced analytics**, which are incorporated into robust systems either in the form of behavioural analysis or sandboxing:

- Behavioural analysis: This technology uses machine learning and artificial intelligence to analyse normal user behaviour and network traffic. Any deviations from the norm that could indicate an attempt at unauthorised communication or another attack are quickly identified.

- Sandboxing and virtual analysis: Potentially malicious code or applications are run in an isolated environment (‘sandbox’), where they can be safely analysed without the risk of damaging the real network or data.

8.1.3 Automated response and remediation

Systems are often equipped with **automated response** tools that enable the rapid isolation of compromised devices, blocking of malicious IP addresses, updating of security policies, or even the automatic application of patches to vulnerabilities.

8.1.4 Integration with other security systems

Last but not least, effective protection of a 5G network requires the integration of IDS/IPS with other security systems, such as firewalls, security information and event management (SIEM) systems, and threat management tools. This integration provides a comprehensive overview of the network’s security status and enables a more effective response to threats.

8.1.5 Continuous updates and learning

To ensure that IDS/IPS systems do not become obsolete in the dynamic world of communications, they must be regularly updated with the latest threat signatures and utilise the latest scientific findings in the field of threat detection. This involves continuous learning from newly detected attacks and adapting to the changing tactics of attackers.

The implementation and correct configuration of these systems requires specialist knowledge and experience, as over- or under-utilisation can lead to false alarms or the overlooking of real threats. This is precisely why it is crucial for organisations to invest not only in these technologies, but also in specialist training for their security teams.

8.2 Data encryption

Data encryption is a fundamental element in protecting communications with external devices on 5G networks, safeguarding them against eavesdropping, tampering or misuse by third parties. This technology ensures that information can only be decrypted and read by authorised users or systems.

When implementing encryption, it is important to balance security, performance and usability. Encryption can increase the load on network resources and devices, which requires careful planning and optimisation. It is also crucial to regularly update and review the encryption algorithms and protocols used to prevent obsolescence and potential security vulnerabilities.

Implementing robust encryption in 5G networks requires a comprehensive approach, involving not only the use of strong encryption algorithms but also proper cryptographic key management and constant attention to security updates and best practices.

Based on the information provided above, we already know that various levels of encryption can be applied. The techniques mentioned below are particularly relevant for data transmission and communication from abroad.

8.2.1 End-to-end encryption

End-to-end encryption is a process in which data is encrypted at the sender's end and decrypted only at the recipient's end. This means that the data remains encrypted throughout its journey across the network, preventing any attacker – including those abroad – from reading or manipulating the data, even if they manage to intercept it.

8.2.2 Network-level encryption

Network-level encryption refers to the encryption of data passing through network infrastructure, such as routers and switches. This encryption is particularly important for protecting data transmitted between different parts of the network and helps to secure communication between devices and network nodes.

8.2.3 Application-level encryption

Application-level encryption focuses on protecting data generated and consumed by specific applications that are deployed, the vendors of which are usually foreign-owned. This includes the encryption of messages, emails, voice calls and any other data processed by the application. Applications may use their own encryption protocols or utilise encryption provided by the operating system or platform.

8.2.4 Protocols, cryptography and encryption standards

Security protocols, cryptographic elements and an emphasis on compliance with encryption standards play a key role in encryption. The protocols and encryption techniques used are presented in the following paragraphs.

- Protocols such as TLS (Transport Layer Security) and its predecessor SSL (Secure Sockets Layer) are widely used to secure communication between web servers and browsers. In the context of 5G, they can also be used to secure communication between network components.
- IPsec (Internet Protocol Security) is a set of protocols for securing communication at the network layer, enabling authentication and encryption of packets at the IP level. This is key to securing VPNs (Virtual Private Networks) and other forms of communication in 5G networks.
- Cryptographic key management is essential for effective encryption. This includes the generation, distribution, storage, exchange, use and disposal of cryptographic keys. Secure key management is essential to prevent unauthorised access to encrypted data.

8.3 Network segmentation and virtualisation

Network segmentation and virtualisation are key techniques used to enhance the security and flexibility of 5G networks in communication. These methods enable the isolation of different parts of the network, thereby reducing the risk of attack propagation and increasing the efficiency of resource management.

Network segmentation divides the network into smaller, manageable segments, often referred to as subnets. These divisions allow for better control over data flow and access to network resources.

Key aspects of network segmentation are:

- Traffic isolation: Segmentation separates sensitive parts of the network (e.g. databases containing personal data) from other parts, thereby reducing the risk that an attack on one part of the network could affect other sensitive parts.
- Limiting the spread of attacks: In the event of a security incident, segmentation prevents the attack from spreading across the entire network, making it easier to isolate and resolve the issue.
- Refining security policies: It allows specific security policies to be created for each segment, which improves overall security and efficiency.

Virtualisation in 5G networks involves creating virtual, separate networks on the same physical infrastructure. This is often achieved using technologies such as SDN (Software-Defined Networking) and NFV (Network Functions Virtualisation).

The key features of virtualisation are:

- Flexibility and scalability: Virtualisation enables the rapid deployment of new services and applications without the need for physical changes to the network infrastructure.

- Better utilisation of resources: It enables more efficient use of network and computing resources by dividing and allocating them according to current needs.

- Dynamic network management: It provides tools for the dynamic management of network traffic and resources, which improves network performance and security.

8.3.1 Specifics of segmentation for applications in 5G networks

5G technology enables the creation of virtual networks (network slices) that can be tailored for specific services or applications, such as autonomous vehicles, IoT devices or critical infrastructure. In this way, an optimal level of performance and security can be ensured for each application.

The implementation of segmentation and virtualisation requires careful planning and management, including the definition of precise security policies for each segment or virtual network, regular reviews and updates of these policies, and network monitoring to identify and respond to security threats. These methods, combined with other security measures, create a robust framework for protecting 5G networks against unauthorised communication and other threats.

8.4 Identity and access management

Identity and access management is a cornerstone of 5G network security, focusing on the authentication and authorisation of users and devices to ensure that only authorised entities are granted access. The aim of these measures is to prevent unauthorised access and the misuse of network resources.

It is important to design identity and access rights management systems to be flexible, easy to manage, and capable of adapting to the rapidly changing requirements of the network and its users.

We will now look at the individual layers of this security approach that are relevant to communication with foreign servers and other technologies.

8.4.1 Centralised identity management

Centralised identity management enables the centralised administration of user accounts and their permissions through processes for creating, managing, deactivating and deleting accounts. Centralised identity management facilitates the monitoring and control of access to network resources.

8.4.2 Authentication and authorisation

Strong authentication requires users or devices to provide unambiguous proof of their identity, often through multi-factor authentication (MFA), which combines something the user knows (a password) with something they have (a security token or mobile phone) or something they are (biometric data).

Authorisation then determines which resources or services an authenticated user or device has access to. This is typically governed by role-based access control (RBAC) or attribute-based access control (ABAC) policies, which define permissions based on the user's role or specific attributes.

8.4.3 Access rights management

Access rights management involves monitoring and reviewing access rights to ensure that users and devices have only the permissions strictly necessary for their tasks (the principle of least privilege). Regular reviews help to identify and remove outdated or redundant permissions.

8.4.4 Identity as a Service (IDaaS)

Identity as a Service (IDaaS) is a cloud-based solution that provides identity and access rights management as a service. As a service, these solutions can offer advanced features, including single sign-on (SSO), cloud-based identity management, and integration with numerous applications and services.

8.4.5 Security tokens and certificates

Security tokens and certificates play a key role in authenticating and encrypting communication between devices and the network. Tokens and certificates are issued by trusted authorities and used to verify identity and secure data.

8.4.6 Biometric authentication

Biometric authentication uses an individual's unique physical or behavioural characteristics (e.g. fingerprints, facial recognition, voice patterns) to verify identity. It provides a higher level of security than traditional passwords or PINs.

8.5 Regular updates and patches

These activities ensure that the software and firmware of all devices and components on the network are protected against known threats and vulnerabilities. Publicly known patch requirements are an easy target for attackers.

The benefits of regular updates and patches in the context of international communications are implemented continuously across individual areas of administration.

- Identification and assessment of vulnerabilities

Active monitoring and assessment of vulnerabilities in the network and devices is the first step. This includes monitoring security bulletins, warnings and recommendations from hardware and software manufacturers, as well as from security organisations and forums.

- Planning and testing updates

Planning and testing updates before deployment is essential to minimise the risk of service disruption or other negative impacts on the network infrastructure. This involves creating test environments that mimic production networks to verify the compatibility and security of updates.

- Automating the update process

Automating the update process can significantly improve the efficiency and consistency of patch deployment. The use of configuration management and automation tools enables network administrators to apply updates regularly and systematically across the entire network.

- Securing update distribution

Securing update distribution is key to preventing attackers from tampering with update packages. This involves using encryption and digital signatures to verify the integrity and authenticity of updates.

- Configuration management

Configuration management is the process of monitoring and maintaining consistent device and software settings across the network. This process helps identify unauthorised changes that could increase the network's vulnerability.

- Creating backups and recovery plans

Backups and recovery plans are essential for rapid recovery in the event of an update failure or security incident. Regular backups of configurations and important data ensure that the network can be quickly restored to a secure state.

- Awareness and training

Communicating best practices, security measures and incident response procedures ensures that everyone involved in network management understands the importance of and procedures for regular updates and patches.

8.6 Monitoring and auditing

Monitoring and auditing are essential components of a security strategy for 5G networks, providing an overview of the current state of the network—whether integrated or communicating with external networks—identifying potential threats, and enabling a proactive response to security incidents. These processes help ensure that any unusual or suspicious activity is quickly detected and addressed.

It takes the form of both network monitoring itself and the use of other techniques.

8.6.1 Continuous network monitoring

Continuous monitoring involves the constant tracking of network traffic, logs, system events and performance metrics. The use of advanced tools and techniques, including SIEM (Security Information and Event Management) systems, enables real-time data analysis and the rapid detection of suspicious or anomalous activity.

8.6.2 Security event analysis

Security event analysis helps to identify potential security incidents and determine their causes. This involves correlating events from various sources, assessing their severity, and classifying them as false positives where appropriate. Effective analysis requires a combination of automated tools and expert knowledge.

8.6.3 Proactive threat hunting

Proactive threat hunting is the process of actively searching for previously unidentified threats on the network. It involves analysing traffic patterns, anomalies and potentially suspicious behaviour that may indicate hidden attacks or compromises.

8.6.4 Auditing and compliance

Auditing involves regular, traffic-independent checks of security policies, configurations and rules to ensure their correct implementation and effectiveness. Compliance with internal and external regulations and standards, such as GDPR, PCI-DSS and other relevant security frameworks, is verified.

8.6.5 Logging and documentation

Logging and documentation form the basis for effective monitoring and auditing. This involves storing detailed records of network activity, configuration changes, system access and detected incidents. These records are crucial for incident analysis, forensic investigations and compliance with legislative requirements.

8.6.6 User education and awareness

User education and awareness play an important role in security monitoring and auditing by helping users recognise and report suspicious activity. Training staff and raising awareness of security threats and best practices can significantly reduce the risk of incidents.

8.6.7 Cooperation and information sharing

Collaboration and information sharing between organisations, security teams and external bodies, such as security forums and government agencies, improves the ability to detect and respond to new threats. The exchange of information on threats and best practices supports a collective defence against cyber attacks.

The implementation of robust monitoring and auditing relies on advanced technologies, skilled personnel and effective processes. Together, these elements form a dynamic defence system that enables rapid identification of and response to security threats, enhances the resilience of 5G networks and protects critical information and services.

8.7 Cooperation with manufacturers and international collaboration

Cooperation with manufacturers and international collaboration helps to identify, address and, consequently, minimise potential threats and vulnerabilities.

8.7.1 Cooperation with manufacturers

Cooperation with manufacturers, which amplifies measures to protect 5G networks, provides an opportunity to enhance their effectiveness in several ways:

- Sharing information on vulnerabilities: Hardware and software manufacturers can share information on identified vulnerabilities and recommendations for fixing them or mitigating risks. This information sharing enables 5G network operators to respond quickly to potential threats.
- Updates and patches: Regular updates and patches from manufacturers are essential for maintaining network security. Collaboration ensures that these updates are rapidly distributed and applied to prevent the exploitation of known vulnerabilities.
- Security recommendations: Manufacturers can provide recommendations and best practices for the configuration and management of devices and systems. This helps operators implement robust security configurations and minimise risks.
- Technical support and cooperation in incident response: In the event of security incidents, manufacturers can provide technical support and cooperate in analysing and resolving issues, which helps to quickly restore secure network operations.

8.7.2 International cooperation

International cooperation is primarily preventive in nature and enables the sharing of know-how. It usually takes the form of:

- Threat intelligence sharing: International cooperation between governments, security agencies and industry organisations enables the exchange of information on cyber threats and vulnerabilities. This improves the ability to detect and respond to global threats.
- Common standards and policies: International organisations and standardisation bodies are working to develop common security standards and policies for 5G networks. Common standards facilitate interoperability and ensure a consistent level of security across different countries and operators.
- Cooperation in addressing cross-border cyber incidents: Cyber attacks often cross national borders, requiring a coordinated international response. Cooperation helps to coordinate the response to these incidents and strengthens global cyber defences.
- Training and exchange programmes: Training and exchange programmes enable the sharing of knowledge and best practices among cybersecurity experts from different countries. This supports the development of stronger and more informed security teams.

International cooperation creates pressure to accelerate the resolution of challenges related to the security of 5G networks globally. Among other things, it supports the sharing of critical information, raises awareness of threats and improves the ability to respond to security incidents.

8.8 Education and awareness

Education and awareness, mentioned in various places throughout the text so far, deserve a separate chapter in the context of international challenges in 5G networks. Education and awareness are essential for progress and for enhancing the security of 5G networks, as the human factor plays a key role in defending against cyber threats. This approach focuses on informing all network participants, from administrators to end users, about potential threats or experiences with incidents, best practices for security, and incident response procedures.

It is implemented through staff training programmes, staff testing, ongoing communication within the organisation, and other techniques.

8.8.1 Employee training programmes

Regular training and educational programmes for staff are essential for maintaining a high level of cyber security awareness. These training sessions should cover information on current threats, social engineering techniques, secure data handling, and responses to security incidents.

8.8.2 Attack simulations and testing

Conducting simulated attacks, such as phishing campaigns, helps to test how well employees recognise and respond to attempts at exploitation. These exercises help to identify areas where training and awareness need to be improved.

8.8.3 Information materials and communication

Regular communication about the latest threats, vulnerabilities and security policy updates is essential to keep all network users informed. This primarily involves email newsletters, internal websites and online forums for discussing security issues.

8.8.4 End-user training

As end users may be the target of attacks such as phishing or malware, it is important to inform them of the risks and how they can protect their devices and data. This includes educating them on safe internet browsing, using strong passwords and keeping software up to date.

8.8.5 Role-Based Training

This is training focused on specific roles. Different roles within an organisation may require specific knowledge and skills in the field of cybersecurity. For example, technicians and administrators need a deeper understanding of security technologies and procedures, whilst staff in contact with clients must be able to recognise and respond to threats targeting customers.

8.8.6 Collaboration and Sharing of Best Practices

Collaboration between organisations, associations and government agencies can promote the sharing of best practices, tools and strategies to enhance the security of 5G networks. This takes the form of conferences, workshops and co-working.

Education and awareness-raising are an ongoing process, and supporting materials must be regularly updated and adapted in line with the evolving nature of security challenges and vulnerabilities. Training programmes and awareness campaigns contribute significantly to the resilience of 5G networks by, at the very least, raising awareness of current threats and promoting a security culture at all levels of the organisation.

9 Proposal for possible methods detecting malicious activity in 5G networks

5G networks offer high throughput, low latency and massive connectivity for the Internet of Things (IoT), opening up new possibilities for real-time operations and integration in applications for autonomous vehicles, smart cities and advanced industrial automation, etc. **Detecting anomalies in 5G networks** is crucial for ensuring the reliability, security and overall performance of these networks.

9.1 Real-time traffic monitoring and analysis

Real-time traffic monitoring and analysis are essential for maintaining the health, performance and security of 5G networks. This process involves monitoring and evaluating network traffic to enable the rapid identification and resolution of any potential issues with a swift response.

Real-time traffic monitoring and analysis therefore provide the essential foundation for the proactive management and protection of 5G networks, enabling operators and network administrators to quickly identify and resolve potential issues before they can have a significant impact on the services provided to end users.

The detection of adverse events begins with the collection of relevant data, utilising various analytical techniques, and involves integration with other systems, ensuring that the process does not remain limited to static recording of the event but instead enables a real-time response.

9.1.1 Data collection

Continuous **data collection** and analysis of the data—including testing for latency, transmission speed, and potential packet loss—play a pivotal role in detecting adverse events.

- Passive monitoring: Continuous monitoring of network traffic without interfering with data transmission. It focuses on analysing metadata and packet headers to gain an overview of traffic characteristics.
- Active testing: Involves generating and sending test packets across the network to measure performance metrics such as latency, data transfer speed and packet loss.

9.1.2 Data analysis

Data analysis is the logical step following data collection. It is primarily aimed at detecting anomalies and identifying deviations in traffic patterns:

- Anomaly detection: The use of algorithms to identify deviations from normal traffic behaviour, which may indicate network congestion, faulty hardware or software errors.
- Pattern analysis: Identifying specific patterns in traffic that may indicate cyberattacks, such as DDoS (Distributed Denial of Service) attacks, malware propagation or phishing attempts.

Various tools and technologies are employed within the analysis to perform in-depth analysis of operational data. The main ones are:

- Advanced analytics platforms: The use of sophisticated tools that combine big data and artificial intelligence technologies for in-depth analysis of traffic data and rapid problem detection.
- Network probes and sensors: Deployment of physical or virtual devices across the network to collect vital information on network traffic and health.

9.1.3 Incident response

Detecting anomalies in 5G networks **with real-time response** involves systems that utilise automated responses and notification systems for network administrators.

- Automated responses: Implementation of systems that automatically respond to detected issues, for example by rerouting traffic, isolating affected parts of the network, or applying security policies to mitigate attacks.

- Notification and escalation: Systems to alert network administrators to potential problems and escalate serious incidents for rapid resolution.

9.1.4 Integration with other systems

Integration with other systems and information sharing significantly support incident response.

Integration with security tools mainly involves collaboration with firewalls, intrusion detection and prevention systems (IDS/IPS) and other security mechanisms for comprehensive network protection.

Integration with threat intelligence platforms enables the network to respond to newly identified threats and reduce response times.

9.2 Advanced machine learning and artificial intelligence techniques

Advanced machine learning (ML) and artificial intelligence (AI) techniques play a key role in detecting and addressing adverse events in 5G networks. ML and AI technologies enable network systems to learn from data, automatically identify behavioural patterns and predict potential problems before they cause outages or security incidents.

Continuous learning and adaptation of AI models is essential to maintain their effectiveness in the dynamic environment of 5G networks, where traffic patterns and threat types are constantly evolving.

LM and AI technologies are used in the detection of anomalies and security threats, predictive maintenance and network optimisation. The more these technologies are integrated with existing network and security systems, the more timely and effective the response to increasingly sophisticated threats becomes, and potentially at a lower cost.

9.2.1 Anomaly detection

Machine learning models are trained on normal network traffic data to learn to recognise typical network behaviour. They can then effectively identify anomalies or deviations that may signal technical issues, network congestion or cyber attacks.

Deep learning, a form of machine learning based on neural networks, is particularly useful for analysing large volumes of data in real time, enabling the detection of complex and subtle anomalies that might escape traditional detection methods.

9.2.2 Predictive maintenance

Predictive algorithms use historical and real-time data to forecast future equipment and infrastructure failures or maintenance requirements. This enables operators to take preventive action before problems arise, thereby improving network reliability and availability.

Data from sensors and logs from equipment and infrastructure provide valuable information for these predictive models, as they enable the detection of patterns that precede failures.

9.2.3 Network optimisation

Machine learning algorithms can automatically adjust network settings to optimise performance and capacity in response to changing traffic patterns and user demands.

Reinforcement learning enables AI models to ‘learn’ from their own actions by constantly evaluating how well their decisions lead to achieving goals, such as increasing throughput or reducing latency.

9.2.4 Security threats

AI and machine learning can identify and classify security threats in real time, detect new types of malware, and automatically implement security policies to defend against these threats.

Intrusion detection and prevention systems (IDS/IPS) utilising AI can more effectively recognise complex attacks, including those that use sophisticated methods to bypass traditional security measures.

9.2.5 Integration with existing network and security systems

Integration with existing network and security systems facilitates real-time sharing of data and threat intelligence across different systems and platforms, enabling a coordinated and effective response to incidents.

9.3 Network slicing and isolation of problem sources

Network slicing is a key technology in 5G architecture, enabling operators to divide a single physical network into several virtual network segments (slices). Each slice can be optimised for the specific needs of different types of services, applications or customer groups. This approach enables more efficient use of network resources and ensures that different types of services can coexist on the same physical infrastructure without negatively affecting one another.

Network slicing enhances methods for detecting adverse events, particularly by accelerating the response to such events, notably by isolating the problematic or affected area from the rest of the network architecture. This is achieved through isolation, allocation, and the application of flexibility, including at the level of guarantees for certain operational parameters.

9.3.1 Isolation and security

- Isolation of problem sources: Network slicing allows problems to be isolated within a single slice, thereby preventing them from spreading to other slices. For example, if congestion occurs in a slice designated for IoT devices, this will not affect the slice for critical communications, such as emergency call services.

- Enhanced security: Each slice can have its own security rules and configurations, enabling better protection against cyber threats and facilitating compliance with regulatory and compliance requirements.

9.3.2 Efficient use of resources

- Dynamic resource allocation: Network slicing leverages the benefits of dynamically allocating network resources according to the current needs of individual slices. This applies to bandwidth, computing capacity and storage, which increases the efficiency of resource utilisation and enables a rapid response to changing service requirements.

- Optimisation for specific applications: Different applications and services have different requirements for network infrastructure. For example, applications requiring low latency, such as autonomous vehicles or industrial automation, can be placed in a slice prioritising low latency, whilst other services requiring high throughput can be placed in a different slice.

9.3.3 Flexibility and scalability

- Rapid response to changing requirements: Network slicing enables operators to respond quickly to changing market demands or specific customer requirements by creating or modifying slices as needed.

- Scalability: This technology allows the network to grow and adapt without the need for significant changes to the physical infrastructure, simplifying the deployment of new services and the expansion of existing ones.

9.3.4 Improved Quality of Service (QoS)

- Quality of Service Guarantees: Each slice can have guaranteed quality of service parameters, ensuring that applications and services running within that slice will have the necessary bandwidth, latency and other network parameters.

- Customisation of services for customers: Operators can offer customers customised network services with guaranteed performance parameters, which increases customer satisfaction and enables product differentiation.

Network slicing in 5G networks therefore brings a revolutionary change to the way network resources are allocated and managed, and offers a powerful tool for ensuring high network performance, security and efficiency whilst meeting the diverse needs of users and applications.

9.4 Security protocols and encryption

These technologies not only ensure the security of communication between devices and the network, but also protect data integrity and privacy. Given the widespread use of 5G networks, from mobile phones and IoT devices to critical infrastructure, data and communication security is key to preventing data leaks, cyberattacks and other security threats.

9.4.1 Security at various levels

Security protocols and encryption are technical measures that prevent negative incidents rather than directly leading to their detection. Appropriate security depends on the levels at which it is applied.

- Data-link-level encryption: Every data stream between a device and a network node is encrypted, ensuring that data remains private and inaccessible to unauthorised parties. This encryption applies to all types of data, including voice communications and data transmission.

- Security protocols for authentication: Protocols such as EAP-AKA (Extensible Authentication Protocol-Authentication and Key Agreement) are used to authenticate devices and users on the network, thereby preventing unauthorised access.

Encryption, security protocols, authentication and compliance with standards are primarily intended to provide preventive protection or an appropriate response to malicious activities, but they cannot be overlooked in the process of identifying such activities, as data from encryption algorithms and attempts to circumvent encryption and protection systems at the very least indicate malicious activity. Let us therefore review, in a simple list, how encryption techniques and other security management techniques can be of use to us.

9.4.2 Encryption algorithms

- Modern encryption algorithms: 5G networks use advanced encryption algorithms, such as AES (Advanced Encryption Standard), which provides a high level of security. These algorithms are regularly updated and strengthened to withstand advanced decryption and cyber attacks.

- Public keys and private keys: Encryption systems based on public and private keys enable the secure exchange of keys between communicating parties without the need to transmit the key over unsecured channels.

9.4.3 Data integrity and authentication

- Protocols for ensuring data integrity: In addition to data encryption, 5G networks implement protocols such as IPsec (Internet Protocol Security) to ensure data integrity and authentication at the internet layer, which prevents data from being tampered with during transmission.

- Message authentication: Digital signatures and certificates are used to authenticate messages and transactions, ensuring that data originates from a legitimate source and has not been tampered with.

9.4.4 End-to-end encryption

- End-to-end encryption: End-to-end encryption ensures that data is encrypted from source to destination, preventing eavesdropping and tampering with data during transmission across various network segments.

- Implementation challenges: Although end-to-end encryption provides a significant level of security, its implementation can be complex due to the need for key management and compatibility between different devices and services.

9.4.5 Compliance with regulations and standards

- Compliance with international standards: 5G networks must comply with international security standards and regulations, such as those set by the International Telecommunication Union (ITU) and the 3rd Generation Partnership Project (3GPP).

- Ongoing updates and assessments: Security protocols and encryption mechanisms must be regularly reviewed and updated to reflect the latest developments in security threats and technologies.

9.5 Penetration testing and attack simulations

Penetration testing and attack simulations are key tools for identifying vulnerabilities in 5G network infrastructure and verifying the effectiveness of implemented security measures. These techniques represent a proactive approach to detecting malicious activity, simulating potential attack scenarios, and helping to identify and address vulnerabilities before they are exploited by actual attackers.

The individual tasks involved in penetration testing or attack simulation can be characterised as follows:

- Identification of vulnerabilities: The aim is to identify weaknesses in the network infrastructure, configuration, software and protocols that could be exploited by attackers.
- Simulation of real-world attack scenarios: Testing involves simulating a wide range of attacks, including DDoS attacks, attacks exploiting software vulnerabilities, phishing and other cyber threats.
- Verification of security measures' effectiveness: The tests help verify how effectively existing security measures and protocols protect the network against potential attacks.

9.5.1 Vulnerability scanning and penetration testing in 5G networks

Vulnerability scanning and penetration testing are techniques used to identify and address security threats in 5G networks. Both methods have their own specific procedures and tools, which complement each other and together provide a comprehensive overview of the network's security status.

The aim **of vulnerability scanning** is the rapid and automated detection of potential security weaknesses in network infrastructure, devices and applications. Vulnerability scanning is carried out regularly to ensure that newly discovered vulnerabilities are quickly identified and addressed.

Furthermore, the advantage of vulnerability scanning is that it can be carried out regularly with minimal manual intervention, can cover a large number of devices and applications in a short time, and is effective at detecting known vulnerabilities for which appropriate security patches or solutions are available.

The vulnerability scanning process comprises the following stages:

- Information gathering: Identifying the network assets, services and applications to be scanned.
- Scanning using tools: Using specialised vulnerability scanners, such as Nessus, OpenVAS or Qualys, to perform automated checks based on databases of known vulnerabilities.
- Analysis of results: Evaluation of scan results to identify specific vulnerabilities, their severity and potential impact on the network.
- Remedial measures: Recommendation and implementation of measures to address identified vulnerabilities, such as applying security patches or changing configurations.

In contrast, **penetration testing** simulates real-world cyber attacks with the aim of identifying vulnerabilities that could be exploited by attackers. Testing not only uncovers vulnerabilities but also verifies how they can actually be exploited and what impact they would have on network security and operations.

The main advantage of penetration testing is that it provides a realistic view of the network's security status by simulating actual attacks. Furthermore, penetration testing is capable of uncovering more complex vulnerabilities that may not be detected by automated scanning and of verifying the effectiveness of security measures.

The penetration testing process is more complex and comprehensive, involving a wider range of activities during its implementation:

- Planning and scope: Defining the objectives and scope of the testing, including determining which systems and applications will be tested.
- Information gathering: Collecting information about the target network and systems, including network mapping, identifying active services and determining software versions.
- Identification of vulnerabilities: Using tools and manual techniques to identify potential vulnerabilities.
- Exploitation of vulnerabilities: Attempts to exploit identified vulnerabilities to gain access or compromise the system, simulating real-world attack techniques.
- Post-exploitation activities: Analysing opportunities for further movement within the network and gaining access to other systems or data.
- Analysis and reporting: Documentation of the steps taken, vulnerabilities identified, and recommendations for addressing them.
- Remediation and verification: Implementation of recommended measures and subsequent verification that vulnerabilities have been effectively resolved.

9.5.2 The importance of detecting malicious activity in 5G networks

Malicious activities in 5G networks, as complex environments, and their detection face increasing demands due to more sophisticated attack techniques and the declared need for innovation; these demands must not be disappointed, ranging from ordinary network users to those in the fields of autonomous technologies and industrial automation. This primarily concerns:

- Ensuring the security of critical infrastructure: Given that 5G networks will serve as the foundation for critical infrastructure and services, it is essential to ensure their maximum possible security.
- Protection against complex and evolving threats.
- Promoting trust and reliability: 5G network operators must ensure that their networks are trustworthy and resilient to attacks, which is key to supporting business and personal applications.

9.6 Cooperation and threat intelligence sharing

Cooperation and the sharing of threat **intelligence** between operators, equipment manufacturers and government agencies is another way to detect malicious activity on 5G networks. Given the rapid evolution and sophistication of these threats, it is essential that all stakeholders in the 5G network ecosystem collaborate and share relevant information, enabling a rapid response and ensuring protection.

By creating shared threat databases, engaging in international and sectoral cooperation, and dynamically updating security measures, all participants are expanding the ways in which security threats can be identified and detected in a timely manner.

9.6.1 Creation of shared threat databases

To identify and share malicious activity, databases serve either as centralised platforms or as databases of malware signatures and indicators of compromise:

- Centralised information-sharing platforms: The creation of shared platforms, such as Threat Intelligence Sharing Platforms, enables the collection, analysis and distribution of threat information amongst stakeholders.
- Databases of malware signatures and indicators of compromise (IoC): Sharing this information helps organisations to quickly identify and respond to newly discovered threats.

9.6.2 International and sectoral cooperation

Cooperation in the detection of malicious activities generally utilises a global network for information exchange (between states, international organisations and sectors), or involves specialised groups (ISACs) that collaborate within a specific sector and share relevant information within their field of activity.

The role of support tools following the detection and sharing of malicious incidents is primarily fulfilled by the dynamic updating of security measures, common standards and protocols, and, last but not least, joint research and development.

- Dynamic updating of security measures – Systems can be configured to automatically receive updates to security signatures and rules based on shared information.
- Common standards and protocols – The use of standardised formats, such as STIX (Structured Threat Information eXpression) and TAXII (Trusted Automated Exchange of Indicator Information), facilitates interoperability and the effective exchange of threat intelligence.
- Research and development – Cooperation supports research and development in the field of advanced defence technologies and strategies to combat cyber threats.

10 Capabilities of 5G networks built in an Open RAN environment to withstand DDoS attacks

Testing and evaluating the ability of 5G networks built in an Open RAN environment **to withstand distributed denial-of-service (DDoS) attacks** is a complex task. 5G networks and Open RAN bring new approaches and technologies to the field of mobile communications, which have the potential to increase flexibility, reduce costs and foster innovation.

10.1 Open RAN architecture

Open RAN, or Open Radio Access Network, is an initiative focused on standardising and opening up interfaces and implementations in radio access networks. This approach allows operators to combine and use hardware and software from different manufacturers, leading to greater flexibility, reduced dependence on a single supplier and potentially lower costs.

The key benefits of Open RAN architecture therefore lie in:

- Flexibility and innovation: Open interfaces facilitate the integration of new technologies and services, which can accelerate innovation.
- Cost reduction: The ability to choose between different suppliers can lead to price competition and lower costs for operators.
- Resilience and reliability: Diversification of suppliers and components can increase the network's resilience to outages and attacks, as the failure of a single component does not necessarily lead to the failure of the entire network.

On the other hand, however, there are **drawbacks associated with the Open RAN architecture**:

- Complexity and integration: Integrating components from different manufacturers introduces complexity, which can make network security and management more difficult.
- Interfaces and standards: Open interfaces require careful security measures to prevent exploitation. Standardisation is key, but it can also present a challenge in a rapidly evolving environment.
- Supply chain: The expansion of the supply chain increases the risk of vulnerabilities and attacks associated with the supply chain.

10.2 The 5G security framework

5G technology brings significant improvements in performance, capacity and efficiency, but also faces new security challenges. **The 5G security framework** is designed to address these challenges, primarily through enhanced encryption, improved user and device identity protection, and advanced mechanisms for data integrity and protection.

10.2.1 Integration with Open RAN:

The 5G security framework must be carefully integrated with the Open RAN architecture to ensure that all open and interoperable components fully respect and utilise the security measures defined for 5G.

This primarily concerns securing interfaces between different parts of the network, protection against supply chain attacks, and the implementation of advanced detection and response mechanisms against DDoS attacks.

10.3 Specifics of DDoS attacks in the context of 5G and Open RAN

5G and Open RAN networks have the ability to respond to the specific characteristics of distributed denial-of-service (DDoS) attacks either by their very nature or through the level of incorporated protective measures. First, let us **summarise the specific characteristics of DDoS attacks in 5G**:

- High speeds and low latency of 5G: 5G networks are designed to support high data transfer speeds and low latency. These characteristics can be exploited in DDoS attacks, as attackers can generate a larger volume of malicious traffic in a shorter timeframe, thereby increasing the potential impact of the attack on target services and infrastructure.

- The distributed and heterogeneous nature of Open RAN: Open RAN architecture supports the integration of components and solutions from different vendors, which can lead to a distributed network model. Whilst this can offer benefits in terms of flexibility and resilience, it can also complicate the detection and mitigation of DDoS attacks, as the attack can be distributed across different parts of the network and resources.

- Exploitation of network functions and protocols: 5G and Open RAN introduce new network functions and protocols that could potentially be exploited to carry out DDoS attacks. For example, if attackers gain control of a sufficient number of devices connected to a 5G network, they can use these devices to generate malicious traffic directed at specific targets.

- Complexity of management and monitoring: The integration and management of heterogeneous network components in an Open RAN environment can be challenging, making it difficult to monitor continuously and respond quickly to potential DDoS attacks.

- Security gaps and vulnerabilities: Potential security gaps between different components and vendors can provide attackers with entry points to launch DDoS attacks.

- Ensuring interoperability and security: Maintaining interoperability between different components whilst ensuring a high level of security is a key challenge that requires careful planning and the implementation of security protocols.

10.3.1 Protective measures and mitigation

Managing DDoS attacks in 5G and Open RAN environments requires technological measures, process security and cross-organisational collaboration. Ensuring resilience against these attacks is an ongoing process that must reflect constantly evolving cyber threats. Specifically, this involves:

- Extended monitoring and detection: The implementation of tools for monitoring network traffic and detecting anomalies is essential for identifying and responding to DDoS attacks in their early stages.

- Advanced detection and analysis: The use of advanced attack detection technologies, such as artificial intelligence (AI) and machine learning (ML), enables the rapid identification of abnormal traffic and potential DDoS attacks. These systems are constantly learning from new data and can adapt their responses to changing attack patterns.

- Network slicing and attack isolation: Network slicing, a key feature of 5G networks, enables operators to create isolated virtual networks (slices) with their own secure and optimised resources. In the event of a DDoS attack, the attack can be isolated to a specific slice, thereby minimising its impact on other parts of the network.

- Dynamic access control and traffic filtering: Dynamic access control and intelligent traffic filtering based on behavioural patterns and IP address reputation can help identify and block malicious traffic before it reaches critical network components.

- Multi-vendor management security: In the heterogeneous Open RAN vendor environment, it is essential to ensure that all components and services from different manufacturers meet the same high security standards. This includes careful vendor selection, regular security audits, and compatibility and security testing between different systems.

- Scalable and Continuous Protection: Protection against DDoS attacks must be scalable to absorb and process large volumes of malicious traffic. This involves utilising cloud services for load balancing and attack absorption, as well as continuously updating protection systems.

- Cooperation and Information Sharing: Collaboration between telecommunications operators, technology providers, security firms and government agencies is crucial for exchanging information on threats, the latest attacker tactics and effective defence methods. Information sharing helps to create a stronger defence against DDoS attacks and improves overall cyber resilience.

- Educational programmes and awareness campaigns: Raising staff awareness and educating them about security threats and best practices for prevention are essential for strengthening the first line of defence. Education may include training on security protocols, recognising potential threats, and responding correctly to incidents

10.4 Standards and best practices

The importance of international standards and best practices for protecting 5G networks and Open RAN-based infrastructure against distributed denial-of-service (DDoS) attacks is gradually increasing. These standards and practices are essential for creating a reliable, secure and resilient telecommunications ecosystem, particularly in terms of common application and a common language.

10.4.1 International standards and security recommendations

Within the context of 5G networks and Open RAN, standards and recommendations can be easily applied as a preventive measure prior to implementation and during security management. Organisations or groups active in this field include:

- 3GPP (3rd Generation Partnership Project): This organisation develops standards covering the entire spectrum of mobile telecommunications, including 5G. 3GPP specifications address various aspects of network security, from radio transmission security to network security architecture. To protect against DDoS attacks, 3GPP standards include mechanisms for user and device identification and authentication, data encryption and signalling integrity.

- ITU (International Telecommunication Union): The ITU, the UN agency for information and communication technologies, publishes standards known as ITU-T Recommendations. These documents cover a wide range of ICT topics, including security aspects of telecommunications networks. The ITU-T X-series of Recommendations cover cybersecurity and data protection, which is relevant to defences against DDoS attacks.

- GSMA (Global System for Mobile Communications Association): The GSMA, an association representing the interests of mobile operators worldwide, develops guidelines and best-practice documents that help members implement security measures in line with the latest standards and technologies. This includes security guidelines for 5G networks and recommendations for protection against DDoS and other cyber threats.

In terms of the outputs from standards and security recommendations – although these are written documents that must be translated into concrete implementation – the following specific recommendations cover key areas of protection against DDoS attacks:

- Threat intelligence sharing: Effective defence against DDoS attacks requires up-to-date information on potential threats and attack methods. Organisations should encourage the sharing of this information amongst themselves and with government security agencies.

- Regular security audits and testing: To identify vulnerabilities in the network infrastructure and verify the effectiveness of implemented security measures, it is essential to conduct regular security audits and penetration testing.

- Implementation of robust security protocols: Securing communication between different network components and protecting against unauthorised access is crucial. This includes the use of strong encryption, authentication and integrity checks.

- Appropriate incident response plans: Creating and maintaining up-to-date plans for responding to security incidents, including DDoS attacks, is essential for a rapid and effective response. These plans should include procedures for isolating attacks, communicating with relevant parties and restoring services.

- Training and awareness: Maintaining a high level of security awareness among staff and customers helps to reduce the risks associated with cyber threats. This includes training on security practices, recognising phishing attempts, and the secure handling of data.

10.5 Testing and validation

Testing and validating the ability of 5G networks and Open RAN infrastructures to withstand distributed denial-of-service (DDoS) attacks serves to identify potential vulnerabilities in the network and verify the effectiveness of the security measures implemented.

The first step is to draw up a detailed testing plan that includes objectives, scope, methodologies, tools used and success criteria. It is important to choose an approach that covers all key aspects of the network and security, including radio access, the network core, applications and services.

Specialised tools and frameworks are then used to generate DDoS attacks, simulating various types of attacks (e.g. volumetric, protocol-based, application-based), and testing how the network responds to and withstands these attacks.

Analysing the data obtained during the tests requires advanced tools capable of processing large volumes of information and identifying anomalies. These tools may utilise AI and ML to detect new or unusual attack patterns.

An important outcome of the testing is the assessment of the network's performance under load and the system's ability to maintain service availability during an attack. The response time to an attack and the effectiveness of both automated and manual attack mitigation measures are also evaluated.

Conclusions and recommendations obtained during testing and validation activities should be documented (key risks, proposed improvements and plans for implementing corrective measures) and shared with relevant teams and management.

One final note: just as cyber threats are constantly evolving, testing and validation must be a continuous process, particularly with regard to the review of test scenarios and security measures. They must confirm high effectiveness at all times, even against new, more sophisticated threats. At the same time, testing should not focus solely on technical aspects, but should also encompass processes, policies and the human factor.

11 Proposal for ensuring the availability of 5G networks even under high load

Ensuring the availability of 5G networks even under high load is a key challenge for operators and technology companies, and this task is fulfilled **by advanced network management technologies, as well as network slicing, cloud and edge computing**, capacity expansion and resource sharing, and the ongoing optimisation and updating of software.

11.1 Advanced network management technologies

Advanced network management **technologies** play a key role in ensuring the availability and efficiency of 5G networks, particularly during periods of high load. These technologies encompass a range of methods and tools that enable operators to better monitor, analyse and manage networks.

11.1.1 Predictive analytics and machine learning

Predictive analytics uses historical data on network usage to forecast future load and potential issues. Operators then adjust resource allocation and capacity before problems arise.

Machine learning and artificial intelligence can automatically analyse vast amounts of data in real time and identify patterns that might indicate emerging problems or opportunities to optimise network performance.

11.1.2 Network management automation

Automated network management tools can automatically implement configuration changes, software updates and network optimisations without the need for manual intervention, thereby increasing efficiency and reducing the likelihood of human error.

Self-organising networks (SON) are capable of optimising, configuring and healing themselves. Transmission power and capacity are automatically adjusted based on current user needs and network conditions

11.1.3 Dynamic resource allocation

Flexible resource allocation enables networks to dynamically redistribute capacity and resources according to current load and user needs. This helps ensure that critical services always have priority and sufficient capacity, and that overall network utilisation is as efficient as possible.

11.1.4 Advanced monitoring and diagnostics

Advanced monitoring systems collect and analyse real-time data on performance, load, service quality and network security, enabling rapid problem detection and resolution.

Diagnostic tools can identify the causes of problems, ranging from service outages to network slowdowns, and help restore normal conditions quickly.

By implementing these advanced technologies and approaches, operators can not only improve the availability and reliability of 5G networks, but also increase overall user satisfaction through better service quality and consistency.

11.2 The use of network slicing

As has been described on several occasions, **network slicing** enables operators to create multiple virtual network slices on the same physical infrastructure. Each of these virtual networks is isolated and can be optimised for a specific type of service or set of

requirements. This flexibility enables operators to manage resources more efficiently and provide services tailored to the specific needs of users or applications.

11.2.1 Optimisation for different types of services

Each slice can be specifically configured for different purposes, such as mass IoT (Internet of Things) devices, critical communications (e.g. for emergency services or autonomous vehicles), or high-speed mobile internet for end users. Optimisation then takes place according to specific requirements for latency, throughput, reliability and mobility.

11.2.2 Efficient use of resources

Thanks to the isolation and specific configuration of each slice, network resources can be allocated and managed more efficiently. This ensures that critical applications always have sufficient resources even during periods of high load, whilst less critical services can be flexibly managed according to available capacity.

11.2.3 Ensuring Quality of Service (QoS) and reliability

Network slicing enables operators to define and adhere to SLAs (Service Level Agreements) for different types of services. This capability ensures that all applications and services operate with predictable quality and reliability, which is essential for critical applications requiring low latency and high availability.

11.2.4 Rapid response to changing requirements

Given the dynamic nature of network slicing, operators can respond quickly to changing market demands or specific events that require an immediate increase in capacity or resources for certain services. This allows networks to be highly flexible and adaptable.

11.2.5 Enhanced security

The isolation between slices means that potential security threats affecting one virtual network do not directly impact other slices. Such separation enhances overall network security and reduces the risk of threats spreading.

11.3 Capacity expansion using Small Cells

Expanding the capacity and coverage of 5G networks using **Small Cells technology** helps ensure network availability even under heavy load, particularly in densely populated areas or locations where there is increased demand for mobile data services. Small Cells are small, low-power transmitters that complement traditional macro cells and enable operators to provide coverage and capacity in specific areas.

11.3.1 Support for high-speed data transfers

Small Cells enable users to enjoy high-speed internet connectivity thanks to the proximity of the transmitter, resulting in lower latency and higher data transfer speeds.

11.3.2 More efficient use of spectrum

Thanks to the smaller coverage area of each small cell and their concentration in high-demand areas, operators can utilise the available spectrum more efficiently and run more simultaneous connections in a given area without mutual interference.

11.3.3 Flexible and cost-effective network expansion

Installing Small Cells is typically less costly and less intrusive than building new macro cells. They can be mounted on existing infrastructure, such as buildings, street lamps or telephone poles, enabling faster and more flexible network expansion.

11.3.4 Reducing the load on macro cells

By distributing the load between macro cells and Small Cells, operators can optimise overall network utilisation. This helps maintain a high level of service even during peak times by reducing the load on individual macro cells.

It is worth noting that the implementation of small cells faces challenges, particularly regarding the need to secure installation permits, signal interference between cells, and integration with existing network infrastructure.

11.4 Dynamic Spectrum Sharing (DSS)

Dynamic Spectrum Sharing (DSS) is an innovative technology that enables mobile network operators to make efficient use of existing spectrum for the simultaneous deployment of networks of different generations, such as 4G LTE and 5G. DSS facilitates the transition from 4G to 5G and allows operators to offer 5G services without the need to acquire new spectrum bands or phase out existing 4G services.

11.4.1 Flexible spectrum utilisation

DSS enables the same frequency band to be dynamically shared between different generations of networks. Depending on current user demand and device availability, the system can adjust the allocation of spectrum between 4G and 5G networks in real time.

11.4.2 Cost and efficiency optimisation

This technology enables operators to rapidly expand 5G network coverage without the need for large initial investments in new spectrum or infrastructure. DSS reduces the costs of deploying 5G networks whilst maximising the use of existing spectrum.

11.4.3 Ensuring a seamless transition between network generations

With DSS, operators can provide 5G services where possible, whilst continuing to maintain and support existing 4G services. This ensures that users with 4G devices are not left behind, whilst users with 5G devices can benefit from higher speeds and lower latency.

11.4.4 Dynamic and efficient load management

DSS enables operators to dynamically manage traffic between 4G and 5G networks, which is particularly useful during periods of high traffic. This ensures more efficient use of available resources and improves overall network performance.

11.4.5 Support for various usage scenarios

DSS is not limited to specific frequency bands or geographical areas, enabling operators to deploy the technology in various environments and for different use cases, from densely populated urban areas to vast rural regions.

11.5 Use of cloud and edge computing technologies

Cloud and edge computing technologies are the latest innovative technologies to be used in 5G networks to ensure the availability and high performance of services, even under heavy load. These technologies rely on the decentralisation of data processing and applications, bringing data and computing resources closer to end users.

11.5.1 Reduced latency

Edge computing processes data directly at the network edge, close to users or IoT devices. This significantly reduces latency, which is critical for applications that prioritise real-time operation, such as autonomous vehicles, industrial automation, telemedicine and virtual/augmented reality.

11.5.2 Relieving the load on central cloud servers

Distributing data processing and storage across edge servers reduces the load on central data centres. This is synergistically linked to more efficient use of resources and a reduced need to transfer large volumes of data across the entire network, thereby increasing the overall efficiency of the network.

11.5.3 Increased reliability and service availability

Edge computing can increase network reliability by ensuring service continuity even in the event of outages or issues in central data centres. Local data processing means that applications can continue to function even if the connection to the main cloud is interrupted.

11.5.4 Efficient use of bandwidth

Moving data processing closer to the source reduces the need to transfer large volumes of data across networks, thereby freeing up bandwidth for other applications and services. This is particularly important during periods of high load, when bandwidth is a valuable resource.

11.5.5 Support for IoT and advanced applications

With its unique characteristics, edge computing is essential for the development of the Internet of Things (IoT), where the volume of data generated by sensors and devices requires rapid processing and quick decision-making or real-time interaction.

11.5.6 Security and privacy

By processing data at the network edge, closer to its source, edge computing can also enhance security and privacy, as sensitive data does not need to leave the local network or geographical area.

Experience to date shows that the implementation of cloud and edge computing technologies requires, in particular, investment in new infrastructure.

11.6 Software optimisation and updates

Optimising and updating network **software** is a well-known and long-established practice for ensuring high availability, reliability and performance of 5G networks. These processes involve regular updates to network software components, improvements to network control algorithms and configuration adjustments to maximise efficiency and service quality.

11.6.1 Increasing network efficiency

Software updates and configuration optimisation can improve algorithms for data routing, network access control and resource allocation, leading to more efficient use of available spectrum and network resources. The result is faster data speeds and better voice service quality for users.

11.6.2 Improving network reliability and resilience

Regular software updates can fix bugs, improve security protocols and increase the network's resilience against outages and attacks. This ensures the network remains available and reliable even under challenging conditions.

11.6.3 Support for new technologies and services

The development of 5G networks is constantly bringing new applications and services, such as IoT, autonomous vehicles, telemedicine and augmented/virtual reality. Software optimisation and updates enable networks to integrate these new technologies by expanding their capabilities and improving performance.

11.6.4 Adaptation to changing demand patterns

Dynamically adjusting network configuration and capacity according to current load and demand patterns can improve the user experience whilst increasing overall network efficiency. The advantage is rapid adaptation to fluctuations in population growth, or major events or disasters.

11.6.5 Minimising operating costs

More efficient use of resources and improved automation through software updates reduce an organisation's operating costs. Synergistically, software updates lead to a reduction in the number of manual interventions, and the automation of routine tasks enables operators to save time and resources.

Regular updates and optimisations are also linked to the need for careful planning and testing of their deployment, i.e. in particular testing the compatibility of new software versions with the existing hardware and software environment.

11.7 Ensuring network redundancy and resilience

Ensuring network redundancy and resilience involves a range of technical and organisational measures that help minimise the impact of potential problems and ensure continuous service availability.

11.7.1 Hardware redundancy and path diversification

The physical deployment of multiple hardware components, such as servers, switches and routers, in different parts of the network ensures that if one component fails, another can immediately take over its function.

Network resilience against outages is achieved by utilising multiple possible paths for data between critical points, thereby rerouting data in the event of problems on a single route.

11.7.2 Software-Defined Networking (SDN) and Network Functions Virtualisation (NFV)

SDN and NFV enable flexible and dynamic network reconfiguration via software. These technologies support rapid, real-time adaptation of network infrastructure and services, which helps maintain service continuity even in the event of hardware or software issues.

11.7.3 Geographical Diversification

Deploying data centres and key network elements across different geographical areas can help minimise the risk of outages caused by local adverse events (power cuts) or even local disasters.

11.7.4 Automated backup and recovery

Regular backups of configurations, software and critical data ensure that, in the event of a failure, systems can be quickly restored to their last stable state.

Automating recovery processes enhances the ability to respond quickly to issues and minimise service downtime

11.7.5 Real-time monitoring and diagnostics

Advanced monitoring and diagnostic tools enable continuous monitoring of network status and the rapid identification and resolution of network unavailability issues.

Early detection and resolution of issues also helps prevent widespread outages.

11.7.6 Contingency and disaster planning

The creation and regular testing of disaster recovery plans are essential for preparing for a range of scenarios, from technical failures to natural disasters. Staff training and regular drills help ensure that the team is ready to respond quickly and effectively to incidents.

12 Proposal for a system for the regular auditing and monitoring security measures in 5G networks

The design of a system for **the regular auditing and monitoring of security measures** in 5G networks is an important step in ensuring the security and resilience of 5G networks against various sophisticated threats and attacks. It always begins with the identification and assessment of assets and risks.

12.1 Identification and assessment of assets and risks

This process helps organisations understand what they need to protect and what threats could endanger their assets. It is based on the auditor's asset mapping.

12.1.1 Asset mapping

The purpose of **asset mapping** is to catalogue identified assets, subsequently assess them, and finally determine the owner of each asset:

- Asset Cataloguing: Creating a comprehensive list of all network components, including physical devices (e.g. servers, switches, base stations), software (operating systems, applications), data (user data, configuration data) and services (internet connectivity, cloud services).
- Asset Classification: Categorising assets based on their importance and sensitivity. This involves determining which data is personal, which has financial value, and which is critical to operations.
- Responsibility for Assets: Assigning responsible individuals or teams to each asset to ensure management, security and updates.

12.1.2 Risk Analysis

Risk analysis is a process familiar from several other sources; we therefore outline the main steps of the process briefly here:

- Threat Identification: Analysing potential external and internal threats to 5G networks, such as cyberattacks, physical damage to infrastructure, software faults, or data loss.
- Vulnerability Assessment: Identifying security weaknesses that could be exploited by threats. This includes outdated software, configuration flaws, and weaknesses in protocols and encryption.
- Impact and Probability: Assessing the potential impact of each threat on the organisation and the likelihood of its occurrence. This helps to identify which threats pose the greatest risk.
- Risk Prioritisation: Based on the impact and likelihood assessment, risks are ranked by priority, enabling the organisation to focus on the most significant threats

12.1.3 Risk Management Plan

Once the risks in the organisation's 5G networks have been identified and assessed, the next step is to work with the owners and responsible parties to decide on **a risk management plan** based on the established priorities**. This is achieved through**:

- Mitigation Strategy – Developing strategies to reduce risks, including technical solutions (e.g. strengthening security, updates and patches) and organisational measures (e.g. process improvements, staff training).
- Planned Measures – Creating a specific plan for implementing risk mitigation and prevention, including a timeline and allocation of resources.
- Monitoring and Review – Regularly evaluating and updating the risk analysis and risk management plan to account for emerging threats and changes in the network or organisation.

Identifying and assessing assets and risks are key to developing an effective 5G security strategy. They provide the foundation for all further security activities, enabling the organisation to better prepare for potential threats and increase the resilience of its 5G network

12.2 Implementation of preventive measures

The implementation of preventive measures focuses on preventing security incidents through various techniques and methods.

Endpoint security, data encryption and network segmentation are used in particular.

- Endpoint security measures:
  - Antivirus and antimalware: Installation and regular updating of antivirus and antimalware software on all endpoints in the network to prevent malicious attacks.
  - Patch and update management: Implementing a process for regularly patching and updating operating systems and applications on endpoints to address known vulnerabilities.
  - Access management: Implementation of strong authentication and authorisation policies, including multi-factor authentication, to restrict access to network resources to authorised users only.
- Data encryption measures:
  - Encryption at rest: Use strong encryption for stored data to protect it from unauthorised access in the event of device loss or theft.
  - Encryption in transit: Ensuring that all data transmitted between devices and over public networks is encrypted, preventing it from being intercepted or tampered with.
  - Key management: Implementing a robust system for managing encryption keys, including their secure storage, rotation and deletion.
- Network segmentation measures:
  - Defining segments: Dividing the network into logical segments based on function, data sensitivity level or security level. This allows for better access control and limits the spread of attacks across the network.
  - Isolation of critical systems: Ensuring that critical systems and data are isolated in secure segments, making it more difficult for potential attackers to gain access.
  - Rules for access between segments: Setting strict rules to control communication between segments, including firewalls and data transfer rules, to minimise the risk of cross-segment attack propagation.
- Additional security measures:
  - Intrusion Detection and Prevention (IDS/IPS): Implementing intrusion detection and prevention systems that continuously monitor network traffic and look for known attack patterns or suspicious behaviour.
  - Security policies and procedures: Developing and implementing clearly defined security policies and procedures that cover all aspects of network security and are regularly updated.

- Physical security: Securing the physical equipment and infrastructure that form part of the 5G network against unauthorised access, theft or damage.

12.3 Regular auditing and monitoring

Regular auditing and monitoring involves tracking network traffic, detecting potential threats and vulnerabilities, and carrying out regular checks to identify and resolve security issues. Examples of suspicious activities that auditing and monitoring can detect are listed below for illustration:

1. Unusual network traffic
   - High volume of data transfer: An increase in data transfer on unusual ports or between unusual IP addresses may indicate an attempt at data exfiltration.
   - Unusual transmission times: Network traffic at unusual times (e.g. at night or at weekends) may be a sign of an attempted attack outside normal working hours, when the network is likely to be less closely monitored.
2. . Anomalous user behaviour
   - Unusual logins: Login attempts from geographical locations from which the user does not normally log in, or repeated failed login attempts, may indicate an attempted brute-force attack.
   - Changes in usage patterns: User activities that are unusual compared to the user's normal behaviour patterns may be a sign of a compromised account.
3. Suspicious access and modifications
   - Unauthorised access: Attempts to access systems, applications or data to which the user does not normally have permission may indicate a misuse of access rights.
   - Unusual configuration changes: Unexpected changes to the configurations of network devices, servers or security settings may be a sign of an attempt to compromise the system.
4. Malware and attacks
   - Malware detection: Activity that matches known patterns of malware behaviour, such as unusual disk writes, attempts to access system files, or unusual communication with external servers.
   - DDoS attacks: A sudden and significant increase in network traffic, causing services to slow down or become unavailable, may be a sign of a Distributed Denial of Service attack.
5. Unknown or suspicious devices on the network
   - New devices: The detection of new devices connected to the network that have not been pre-approved or are unknown may indicate an attempt at unauthorised access.
   - Devices with known vulnerabilities: Identification of devices on the network that contain known vulnerabilities and may be targets for attacks.
6. Attempts to circumvent security measures
   - Changes to firewall rules: Unauthorised changes to firewall rules that may allow unwanted access to the network.
   - Attempts to disable security tools: Actions aimed at disabling or circumventing security systems such as antivirus, IDS/IPS or SIEM.

Regular auditing and monitoring are supported by automated network monitoring tools.

12.3.1 Automated network monitoring tools

We will now list the network monitoring tools that are well-known and applicable in 5G networks:

- Implementation of SIEM systems (Security Information and Event Management): These systems collect and analyse logs and events from various sources across the network in real time to identify suspicious activity or security incidents.

- Intrusion detection and prevention tools (IDS/IPS): Intrusion detection and prevention systems monitor network traffic and look for known attack patterns or anomalous behaviour that could indicate a security threat.

- Vulnerability monitoring: The use of tools to regularly scan the network and its components to identify newly discovered vulnerabilities that could be exploited by attackers.

12.3.2 Regular security audits

Depending on their focus, security audits are divided into:

- External security auditing: Regular security audits carried out by external experts, who can provide an independent view of the network's security status and uncover weaknesses that the internal team may have become accustomed to.

- Penetration testing: Simulating attacks on the network to test resilience against real-world threats and identify weaknesses in security measures.

- Review of policies and procedures: Periodic review and updating of security policies and procedures to ensure they align with the current security landscape and threats.

The results of the assessment carried out as part of network auditing and monitoring subsequently lead to the application of a certain level of updates or patching, or may form part of a training programme, involving the addition of further security threats and learning the correct responses and procedures to deal with them.

- Updates and patching can have several functional components in the context of 5G networks. These are:
    - Patch management: Implementing a process for the regular patching of software and firmware on all devices in the network, including routers, switches, base stations and endpoints.
    - Security tool updates: Ensuring that all security tools and systems are constantly updated to effectively protect the network against the latest threats.
    - Records and documentation: Keeping detailed records of all updates and patches applied, including installation dates and versions, to facilitate monitoring and auditing.

12.4 Incident response and recovery

Focusing on **incident response and** recovery are key aspects of ensuring the resilience of 5G networks against security threats. This phase requires careful planning and preparation to ensure the organisation is able to respond quickly and effectively to security incidents and minimise their impact.

Incident response begins with drawing up a plan for how to respond to selected groups or specific significant types of incidents. For potential recovery following an incident, it is advisable to have a backup system in place that can restore the situation to the state prior to the incident. Sufficient and timely communication is then a key factor in incident response. **Below, we provide a brief overview of the main areas in which individual activities are directed, both generally and specifically in relation to 5G networks.**

12.4.1 Incident response plan

- Development of an incident response plan: Creation of a detailed plan describing the procedures and steps to be taken in the event of a security incident. The plan should include a definition of an incident, communication strategies, the roles and responsibilities of the incident response team, and escalation procedures.

- Incident Response Team (IRT): Assembling a specialised team responsible for managing security incidents. The team should have clearly defined roles, including incident managers, security analysts, legal advisers and communications specialists.

- Training and exercises: Regular training and simulation exercises for the Incident Response Team to ensure team members are well prepared and know their tasks in the event of a real incident.

12.4.2 Data backup and recovery

- Backup strategy: Developing and implementing a data backup strategy that includes regular backups of critical data and systems. It is important to have multiple copies of backups in different locations, including off-site locations, to increase resilience against physical disasters or cyber attacks.

- Disaster Recovery Plan (DRP): Developing a plan that outlines procedures for restoring operations and data following a security incident or disaster. The plan should include prioritising systems and applications for recovery and testing recovery procedures.

- Recovery testing: Regular testing of the organisation’s ability to restore systems and data from backups. Testing helps identify potential issues in the recovery process and allows them to be rectified before an actual incident occurs.

12.4.3 Communication during incidents

- Communication plan: Developing a communication plan that specifies how and when to communicate with internal and external parties during a security incident. This includes determining who is authorised to speak on behalf of the organisation and what information will be shared with the media, customers and regulatory authorities.

- Transparency and trust: Maintaining transparency during incident management can help preserve the trust of customers and partners. It is important to communicate clearly and regularly update all stakeholders on developments and the measures taken.

12.4.4 Post-incident steps

- Post-incident analysis: Once the incident has been resolved, conduct a thorough analysis of what happened, how the incident was handled, and what steps were taken to resolve it. The aim is to identify weaknesses in security measures and processes and to identify lessons that can be used for improvement.

- Incident report: Prepare a detailed incident report, including a description of the incident, an analysis of the causes, an overview of the response to the incident, and recommendations for future improvements.

12.5 Training and awareness-raising

Training and awareness-raising help to ensure that all staff and network users understand the security risks and are familiar with best practices for minimising them.

Training and awareness-raising are applied to various user groups, i.e. employees, experts and the public. As this has already been reiterated in several places in the text, we **present the main focus of training and awareness-raising** here **only in brief points.**

12.5.1 Employee training

- Regular training and workshops: Organisations should provide regular training on cybersecurity, covering current threats, the company's security policies, and procedures for ensuring data and network security. Training should be tailored to different levels of staff, from technical personnel to management.

- Simulation of cyber attacks and phishing campaigns: Conducting simulated attacks or phishing campaigns can help employees better understand what these threats look like and how to respond to them, significantly increasing their ability to detect and prevent real attacks.

- Engagement in a security culture: Creating a strong security culture within the company, where security is seen as a shared responsibility, can significantly contribute to the security of 5G networks.

12.5.2 Public awareness

- User awareness campaigns: Launching awareness campaigns that educate users about the risks associated with using 5G networks and how they can protect their data and devices. These campaigns could include tips on safe internet use, the importance of software updates, and the importance of strong passwords.

- Use of social media and websites: Social media and websites can be used effectively to disseminate awareness materials. This will reach a wider audience and can raise awareness of security threats and how to defend against them.

- Partnership programmes with educational institutions: Collaboration with schools, universities and other educational institutions can help raise awareness of cybersecurity among younger generations. This may include hosting workshops, lectures and competitions on cybersecurity.

12.6 Cooperation and information sharing

Effective collaboration and the open exchange of information between various organisations, government agencies and industry groups enable threats to be identified more quickly, incidents to be responded to, and awareness of best security practices to be raised. Cooperation and information sharing are essential for improving the security of 5G networks at a global level. By pooling the resources and expertise of various stakeholders, cyber threats can be addressed more effectively and the secure development and use of 5G technologies can be promoted. **Cooperation and information sharing take place at various levels, examples of which include:**

- Security partner networks: Establishing and maintaining partnerships between organisations within the same industry or sector to share information on threats, vulnerabilities and incidents. These networks may include private companies, non-profit organisations and government institutions.

- Security forums and associations: Participation in security forums and associations provides a platform for exchanging knowledge and experience in the field of cybersecurity. Organisations can benefit from access to a wide range of resources, including research, analyses and threat detection tools.

- National and international initiatives: Collaborating with national and international government agencies on initiatives aimed at improving cybersecurity. This may include participation in national cybersecurity centres, sharing threat intelligence, and collaborating on the development of security standards and policies.

- Government information-sharing programmes: Participation in programmes that promote information-sharing between the public and private sectors. These programmes often provide valuable insights into current threats and help coordinate incident response.

- Conferences and seminars: Active participation in cybersecurity conferences and seminars enables experts to share their knowledge, findings and best practices with the wider community. This may include presentations, workshops and panel discussions.

- Specialist publications and research: Contributing to specialist journals, blogs and online forums can help raise awareness of new threats, technologies and defence methods. Sharing research findings and case studies promotes collective learning and innovation in the field of security.

- Shared threat and vulnerability databases: Utilising online databases and repositories that provide information on known cyber threats, vulnerabilities and their solutions. Access to this information can help organisations quickly identify and address potential weaknesses.

- Shared analytical tools: The use of tools and platforms that enable the sharing and analysis of security incident data in real time can improve organisations' ability to respond to newly discovered threats.

13 Proposal for ensuring an immediate response to potential security incidents

Ensuring an immediate response to potential security incidents requires a well-thought-out plan that includes pre-defined procedures, communication, tools and a team.

13.1 Establishing an Incident Response Team (IRT)

Establishing an incident response team (IRT) **requires a detailed consideration of its structure, composition, training and roles.**

13.1.1 Team structure

The structure of a team that handles security incidents must cover the following key roles, at a minimum:

- Team leader: An experienced leader who has a good understanding of security procedures and can effectively manage the response to incidents.
- Technical experts: Specialised IT security experts focused on malware analysis, forensic analysis, and system and network security.
- Lawyers specialising in cyber law and regulatory requirements, who can provide advice on the legal and compliance aspects of incidents.
- Communications experts who prepare and coordinate all external and internal communications relating to the incident.
- Representatives from business and operational units: Representatives from key business and operational departments who help assess the impact of the incident on the business and coordinate measures to minimise this impact.

13.1.2 Putting the team together

When selecting IRT members, it is important to look for individuals with the appropriate skills, experience and ability to work under pressure.

It is also necessary to ensure that the team includes experts from various relevant fields so that it can cover all aspects of incident response.

13.1.3 Roles and responsibilities

Each team member should have clearly defined roles and responsibilities that do not overlap with responsibilities in another role. Team members must be aware of their primary tasks during an incident and the basic principles and procedures for communication.

13.1.4 Readiness and availability

Ensuring an immediate response to a security incident is not possible where team members are unable to respond to incidents at any time (this may require the introduction of shifts or on-call systems).

Communication and escalation processes must always be properly documented for future reference.

13.1.5 Team performance evaluation and improvement

Following an incident, it is important to assess the team's performance. Exercises or involving the team in responding to real-life incidents are effective ways of improving the team's response capabilities. The opportunity for open feedback, where team members can share ideas for improving processes and incident response methods, also leads to better responses to potential security incidents.

13.2 Incident identification and assessment

Incident identification and assessment supports an effective response to security incidents. It involves processes and tools for detecting incidents, categorising them, prioritising them and resolving them correctly.

13.2.1 Incident detection

By implementing and regularly updating sophisticated monitoring and detection tools, such as intrusion detection and prevention systems (IDS/IPS), security information and event management (SIEM) systems, antivirus software and traffic analysis tools, the process gains immediate information to respond to potential incidents.

Another technique that significantly influences the incident detection system is logging and auditing. Systems that maintain detailed logs can be further used to identify and analyse incidents.

Incident detection works much better if the established communication channels foster a culture of security among staff and there is a simple process in place for reporting suspicious activity or security incidents.

13.2.2 Incident assessment

Incident assessment is carried out through a series of sequential steps. It begins with classification and prioritisation; the incident is then analysed and subsequently handed over to the relevant handler, or the parties involved in the incident and other stakeholders are notified. The requirements for each task are summarised as follows:

- Classification and prioritisation: Establish a system for classifying incidents according to their severity and potential impact on the organisation. This system should enable rapid prioritisation of incidents so that the most serious ones are addressed first.
- Initial analysis: Once an incident has been detected, carry out a rapid initial analysis to gain an understanding of the scope, type of attack, affected systems and potential impact.
- Escalation process: Establishing clear rules for incident escalation will ensure that information about incidents reaches the right people, including the IRT, management and, where necessary, external experts, to enable a rapid and effective response.

13.2.3 Communication during the incident

Pre-prepared communication protocols speed up incident resolution. They specify who, when and how will be informed about the incident, including internal teams, company management and, where appropriate, external parties.

Communication until the incident is resolved is a continuous process, requiring ongoing updates on the status of the incident resolution for all stakeholders so that they are kept informed of progress and the measures being taken.

13.2.4 Documentation and records

Documentation and records of an incident help ensure an effective and immediate response to a potential incident. It must be recorded at a minimum level covering all detected incidents, including a description of the incident, the response, the facts established, the measures taken and the results of analyses. Incident documentation is essential for understanding threats, lessons learnt and improvements to security procedures.

After resolving each incident, it is recommended that a thorough analysis be carried out to identify the root causes of the incident, evaluate the team's overall performance, and propose necessary improvements to processes and security measures.

13.3 Communication Plan

Although this section is often placed at the end, **a communication plan** is an essential tool for incident management in ensuring rapid resolution. A communication plan ensures that all stakeholders are identified and contacted regarding the resolution, and are kept informed of the situation and the measures taken. A well-thought-out communication plan helps maintain trust and minimise damage to the organisation's reputation.

Communication planning includes elements such as creating communication protocols, establishing communication channels, and appointing a team; testing or reviewing the communication plan then serves to further improve it. Below is a summary of the relevant tasks for these sections:

13.3.1 Creating communication protocols

1. Pre-defined templates: This involves developing templates for communication in various situations, which can be quickly adapted to specific incidents. Templates should include internal announcements, customer notifications, press releases and FAQs for quick responses to questions.

2. Identifying key messages: Determining the key message that needs to be communicated for different types of incidents saves time. The key message contains information on what has been affected, what steps have been taken, and what further steps you plan to take.

13.3.2 Establishing communication channels

3. Internal communication: If suitable channels for internal communication, such as emails, the intranet, SMS, team chat platforms or dedicated meeting rooms, are selected in advance, all staff will be accustomed to responding to such communications in a timely manner.

4. External communication: By defining which channels will be used for communication with external parties, including press conferences, social media, websites and direct communication with affected customers or partners, the organisation can mitigate reputational risk.

13.3.3 Appointing a communications team

5. Allocation of roles: It is necessary to determine who will be responsible for communication during an incident. Roles may be filled by a spokesperson, a social media team, customer contact points, and technical experts for more detailed information.

6. Training the team: The communications team must be well-trained in crisis communication and understand the technical information relevant to different types of incidents.

7. Consultation with legal advisers: Before any information is published, there must be assurance that the communication complies with legal and regulatory requirements, including the protection of personal data and trade secrets.

13.3.4 Communication planning

8. Regular updates: The plan sets out deadlines and specifies at which stages of the incident updates will be provided across all channels.

9. Responding to enquiries: Enquiries from employees, customers, the media and the public must be answered in a timely manner; therefore, the preparation and, where necessary, approval of standard responses by the relevant personnel must not be underestimated.

13.3.5 Testing and reviewing the communication plan

10. Simulations and exercises: Regular testing of the communication plan through simulations and exercises will help identify its weaknesses and ensure that all stakeholders are prepared to communicate quickly and effectively in real-life situations.

11. Feedback and updates: Gathering feedback following exercises and actual incidents serves to continuously improve communication protocols and procedures.

13.4 Response and mitigation of the impact of a security incident

Once incidents have been identified and assessed, **a response** must be initiated **to mitigate the impact of the security incident**. This represents the specific action taken to address the security incident. It begins with isolating the threat, followed by a deeper analysis of the incident, which leads to the elimination of the threat and the restoration of affected systems.

13.4.1 Isolation and damage limitation

In the first step, incident responders do their utmost to isolate the rest of the network from the incident in order to minimise damage and gather evidence regarding the situation both before and during the incident:

- Isolation of affected systems: Affected systems must be isolated from the rest of the network to prevent the threat from spreading further. This is done, for example, by disconnecting them from the internet and powering down the devices.

- Securing evidence: Before commencing the clean-up process, it is recommended to document the state of the system, in particular to collect all relevant logs and evidence for forensic analysis and legal purposes.

13.4.2 Incident analysis

Once the critical impacts of the incident have been mitigated, the team proceeds with the incident analysis. They will focus on:

- Identifying the source and method of the attack, using information and forensic tools to determine how the attack was carried out and which vulnerabilities were exploited.

- Assessing the impact, i.e. determining the extent of the incident's impact on the organisation's data, systems and operations, including identifying what data has been affected or lost.

13.4.3 Threat removal and recovery

Using the information from the incident analysis, work begins on threat removal, i.e. activities aimed at comprehensively rectifying the situation and restoring data, systems and operations to a flawless state, and bringing the network back online. This is carried out through:

- Malware removal and patching: A thorough clean-up of the affected systems is carried out, including the removal of all traces of malware and the application of the latest security patches to vulnerable software.

- Restoring backups: If data has been damaged or lost, recent backups will be used to restore systems and data to their pre-incident state, and their recovery will be verified.

- Gradual recovery: The affected systems are brought back online, and their standard behaviour is restored in a controlled and gradual manner to ensure that no hidden threats are overlooked.

- Verification of system and data integrity: Before fully restoring operations, it must be verified that the systems are free of any malware and that the data has not been compromised.

13.4.4 Communication during the response

The team regularly provides updates to other internal teams, management and, where appropriate, affected parties on the status of the response and recovery. It strives to manage communication transparently to maintain the trust of customers and partners in the organisation.

13.4.5 Review of security procedures

The following sections cover the follow-up steps after the restoration of systems and data. These include conducting a thorough analysis of what happened, why the incident occurred, and updating security measures. This involves incorporating the results of the analysis into the revision of security policies, procedures and, where necessary, other tool configurations, in order to enhance the organisation's resilience against future threats.

13.4.6 Testing and training

Two activities in particular have a preventive effect and mitigate the impact of security incidents: recovery and response testing, and staff training. Regular testing of disaster recovery and incident response plans ensures that procedures are effective and that staff are properly prepared. Training staff on security threats and best practices serves to minimise risks and ensure an effective response to incidents.

13.5 Analysis and recovery

Analysis and recovery following an incident is the final phase of the security incident response process. This phase focuses on a detailed evaluation of the incident, identifying its causes, restoring normal operations, and implementing measures to prevent future incidents.

13.5.1 Detailed analysis and incident report

The team now has the time and resources to examine the incident in greater detail and reconsider whether any aspects of the incident were overlooked during the resolution process. This is aided by:

- Forensic analysis: Forensic analysis provides an in-depth understanding of how the incident occurred, which systems were affected, and the method of attack. The analysis helps to identify vulnerabilities and the causes of the incident.

- Summary of events: This is a chronological record of the events that occurred and the responses of the teams involved during the incident.
- Documentation of findings: The team compiles a detailed incident report, including a description of the incident, analysis, response, impact on the organisation, and recommendations for future prevention.
- Sharing with key stakeholders (company management, security teams and, where applicable, external regulators or interested parties) promotes awareness within the organisation and strengthens trust in the organisation.

13.5.2 Improving security measures

Following any critical security incident, the organisation should consider enhancing the resilience of its systems. This can be achieved by strengthening the protection of critical systems and data through better security tools, encryption and authentication processes.

13.5.3 Reviewing and testing incident response plans

The final tasks that will improve future immediate response to security incidents involve reviewing response plans and updating regular training and exercises. More specifically:

- Review of response plans: Based on experience and lessons learnt from the incident, incident response plans and disaster recovery processes are reviewed and updated.
- Regular training and exercises: Organising regular training sessions and simulation exercises for staff and response teams helps to keep procedures and plans up to date.

13.5.4 Feedback and continuous improvement

From the perspective of analysing and recovering from a security incident, there is one final step ahead of us, and that is working on feedback and further improvement. Regularly evaluating the effectiveness of implemented security measures, adapting them, and fostering an environment in which staff and management can provide feedback on security procedures and incident response are the tasks that prevent stagnation in the process of defending against security incidents.

13.6 Improvement and prevention

We have previously discussed how updating and adjusting security measures, along with other follow-up activities immediately after recovering from an incident, contribute **to improving responses and preventing further security incidents**. To avoid repetition, we would like to highlight three activities that must have the support of the organisation's management and which provide the internal team with the assurance that security threats are not sidelined within the organisation and that the team's work is regarded as important. These are investment in security technologies and resources, collaboration and information sharing, and, last but not least, the implementation of regular security audits

Organisations should strengthen their technological capabilities, i.e. invest in the latest security technologies and tools, such as advanced intrusion detection and prevention systems, data encryption and multi-factor authentication. Organisations must develop security systems and measures with sufficient resources, i.e. possess and allocate sufficient financial and human resources to support security initiatives and response activities.

Participation in communities and engagement in partnerships for sharing information on cyber threats can help an organisation identify and respond to new threats in a timely manner.

13.7 Compliance with legal and regulatory requirements

The final element of the security incident response system, which we will now examine in more detail, **is the managed compliance with legal and regulatory requirements**. All steps taken before, during and after an incident must comply with the relevant legal and regulatory requirements; on the one hand, this involves measures to protect personal data, trade secrets and other sensitive information, as well as compliance with specific industry and national security standards; on the other hand, it presents the organisation in a better light, at the very least as trustworthy and reliable.

By proactively incorporating legal requirements into its plans and procedures, an organisation minimises legal risks and improves its ability to protect sensitive information and maintain the trust of stakeholders.

13.7.1 Understanding applicable regulations

Understanding applicable regulations is a key prerequisite for compliance. Identifying only those that are relevant and monitoring them on an ongoing basis ensures that the organisation is aware of its legal boundaries in its external communications:

- Identifying relevant regulations, i.e. determining which legal and regulatory requirements apply to the organisation, including the GDPR and other specific industry standards.

- Ongoing monitoring of changes involves tracking changes in legal and regulatory requirements that could affect the organisation's incident response procedures.

13.7.2 Incorporating legal requirements into response plans

Applicable regulations must be incorporated into the relevant documents, both within the organisation and in written agreements with third parties. Security policies and incident response procedures must therefore include the steps necessary to comply with legal and regulatory requirements, just as contracts with suppliers and partners must incorporate clauses on data security and regulatory compliance.

13.7.3 Responsibility for incident reporting and ensuring protection

Under applicable regulations, and in particular the provisions concerning obligations and penalty clauses, responsible persons must be designated to ensure the timely reporting of incidents to the relevant regulatory authorities and affected parties, as required by the relevant legislation. To ensure compliance with legal requirements, it is essential to develop a strategy for communicating with affected parties, including customers and the public.

Ensuring the protection of personal data entails the need to implement data protection measures, such as encryption and a 'data minimisation' policy when processing personal data, and to set up processes so that responsible persons provide an adequate service in accordance with the requirements of data subjects, such as access to data, rectification or erasure.

13.7.4 Review and audit

Conducting regular audits of security and response plans will further support internal efforts to comply with current legal and regulatory requirements. The review typically includes checking for the existence of documentation and detailed records of security incidents, responses and decisions. This will facilitate compliance reviews and serve as evidence in the event of a legal investigation by auditors or other independent bodies.

13.7.5 Training and awareness

It is recommended that all employees, particularly those involved in the processing of personal and sensitive data, receive regular training on the legal and regulatory requirements relating to data protection and incident response.

14 Assessing potential threats to data backup and recovery in 5G networks

When assessing potential threats to data backup and recovery in 5G networks, it is important to focus on several key aspects that may be vulnerable or pose security risks. 5G networks offer advanced technologies and high data transfer speeds.

14.1 Network infrastructure security

The 5G network infrastructure is complex and extensive, operating not only traditional large base stations but also a large number of small cells located in various places, such as street lighting columns, buildings and other structures. This expansion increases the network's exposure to potential attacks.

Security must take this complexity into account and must not overlook or rely on outdated methods to ensure the required level of security, nor underestimate the security resources allocated.

The assessment of threats to data backup and recovery is subject to physical security, cybersecurity, and specific segmentation and isolation techniques in 5G networks.

14.1.1 Physical security

Physical security tasks consist of:

- Protecting small cells and other equipment: Ensuring that small cells and other critical infrastructure are physically protected against unauthorised access, vandalism or sabotage.
- Monitoring and response: Implementing systems to monitor physical access and respond rapidly to any security breaches.

14.1.2 Cybersecurity

Current objectives for implementing cybersecurity for data backup and recovery focus on:

- Securing network transmission – i.e. using advanced encryption techniques to protect data transmitted between small cells and the network core against eavesdropping and tampering.
- Protection against DDoS attacks – in particular, by implementing solutions to detect and mitigate distributed denial-of-service (DDoS) attacks that could target the network infrastructure and disrupt its operation.
- Vulnerability updates and management – to address vulnerabilities, regular software and firmware updates are deployed across network devices to ensure the infrastructure is protected by the latest security patches.

14.1.3 Segmentation and isolation

As with the security incident response process, segmentation and isolation must be designed for backup and recovery elements and technologies. This is achieved through:

- Network slicing: The use of network slicing to isolate different types of traffic and services within a 5G network, thereby limiting the spread of potential attacks and simplifying security management.
- Access and identity management: The use of advanced identity and access management systems to restrict access to network resources to authorised users and devices only.

14.1.4 Incident detection and response

Backup and recovery systems can also be targets of attack. The same applies to them as to other elements, devices and systems of 5G networks, i.e. they must be monitored and subjected to security analysis, and these components must be included in the incident response plan.

14.2 Edge computing

Edge computing in the context of 5G networks highlights important aspects of data backup and recovery. Implementing robust data backup and recovery solutions on edge devices ensures that critical data will not be lost even in the event of physical damage or cyber attacks.

Edge computing brings data processing and computational tasks closer to where they are generated, i.e. to the network edge, which can bring significant benefits in the form of lower latency and reduced load on central data centres. However, this distribution also presents **specific security challenges**.

14.2.1 Expansion of entry points and attack vectors

Edge servers are often located in less secure and harder-to-access locations, which increases the risk of physical attacks, theft or damage.

Furthermore, a larger number of edge devices means more points that need to be protected against cyberattacks, including malware, ransomware and distributed denial-of-service (DDoS) attacks.

14.2.2 Management and configuration

Given the large number of edge devices, automation is essential for the effective management of security policies, updates and configurations. Similarly, maintaining a consistent level of security across all edge devices and servers is challenging but essential for protecting the entire network.

14.2.3 Authentication and access

For edge computing in the context of 5G networks, the rule of reliable authentication and controlled access applies with even greater urgency. Security can be ensured through:

- Robust authentication: Ensuring that all communications and access to edge devices are properly authenticated is essential for preventing unauthorised access.
- Identity management: Effective and reliable management of identities and access rights for users and devices communicating with edge servers plays a significant role in network security.

14.2.4 Data and its protection

Data stored on edge devices, as well as data transferred between edge devices and the central data centre, must always be encrypted to ensure secure transmission.

14.2.5 Monitoring and detection

The monitoring and detection of edge devices must meet high security standards so that data backup and recovery are not compromised. This requires the use of advanced monitoring technology capable of continuously monitoring and analysing traffic on edge devices, thereby helping to detect potential security threats and anomalies in a timely manner.

A rapid and effective response to security incidents, including the isolation of affected devices, is a critical factor in terms of data recovery within the edge computing environment.

14.2.6 Compatibility and integration

Edge computing should be designed and implemented with a view to integration with the organisation’s existing security systems and policies, and security solutions must be flexible and capable of adapting to the new technologies and standards that edge computing brings.

14.3 Spectrum sharing and network slicing

Spectrum sharing and network slicing are regarded as two key concepts of 5G technology, offering significant benefits in terms of efficiency and service personalisation.

14.3.1 Spectrum sharing

Spectrum sharing allows different operators or services to use the same portion of the radio spectrum, maximising the efficiency of its utilisation. However, this approach requires advanced management and coordination to prevent collisions or interference between services that could impact the integrity and availability of communications.

For the purposes of backup and recovery, it is necessary to implement sophisticated methods for detecting and preventing unauthorised use of the spectrum, including spectrum monitoring and automatic conflict resolution.

14.3.2 Network slicing

Network slicing enables the creation of virtually isolated networks on the same physical infrastructure. Each slice is optimised for a specific type of service or set of requirements, allowing operators to allocate network resources flexibly and efficiently

Ensuring strict isolation between individual networks is key to protecting data and services within each slice, thereby minimising risks to data backup and recovery. Conversely, any failure in isolation can lead to data leaks or cross-boundary attacks.

Each slice may have different security and operational requirements, which necessitates a comprehensive policy management and enforcement system capable of handling the diversity and dynamics of the 5G environment.

In a multi-slice environment, there is a higher risk of targeted attacks on specific services and, consequently, greater demands on backup systems and the recovery process. It is essential to have advanced threat detection systems that can identify and isolate attacks specific to individual slices, whilst minimising the impact on other services.

14.3.3 Solutions and strategies

In the field of spectrum sharing/network slicing, **the following** solutions and strategies are implemented to prevent and minimise threats to backups and data recovery:

- Advanced encryption and authentication: Securing data and communications between slices and within the shared spectrum requires strong encryption and robust authentication mechanisms.
- Dynamic spectrum management: The use of advanced algorithms for dynamic spectrum management and allocation can help minimise the risk of interference and unauthorised access.
- Flexible security policies: The creation and flexible management of security policies will enable a rapid response to changing requirements and threats in the dynamic environment of 5G networks.
- Real-time monitoring and analysis: Continuous real-time monitoring and analysis of traffic enables rapid detection and resolution of security incidents.

Spectrum sharing and network slicing in 5G networks enable operators and users to harness the full potential of 5G technology without being exposed to unacceptable risks to data backup and recovery.

14.4 Authentication and encryption

Authentication and encryption in the context of 5G networks highlight critical areas where advanced security methods play a key role in enhancing security and data protection. 5G technology brings innovations that require a review and strengthening of existing security protocols, particularly in the areas of authentication and encryption.

14.4.1 Strengthening authentication

In 5G networks, authentication is essential for verifying the identities of users, devices and network services. Advanced authentication mechanisms ensure that communications and access to data are protected against unauthorised attempts. **In 5G networks, this is achieved primarily through:**

- Multi-factor authentication (MFA), i.e. a combination of several independent factors to enhance security when accessing network services.

- Unified Identity Management (UIM): Centralised identity management ensures consistent and secure authentication across various services and applications within the 5G ecosystem.

- Authentication and Key Agreement (AKA): Protocols for secure authentication and the exchange of encryption keys between users and the network, which are resistant to various attacks, including eavesdropping and spoofing.

14.4.2 Strengthening encryption

Encryption plays a vital role in protecting the integrity and privacy of data transmitted or stored on 5G networks. Thanks to advanced encryption algorithms, information can be protected against unauthorised access, tampering and eavesdropping. **The following are used:**

- End-to-end encryption (E2EE): Ensures that data is encrypted on the source device and decrypted only on the destination device, preventing eavesdropping during transmission over the network.

- Network-layer encryption: Provides an additional level of protection for data in transit, ensuring that all data transmitted between devices and the network infrastructure is protected.

- Dynamic encryption key management: The use of protocols for the dynamic exchange and renewal of encryption keys enhances security by preventing the long-term use of a single key that could be compromised.

14.4.3 Solutions and strategies

Although advanced authentication and encryption methods provide a strong foundation for 5G network security, the following solutions must be implemented or strategies applied to ensure data backup and recovery:

- Key and identity management: Effective and secure management of encryption keys and identities requires a robust infrastructure and policies capable of handling the large number of devices in 5G networks.

- Performance vs. security: Ensuring high performance whilst maintaining strong encryption and authentication is a challenge, particularly in environments with high latency and throughput requirements.

- Standardisation and compatibility: The development and implementation of globally accepted security standards is key to interoperability and security across different operators and devices in the global scale of 5G networks.

14.5 Manufacturer-specific risks

Dependencies on technologies and devices from specific manufacturers in the world of 5G networks also pose a major problem in terms of threats to data backup and recovery. These threats stem both from the very existence of the supply chain itself and from varying levels of standardisation and interoperability.

Supply chain risks can be characterised as follows:

- Dependence on a limited number of suppliers for key components of 5G infrastructure increases the risk that problems with a single supplier, such as security flaws or production outages, could have a serious impact on the entire network.

- There is concern that equipment and software from certain manufacturers may contain backdoors or other vulnerabilities that could be exploited for espionage, sabotage or other malicious activities.

From the perspective of non-compliance with standardisation and a lack of interoperability, the following risks must be considered:

- Different manufacturers may implement 5G standards in different ways, which can lead to interoperability issues between devices and systems from different manufacturers.

- Different manufacturers' approaches to software and hardware updates may affect the security and long-term sustainability of devices on the network.

14.5.1 Solutions and strategies

Extending the measures applied at the technology level will similarly serve their purpose within the supply chain. When mitigating risks, a 5G network operator has the option to select or apply solutions from the list below:

1. Diversifying suppliers and manufacturers can reduce the risks associated with over-reliance on a single supplier and increase network resilience.

2. Supporting and using open standards and protocols can improve interoperability between devices from different manufacturers and reduce dependence on proprietary solutions.

3. Independent security auditing and certification of devices and software can help identify and eliminate potential vulnerabilities or backdoors.

4. Implementing systems for continuous monitoring of the security status of devices and regular updates of device software and firmware to address known vulnerabilities.

Another, and not often mentioned, strategy is for the organisation to engage in supporting innovation and competitiveness. If the organisation dedicates resources to supporting start-ups and innovation, this can lead to greater diversification and resilience within the supply chain. Another area where it is worth monitoring the situation or investing resources is research and development. Investment in the research and development of new technologies and security solutions can engage the organisation in a community that will provide it with cutting-edge and highly innovative solutions.

14.6 Data speed and volume

The risks associated with the speed and volume of data in 5G networks, which may affect the ability to monitor and analyse traffic to ensure security, are very significant. Fifth-generation mobile networks deliver unprecedented speeds and capacities, enabling support for new applications and services, from the Internet of Things (IoT) to virtual and augmented reality. However, these innovations also bring new challenges in the areas of security and privacy.

14.6.1 Increased data volumes

The enormous volume of data generated and transmitted in 5G networks requires advanced technologies for real-time processing and analysis, which is essential for identifying potential security threats.

14.6.2 Data transfer speeds

High data transmission speeds can make it difficult to identify and respond to security threats in a timely manner, particularly when traditional security mechanisms may not be fast enough.

14.6.3 Use of artificial intelligence and machine learning

Automated data analysis can provide an advantage by utilising AI and machine learning for automated pattern and anomaly detection in the massive volumes of data produced in 5G networks, but requires careful design and ongoing monitoring of these tools.

Artificial intelligence can enhance processes involving fast and massive volumes of data by implementing AI-based predictive security systems that can forecast potential threats and vulnerabilities based on the analysis of trends and behaviour within the network.

14.6.4 Advanced encryption and security protocols

The use of advanced encryption techniques and security protocols that can operate effectively even in environments with high data speeds and large volumes is key to eliminating data threats.

14.6.5 Distributed security architectures

The implementation of NFV and SDN can provide more flexible and dynamic management of network resources and security policies, enabling faster adaptation to changing situations related to data transmission and associated threats. Furthermore, processing data closer to its source can reduce latency and the load on central systems, and from the perspective of data backup and recovery, it creates scope for the targeted use of edge computing (at the point of data generation).

14.6.6 Updates

Finally, ensuring that all systems and applications are regularly updated contributes to the overall security management and incident response system, whilst significantly reducing threats to the data itself or its backup and recovery.

15 Overview of Open RAN and Open Core support in other technologically advanced countries

When considering the use of Open RAN and Open Core equipment in technologically advanced countries, it is important first to understand the basic principles and motivations behind this trend in telecommunications. **Open RAN and Open Core are initiatives aimed at increasing interoperability and openness in network architectures, which enhances their competitiveness and supports innovation and flexibility in the construction and operation of telecommunications networks.**

The transition to Open RAN and Open Core architectures represents a fundamental transformation in the telecommunications industry. This approach is based on the idea that open, standardised interfaces and protocols will enable telecommunications operators to more easily integrate and utilise equipment and services from different manufacturers. The main motivation behind this transformation is to strengthen competitiveness, increase the efficiency of developing and deploying new technologies such as 5G and future networks, whilst reducing dependence on individual suppliers. This opens up opportunities for new market players, fosters innovation and ensures that networks are better able to adapt to changing requirements and technologies. **This initiative also presents challenges, including ensuring security, reliability and compatibility within a more diverse and dynamic ecosystem**. To ensure the successful implementation of these principles, cooperation between government bodies, telecoms operators, equipment manufacturers and the academic sector is key to promoting open standards, ensuring interoperability and addressing security risks.

15.1 Openness and interoperability

Openness and interoperability in the context of Open RAN and Open Core are the cornerstones upon which these initiatives are built. These principles not only support technological progress and innovation in the telecommunications industry, but also deliver wider economic and social benefits.

15.1.1 Openness

Openness refers to the use of open standards and specifications that are publicly available and promote broad collaboration between various industry players. This enables telecommunications operators and suppliers to develop and offer products and services that are interoperable, regardless of who manufactured them. Openness means transparency in the development and standardisation process, which leads to greater trust between users and providers.

15.1.2 Interoperability

Interoperability is the ability of different systems, devices, applications or services to work together and effectively exchange and utilise information without the need for major changes or specific adaptations. In an Open RAN and Open Core environment, this means that equipment and software components from different manufacturers can work reliably together within a single network, enabling operators to flexibly combine and compare different technological solutions to achieve optimal performance and efficiency.

15.1.3 The rationale behind openness and interoperability

Although the main elements of the motivation are evident from the text above, we can summarise them as follows:

- Increased competition: Opening up markets to new suppliers reduces dependence on individual large suppliers and promotes competitiveness, leading to better prices and innovative solutions.

- Innovation potential: It lowers barriers to entry for new players and enables faster adoption of new technologies, which helps accelerate the development and deployment of innovative services and applications.

- Network flexibility and resilience: It enables operators to flexibly adapt and expand their networks according to current needs and demand, whilst ensuring a high level of resilience and reliability.

- Global standardisation: Support for open standards contributes to the harmonisation of technical solutions at an international level, facilitating global cooperation and the development of telecommunications infrastructure.

Openness and interoperability drive the construction of resilient, flexible and innovative telecommunications networks, ready to meet the challenges of the future in terms of required speeds and data volumes.

15.2 Flexibility and innovation

Flexibility and innovation are key principles driving the adoption and development of Open RAN and Open Core technologies in the telecommunications industry. These principles not only enable rapid adaptation to changing technological and market requirements, but also support the creation and implementation of new services and features that respond to user needs.

As a result of this flexibility, networks with the following characteristics are emerging:

- Modular and scalable architectures: Open RAN and Open Core offer a modular approach to network construction, where different components can be developed, tested and deployed independently of one another. This makes it easier for operators to upgrade or adapt their networks to new technologies and standards without the need for a complete overhaul of the existing infrastructure.

- Architectures that adapt quickly to market changes: Flexible architectures facilitate the rapid deployment of new technologies and services, enabling operators to respond better to changing market demands and user preferences.

Innovation is driven by networks whose key characteristics include:

- Support for the development of new services: Open and interoperable platforms provide an ideal foundation for innovation, enabling developers and businesses to experiment with new applications and services such as IoT (Internet of Things), edge computing, virtual and augmented reality, which require high throughput, low latency and high reliability.

- Increased competitive dynamics: Access to common open standards and interfaces lowers barriers to entry for new market players and fosters greater competition. This stimulates innovation, as companies strive to differentiate their products and services to better meet customer needs.

15.2.1 The motivation behind flexibility and innovation

The reasons why flexibility and innovation in 5G networks work are primarily economic. Network flexibility and modularity can significantly reduce capital and operational costs (CAPEX and OPEX) by enabling more efficient use of resources and easier technology upgrades.

Linked to economic efficiency is the ability to deploy new services and features quickly and effectively. This can improve the user experience and increase user satisfaction and loyalty.

A flexible and innovative infrastructure is key to supporting future technologies, such as 6G and other advanced digital services, which will require even higher levels of adaptability and performance.

15.3 Competition and cost reduction

Competition and cost reduction are driving the adoption of Open RAN and Open Core technologies and are of key importance for the transformation of the telecommunications industry. These principles not only help to create a healthy and dynamic market environment, but also bring significant economic benefits for both operators and end-users.

15.3.1 Competition

Open RAN and Open Core expand opportunities for new suppliers to enter the market for telecommunications equipment and services. This increases competition among suppliers and leads to further innovation, better service quality and lower prices. Competition encourages suppliers to create unique and innovative solutions to differentiate themselves from the competition. This provides operators and end-users with a wider choice and access to advanced technologies.

Increased competition also contributes to market dynamism and stimulates the growth and development of the entire sector, which is in the interests of all stakeholders.

15.3.2 Cost reduction

With a wider range of suppliers and solutions to choose from, operators can optimise their investments and achieve greater efficiency in building and operating their networks.

The fall in equipment and service prices reduces both capital expenditure (CAPEX) and operating expenditure (OPEX), and this is reflected in the overall pricing structure of services for end-users.

Network flexibility and scalability also influence operators' behaviour, enabling them to respond to changing demand and market needs with different resources without the need for extensive investment in new infrastructure.

15.3.3 The drive for competition and cost reduction

Competition is a driving force for innovation, which helps the growth and development of the telecommunications industry, benefiting all stakeholders.

At the same time, cost reduction and greater competitiveness can lead to wider availability of telecommunications services, enabling a larger number of users to benefit from advanced digital technologies.

Competition and cost reduction will therefore ensure wider availability and accessibility of services, and support an innovation ecosystem that responds to the needs of the market and society.

15.4 The European Union

The European Union (EU) is a significant example of an organisation that actively supports the development and adoption of Open RAN and Open Core technologies as part of a broader strategy for digitalisation and ensuring technological sovereignty. The EU emphasises innovation, security, competitiveness and sustainability in the telecommunications sector.

The European Union supports research, establishes a regulatory framework and focuses on promoting innovation and the ecosystem. Examples of individual measures and activities are listed below.

15.4.1 Research funding and support

- Funding programmes: The EU provides significant funding for research and development in the telecommunications sector through various programmes, such as Horizon 2020 and its successor, Horizon Europe. These programmes support projects focused on innovation in Open RAN, cybersecurity, cloud computing and other key areas.

- 5G Public Private Partnership (5G PPP): This partnership between the EU and the telecommunications industry supports research, development and the deployment of 5G networks, including projects related to Open RAN. The aim is to strengthen European leadership in 5G technologies and pave the way for future generations of networks.

15.4.2 Regulatory framework and standardisation

- Support for open standards: The EU actively supports the development and adoption of international standards that are key to interoperability and security in Open RAN networks. It relies on close cooperation with international standardisation organisations and support for European companies in these processes.

- Security initiatives: Security is a key priority for the EU, which is why initiatives such as the Cybersecurity Act have been introduced, establishing a framework to ensure the security of networks and information systems, including those based on Open RAN.

15.4.3 Support for innovation and the ecosystem

- Innovation hubs and collaboration: The EU supports the creation of innovation centres and networks of excellence that connect universities, research institutions, start-ups and industry partners. The aim is to stimulate the development and commercialisation of new technologies in the field of Open RAN.

- Green agenda and sustainability: The EU is integrating sustainability principles into its support for telecommunications technologies, including Open RAN, as part of a broader effort to achieve climate neutrality by 2050. Open RAN technologies can contribute to more efficient use of energy resources and a reduction in CO2 emissions.

15.4.4 International cooperation

The EU is seeking to cooperate with international partners in promoting open technologies and standards, which includes dialogue and partnerships with other regions and countries to support global interoperability and the security of telecommunications networks.

The European Union therefore takes a comprehensive approach to supporting Open RAN and Open Core technologies, with an emphasis on innovation, security, sustainability and international cooperation. In doing so, the EU aims to strengthen its technological sovereignty and competitiveness, ensure secure and sustainable telecommunications networks, and support economic growth and social development.

15.5 United States

The **United States** is another example of how a technologically advanced country approaches the adoption and support of Open RAN and Open Core technologies. This approach forms part of the country's broader strategy to enhance national security, strengthen the domestic telecommunications industry and promote global competitiveness.

Support in the US involves boosting investment, stimulating industrial development and, as a global leader, establishing a regulatory framework. Examples of specific measures and activities are listed below.

15.5.1 Support at federal level and investment

- Strategic funding: The US government and federal agencies, such as the Federal Communications Commission (FCC), recognise the importance of open and interoperable networks for the country's future competitiveness and security. Funding and grant programmes have been introduced to support the research, development and deployment of Open RAN technologies.
    - Broadband Technology Opportunities Program (BTOP): This programme, administered by the National Telecommunications and Information Administration (NTIA), provides funding for projects that improve access to broadband internet, including support for the implementation of Open RAN technologies, which can enhance competitiveness and innovation in network development.
    - 5G Experimentation and Test Beds: The US Department of Defence funds research and development of 5G technologies, including Open RAN, by establishing test laboratories and experimental environments where new technologies can be tested under secure and controlled conditions.
    - Trusted Capital Marketplace: The DoD is also collaborating with the private sector to secure safe and reliable sources of capital for start-ups and companies working on critical technologies, including Open RAN, which helps protect US technological infrastructure from foreign influence.
    - Future of Networks Initiative: The NSF provides grants for research into advanced network technologies, including projects focused on the development of Open RAN. These projects often involve collaborative research between universities, industry and government laboratories.
    - Partnerships for Innovation: An NSF programme that supports the transformation of knowledge from academic research into socially beneficial applications, including the commercial use of Open RAN technologies.

- Due to concerns about security risks associated with the use of equipment from suppliers in certain countries, the US has focused on supporting and implementing Open RAN as a means of diversifying the supply chain and reducing dependence on foreign technologies.

15.5.2 Support for innovation and industrial development

- Innovation ecosystem: The US supports the development of a domestic Open RAN ecosystem, which includes start-ups, academic institutions and existing telecommunications companies. The aim is to accelerate innovation and the commercialisation of new solutions in the field of wireless networks.

- Collaboration with industry: The US government and industry groups, such as the Open RAN Policy Coalition, are working to promote policies and initiatives that facilitate collaboration between the private sector and government institutions. This collaboration includes sharing best practices, standardisation and the creation of joint research programmes.

15.5.3 Global leadership and standardisation

- Leadership in international standardisation: The US plays an active role in international standardisation organisations, such as 3GPP, with the aim of promoting the global adoption of open standards and technologies. US companies and institutions are often at the forefront of developing new standards that enable network interoperability and security.

- International cooperation: The United States is also working to collaborate with international partners and allies to support the global adoption and harmonisation of Open RAN standards. This includes bilateral and multilateral agreements focused on joint research, development and deployment of open telecommunications technologies.

The US approach to Open RAN and Open Core encompasses a wide range of initiatives, from federal support and innovation ecosystems to international cooperation and standardisation. This approach aims to ensure that open telecommunications technologies play a key role in the country's future security, economic growth and technological sovereignty.

15.6 Japan and South Korea

Japan and South Korea are leading examples of countries committed to the development and deployment of Open RAN and Open Core technologies, which form part of their national strategies for 5G and future generations of telecommunications networks. These countries take a strategic approach to innovation in the telecommunications sector, with the aim of strengthening their global competitiveness and security.

15.6.1 Japan

Support for 5G networks in Japan is driven by strategic government initiatives, taking place through collaboration with industry and in the field of standardisation. Examples of specific forms of support are listed below.

- Strategic government initiatives: The Japanese government supports research and development in the field of Open RAN through various initiatives and grants, with the aim of accelerating the adoption of this technology and supporting domestic industry. This involves investment in pilot projects and demonstration tests of 5G networks based on Open RAN.

- Cooperation with industry: Japan focuses on fostering collaboration between the government, telecommunications operators and equipment manufacturers. Major players such as NTT Docomo, Rakuten Mobile and others are actively involved in the deployment and development of Open RAN networks, thereby contributing to innovation and the competitiveness of the Japanese telecommunications sector.

- Support for domestic and international standardisation: Japan plays an active role in international standardisation organisations and strives to promote global harmonisation and interoperability of Open RAN technologies. Standardisation takes the form of collaboration within consortia and working groups focused on the development of open standards.

15.6.2 South Korea

South Korea's approach to supporting Open RAN and Open Core technologies is being implemented not only through increased government-level activities but also via leading operators. Examples of specific initiatives to drive the development of 5G networks are set out below:

- Government investment in 5G and future technologies: South Korea is known for its rapid deployment of 5G networks, and the government is actively investing in research and development of next-generation technologies, including Open RAN. These investments form part of a broader strategy to strengthen the country's technological leadership.

- Leading operators and the innovation ecosystem: Korean operators such as SK Telecom, KT Corporation and LG Uplus are at the forefront of utilising Open RAN technologies to innovate their networks. They collaborate with both domestic and international suppliers and contribute to the rapid development and commercialisation of new services and applications.

- Commitment to global cooperation: South Korea actively promotes international cooperation and technology exchange, which includes participation in global innovation networks and standardisation bodies. In this way, it seeks to support the global adoption and development of Open RAN as a key industry standard.

Japan and South Korea share several key elements in their approaches to Open RAN and Open Core:

- Innovation Leaders: Both countries focus on supporting innovation and technological development in their telecommunications sectors as a means of ensuring global competitiveness and economic growth.

- Support for Domestic Industry: There is a strong emphasis on supporting domestic companies and the start-up ecosystem through investment, research and development, which helps to strengthen the local industrial base and create jobs.

- International cooperation and standardisation: Both countries are active in international forums and standardisation bodies, which promotes global interoperability and security of Open RAN technologies.

In this way, Japan and South Korea are contributing to the rapid development and adoption of Open RAN and Open Core technologies, which is helping to shape the future of global telecommunications networks.

15.7 Support for research and development (R&D)

Support for research and development (R&D) in the field of Open RAN and Open Core accelerates innovation, ensures competitiveness and safeguards the telecommunications sector. For countries seeking to harness the potential of these open technologies, support for R&D is indispensable.

Through strategic investment and collaboration, it is possible to accelerate the development and deployment of the open, interoperable and secure networks of the future.

How can we encourage research and development activities in the areas of Open RAN and Open Core and ensure that R&D results are applicable to domestic industry? The experiences of advanced economies and the individual steps of applicable R&D are described in the following paragraphs.

15.7.1 Setting research priorities

Research is often uncoordinated and fragmented into individual tasks. If R&D is to lead to applicable development and research, its priorities must be set. Governments and regulatory bodies should identify and define key areas for research and development. They know which areas are critical to national interests and industrial development, such as cybersecurity, scalability, energy efficiency and integration with advanced applications (e.g. IoT, AI).

A key aspect of setting priorities is focusing on innovation; in other words, the list of projects should include those that focus on innovative solutions and overcoming technical challenges in the areas of Open RAN and Open Core, with the potential for commercial application and enhanced competitiveness.

15.7.2 Financial and material support

Resources are the factors that translate ideas into reality. They can be provided in the form of grants, subsidies or other forms of funding for research institutions, universities and industrial partners.

It is worth noting that researchers and developers work with high-quality research equipment and require the environment and data necessary for experimenting with and testing new technologies.

15.7.3 Cooperation and partnerships

Encouraging collaboration between the academic sector, industry and government agencies (by creating consortia or innovation clusters focused on specific research topics) leads to the sharing of knowledge, resources and best practices. Supporting international research partnerships and exchange programmes for researchers also helps to integrate global perspectives and expertise into local research and development.

15.7.4 Education and talent development

The final elements of support for research and development are investments in education. Support for educational programmes and courses focused on teaching the skills and knowledge required to work with Open RAN and Open Core technologies, including the provision of scholarships and internships for students and young researchers, will attract new talent to the sector with fresh approaches and flexibility in embracing new ideas and research findings.

The development of the professional skills and knowledge of the existing workforce in the telecommunications industry is a significant factor in the adoption of R&D results, as it prepares employees for the transition to new technologies and working methods.

15.8 Regulatory and standards support

Regulatory and standardisation support plays a key role in facilitating the adoption and development of Open RAN and Open Core technologies. The approach to regulation and standards should be balanced to support innovation, ensure security and privacy, whilst allowing flexibility for rapid adaptation to new technologies.

15.8.1 Establishing transparent regulations

It is important for regulatory authorities to create a clear, predictable and transparent regulatory environment. Regulation involves defining standards for interoperability, security, data protection and other key aspects related to Open RAN and Open Core technologies.

Regulatory bodies should support the development and adoption of open standards that facilitate interoperability and ensure broader compatibility between different systems and devices.

15.8.2 Ensuring security and privacy

Regulatory authorities should collaborate with industry and academia on the development and implementation of security standards and rules for Open RAN and Open Core networks, ensuring that standards are not merely restrictive or the embodiment of concerns, and do not hinder innovation or flexibility.

It is also important to incorporate measures that ensure new technologies respect user privacy and comply with data protection legislation, such as the GDPR in the European Union.

15.8.3 Support for innovation and experimentation

Regulatory authorities should provide mechanisms and support activities, such as temporary test licences, that enable developers and operators to experiment with new technologies in real-world conditions without having to fully comply with all regulatory requirements.

Allowing a degree of flexibility within the regulatory framework can foster innovation by enabling the industry to respond more quickly to technological developments and changing market conditions.

15.8.4 Promoting international cooperation

Active participation in international forums and standardisation organisations is key to achieving global harmonisation of technical standards. This reduces technical barriers to international trade, which in turn supports global interoperability.

International cooperation is also important for sharing best practices, knowledge and information on threats and vulnerabilities, which strengthens the overall resilience of telecommunications networks against cyber attacks.

15.9 Cooperation between stakeholders

Cooperation between various stakeholders leads to the success and development of Open RAN and Open Core technologies. Cooperation takes place at many levels and between various entities, including governments, telecommunications operators, equipment manufacturers, research institutions and the academic sector.

15.9.1 Establishing multi-sector partnerships

Establishing or supporting industry consortia and alliances that bring together various stakeholders to participate in joint research, development and standardisation of Open RAN and Open Core technologies can promote the sharing of knowledge, experience and best practices globally. Governments should facilitate this dialogue and cooperation.

15.9.2 Supporting innovation ecosystems

The emergence of innovation hubs, incubators and accelerators creates an environment for start-ups and small and medium-sized enterprises (SMEs) focused on developing Open RAN and Open Core solutions. They offer them mentoring, access to a network of potential partners and customers, or can provide financial or other material support.

Strengthening cooperation between academic institutions and industry for joint research and development, including joint projects, facilitates the sharing of equipment and the implementation of exchange programmes for students and researchers.

15.10 Security and trust

Security and trust are the cornerstones of the successful implementation and widespread adoption of Open RAN and Open Core technologies. Given the growing cyber threats and society's increasing reliance on digital communications, it is essential that these technologies are secure and trustworthy.

15.10.1 Security by design

Security should be integrated into all phases of the product development cycle, from design through development, testing and deployment, right through to maintenance. This approach ensures that security is not an afterthought, but an integral part of the product.

Security verification is carried out through the implementation of ongoing security assessment processes and penetration testing, helping to identify and rectify security configurations before a security incident occurs.

15.10.2 Building trust and transparency

Building trust and transparency is based on the use of proven techniques. In addition to references, valid certifications and accreditations can serve as indicators of transparent conditions. Whilst certification and accreditation programmes for verifying security features and compliance with standards strengthen trust in Open RAN and Open Core products and solutions, open standards and protocols are increasingly applied in operation and enable independent verification and auditing of product security features. This increases the confidence of users and operators in the technologies being used.

15.10.3 Strengthening cyber resilience

Support for platforms and initiatives to share information on cyber threats and vulnerabilities among operators, manufacturers and government agencies helps to create a coordinated defence against cyber attacks.

15.10.4 Education and training

Security and trust are not insignificant for all stakeholders, including employees, management and end users. Their education and training ensure that organisations have not only qualified experts to manage and protect their networks, but also staff who trust the product and strive to improve it.