big data and cognitive computing

MDPI

Article

Assessment of Security KPIs for 5G Network Slices for Special Groups of Subscribers

Roman Odarchenko [1], Maksim Iavich [2], Giorgi Iashvili [2], Solomiia Fedushko [3,4,*] and Yuriy Syerov [3,4]

[1] Department of Telecommunication and Radioelectronic Systems, National Aviation University, 03058 Kyiv, Ukraine; odarchenko.r.s@ukr.net
[2] Department of Computer Science, Caucasus University, 0102 Tbilisi, Georgia; miavich@cu.edu.ge (M.I.); giiashvili@cu.edu.ge (G.I.)
[3] Department of Social Communication and Information Activity, Lviv Polytechnic National University, 79000 Lviv, Ukraine; yurii.o.sierov@lpnu.ua
[4] Department of Information Systems, Faculty of Management, Comenius University in Bratislava, 820 05 Bratislava, Slovakia
* Correspondence: solomiia.s.fedushko@lpnu.ua

Abstract: It is clear that 5G networks have already become integral to our present. However, a significant issue lies in the fact that current 5G communication systems are incapable of fully ensuring the required quality of service and the security of transmitted data, especially in government networks that operate in the context of the Internet of Things, hostilities, hybrid warfare, and cyberwarfare. The use of 5G extends to critical infrastructure operators and special users such as law enforcement, governments, and the military. Adapting modern cellular networks to meet the specific needs of these special users is not only feasible but also necessary. In doing so, these networks must meet additional stringent requirements for reliability, performance, and, most importantly, data security. This scientific paper is dedicated to addressing the challenges associated with ensuring cybersecurity in this context. To effectively improve or ensure a sufficient level of cybersecurity, it is essential to measure the primary indicators of the effectiveness of the security system. At the moment, there are no comprehensive lists of these key indicators that require priority monitoring. Therefore, this article first analyzed the existing similar indicators and presented a list of them, which will make it possible to continuously monitor the state of cybersecurity systems of 5G cellular networks with the aim of using them for groups of special users. Based on this list of cybersecurity KPIs, as a result, this article presents a model to identify and evaluate these indicators. To develop this model, we comprehensively analyzed potential groups of performance indicators, selected the most relevant ones, and introduced a mathematical framework for their quantitative assessment. Furthermore, as part of our research efforts, we proposed enhancements to the core of the 4G/5G network. These enhancements enable data collection and statistical analysis through specialized sensors and existing servers, contributing to improved cybersecurity within these networks. Thus, the approach proposed in the article opens up an opportunity for continuous monitoring and, accordingly, improving the performance indicators of cybersecurity systems, which in turn makes it possible to use them for the maintenance of critical infrastructure and other users whose service presents increased requirements for cybersecurity systems.

Keywords: 5G network; communication systems; transmitted data; hybrid warfare; cybersecurity; security systems; cellular networks

Citation: Odarchenko, R.; Iavich, M.; Iashvili, G.; Fedushko, S.; Syerov, Y. Assessment of Security KPIs for 5G Network Slices for Special Groups of Subscribers. *Big Data Cogn. Comput.* **2023**, *7*, 169. https://doi.org/10.3390/bdcc7040169

Academic Editors: Peter R.J. Trim and Yang-Im Lee

Received: 17 September 2023
Revised: 22 October 2023
Accepted: 23 October 2023
Published: 26 October 2023

1. Introduction

It is clear that 5G networks have become an integral part of today's digital society. This technology is already implemented in many places worldwide and continues to be implemented rapidly, offering many benefits for ordinary users of cellular networks (standard services) and business and specialized services (government communications, military,

firefighters, etc.). In the context of the latest special user introductions, 5G provides high throughput, low latency, and fairly high levels of reliability, opening up many opportunities for special missions and entirely new use cases. For example, 5G technology allows specific services to provide mission-critical communications whenever needed. It is clear that as specialized users implement more sensors, services, and subscribers, there may be additional operational needs, such as cybersecurity. It has become critical in the modern world, full of all kinds of threats, from single hackers to entire groups and even states. In this case, a single converged network capable of managing all of these functions gives operators the flexibility and control to manage high-bandwidth and low-latency applications while maintaining the required level of cybersecurity.

With emerging technologies such as artificial intelligence and machine learning, 5G's potential is truly impressive. It can provide special users with improved situational awareness, allowing entire units and platforms to respond faster and more accurately to threats in a dynamic environment. Furthermore, 5G's below-millisecond latency and reliability mean it can fit into various military and other government use cases.

The problem is that existing 5G communication systems cannot fully ensure the required quality of government line data service and the security of transmission in the widespread use of the concept of the Internet of Things, as well as in the context of hostilities, hybrid warfare, and cyberwar. Now, it is possible to intercept text messages, listen to conversations, and then use the data obtained against individuals and the military, government, etc. In addition, a remarkable landscape of other cyberattacks has appeared over the last decade. The current 5G network increases the range and adaptability of various services but also faces numerous security and privacy issues from attackers inside and outside the system perimeter. For example, 35 types of cyber threats were identified that pose significant risks in different areas of cybersecurity [1,2]: confidentiality, authentication, integrity, and availability in networks. This creates new serious threats that may become critical in the future. For example, an attacker can initiate eavesdropping to intercept data packets, conduct man-in-the-middle attacks to obtain session keys, or conduct location-tracking attacks on legitimate subscribers. These external threats that undermine the security of services for special users, the Internet of Things, etc., are the main security threats for every component in the structure of the modern 5G network, which is focused on providing high-quality services to its users. All this indicates the low efficiency of the applied methods of 5G network planning, the imperfection of the applied security technologies for the most secure data transmission, and the lack of ability to respond quickly to cyber incidents, etc.

The most spread-specific challenges and vulnerabilities in existing 5G communication systems that hinder the quality of service and data security for government lines and IoT applications were collected and reflected in Table 1.

Table 1. Specific challenges and vulnerabilities in existing 5G communication systems.

# Challenge	Security Threat	Target Point/Network Element	Effected Technology			Links	Privacy
			SDN	NFV	Cloud		
1.	DoS attack	Centralized control elements	+	+	+		
2.	Hijacking attacks	SDN controller, hypervisor	+	+			
3.	Signaling storms	5G core network elements			+	+	
4.	Resource (slice) theft	Hypervisor, shared cloud resources		+	+		
5.	Configuration attacks	SDN (virtual) switches, routers	+	+			

Table 1. *Cont.*

# Challenge	Security Threat	Target Point/Network Element	Effected Technology			Links	Privacy
			SDN	NFV	Cloud		
6.	Saturation attacks	SDN controller and switches	+				
7.	Penetration attacks	Virtual resources, clouds	+		+		
8.	User identity theft	User information data bases			+		+
9.	TCP level attacks	SDN controller-switch communication	+			+	
10.	Man-in-the-middle attack	SDN controller-communication	+			+	+
11.	Reset and IP spoofing	Control channels				+	
12.	Scanning attacks	Open air interfaces				+	+
13.	Security keys exposure	Unencrypted channels				+	
14.	Semantic information attacks	Subscriber location				+	+
15.	Timing attacks	Subscriber location			+		+
16.	Boundary attacks	Subscriber location					+
17.	IMSI catching attacks	Base station, identity registers				+	+

Therefore, scientifically based planning and optimization of cellular network security systems that provide the requested services with specified performance indicators for special groups of subscribers (transmission speed, delay, security of transmitted data) is a very complex scientific, technical, and economic problem, without which it is impossible to create an information infrastructure that meets the needs of a developed world-class information society.

As a leading standardization body in the field, 3GPPP pays great attention to the problem of network slice management in 5G [3]. Then, 5GPPP considered network slice KPIs and issued the White Paper on KPI Measurement Tools from KPI Definition to KPI Validation Enablement. Complete 5G projects, or parts of them, are dedicated to managing network slices and monitoring them. For example, 5G-DRIVE [4] was partially dedicated to researching critical innovations in networking slicing, network virtualization, etc. Moreover, 5G-MoNArch [5] in Work Package 3 worked on resilience and security and therefore developed secure network services and slices for them.

Leading manufacturers of telecommunications equipment also pay significant attention to this topic. For example, Juniper Networks described their end-to-end solution to manage service quality [6], Accedian paid attention to the active monitoring of network slices and the appropriate tools [7], Emblasoft developed flexible testing and active monitoring for 5G slices [8], and Huawei issued a white paper on 5G network cutting self-management [9]. Also, many research papers are devoted to monitoring network slices, the measurement of KPIs, level of security, etc. [10], focusing on the security challenges of the implementation of network slices in 5G networks [11,12]. The authors proposed that network slice controllers support security by enabling security controls at different

network layers. The researchers [13] proposed the AI-based approach for cybersecurity in network slices and provided a comprehensive analysis [14] of the division of the network to develop commercial needs and challenges in the network. In [15], the authors considered the strategy for deploying and integrating one or more network management software with managed services. Furthermore, in [16], the authors proposed a principally novel framework for 6G network slices.

As we found from the analysis of the above projects and articles, insufficient attention is paid to the problems of monitoring the performance indicators of network layer security systems.

The article offers an analysis of key performance indicators (KPIs) and provides security KPIs. The calculation model and the study of the corresponding KPIs are provided. The paper also offers the architecture of the system to collect and estimate security KPIs and make the most appropriate decision. The algorithm was developed that automatically checks the organization's security KPIs based on the corresponding parameters.

The rest of the paper is organized as follows. The next section of the paper analyzes existing related resources and concludes with a problem statement, the goals of the paper, and the establishment of subtasks.

2. Review of the Literature

In the paper [17], the authors propose minimized sets of security KPIs, focusing mainly on computing and memory resources. In the article, certain key performance indicators (KPIs) are intricately linked with the Management and Orchestration (MANO) framework, necessitating their definition as integral components of the said MANO orchestration.

In the paper [18], the authors define the main requirements and KPIs of 5G networks. The offered methodology's primary focus is providing diverse vertical sectors with ultra-reliable communication and minimizing latency. As a result, the authors provide the requirements and key performance indicators for 5G networks.

In the article [19], the main objective of the study is to stimulate future research towards the secure implementation of Machine Learning (ML) methodologies within 5G infrastructures and prospective wireless networks. In the papers [20,21], the authors offer an approach to increase the flexibility of key performance indicators in 5G networks. However, one of the crucial indicators, Network Availability, is not considered in the mentioned papers. This indicator's emphasis on network availability aligns with existing 5G practices that prioritize high availability through network slicing and virtualization. This technique ensures that critical services remain operational, even during security incidents or disruptions. In the papers [22–24], the security aspect of 5G networks is not fully covered.

In the paper [25], the main focus is on understanding and managing the quality and performance of services to meet the technical quality of service (QoS) and the quality of experience (QoE). One of the critical security KPIs of 5G networks is Mean Time to Detect (MTTD), which shows 5G's advanced monitoring capabilities, AI-driven analytics, and machine learning algorithms to contribute to a shorter MTTD than traditional methods. This enables security teams to identify potential threats faster and respond proactively. This security KPI is not used in the above-mentioned paper. Another essential security KPI is the Mean Time to Respond (MTTR). This KPI gives 5G's improved data processing capabilities and network speed, leading to a quicker MTTR when compared to conventional response methods. Faster data analysis and communication enable efficient incident investigation and remediation. The mentioned KPI can significantly increase the security of the level of services to fulfill the technical quality of the service working with QoS/QoE.

Another important KPI is Data Leakage Rate, which makes 5G's implementation of advanced encryption protocols and secure communication channels reduce the data leakage rate compared to less secure approaches. Robust encryption ensures the confidentiality of sensitive information during transmission, which is essential for the security level in

5G networks and is not presented in the articles [26,27], in which the authors perform experiments on optimizing monitoring processes in 5G networks.

Several key performance indicators (KPIs) for security are not completely represented in the articles [28,29]. Compared to traditional network security approaches, incident response time is not used in the documents. In addition, 5G's incident response time benefits from lower latency and higher data transfer rates. This allows security teams to detect and respond to incidents more quickly, reducing the time between identifying a threat and taking appropriate actions to mitigate it.

Key performance indicator Security Patch Management ensures faster and more efficient distribution of security patches and updates. It offers 5G's more rapid data transfer rates, enabling more efficient security patch management compared to slower network technologies. In the papers [30–32], the authors offer 5G network functions and characterize the performance of location management functions in 5G core networks. Security patch management provides better distribution of security patches, reducing exposure to known vulnerabilities and enhancing the network's overall security while working with the mentioned functions. In the papers [33,34], the security aspect is not fully covered, which is one of the essential aspects of building a 5G network infrastructure. The compliance indicator with security standards is vital for 5G network security. The security concepts of the 5G network are designed with security standards in mind, making them more compliant than the older approaches. Adherence to security standards ensures that best security practices are followed, reducing the likelihood of vulnerabilities.

In the paper [35], the authors show the open challenge of integrating satellites into 5G cellular networks. During the investigation of the open challenges of satellite integration into 5G networks, comparing the 5G network security KPIs with existing approaches is an important aspect, demonstrating how 5G leverages its inherent technological advantages to strengthen network security [36,37]. Integrating faster data transfer, improved data processing, and advanced security mechanisms contribute to better incident response, threat detection, authentication, intrusion prevention, data protection, and compliance with security standards.

Problem Statement

The main goal of this work is to develop a system to monitor security KPIs in fifth-generation and subsequent-generation cellular networks. It will give the possibility of continuous control and optimization of the network.

Achieving the set goal requires solving the following tasks:

1. Analysis of key performance indicators of 5G cellular networks.
2. Selection of optimal indicators that describe the state of cyber security in the cellular network.
3. Development of a mathematical apparatus to evaluate safety KPIs.
4. Improvement of the 4G/5G network core to ensure continuous monitoring of security KPIs.
5. Development of an algorithm and pseudocode for continuous monitoring and evaluation of safety KPIs.

3. Definition of Performance and Security KPIs

The development of advanced communication networks is based on the establishment of internationally accepted standards to ensure compatibility, cost-effectiveness, and widespread adoption. This collaboration aims to empower the European industry to lead the advancement of 5G standards and secure a minimum of 20% of the 5G SEP (standard essential patents) for development and use.

We have identified the benchmarks for the new network's operational characteristics:

- A thousand-fold increase in mobile data volume per unit area.
- Ten to a hundred times more connected devices.
- Ten to a hundred times higher average user data rate.

- A tenfold reduction in energy consumption.
- End-to-end latency of less than one millisecond.
- Universal 5G access, even in low-density regions.

This high-performance network will operate through a scalable management framework that enables the rapid deployment of innovative applications, including sensor-based solutions. It will also reduce network management operating expenses by at least 20% compared to current standards. Furthermore, the network will incorporate new lightweight yet robust security and authentication measures designed to address the challenges posed by pervasive multidomain visualized networks and services in the modern era.

The main categories of 5G key performance indicators (KPIs) typically include the following.

Enhanced Mobile Broadband (eMBB): This category focuses on improving mobile broadband services. Ultra-Reliable and Low-Latency Communications (URLLC) emphasizes reliable and low-latency communication, crucial for applications such as autonomous vehicles or remote surgery. Massive Machine-Type Communications (mMTC): This category addresses the requirements for connecting many IoT devices. ITU, NGMN, and 3GPP have globally characterized 5G use cases and related requirements since their development. Some 5G technology use cases include broadband access in densely populated areas, high user mobility, massive IoT connectivity, tactile Internet, support during natural disasters, electronic health services, and broadcast services.

Table 2 below summarizes the KPIs for 5G wireless technology at the ITU level, representing the minimum performance requirements:

Table 2. KPIs for 5G wireless technology at the ITU level [38].

The Type of 5G Performance Requirement	Minimum KPI Requirement and Category
Peak Spectral Efficiency	The downlink spectral efficiency is 30 bits per second per hertz (bps/Hz), whereas the uplink spectral efficiency is 15 bits per second per hertz (bps/Hz). (eMBB)
Peak Data Rate	The downlink speed for data transmission is 20 Gbps, while the uplink speed is 10 Gbps. (eMBB)
Area Traffic Capacity	In an indoor hotspot, the downlink data rate is 10 Mbps per square meter. (eMBB test environment)
Data Rate of User Experience	The downlink speed for data transmission is 100 Mbps, while the uplink speed is 50 Mbps. (eMBB)
Connection Density	106 devices/Km^2 (mMTC)
Latency (Control Plane)	The specified target latency is 20 milliseconds, with 10 milliseconds being the encouraged latency whenever possible. (eMBB, URLLC)
Latency (User Plane)	The specified latency requirement for enhanced mobile broadband (eMBB) is 4 milliseconds, whereas for ultrareliable low latency communications (URLLC), the latency target is 1 millisecond. (eMBB, URLLC)
Average Spectral Efficiency	Indoor coverage area with high-speed Internet: Download (DL) speed of 9 Mbps and upload (UL) speed of 6.75 Mbps. Dense urban coverage area: Download (DL) speed of 7.8 Mbps and upload (UL) speed of 5.4 Mbps. Rural coverage area: Download (DL) speed of 3.3 Mbps and Upload (UL) speed of 1.6 Mbps. (eMBB)
Reliability	1×10^{-5} the probability of successfully transmitting a layer-2 protocol data unit (PDU) consisting of 32 bytes in a 1 millisecond timeframe in an urban macro-URLLC test environment with edge channel coverage quality. (URLLC)
Energy Efficiency	Demonstrating Efficient Data Transmission (Loaded Case): The effectiveness of data transmission can be assessed by evaluating the "average spectral efficiency" metric. Minimizing Energy Consumption (No-Data Case): This test case aims to support a high sleep ratio and long sleep duration to achieve low energy consumption. It is designed to optimize the system for scenarios without data transmission. (eMBB)

Table 2. *Cont.*

The Type of 5G Performance Requirement	Minimum KPI Requirement and Category
Mobility	In a dense urban environment, the maximum speed considered is up to 30 Km/h, while in a rural setting it can reach up to 500 Km/h. (eMBB)
Mobility Interruption Time	0 ms (eMBB, URLLC)
Bandwidth (Maximum Aggregated System)	For operation in high-frequency bands (above 6 GHz), the minimum required bandwidth is at least 100 MHz, while the maximum supported bandwidth can reach up to 1 GHz. (IMT-2020)

Here are some of the key challenges and vulnerabilities that must be addressed during the design and deployment of 5G network services for special groups of subscribers.

1. Security concerns:
    - Spectrum vulnerability—the use of shared and unlicensed spectrum in 5G networks can make them susceptible to interference and jamming, which can disrupt government and IoT communications.
    - Cyberattacks—with more connected devices and a larger attack surface, the risk of cyberattacks, such as distributed denial of service (DDoS) attacks, increases, potentially affecting government and IoT services.
    - Device Vulnerabilities—IoT devices often have limited security features and can be vulnerable to hacking, compromising data security.
2. Privacy Concerns:
    - Data privacy—the massive amount of data generated by IoT devices, including personal information, can raise concerns about data privacy and unauthorized access, particularly in government applications.
    - Data Localization—governments may require data to be stored within their borders, creating challenges for global IoT deployments.
3. Compatibility and Interoperability:
    - Legacy systems—Integrating 5G with existing communication systems can be challenging, particularly for government agencies with legacy infrastructure.
    - IoT standards—The lack of universal IoT standards can hinder interoperability and create compatibility issues.
4. Risks to the supply chain:
    - Vendor Dependencies: Relying on specific vendors for 5G infrastructure or IoT devices can create supply chain vulnerabilities, especially if the vendors are from countries with conflicting interests.
5. Regulatory and Compliance Challenges:
    - Spectrum Regulations—Regulations and licensing for spectrum use can vary by region, complicating IoT device deployment and government communication systems.
    - Security and Privacy Regulations—Compliance with data security and privacy regulations, such as GDPR or HIPAA, can be complex, especially in cross-border scenarios.

Addressing these challenges and vulnerabilities in 5G communication systems for government lines and IoT applications requires a comprehensive approach that includes robust security measures, privacy protections, resilience, and interoperability. Collaboration between governments, industry stakeholders, and standardization bodies is crucial to effectively implement secure and reliable 5G and IoT solutions.

For today's 5G networks, a new cybersecurity approach must be defined, and precise metrics must be established to inform all stakeholders about potential threats and breaches. Typically, the leaders of large cellular service consumers are looking for clear security metrics that demonstrate costs and anticipated potential impacts on their business goals. The following study results can be cited as an example of such losses. A breach lasting

more than two hundred days has been shown to cost an organization 4.56 million USD, which is 37% more than the cost of a breach lasting less than two hundred days (3.34 million USD) [39].

Furthermore, the results of the study [39] showed that 44% of those surveyed said that their organization's security approach has improved significantly in recent years. Figure 1 lists the specific metrics companies used to measure this improvement. They mainly include the number of attacks prevented [40], the time taken to identify the incident, and the time required to locate the incident.

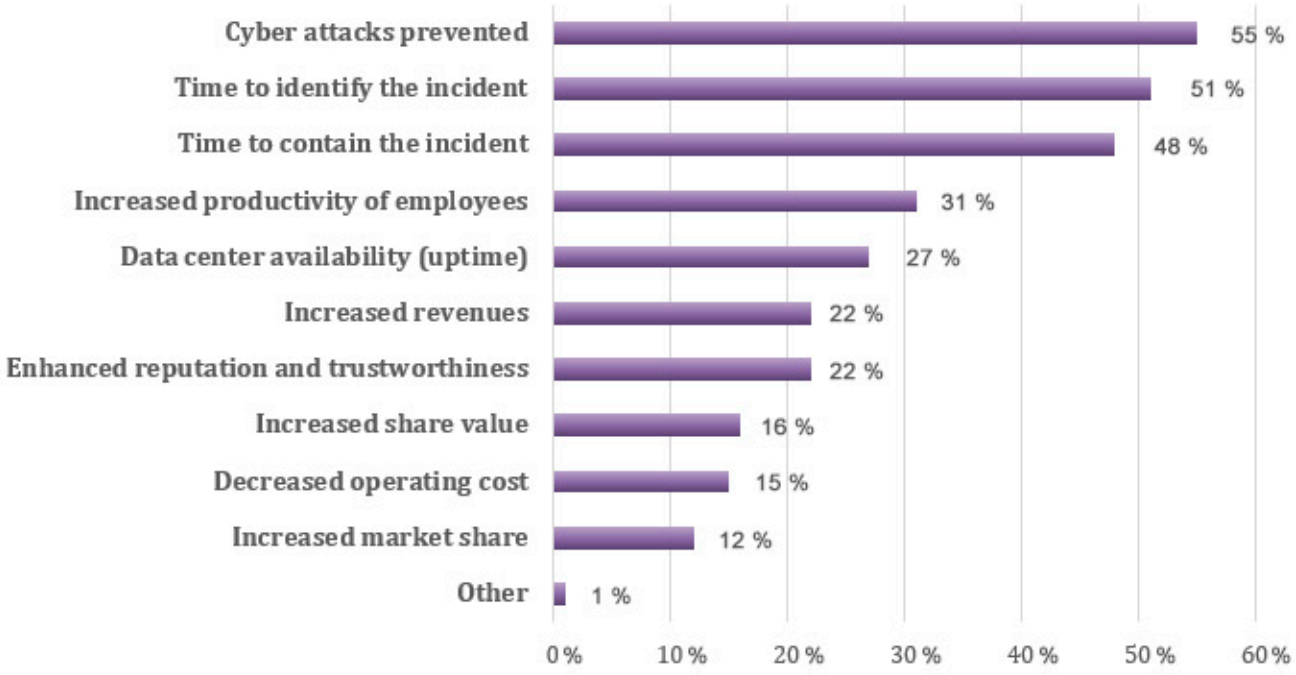

Figure 1. Results of the cyber security survey [41].

These KPIs outline the performance requirements for 5G wireless technology according to the ITU.

It is essential to determine security KPIs for 5G wireless networks. Security key performance indicators (KPIs) for 5G networks can help assess the effectiveness and efficiency of the security measures in place. Based on our research, we have identified the following security KPIs for 5G networks:

1. Incident Response Time: Measures the time taken to detect and respond to security incidents, such as network breaches or unauthorized access attempts.
2. Mean Time to Detect (MTTD): Measures the average time to detect security incidents or anomalies within the 5G network.
3. Mean Time to Respond (MTTR): Measures the average time it takes to respond and resolve security incidents or vulnerabilities identified within the 5G network.
4. Network availability: Measures the percentage of time the 5G network is available and operational without any security-related disruptions.
5. Network Resilience: Measures the ability of the 5G network to withstand and recover from security attacks or incidents without significant impact on network performance.
6. Authentication Failure Rate: Measures the percentage of failed authentication attempts within the 5G network, which can indicate potential security breaches or unauthorized access attempts.
7. Intrusion Detection and Prevention Effectiveness: Measures the accuracy and effectiveness of intrusion detection and prevention systems deployed within the 5G network in detecting and blocking security threats.

8. Data Leakage Rate: Measures the occurrence of data leaks or unauthorized access to sensitive information within the 5G network.
9. Compliance with Security Standards: Measures the level of compliance with security standards and regulations relevant to 5G networks, such as the 3GPP security specifications or industry best practices.
10. Security Patch Management: Measures the frequency and timeliness of applying security patches and updates to network equipment and software within the 5G network.

It is important to note that specific security KPIs may vary depending on the network operator, service provider, or organization that implements the 5G network. These KPIs can be tailored to suit the network infrastructure's specific security goals and requirements. To ensure the success of the concrete 5G business, it is crucial to establish a well-defined cybersecurity approach and use accurate metrics to inform relevant stakeholders. C-level executives and board members are actively looking for security metrics that clearly understand the costs involved and the anticipated impact on their business objectives. According to the IBM research findings [39], organizations experience a significantly higher cost of 4.56 million USD when a breach lasts more than two hundred days. This amount is 37% greater than the cost incurred when a breach is resolved in a shorter period, which is 3.34 million USD.

Furthermore, the study highlights that 44% of the respondents surveyed reported notable improvements in their organization's security approaches during the past 12 months. These metrics include primarily the number of prevented attacks, the time required to identify an incident, and the time required to contain an incident. Approximately 55%, 51%, and 48% of companies use these respective metrics for measurement purposes. Based on this study, we can identify the security KPIs for 5G networks. To effectively assess security operations, metrics such as Mean Time to Identification (MTTI) and Mean Time To Contain (MTTC) are considered essential to measure cybersecurity intrusions or incidents in 5G networks. Based on related articles, we have identified a set of main KPIs for security measures (Table 3).

Table 3. The most relevant 5G cybersecurity KPIs.

The Type of 5G Security Requirement	Minimum Security KPI Requirements	Formula/Symbol	Challenges Addressed (from Table 1)
Intrusion Attempts [42]	As a cybersecurity operative, you must monitor intrusion attempts on your organization's network. Similarly, you can regularly review your firewall logs to see if anyone has unauthorized access to the network.	NIA	1–3, 5–7, 9–17
Number of Security Incidents [43]	This KPI quantifies the total number of security incidents or breaches detected in the 5G network over a specific period. Monitoring this metric helps to track the security posture and identify trends or patterns.	NSI	1–17
Mean Time to Identification (MTTI) [43]	The whole process must take a maximum of 12 h.	$MTTI = \frac{S_{IT}}{N_I}$, where: S_{IT}—sum of identification times; N_I—number of incidents.	1–17
Mean Time To Contain (MTIC) [43]	The entire process must take a maximum of 12 h.	$MTIC = \frac{S_{CT}}{N_I}$, where: S_{CT}—sum of contain times N_I—number of incidents.	1–17
Mean Time to Recover (MTTR) [44]	This KPI measures the average recovery time from a security incident or breach. A shorter MTTR indicates effective incident response and recovery capabilities, minimizing impact on network operations.	$MTTR = \frac{S_{TTR}}{N_I}$, where: S_{TTR}—total time taken to recover from incidents N_I—number of incidents.	1–17

Table 3. *Cont.*

The Type of 5G Security Requirement	Minimum Security KPI Requirements	Formula/Symbol	Challenges Addressed (from Table 1)
Incident Response Time [43]	Aim for a rapid incident response time to ensure timely detection and mitigation of security incidents. A specific target can be set, such as responding to critical incidents within a defined timeframe (e.g., within 1 h).	$IRT = Timestamp_{IR} - Timestamp_{ID}$, where: $Timestamp_{IR}$—time of incident resolution; $Timestamp_{ID}$—time of incident detection.	1–3, 5–7, 9–17
Mean Time to Detect (MTTD) [45]	Strive to minimize the average time taken to detect security incidents. Setting a target, such as keeping the MTTD below a certain threshold (e.g., within 30 min), can help promptly identify potential threats.	$MTTD = \frac{S_{ID}}{N_I}$, where: S_{ID}—sum of detection times; N_I—number of incidents.	1–3, 5–7, 9–17
Mean Time to Respond (MTTRes) [45]	The aim is to minimize the average time taken to respond and resolve security incidents. Establishing a target, such as keeping the MTTR below a specific value (e.g., within 2 h), can help expedite incident resolution.	$MTTR = \frac{S_{RT}}{N_I}$, where: S_{RT}—sum of respond times; N_I—number of incidents.	1–3, 5–7, 9–17
Network Availability [46]	Aim for high network availability to minimize disruptions due to security incidents. Setting a target, such as maintaining network availability at a high percentage (e.g., 99.99%), ensures that security events do not significantly impact network services.	$NA = \frac{t_{up}}{t_{total}}$, where: t_{up}—total uptime; t_{total}—total time.	1–3, 9, 11
Authentication Failure Rate [47]	Try to keep the authentication failure rate as low as possible. Although the acceptable rate may depend on the specific network context, aiming for a minimal failure rate (for example, less than 1%) helps reduce the risk of unauthorized access.	$AFR = \frac{N_{AF}}{N_{AA}}$, where: N_{AF}—number of authentication failures; N_{AA}—total number of authentication attempts.	10, 17
Intrusion Detection and Prevention Effectiveness [48]	Implement robust intrusion detection and prevention systems with high accuracy rates. Regularly assess and monitor the effectiveness of these systems, with a goal of a high detection and prevention rate (for example, above 95%).	$TPR = \frac{N_{TP}}{N_{AI}}$, $TPR = \frac{N_{FP}}{N_{AI}}$, where: N_{TP}—number of true positives; N_{FP}—number of false positives; N_{AI}—total number of actual intrusions.	4, 7, 8, 10, 17
Data Leakage Rate [49]	Aim for a minimal data leakage rate within the 5G network. This can be achieved through solid access controls, encryption, and monitoring mechanisms. Setting a target, such as keeping the data leakage rate below a specific value (e.g., 0.5%), helps ensure data protection.	$DLR = \frac{N_{DLI}}{TV_{DH}}$, where: N_{DLI}—number of data leakage incidents; TV_{DH}—total volume of data handled.	13
Threat Detection Time [50]	This KPI measures the time it takes to detect and identify a security threat or intrusion on the 5G network. A shorter detection time indicates a more proactive and effective security system.	$T_D = T_{TD} - T_{TO}$, where: T_{TD}—time of threat detection; T_{TO}—time of threat occurrence.	1–17
Patching and Vulnerability Management [51]	This KPI evaluates the time to apply security patches and updates to address known vulnerabilities in the 5G network infrastructure. Correct patching helps minimize the risk of exploitation. Time taken to apply patches and updates	PVMT	1–17
Compliance with Security Standards [52]	This KPI evaluates the extent to which the 5G network adheres to relevant cybersecurity standards and regulations. Compliance with standards such as the 3GPP security specifications ensures a robust security posture.	$CR = \frac{N_{CRM}}{N_{TNCR}}$, where: N_{CRM}—number of compliance requirements met; N_{TNCR}—total number of compliance requirements.	1–17

Table 3 is a set of performance indicators for cybersecurity systems in cellular 4G/5G networks. It contains indicators that describe the state of security in the network as a whole and individual elements that describe the state of individual network elements. The table also includes both indicators (Intrusion Attempts) that need to be constantly measured. Their deviation may indicate the occurrence of a cybersecurity incident, as well as indicators that are measured over time and therefore require preliminary collection (accumulation) of information (number of Security Incidents, Mean Time To Identification, Mean Time To Contain, Mean Time to Identification, Mean Time to Detect, Mean Time to Respond,

Network Availability, Authentication Failure Rate, Intrusion Detection and Prevention Effectiveness, Data Leakage Rate, Threat Detection Time, Patching, and Vulnerability Management). Their assessment indicates the need for comprehensive changes (possibly a revision of current approaches) in the security system. Such a KPI, like "Compliance with Security Standards", has to be fully satisfied and continuously reviewed (Table 4).

Table 4. Table of threshold values of security KPIs.

Security KPIs	Network Slice-Type Thresholds			
	Slice 1 (i.e., eMBB)	**Slice 2 (i.e., MCC)**	...	**Slice *N***
NIA	*NIA1*	*NIA2*	...	*NIAN*
NSI	*NSI1*	*NSI2*	...	*NSI2*
MTTI	*MTTI1*	*MTTI2*	...	*MTTIN*
MTTR	*MTTR1*	*MTTR2*	...	*MTTRN*
MTTD	*MTTD1*	*MTTD2*	...	*MTTDN*
MTTRes	*MTTRes1*	*MTTRes2*	...	*MTTResN*
NA	*NA1*	*NA2*	...	*NA3*
AFR	*AFR1*	*AFR2*	...	*AFRN*
TPR	*TPR1*	*TPR2*	...	*TPRN*
FPR	*FPR1*	*FPR2*	...	*FPRN*
DLR	*DLR1*	*DLR2*	...	*DLRN*
TDT	*TDT1*	*TDT2*	...	*TDTN*
PVMT	*PVMT1*	*PVMT2*	...	*PVMTN*
CR	*CR1*	*CR2*	...	*CRN*

Minimal KPI requirements can vary depending on the organization's specific risk appetite and security objectives.

4. Development of Architecture

To achieve low latency, high data transfer rates, and a higher level of security, the concept of network cutting was defined in 5G. This technology allows network operators to divide their physical infrastructure into multiple logical networks, each configured according to its characteristics and needs. As shown in Figure 2, each network layer is an independent virtual subnet from end to end and can even be owned by different tenants (or vertical markets) that manage the physical, virtualized, and service layers with different key performance indicators (KPIs), including security metrics.

Using emerging advances in virtualization and network management, such as software-defined networking (SDN) and network function virtualization (NFV), network partitioning creates virtual networks that provide a customized network experience that meets pre-defined key performance indicators (KPIs). Therefore, there are known security issues associated with these underlying SDN and NFV technologies and access networks. Thus, the central part of the security in the division of the network is to determine what constitutes the main potential threats to this segment, the establishment of minimum requirements, and their mandatory implementation. In this case, it is imperative to define isolation attributes, create an abstraction layer to provide end-to-end isolation at a particular level, and introduce appropriate security policies for each layer.

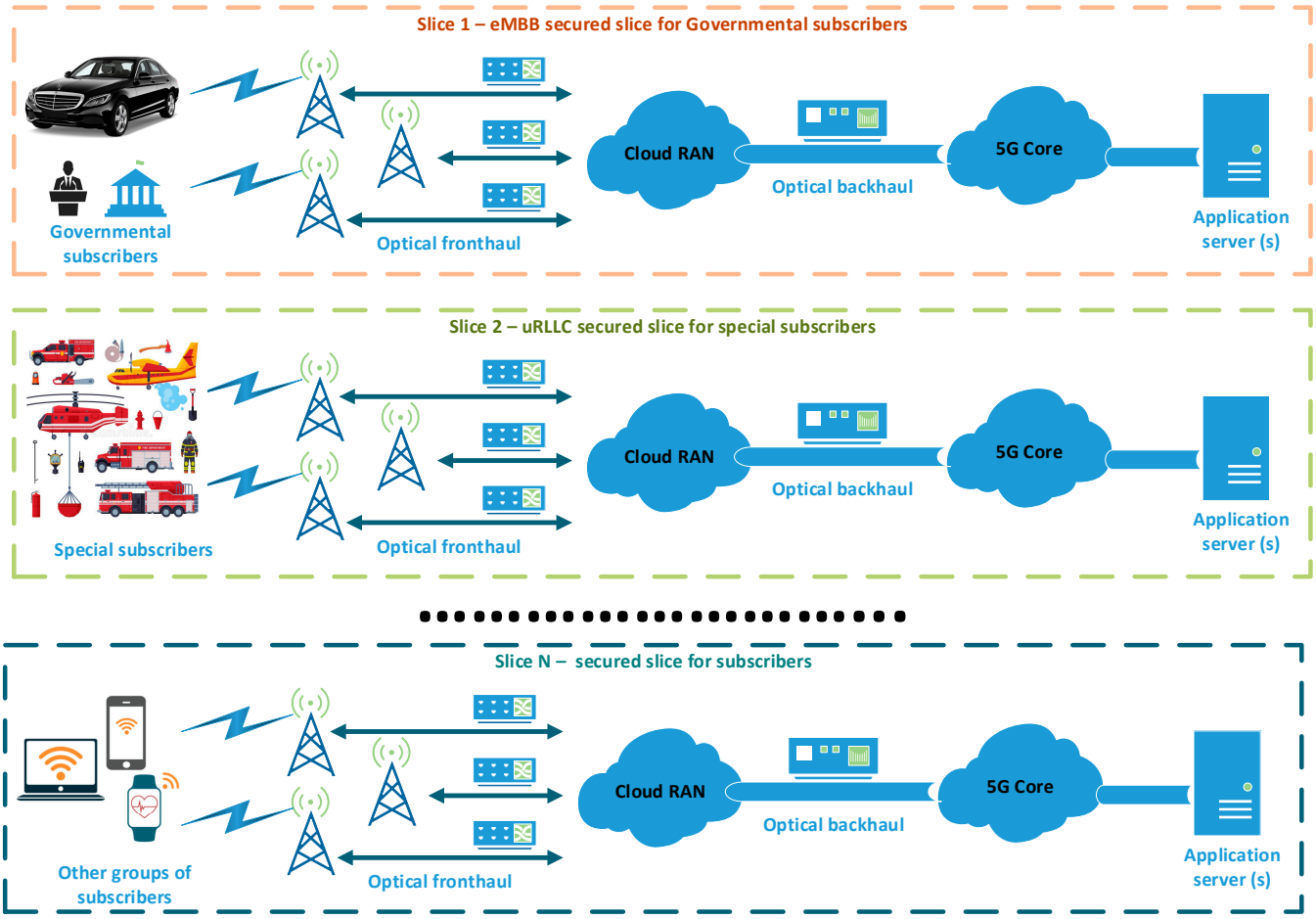

Figure 2. Network slices concept for the special subscribers' groups.

Therefore, an effective network partitioning solution requires integrated management, performance, and security considerations. In this case, attacks directed against one segment must not affect others. Therefore, security functions must act independently for each layer. Thus, the main challenge in designing a network partitioning solution is to satisfy all the requirements of the segment owner while ensuring the security of each segment independently.

As illustrated in Figure 3, a 5G network may accommodate different use cases, and each can be served by single or multiple network slices, which can be applied to monitoring mechanisms [53]. When the subscribers are geographically dispersed, dedicated or shared network slices can also serve the horizontal use cases. Each network slice owns logically isolated computation and storage resources to perform data processing and storage tasks for all use cases that receive their services. Each network layer, which must serve a specific group of subscribers to ensure the required quality of service and secure data transmission, is characterized by its specific network characteristics and network security indicators (KPIs). To respond immediately to emerging anomalies, degradation of service quality, or lowering the level of information security, it is necessary to continuously monitor the above parameters. This process is reflected in Figure 3. In addition, also it is also possible to perform forced penetration tests of layers. For these two procedures, a specialized network slices monitoring server can be used (Figure 3).

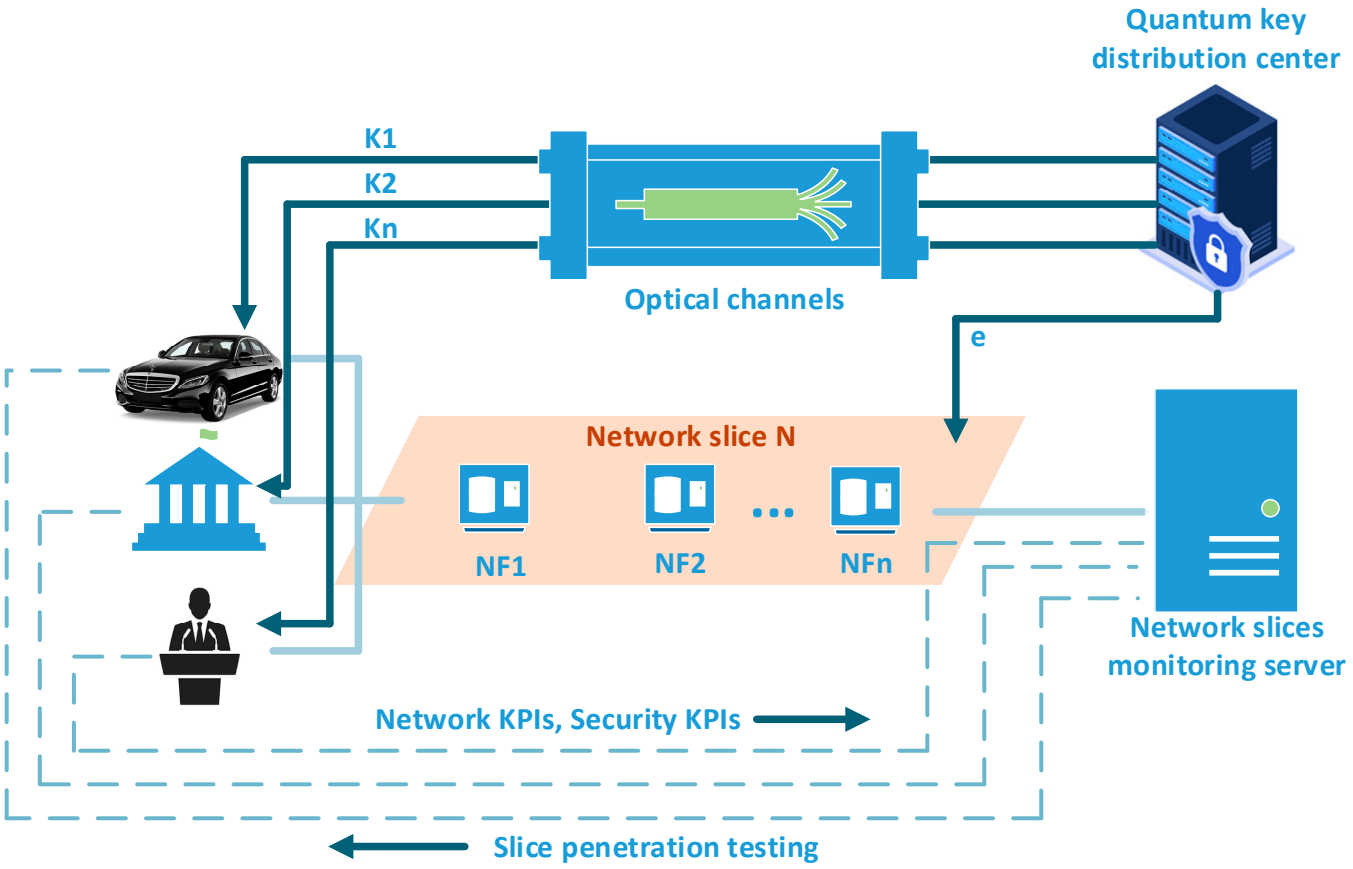

Figure 3. Graphical representation of delivering security credentials in the key management scheme.

The operation of this system obviously must be in synchronization with the cybersecurity systems. As an example, the figure shows a case of potential use of a quantum key distribution system, described in detail in [54], to increase the confidentiality level of transmitted data. Thus, in the case of measuring security indicators and identifying problems, for example, with confidentiality, quantum fundamental distribution mechanisms can be used. However, in general, the study aims to describe a generalized model and, accordingly, the architecture of the monitoring system that will ensure the main security principles, traditionally categorized as confidentiality, authentication, authorization, availability, and integrity.

5. The Offered Model

Based on the above, using the security KPIs from Table 2, a set of safety KPIs for the evaluation analysis model is proposed, which can be objectively evaluated. There is a set of network layers for which both the QoS quality of service indicators and the security KPI indicators are clearly defined.

$$\left\{ \bigcup_{i=1}^{n} Slice_i \right\} = \{Slice_1, Slice_2, I, Slice_n\},$$

where

- network layers: $Slice_i \subseteq Slice$, $\left(i = \underline{1, n}\right)$, n is the number of these layers.
- $KPI_i^{sec} = \left\{ \cup_{j=1}^{m_i} KPI_{i,j}^{sec} \right\} = \left\{ KPI_{i,1}^{sec}, KPI_{i,2}^{sec}, \ldots KPI_{i,m_i}^{sec} \right\}$, $KPI_{i,j}^{sec} \left(j = \underline{1, m_i}\right)$ is a subset KPI for cyber security systems (Table 2).

In order to collect information about any operations that occur on the network, analyze them, and, accordingly, make decisions based on the assessments made, it is proposed to add either an additional network function to the core of the network, which will contain all

the functionality necessary for this or, more straightforward at first, especially for testing the system, is to add an external server that will be connected to the network core via standard interfaces. This approach is reflected in Figure 4.

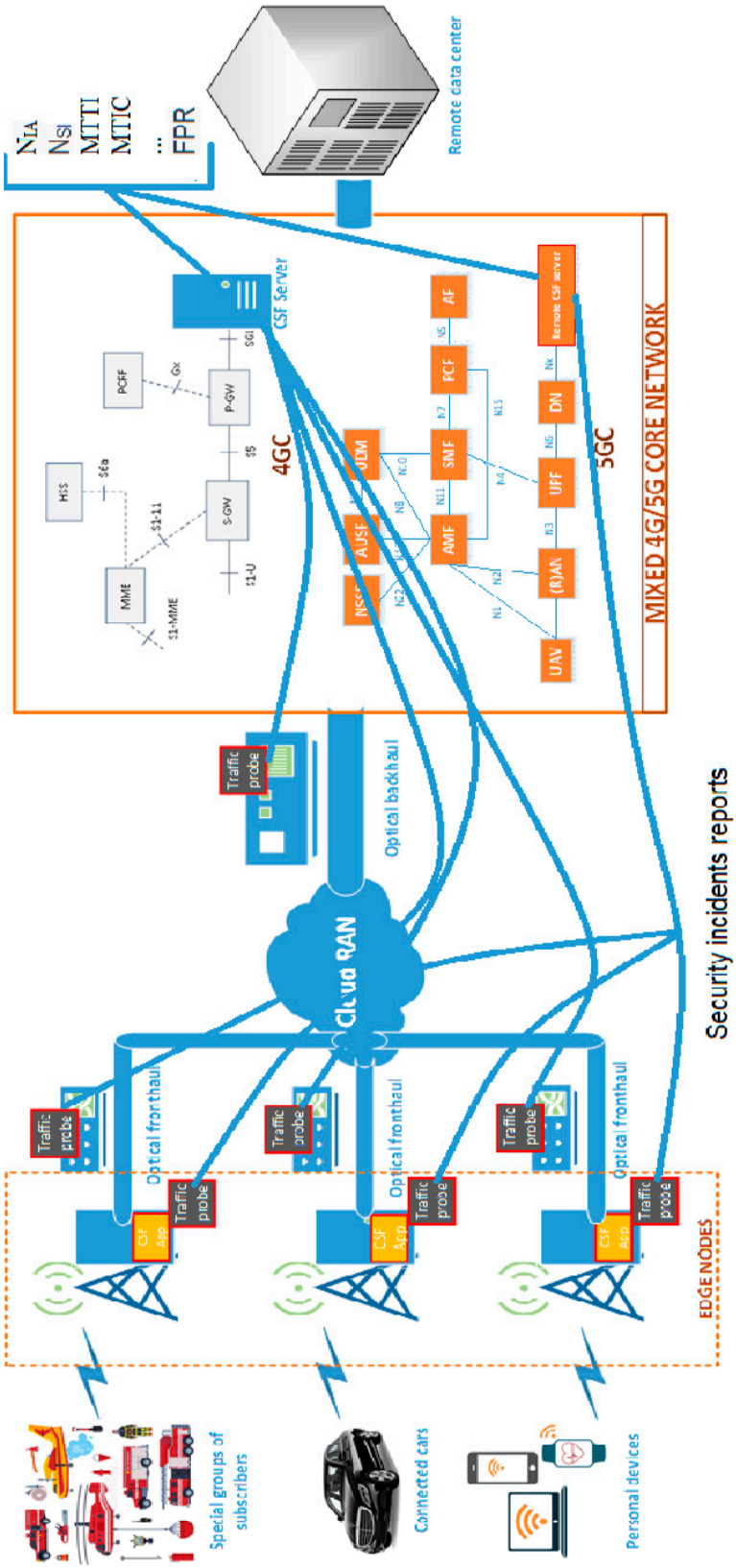

Figure 4. Continuous security KPIs monitoring system for 4G/5G/6G.

Thus, all the KPIs mentioned above will be collected in different parts of the network (different nodes) and stored in a specialized database that can be combined with the Cybersecurity Function Server (CSF) (Figure 4).

Furthermore, due to constant monitoring, the database will be filled in real-time with primary security KPIs, for which statistics on the number of incidents, their impact, scale, duration, etc., can be used. In the future, these primary indicators can be used to estimate secondary parameters using the mathematical apparatus in Table 2. The following pseudocode defines the algorithm developed for this assessment.

```
class Secure_KPI():
def __init__(self):
#defining the dictionary with the security KPIs as the keys and lists of desired parameters for the corresponding KPI for the concrete organization.
self.KPI={NIA:[parameters], NSI:[parameters], MTTI:[parameters], MTTR:[parameters], MTTD:[parameters], MTTRes:[parameters], NA:[parameters], AFR:[parameters], TPR:[parameters], FPR:[parameters], DLR:[parameters], TDT:[parameters], PVMT:[parameters]}
def input_data(self):
        # the array for storing the lists of parameters
self.data=[]
# appending the list with the needed number of empty lists
        for i in range(len(self.KPI)):
            self.KPI.append([])
        #filling the lists with the secure KPIs data for the concrete organization
        for kpi in self.KPI:
            number=0
            for i in self.KPI[kpi]:
                d=input("the desired data for your organization")
                self.data[number].append(d)
            number=number+1
#checking security KPIs with the defined formulas
def check(self):
        for kpi in self.KPI:
            for i in self.KPI[kpi]:
Calculate the corresponding security kpi according to the formulas in Table 2.
If security kpi > corresponding element in data list:
        alert(self.kpi)
#taking the security measures to mitigate the corresponding vulnerability, it will be defined in future works
def alert(self, problematic_kpi):
        taking the corresponding measures
#creating the object of the concrete organization
organization_x=Secure_KPI()
#inputting the data of the organization
organization_x.input_data()
#calculating and checking security KPI
organization.check()
```

The pseudocode offered is divided into 5 stages. The class is named Secure_KPI, designed to manage and assess key performance indicators (KPIs) related to security for a specific organization.

1. Initialization (Constructor):

The __init__ method is the constructor that initializes the class. Inside it, a dictionary called KPI is defined. This dictionary stores security KPIs as keys and lists the desired parameters for those KPIs as values.

2. Input Data:

The input_data method is intended to gather data related to the security KPIs for the organization. Create an empty list called self.data and append it multiple times based on the number of KPIs in the KPI dictionary. Then, it iterates over each KPI, asking for user input to populate the lists in self.data with the desired data for each KPI.

3. Checking Security KPIs:

The check method is used to assess the security KPIs. It iterates through the KPIs in the KPI dictionary and compares each KPI to the corresponding data from the self.data list; if a security KPI is greater than the corresponding element in the data list, it calls the alert method with the problematic KPI as an argument.

4. Alerting:

The alert method is intended to take appropriate security measures to mitigate vulnerabilities when a problematic KPI is detected. However, implementing this method is incomplete, and it mentions taking measures not defined in the provided code.

5. Creating an Organization and Using the Class:

At the end of the code, an instance of the Secure_KPI class is created, named organization_x.
Data for the organization are input using the input_data method.
The security KPIs are calculated and checked using the check method.
Additionally, the database should contain threshold values for the parameters of each layer (Table 3).

Based on the comparison of actual measured (estimated) KPIs with threshold values, a decision is made on the need to improve certain parameters (D), if necessary, based on Decision Rules (DR) matrices for each KPI.

$$D = \begin{cases} Rule_1 & if & cond_1 = true \\ \dots & \dots & \dots \\ Rule_N & if & cond_N = true \end{cases},$$

where

$$DR = \begin{pmatrix} Rule_1 & cond_1 \\ \dots & \dots \\ Rule_N & cond_N \end{pmatrix}$$

where $Rule_N$ is the action that has to be applied if the condition $cond_N$ is true.

These formulas are introduced to complete the work of the approach in a comprehensive way. In the future, specific rules will be developed for certain conditions corresponding to deviations in the measured indicators.

6. Conclusions

In conclusion, 5th generation cellular networks actively replace communication in many areas of human life. The number of industries decreases, in which it is impossible or impractical to use 5G networks. Operators of critical infrastructure, special users (such as the police), governments, and the military are not the exception. Modern cellular networks can and must be easily adapted to the needs of special users. In this scenario, the network is subject to more stringent demands regarding reliability, performance, and, most importantly, data security. This scientific article focuses on the challenges related to ensuring cybersecurity.

To effectively increase the level of cybersecurity or ensure its sufficient level, it is necessary to measure the leading indicators of the effectiveness of security systems. At the moment, there are no comprehensive lists of these key indicators that require priority monitoring. Therefore, this article first analyzed the existing similar indicators and presented their list, which will make it possible to continuously monitor the state of cyber security systems of 4G/5G cellular networks with the aim of using them for groups of special users.

Therefore, this article proposed a method to determine these indicators and their evaluation. For this method, a meaningful analysis of possible groups of performance indicators was performed, the most relevant ones were selected, and a mathematical apparatus was proposed for their quantitative evaluation. Furthermore, within the framework of solving research problems, improvements were proposed for the core of the 4G/5G network, which allows data and performing statistical analysis at the expense of special sensors and the existing server.

Thus, to improve cybersecurity in critical infrastructure, government, military, and particular user networks using 5G technology, it is necessary to continuously monitor the performance of security systems. The first step is to ensure that the security architecture and practices comply with all the regulations governing the special user groups. After this, it is necessary to continuously monitor the presence of cyber incidents, log any violations, and perform more comprehensive assessments of the cybersecurity parameters in Table 3. If thresholds are exceeded, these assessments should become the basis for making decisions about an immediate response to cybersecurity problems or a comprehensive change to cybersecurity approaches.

Thus, the approach proposed in the article opens up an opportunity for continuous monitoring and, accordingly, improving the performance indicators of cybersecurity systems, which in turn makes it possible to use them for the maintenance of critical infrastructure and other users whose service requires increased requirements for cybersecurity systems.

Future scientific research will be directed toward implementing the proposed method and evaluating its validity. Additionally, there are plans to take advantage of artificial intelligence to process large datasets and make informed decisions based on established rules.

Author Contributions: Conceptualization, R.O., M.I., G.I., S.F. and Y.S.; methodology, R.O., M.I., G.I., S.F. and Y.S.; software, R.O., M.I., G.I., S.F. and Y.S.; validation, R.O., M.I., G.I., S.F. and Y.S.; formal analysis, R.O., M.I., G.I., S.F. and Y.S.; investigation, R.O., M.I., G.I., S.F. and Y.S.; resources, R.O., M.I., G.I., S.F. and Y.S.; data curation, R.O., M.I., G.I., S.F. and Y.S.; writing—original draft preparation, R.O., M.I., G.I., S.F. and Y.S.; writing—review and editing, R.O., S.F. and Y.S.; visualization, R.O., M.I., G.I., S.F. and Y.S.; project administration, R.O. and S.F. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

Acknowledgments: This work was supported by the Shota Rustaveli National Foundation of Georgia (SRNSFG) (NFR-22-14060), the National Scholarship Programme of the Slovak Republic and EU Next Generation EU through the Recovery and Resilience Plan for Slovakia under project No. 09I03-03-V01-000153.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Pateria, J.; Ahuja, L.; Som, S.; Seth, A. Applying Clustering to Predict Attackers Trace in Deceptive Ecosystem by Harmonizing Multiple Decoys Interactions Logs. *Int. J. Inf. Technol. Comput. Sci.* **2023**, *15*, 35–44. [CrossRef]
2. Khaleefah, A.D.; Al-Mashhadi, H.M. Methodologies, Requirements and Challenges of Cybersecurity Frameworks: A Review. *Int. J. Wirel. Microw. Technol.* **2023**, *13*, 1–13. [CrossRef]
3. 5G Network Slice Management. Available online: https://www.3gpp.org/technologies/slice-management (accessed on 10 July 2023).
4. 5G-Trials—From 5G Experiments to Business Validation. Available online: https://5g-drive.eu/ (accessed on 9 September 2023).
5. 5G-MoNArch: 5G Mobile Network Architecture for Diverse Services, Use Cases, and Applications in 5G and Beyond. Available online: https://5g-ppp.eu/5g-monarch/ (accessed on 17 June 2022).
6. Juniper Networks Whitepaper. Managing 5G Slice Quality of Service End-to-End. Available online: https://www.juniper.net/content/dam/www/assets/flyers/us/en/managing-5g-slice-quality-of-service-end-to-end.pdf (accessed on 22 April 2021).
7. Hallé, C. Why Network Slicing Requires Active Monitoring, Passive Monitoring AND True APM. Available online: https://accedian.com/blog/why-network-slicing-requires-active-monitoring-passive-monitoring-and-true-apm/ (accessed on 16 November 2020).

8. Emblasoft. Innovate, Validate, Operate. Available online: https://emblasoft.com/ (accessed on 6 December 2022).
9. 5G Network Slicing Self-Management White Paper. Available online: https://www-file.huawei.com/-/media/corporate/pdf/news/5g-network-slicing-self-management-white-paper.pdf?la=en (accessed on 19 October 2020).
10. Wichary, T.; Mongay Batalla, J.; Mavromoustakis, C.X.; Żurek, J.; Mastorakis, G. Network Slicing Security Controls and Assurance for Verticals. *Electronics* **2022**, *11*, 222. [CrossRef]
11. Ogidiaka, E.; Ogwueleka, F.N.; Irhebhude, M.E. Game-Theoretic Resource Allocation Algorithms for Device-to-Device Communications in Fifth Generation Cellular Networks: A Review. *Int. J. Inf. Eng. Electron. Bus.* **2021**, *13*, 44–51. [CrossRef]
12. Mallipudi, C.C.; Chandra, S.; Prakash, P.; Arya, R.; Husain, A.; Qamar, S. Reinforcement Learning Based Efficient Power Control and Spectrum Utilization for D2D Communication in 5G Network. *Int. J. Comput. Netw. Inf. Secur.* **2023**, *15*, 13–24. [CrossRef]
13. Majeed, A.; Alnajim, A.M.; Waseem, A.; Khaliq, A.; Naveed, A.; Habib, S.; Islam, M.; Khan, S. Deep Learning-Based Symptomizing Cyber Threats Using Adaptive 5G Shared Slice Security Approaches. *Future Internet* **2023**, *15*, 193. [CrossRef]
14. Zahoor, S.; Ahmad, I.; Othman, M.; Mamoon, A.; Rehman, A.U.; Shafiq, M.; Hamam, H. Comprehensive Analysis of Network Slicing for the Developing Commercial Needs and Networking Challenges. *Sensors* **2022**, *22*, 6623. [CrossRef]
15. De Jesus Martins, R.; Wickboldt, J.A.; Granville, L.Z. Assisted Monitoring and Security Provisioning for 5G Microservices-Based Network Slices with SWEETEN. *J. Netw. Syst. Manag.* **2023**, *31*, 36. [CrossRef]
16. Kuklinski, S.; Tomaszewski, L.; Kolakowski, R.; Chemouil, P. 6G-LEGO: A framework for 6G network slices. *J. Commun. Netw.* **2021**, *23*, 442–453. [CrossRef]
17. Kukliński, S.; Tomaszewski, L. Key Performance Indicators for 5G network slicing. In Proceedings of the IEEE Conference on Network Softwarization (NetSoft), Paris, France, 24–28 June 2019; pp. 464–471. [CrossRef]
18. El Azzaoui, A.; Singh, S.K.; Pan, Y.; Park, J.H. Block5GIntell: Blockchain for AI-Enabled 5G Networks. *IEEE Access* **2020**, *8*, 145918–145935. [CrossRef]
19. Suomalainen, J.; Juhola, A.; Shahabuddin, S.; Mammela, A.; Ahmad, I. Machine Learning Threatens 5G Security. *IEEE Access* **2020**, *8*, 190822–190842. [CrossRef]
20. Zhang, S. An Overview of Network Slicing for 5G. *IEEE Wirel. Commun.* **2019**, *26*, 111–117. [CrossRef]
21. Koumaras, H.; Tsolkas, D.; Gardikis, G.; Gomez, P.M.; Frascolla, V.; Triantafyllopoulou, D.; Emmelmann, M.; Koumaras, V.; Osma, M.L.G.; Munaretto, D.; et al. 5GENESIS: The Genesis of a flexible 5G Facility. In Proceedings of the 2018 IEEE 23rd International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), Barcelona, Spain, 17–19 September 2018; pp. 1–6. [CrossRef]
22. Doukoglou, T.; Gezerlis, V.; Trichias, K.; Kostopoulos, N.; Vrakas, N.; Bougioukos, M.; Legouable, R. Vertical Industries Requirements Analysis & Targeted KPIs for Advanced 5G Trials. In Proceedings of the 2019 European Conference on Networks and Communications (EuCNC), Valencia, Spain, 18–21 June 2019; pp. 95–100. [CrossRef]
23. Gupta, M.; Legouable, R.; Rosello, M.M.; Cecchi, M.; Alonso, J.R.; Lorenzo, M.; Kosmatos, E.; Boldi, M.R.; Carrozzo, G. The 5G EVE End-to-End 5G Facility for Extensive Trials. In Proceedings of the 2019 IEEE International Conference on Communications Workshops (ICC Workshops), Shanghai, China, 20–24 May 2019; pp. 1–5. [CrossRef]
24. Boero, L.; Bruschi, R.; Davoli, F.; Marchese, M.; Patrone, F. Satellite Networking Integration in the 5G Ecosystem: Research Trends and Open Challenges. *IEEE Netw.* **2018**, *32*, 9–15. [CrossRef]
25. Banović-Ćurguz, N.; Ilišević, D. Mapping of QoS/QoE in 5G Networks. In Proceedings of the 2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 20–24 May 2019; pp. 404–408. [CrossRef]
26. Christopoulou, M.; Xilouris, G.; Sarlas, A.; Koumaras, H.; Kourtis, M.-A.; Anagnostopoulos, T. 5G Experimentation: The Experience of the Athens 5GENESIS Facility. In Proceedings of the 2021 IFIP/IEEE International Symposium on Integrated Network Management (IM), Bordeaux, France, 17–21 May 2021; pp. 783–787.
27. Saha, N.; James, A.; Shahriar, N.; Boutaba, R.; Saleh, A. Demonstrating Network Slice KPI Monitoring in a 5G Testbed. In Proceedings of the NOMS 2022–2022 IEEE/IFIP Network Operations and Management Symposium, Budapest, Hungary, 25–29 April 2022; pp. 1–3. [CrossRef]
28. Xie, M.; Gonzalez, A.J.; Gronsund, P.; Lonsethagen, H.; Waldemar, P.; Tranoris, C.; Denazis, S.; Elmokashfi, A. Practically Deploying Multiple Vertical Services into 5G Networks with Network Slicing. *IEEE Netw.* **2022**, *36*, 32–39. [CrossRef]
29. Lagen, S.; Bojovic, B.; Koutlia, K.; Zhang, X.; Wang, P.; Qu, Q. QoS Management for XR Traffic in 5G NR: A Multi-Layer System View & End-to-End Evaluation. *IEEE Commun. Mag.* **2023**, 1–7. [CrossRef]
30. Vordonis, D.; Giannopoulos, D.; Papaioannou, P.; Tranoris, C.; Denazis, S.; Rahav, R.; Altman, B.; Bosneag, A.-M.; Jain, S.; Margolin, U.; et al. Monitoring and Evaluation of 5G Key Performance Indicators in Media Vertical Applications. In Proceedings of the 2022 IEEE International Mediterranean Conference on Communications and Networking (MeditCom), Athens, Greece, 5–8 September 2022; pp. 203–208. [CrossRef]
31. Bolla, R.; Bruschi, R.; Davoli, F.; Lombardo, C.; Pajo, J.F.; Siccardi, B. Machine-Learning-Based 5G Network Function Scaling via Black- and White-Box KPIs. In Proceedings of the 21st Mediterranean Communication and Computer Networking Conference (MedComNet), Island of Ponza, Italy, 13–15 June 2023; pp. 143–150. [CrossRef]
32. Pinto, A.; Santaromita, G.; Fiandrino, C.; Giustiniano, D.; Esposito, F. Characterizing Location Management Function Performance in 5G Core Networks. In Proceedings of the IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), Phoenix, AZ, USA, 14–16 November 2022; pp. 66–71. [CrossRef]

33. Abdellatif, A.A.; Mohamed, A.; Erbad, A.; Guizani, M. Dynamic Network Slicing and Resource Allocation for 5G-and-Beyond Networks. In Proceedings of the 2022 IEEE Wireless Communications and Networking Conference (WCNC), Austin, TX, USA, 10–13 April 2022; pp. 262–267. [CrossRef]
34. Beaubrun, R. Technical Challenges and Categorization of 5G Mobile Services. In Proceedings of the 2022 Thirteenth International Conference on Ubiquitous and Future Networks (ICUFN), Barcelona, Spain, 5–8 July 2022; pp. 345–350. [CrossRef]
35. De Gaudenzi, R.; Luise, M.; Sanguinetti, L. The Open Challenge of Integrating Satellites into (Beyond-) 5G Cellular Networks. *IEEE Netw.* **2022**, *36*, 168–174. [CrossRef]
36. Fkih, F.; Al-Turaif, G. Threat Modelling and Detection Using Semantic Network for Improving Social Media Safety. *Int. J. Comput. Netw. Inf. Secur.* **2023**, *15*, 39–53. [CrossRef]
37. Shaikh, N.S.; Yasin, A.; Fatima, R. Ontologies as Building Blocks of Cloud Security. *Int. J. Inf. Technol. Comput. Sci.* **2022**, *14*, 52–61. [CrossRef]
38. Redefining Security KPIs for 5G Service Providers. Available online: https://www.helpnetsecurity.com/2019/11/19/5g-security-kpis/ (accessed on 19 November 2019).
39. Help Net Security. Average Data Breach Cost Has Risen to $3.92 Million. Available online: https://www.helpnetsecurity.com/2019/07/24/data-breach-cost/ (accessed on 24 July 2011).
40. Avkurova, Z.; Gnatyuk, S.; Abduraimova, B.; Fedushko, S.; Syerov, Y.; Trach, O. Models for early web-attacks detection and intruders identification based on fuzzy logic. *Procedia Comput. Sci.* **2022**, *198*, 694–699. [CrossRef]
41. Aurobindo, S. An introduction to intrusion detection. *Crossroads* **1996**, *2*, 3–7.
42. Kuypers, M.A.; Maillart, T.; Paté-Cornell, E. *An Empirical Analysis of Cyber Security Incidents at a Large Organization*; Department of Management Science and Engineering, Stanford University, School of Information: Stanford, CA, USA, 2016.
43. Doerrfeld, B. 5 Mean-Time Reliability Metrics to Follow. 7 July 2022. Available online: https://devops.com/5-mean-time-reliability-metrics-to-follow (accessed on 7 July 2023).
44. Hou, L.; Lao, Y.; Wang, Y.; Zhang, Z.; Zhang, Y.; Li, Z. Modeling freeway incident response time: A mechanism-based approach. *Transp. Res. Part C Emerg. Technol.* **2013**, *28*, 87–100. [CrossRef]
45. Oggerino, C. *High Availability Network Fundamentals*; Cisco Press: Indianapolis, IN, USA, 2001; 25p, ISBN 1-58713-017-3.
46. Azenkot, S.; Rector, K.; Ladner, R.; Wobbrock, J. PassChords: Secure multi-touch authentication for blind people. In Proceedings of the 14th international ACM SIGACCESS conference on Computers and Accessibility, Boulder, CO, USA, 22–24 October 2012; pp. 159–166.
47. Campos, L.M.; Ribeiro, L.; Karydis, I.; Karagiannis, S.; Pedro, D.; Martins, J.; Marques, C.; Armada, A.G.; Leal, R.P.; Lopez-Morales, M.J.; et al. Reference Scenarios and Key Performance Indicators for 5G Ultra-dense Networks. In Proceedings of the 12th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP), Porto, Portugal, 20–22 July 2020; pp. 1–5. [CrossRef]
48. Patel, A.; Qassim, Q.; Wills, C. A survey of intrusion detection and prevention systems. *Inf. Manag. Comput. Secur.* **2010**, *18*, 277–290. [CrossRef]
49. Alneyadi, S.; Sithirasenan, E.; Muthukkumarasamy, V. A survey on data leakage prevention systems. *J. Netw. Comput. Appl.* **2016**, *62*, 137–152. [CrossRef]
50. Lobato, A.G.P.; Lopez, M.A.; Sanz, I.J.; Cardenas, A.A.; Duarte, O.C.M.; Pujolle, G. An adaptive real-time architecture for zero-day threat detection. In Proceedings of the IEEE International Conference on Communications (ICC), Kansas City, MO, USA, 20–24 May 2018; pp. 1–6.
51. Kitchen, J.T.; Coogan, D.R.; Christian, K.H. The Evolution of Legal Risks Pertaining to Patch Management and Vulnerability Management. *Duq. L. Rev.* **2021**, *59*, 269.
52. Susanto, H.; Almunawar, M.N. *Information Security Management Systems: A Novel Framework and Software as a Tool for Compliance with Information Security Standard*; CRC Press: Boca Raton, FL, USA, 2018; 302p, ISBN 1771885777.
53. Perez, R.; Garcia-Reinoso, J.; Zabala, A.; Serrano, P.; Banchs, A. A monitoring framework for multi-site 5G platforms. In Proceedings of the IEEE European Conference on Networks and Communications (EuCNC), Dubrovnik, Croatia, 15–18 June 2020; pp. 52–56. [CrossRef]
54. Porambage, P.; Miche, Y.; Kalliola, A.; Liyanage, M.; Ylianttila, M. Secure Keying Scheme for Network Slicing in 5G Architecture. In Proceedings of the IEEE Conference on Standards for Communications and Networking (CSCN), Granada, Spain, 28–30 October 2019; pp. 1–6. [CrossRef]