Review

A Comprehensive Review of Cybersecurity Threats to Wireless Infocommunications in the Quantum-Age Cryptography

Ivan Laktionov * , Grygorii Diachenko , Dmytro Moroz , Iryna Getman

Posted Date: 28 July 2025

doi: 10.20944/preprints202507.2242.v1

Keywords: infocommunication; mobile networks; satellite communications; post-quantum cryptography; cybersecurity; hybrid cryptographic algorithms

Review

A Comprehensive Review of Cybersecurity Threats to Wireless Infocommunications in the Quantum-Age Cryptography

Ivan Laktionov [1,*], Grygorii Diachenko [2], Dmytro Moroz [1] and Iryna Getman [3,4]

[1] Department of Software of Computer Systems, Faculty of Information Technologies, Dnipro University of Technology, Av. Dmytra Yavornytskoho, 19, UA49005 Dnipro, Ukraine

[2] Department of Electric Drive, Faculty of Electrical Engineering, Dnipro University of Technology, Av. Dmytra Yavornytskoho, 19, UA49005 Dnipro, Ukraine

[3] Department of Computer Information Technologies, Donbas State Engineering Academy, Fedkovych Str., 9, UA41009 Ternopil (Kramatorsk), Ukraine

[4] Department of Digital Technologies and Project Decision Analysis, «Technical University «METINVEST POLYTECHNIC», METINVESTHOLDING LLC, Pivdenne Hwy, 80, UA69008, Zaporizhzhia, Ukraine

* Correspondence: laktionov.i.s@nmu.one

Abstract

The dynamic growth in the dependence of numerous industrial sectors, businesses, and critical infrastructure on infocommunication technologies necessitates the enhancement of their resilience to cyberattacks and radio-frequency threats. This article addresses a relevant scientific and applied issue, which is to formulate prospective directions for improving the effectiveness of cybersecurity approaches for infocommunication networks through a comparative analysis and logical synthesis of the state-of-the-art of applied research on cyber threats to the information security of mobile and satellite networks, including those related to the rapid development of quantum computing technologies. The article presents results on the systematisation of cyberattacks at the physical, signalling and cryptographic levels, as well as threats to cryptographic protocols and authentication systems. Particular attention is given to the prospects for implementing post-quantum cryptography, hybrid cryptographic models and the integration of threat detection mechanisms based on machine learning and artificial intelligence algorithms. The article proposes a classification of current threats according to architectural levels, analyses typical protocol vulnerabilities in next-generation mobile networks and satellite communications, and identifies key research gaps in existing cybersecurity approaches. Based on a critical analysis of scientific and applied literature, this article identifies key areas for future research. These include developing lightweight cryptographic algorithms, standardising post-quantum cryptographic models, creating adaptive cybersecurity frameworks and optimising protection mechanisms for resource-constrained devices within information and digital networks.

Keywords: infocommunication; mobile networks; satellite communications; post-quantum cryptography; cybersecurity; hybrid cryptographic algorithms

1. Introduction

1.1. Relevance of the Topic and Research Motivation

In today's world, wireless infocommunication technologies, including mobile and satellite communication networks, as well as Internet of Things (IoT) systems, support industrial, domestic and critical infrastructure. They serve global navigation systems, telemetry, general-purpose and specialised communication systems, transportation logistics, energy facilities, and more. Given the rapid growth in dependence of industry, business, transportation, logistics and telecommunications on wireless mobile and satellite communication technologies, the need to ensure their reliability and resilience against a wide range of cyberattacks and radio-frequency (RF) threats is becoming increasingly urgent. These threats include signal interception, jamming, spoofing, attacks on authentication protocols, cryptographic mechanisms and channel control systems.

Statistical studies demonstrate a sharp increase in the number of reported cyberattack incidents, highlighting the urgency of developing and deploying highly effective means to combat both cyber and RF threats. For example, according to the International Air Transport Association (IATA), in 2024, the number of global positioning system (GPS) jamming incidents increased by 1.75 times, and spoofing incidents grew fivefold compared to 2023. Overall, global GPS signal disruption events (jamming and spoofing) increased by 2.2 times between 2021 and 2024 [1,2]. Another analytical confirmation of this trend is presented in [3], which reports that global navigation satellite system (GNSS) jamming incidents rose more than fivefold in 2024. The authors of [3] emphasize that relatively simple and inexpensive jamming devices can effectively disrupt the operation of GNSS receivers using GPS and Galileo systems. According to current data from SeRo Systems, since mid-2023, GNSS signal distortion has been recorded almost daily, with a stable upward trend in the frequency of such incidents in the business, transport and industrial sectors starting in early 2024 [4].

Particular attention in this context should be given to the development of quantum attack technologies, which are rapidly advancing at present. According to National Institute of Standards and Technology (NIST) forecasts, up to 75% of current cryptographic algorithms used in mobile and satellite networks are expected to become vulnerable to quantum attacks within the next decade [5]. Although no widespread real-world cases of successful quantum attacks on mobile or satellite networks have been reported to date, there is a clear trend toward the active adoption of post-quantum standards. For instance, in 2023, NIST officially approved a set of algorithms as core post-quantum cryptographic (PQC) standards [6].

In response to the continuous increase in cyber threats in terms of both quantity and quality, the regulation of the security of mobile and satellite communications is being intensified. For instance, the International Telecommunication Union (ITU) is developing recommendations for cybersecurity in satellite channels, including physical layer protection and cryptographic requirements for telemetry channels [7,8]. The European Union Agency for Cybersecurity (ENISA) has published guidelines on the cybersecurity of satellite systems, covering aspects of the physical layer, access control, and cryptography [9]. The 3rd Generation Partnership Project (3GPP) has established standards that define cybersecurity measures for 5G networks, including authentication protocols, encryption and attack protection mechanisms [10]. Additionally, 3GPP has released an analytical report on the integration of quantum-resistant algorithms into 5G infrastructures [11].

The importance of improving cybersecurity in satellite and mobile networks is reinforced by findings in the scientific community, particularly in light of the growing threat posed by quantum computing and quantum-capable algorithms. For instance, the authors of [12] proposed a deep learning-based method for detecting GNSS spoofing, achieving an accuracy of up to 99%. In [13], the security challenges of satellite communication are examined, emphasizing the need for cryptographic solutions resilient to quantum attacks. The study in [14] focuses on optimising PQC algorithms for resource-constrained IoT devices.

Therefore, considering the rapid increase in cyberattacks on satellite and mobile networks, as well as the accelerated development of quantum technologies, ensuring their cryptographic resilience has become critically important. Wireless infocommunication networks operating under constrained resources and without constant supervision are particularly vulnerable. Addressing this challenge requires not only updating communication protocols to post-quantum standards but also rethinking network architectures, integrating intelligent attack detection systems, and establishing regulatory requirements at the international level.

1.2. Historical Development, Current State and Future Trends

During the rapid scientific and technological progress, wireless infocommunication networks, in particular mobile and satellite networks, have become the foundation of the global digital transformation of businesses, manufacturing enterprises, and infrastructure. At the same time, these networks have become the focus of cyberattacks, which has driven the development of data and information protection methods as well as electronic warfare techniques to combat interception, spoofing and sophisticated cryptographic attacks. The historical evolution of security in these systems demonstrates a gradual transition from basic authentication mechanisms to the integration of PC algorithms, artificial intelligence (AI) and zero-trust architectures. In this context, there is an urgent need for a comprehensive analysis of the evolutionary path and current challenges, while considering future directions in the field of cybersecurity for wireless infocommunication networks. A graphical interpretation of this evolution, created based on the analysis and systematisation of scientific works [14–19], is shown in Figure 1.

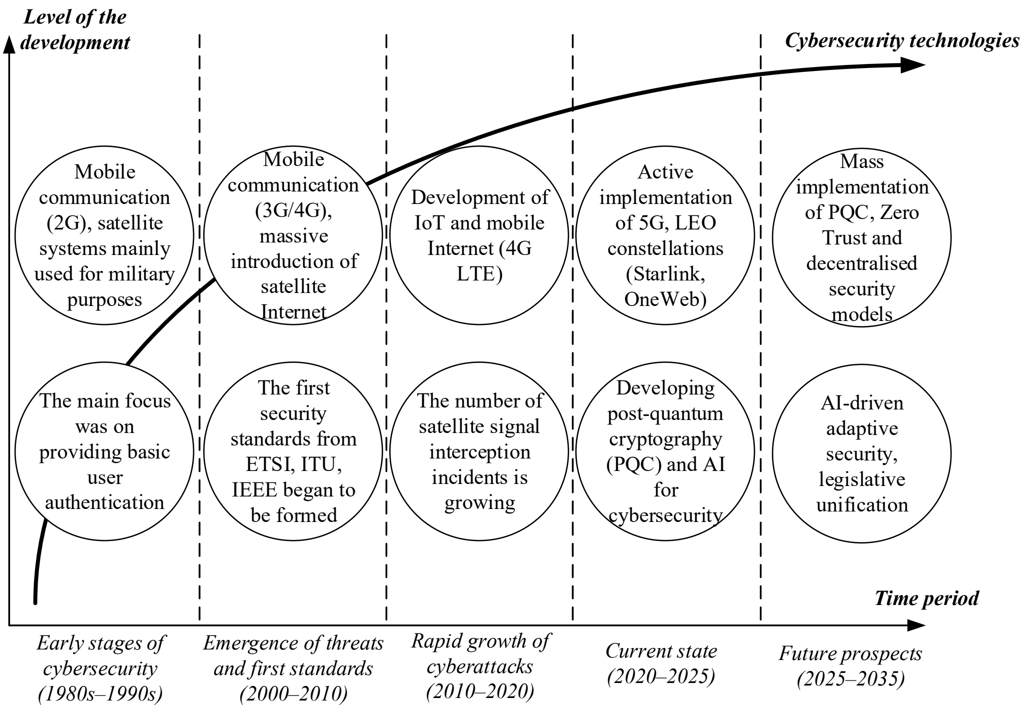

Level of the development
Cybersecurity technologies
Mobile communication (2G), satellite systems mainly used for military purposes
Mobile communication (3G/4G), massive introduction of satellite Internet
Development of IoT and mobile Internet (4G LTE)
Active implementation of 5G, LEO constellations (Starlink, OneWeb)
Mass implementation of PQC, Zero Trust and decentralised security models
The main focus was on providing basic user authentication
The first security standards from ETSI, ITU, IEEE began to be formed
The number of satellite signal interception incidents is growing
Developing post-quantum cryptography (PQC) and AI for cybersecurity
AI-driven adaptive security, legislative unification
Time period
Early stages of cybersecurity (1980s–1990s)
Emergence of threats and first standards (2000–2010)
Rapid growth of cyberattacks (2010–2020)
Current state (2020–2025)
Future prospects (2025–2035)

Figure 1. Graphical interpretation of historical, current and future trends in cybersecurity.

A logical systematisation of recent scientific works confirms that cybersecurity for wireless infocommunication networks has transformed into a synergetic discipline that combines classical and physical network protection methods, innovative cryptography based on post-quantum and AI-driven adaptive approaches, and adaptive regulatory frameworks for responding to cyber threats. This combined approach enables effective resistance against existing attacks (such as jamming and spoofing), adapts to potential quantum threats, and ensures the reliable operation of critical infrastructures on a global scale.

1.3. Global Issues of the Sustainable Development of Cybersecurity of Infocommunicanion Networks

In the context of rapid scaling and increasing technological complexity of infocommunication (mobile and satellite) networks, their cybersecurity is becoming critically important. The significant evolution of threats from traditional DDoS attacks to sophisticated quantum and spoofing influences demands the development and implementation of new approaches to security at both the physical level of devices and the levels of network protocols and software. In this regard, the scientific community and standards developers are focusing on a number of key issues, including protection against electronic warfare attacks, the implementation of PQC and the autonomous detection of threats using machine learning (ML) and AI algorithms. Based on the analysis and logical systematisation of relevant scientific sources [20–26], a graphical interpretation has been developed, shown in Figure 2, which illustrates current issues, promising approaches and the expected practical outcomes that can be achieved through modern research in the field of cybersecurity for infocommunication networks.

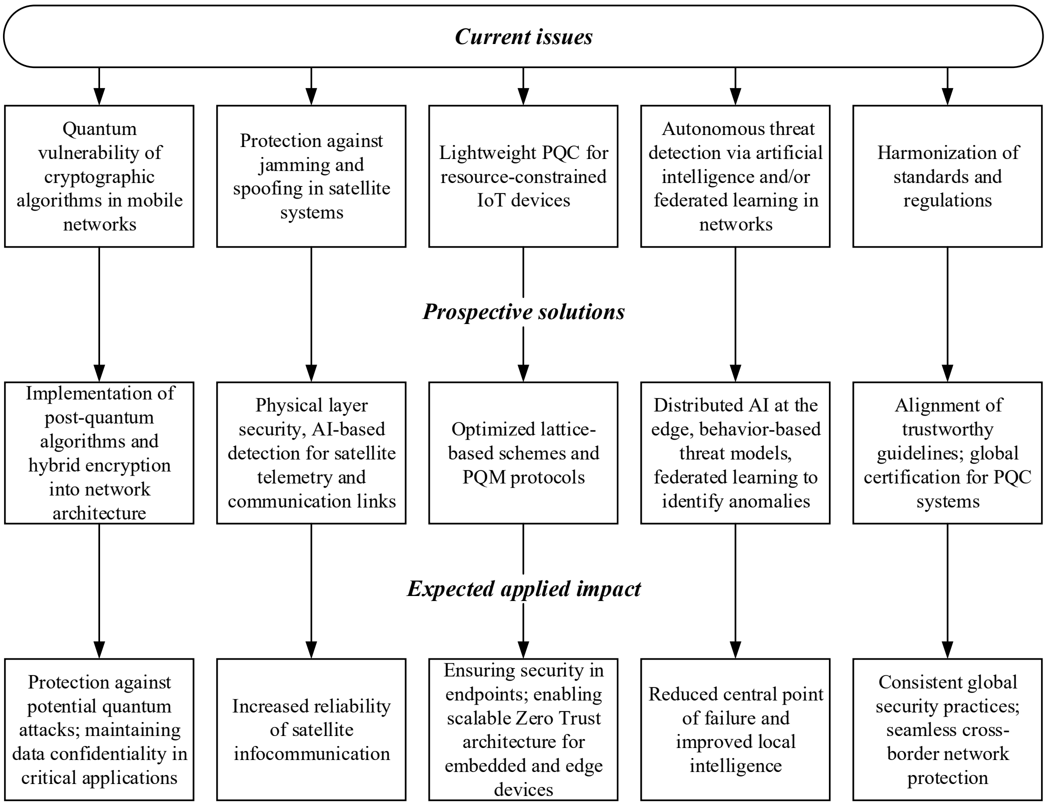

Current issues
Quantum vulnerability of cryptographic algorithms in mobile networks
Protection against jamming and spoofing in satellite systems
Lightweight PQC for resource-constrained IoT devices
Autonomous threat detection via artificial intelligence and/or federated learning in networks
Harmonization of standards and regulations
Prospective solutions
Implementation of post-quantum algorithms and hybrid encryption into network architecture
Physical layer security, AI-based detection for satellite telemetry and communication links
Optimized lattice-based schemes and PQM protocols
Distributed AI at the edge, behavior-based threat models, federated learning to identify anomalies
Alignment of trustworthy guidelines; global certification for PQC systems
Expected applied impact
Protection against potential quantum attacks; maintaining data confidentiality in critical applications
Increased reliability of satellite infocommunication
Ensuring security in endpoints; enabling scalable Zero Trust architecture for embedded and edge devices
Reduced central point of failure and improved local intelligence
Consistent global security practices; seamless cross-border network protection

Figure 2. Graphical interpretation of current issues in cybersecurity, prospective solutions and expected applied impact of their solving.

Thus, from the analysis of the block diagram presented in Figure 2, it is evident that modern approaches to the development of cybersecurity mechanisms for infocommunication networks are multifaceted and based on a synthesis of quantum cryptography algorithms, ML, AI and regulatory frameworks. Successfully addressing these issues will not only enhance the security level of infocommunication networks but also improve the level of trustworthiness in networked digital technologies during cross-layer and machine-to-machine interactions.

1.4. Main Aim, Objectives and Approaches to the Research

The main aim of this article is to outline the prospects for developing methods and means to enhance the effectiveness of cybersecurity approaches for infocommunication networks through a comparative analysis and logical systematisation of the state-of-the-art of applied scientific research on relevant cyber threats to the information security of mobile and satellite networks, particularly in light of the active advancement of quantum computing technologies. Unlike existing studies, this article focuses specifically on analysing cyber threats across the architectural layers of large-scale infocommunication networks. These layers include the physical layer, vulnerabilities in cryptographic protocols and authentication mechanisms, and the potential implementation of post-quantum cybersecurity methods.

The following research tasks have been identified and addressed in this work through the decomposition of the main aim of the article:

1. Analysis and logical systematisation of historical, current, and future trends in cybersecurity, followed by the formulation of relevant challenges and potential solutions to enhance the cybersecurity of infocommunication networks.

2. Analysis and architectural decomposition of the structure and functional features of mobile and satellite networks, which have gained widespread practical application in current conditions.

3. Review and detailing of the most common types of cyberattacks, such as spoofing, jamming, man-in-the-middle and others.

4. Comparative analysis and logical systematisation of current scientific research and practical solutions that demonstrate real-world effectiveness and development prospects for cryptographic mechanisms.

5. Substantiation of promising research directions for improving cybersecurity means in mobile and satellite communication systems, including the potential transition to post-quantum cryptography.

The object of the research is the network information processes occurring within infocommunication technologies (mobile and satellite) that require enhanced levels of cybersecurity.

The subject of the research is the mechanisms for ensuring information security in mobile and satellite communication networks and data-oriented communications, specifically: vulnerabilities in network communication and authentication protocols; classification of cyber threats at the physical and protocol levels; approaches and prospects for the development and implementation of post-quantum and cross-layer protection technologies.

2. Methodology

2.1. Information Sources and Search Strategy

The research presented in this article is devoted to a comprehensive information analysis and systematisation of modern approaches, methods and means for ensuring cybersecurity in mobile and satellite infocommunication technologies, taking into account current conditions and the prospects of quantum computing development. The fundamental methodological approaches used in this study include: information and analytical search and review, comparative analysis and logical synthesis of known results in the field of research and development related to cybersecurity mechanisms for data and message transmission channels, cryptographic protocols and authentication tools.

This scientific work involves the identification and systematisation of relevant scientific and analytical information sources, corresponding to the current state of the problem of vulnerabilities in mobile and satellite communication networks to major types of cyber threats, such as jamming, spoofing, man-in-the-middle (MITM), and distributed denial of service (DDoS) attacks, as well as potential cryptographic threats arising from the emergence of quantum computing technologies. The key criteria and characteristics of the information search and literature analysis used in this article are presented in Table 1.

The logical structure of this research is based on the principle of decomposing the subject area into the following main stages, as shown in the form of a block diagram in Figure 3.

Table 1. Characteristics of search and analysis of known scientific information sources.

Category	Criteria for the Selection and Evaluation of Scientific Literature
Primary publication time range	2020–2025
Extended publication time range	2015–2025
Scientometric databases	Web of Science, Scopus
Main digital libraries	MDPI, Elsevier, IEEE Xplore, ArXiv

Types of literature	Scientific papers in peer-reviewed periodicals, international conference proceedings, preprints, information and analytical web resources
Primary language	English
Main subject areas	Cybersecurity, computer networks and communications, signal processing, artificial intelligence
Additional subject areas	Computer science applications, control and systems engineering, electrical and electronic engineering
Main search query	Cybersecurity AND (Post-quantum cryptography OR PQC) AND (Mobile communication OR Satellite communication OR Infocommunication)
Additional keywords	5G, 6G, LTE, RF spoofing, security, IoT encryption, GNSS jamming, cryptography algorithms, communication protocols, cyberattacks, network

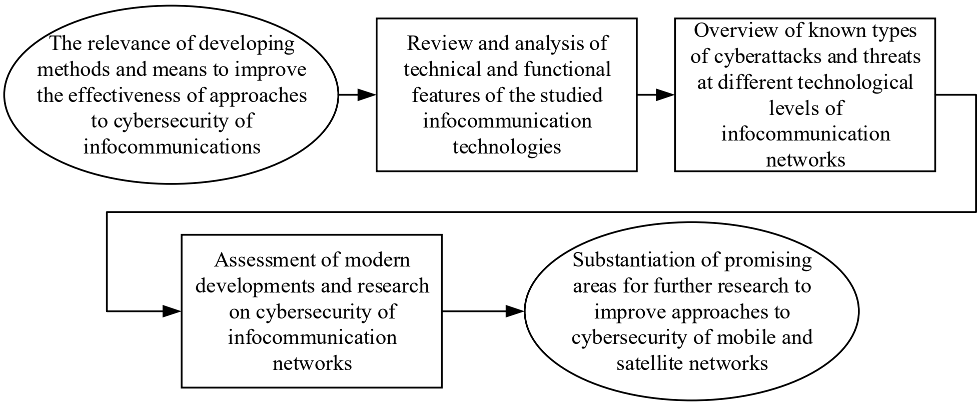

The relevance of developing methods and means to improve the effectiveness of approaches to cybersecurity of infocommunications
Review and analysis of technical and functional features of the studied infocommunication technologies
Overview of known types of cyberattacks and threats at different technological levels of infocommunication networks
Assessment of modern developments and research on cybersecurity of infocommunication networks
Substantiation of promising areas for further research to improve approaches to cybersecurity of mobile and satellite networks

Figure 3. Generalised logical structure of the article's research.

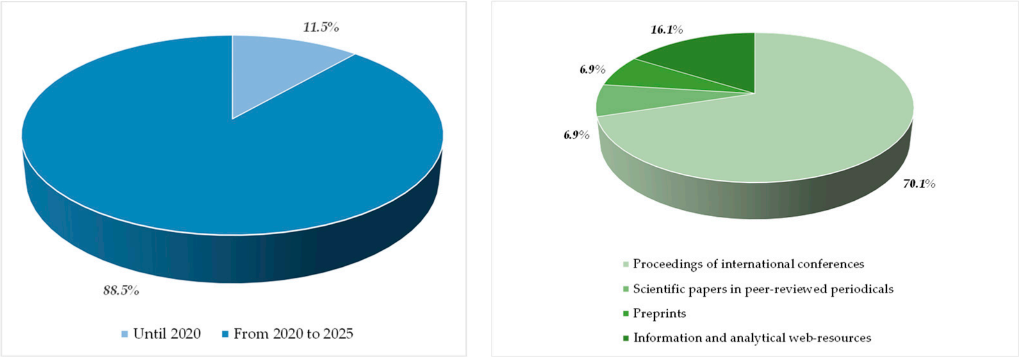
An additional factor considered during the information search was the globalisation of the development of cybersecurity methods and means, specifically the diversity of infocommunication systems and network types, as well as the geographical scope of the research. The conducted information analysis encompasses applied scientific studies by researchers from various countries with advanced cyber technologies, including those in Europe, Asia and North America.

Such a comprehensive approach made it possible to identify the most promising methods, means and technologies for cybersecurity of mobile and satellite infocommunication networks, as well as to highlight issues that require further development in light of the research nature of emerging technological challenges.

2.2. Data Items

This article analysed 87 scientific, applied research, and information and analytical publications in accordance with the characteristics and criteria presented in Table 1. A graphical interpretation of the statistical analysis of the processed sources based on the main indicative indicators is shown in Figure 4.

The obtained statistical results confirm that this article, of a review nature, focuses on the most relevant global achievements of the past five years in the field of cybersecurity for mobile and satellite communications, taking into account the wide geographical distribution of scientific publications in peer-reviewed and cited journals.



a) Years of publications

b) Types of publications

Figure 4. Graphical interpretation of the analysed literature sources.

3. Technical and Functional Features of the Studied Infocommunication Technologies

3.1. Distinctive Features of Mobile Communication

In modern conditions, mobile services are the functional and communication basis of infrastructure facilities and processes for various purposes. The key characteristics of modern mobile networks and technologies include global coverage, topology reconfiguration and mobility support, which ensure reliable and continuous data and information transmission in dynamic motion. Mobile communication networks are a multi-level architecture based on radio access facilities, base stations and the network core, as well as standardised communication protocols and traffic encryption and authentication tools [27,28], as summarised in Figure 5.

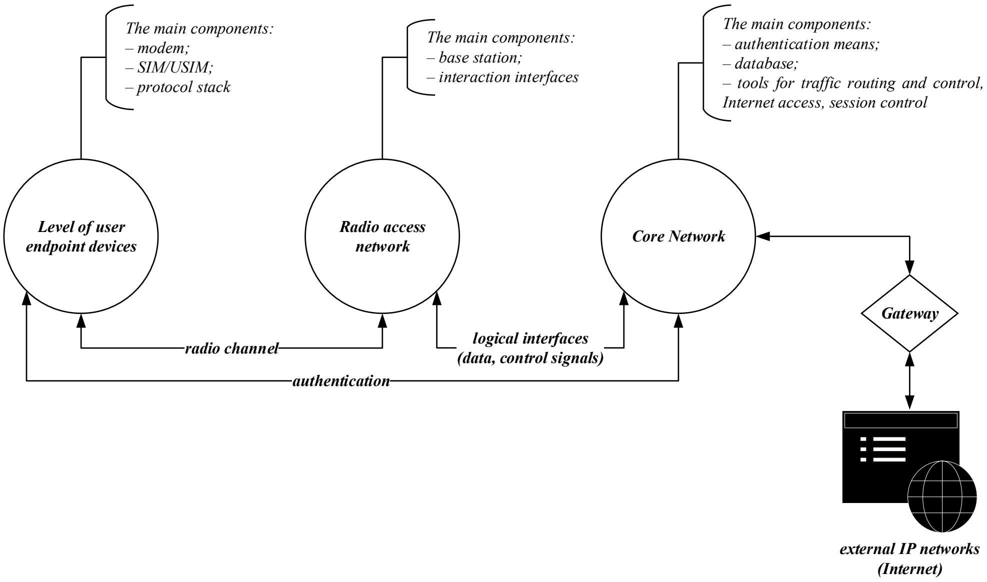


Figure 5. Generalised mobile infocommunications architecture.

From the perspective of mobile network cybersecurity, it is important to emphasize that wireless access, in particular in 5G and LTE, is primarily carried out through open transmission environments (radio channels), which are vulnerable to attacks such as jamming, eavesdropping, spoofing and MITM. Typical authentication in mobile networks is based on the SIM card and the AKA protocol, which, despite its long-standing development and use, remains susceptible to cyberattacks. The main vulnerabilities of LTE and 5G networks today include user identity compromise, signaling-level attacks, lack of full end-to-end encryption, replay attacks on authentication and others [29–31].

doi:10.20944/preprints202507.2242.v1

In the context of the rapid development of quantum computing and the growing potential of related threats, special attention should be paid to the fact that mobile networks widely use public-key cryptographic algorithms such as RSA and ECC, which can be broken using Shor's algorithm. As most mobile networks currently rely on a centralised key control mechanism, the advent of quantum computing technologies poses a potential threat to the long-term security of communication channels, particularly for encrypted traffic that is stored [32].

Moreover, the development of device-to-device infocommunication technologies within the framework of the Internet of Things (IoT) concept in mobile networks necessitates consideration of the autonomous energy constraints of devices. This, in turn, complicates the integration of PQC algorithms without compromising performance [33–35].

Thus, the main tasks in enhancing the effectiveness of mobile communication cybersecurity mechanisms in the face of quantum threats include: reducing the vulnerability of radio channels, ensuring cryptographic resilience, adapting authentication protocols and providing sufficient performance of PQC algorithms when deploying them on energy-constrained devices.

3.2. Distinctive Features of Satellite Communication

Satellite communication is a global technology used in infocommunication across a wide range of key sectors, including industry, business and infrastructure. The architecture of satellite communication systems differs significantly from that of mobile networks due to the involvement of orbital platforms, which determines the spatial scalability of their structural and functional design. In general, the hierarchical structure of satellite communication systems includes space, ground and user segments [36,37], as illustrated in the graphical interpretation in Figure 6.

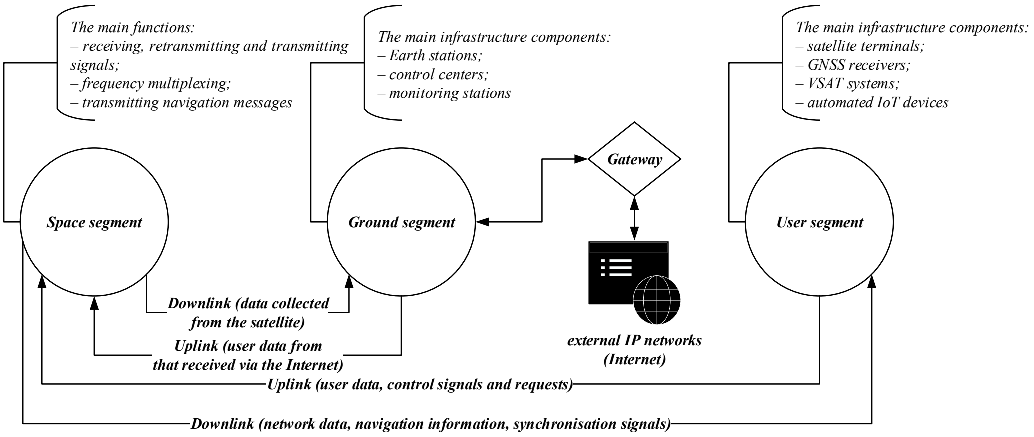

The main functions:
– receiving, retransmitting and transmitting signals;
– frequency multiplexing;
– transmitting navigation messages
The main infrastructure components:
– Earth stations;
– control centers;
– monitoring stations
The main infrastructure components:
– satellite terminals;
– GNSS receivers;
– VSAT systems;
– automated IoT devices
Gateway
Space segment
Ground segment
User segment
Downlink (data collected from the satellite)
Uplink (user data from that received via the Internet)
external IP networks (Internet)
Uplink (user data, control signals and requests)
Downlink (network data, navigation information, synchronisation signals)

Figure 6. Generalised satellite infocommunications architecture.

From the perspective of satellite network cybersecurity, it is important to emphasize that their modern architecture is highly susceptible to cyber threats at all levels [38,39], which necessitates the development and implementation of protection methods and means against cyberattacks such as jamming, spoofing, eavesdropping, MITM and modchip attacks. A comprehensive review presented in [40] confirms that satellite communication systems are targeted by attacks at the space segment, the ground segment, and across communication links between these segments. The main types of such cyber threats include DDoS, spoofing, eavesdropping and the compromise of control commands.

Thus, satellite communication systems require the development and implementation of a comprehensive cybersecurity approach that includes data protection mechanisms, signal encryption and authentication.

3.3. *Classification of Cyberthreats*

A hierarchical classification of threat types to mobile and satellite communication systems has been developed based on a comparative analysis and logical synthesis of well-known and recent scientific studies [41–44], as shown in Table 2.

Table 2. Types of cyberthreats in mobile and satellite communications by architectural levels.

Hierarchical level	Mobile communication	Satellite communication
Physical	Radio channel jamming, signal spoofing, passive eavesdropping, signal distortion or delay (signal overshadowing)	jamming of satellite signals, radio interception of broadcast signals, unauthorised signal capture in receivers, spoofing of navigation or relay data
Channel	use of fake base stations for a 'man-in-the-middle' cyberattack, impact on retransmission algorithms (RLC-layer manipulation), resource exhaustion through creation of fake connections	injection of malicious data into open channels, formation of false messages
Signal	forced downgrading of encryption or technology, attacks on the handover process to overload	compromise of telemetry, substitution of control signals for navigation systems
Authentication	vulnerabilities of authentication protocols, lack of encryption at the level of certain messages	absence or weak means of checking the integrity of commands
Infrastructure	compromise of kernel nodes, attacks on key management systems, DNS spoofing	disruption of communication between network segments, unauthorised access to satellite system gateways

Thus, from Table 2, it is evident that all hierarchical levels of mobile and satellite communication networks are vulnerable to cyberattacks. For example, the physical layer is the most vulnerable in an open-air environment, the data link (channel) layer can be exploited for overload or interception of information, the signalling layer can potentially be used for creating false messages or altering connection parameters, the authentication layer is a weak link in terms of traffic protection and authentication and it is the most vulnerable to cyberattacks based on quantum algorithms.

4. Classification and Characterisation of Cyberthreats at the Architectural Levels of Information and Communication Systems

4.1. *Threats at the Physical Level*

The physical layer of mobile and satellite infocommunication networks is particularly vulnerable to cyberattacks due to the potential availability of hardware and open air. The main modern cyber threats and vectors of attack development include the following: jamming, spoofing, overshadowing and passive eavesdropping. In this article, based on the analysis and systematisation of the results presented by the authors in scientific articles [42,45–48], a generalised logical block-diagram is formed that reveals the content of the characteristics, consequences and potential approaches to cyber defence of the physical layer of mobile and satellite communication networks, which is shown graphically in Figure 7.

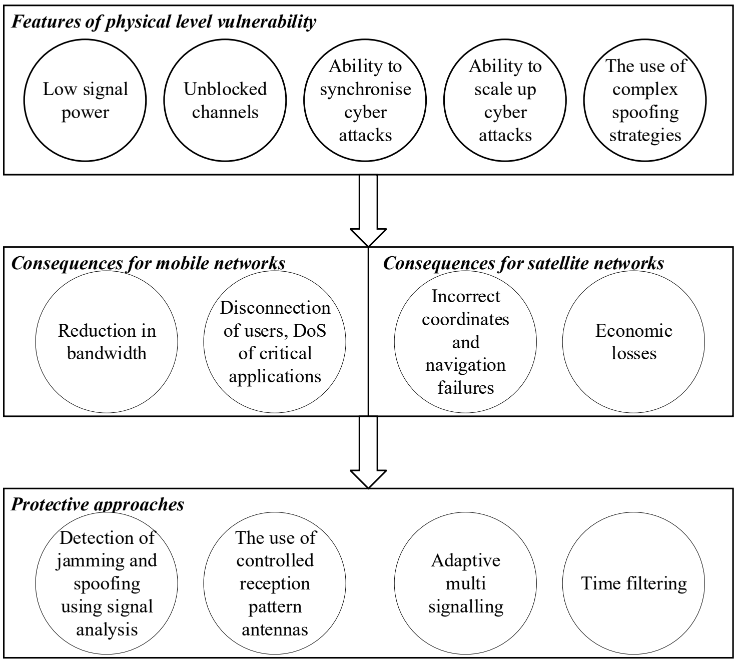

Features of physical level vulnerability
Low signal power
Unblocked channels
Ability to synchronise cyber attacks
Ability to scale up cyber attacks
The use of complex spoofing strategies
Consequences for mobile networks
Reduction in bandwidth
Disconnection of users, DoS of critical applications
Consequences for satellite networks
Incorrect coordinates and navigation failures
Economic losses
Protective approaches
Detection of jamming and spoofing using signal analysis
The use of controlled reception pattern antennas
Adaptive multi signalling
Time filtering

Figure 7. Graphical interpretation of cyber threats and methods of resisting them at the physical level.

The information shown in Figure 7 proves that the physical layer of mobile and satellite communication networks is both an endpoint for cyberattacks and a location that requires comprehensive protection to ensure the information stability and security of these networks as a whole.

4.2.'Man-in-the-Middle' in Radio Channels

The essence of 'Man-in-the-Middle' (MITM) cyberattacks in radio channels of information and communication networks is to intercept and modify traffic between two parties to communication without being noticed. In the context of mobile and satellite communications, this type of cyber threat is mostly manifested through the creation of fake base stations in mobile networks or the retransmission of an altered signal in satellite networks. These attacks allow not only passive eavesdropping on traffic, but also actively changing messages, authentication or navigation coordinates. Such attacks are particularly dangerous due to the lack of two-way authentication in most radio layer protocols [49,50].

4.3. DDoS and Jamming Cyberthreats

The essence of cyberattacks such as DDoS (Distributed Denial of Service) and jamming is the targeted disruption of the availability of a radio channel or service. In the case of mobile networks, DDoS attacks can be carried out using two main variations: signal-level overload or jamming of physical-layer frequency resources [51,52]. In satellite networks, RF-jamming is most often used, during which stronger signals are created at the receiving frequency, making it impossible to receive weak signals from satellites [53,54]. These types of cyberattacks are particularly influential and dangerous in the context of critical services and infrastructure, such as navigation, flight control, logistics, power system synchronisation and others. Effective counteraction to these attacks requires the implementation of an integrated approach using adaptive frequency hopping algorithms, directional antennas and signal anomaly detection means.

4.4. Cyberthreats in Cryptographic Protocols and Authentication

Cyberthreats in cryptographic protocols and authentication tools relate to the information processes of establishing the degree of trust, exchanging cryptographic keys, encrypting and verifying the authenticity of the parties. In information and communication networks, such vulnerabilities can lead to interception or loss of data, breach of confidentiality or substitution of a user's device or identity [55–57]. Based on the analysis, a logical chain detailing threats in cryptographic protocols and authentication in mobile and satellite communication networks, as well as current approaches to protecting against these types of cyber threats, as shown in Figure 8, has been proposed.

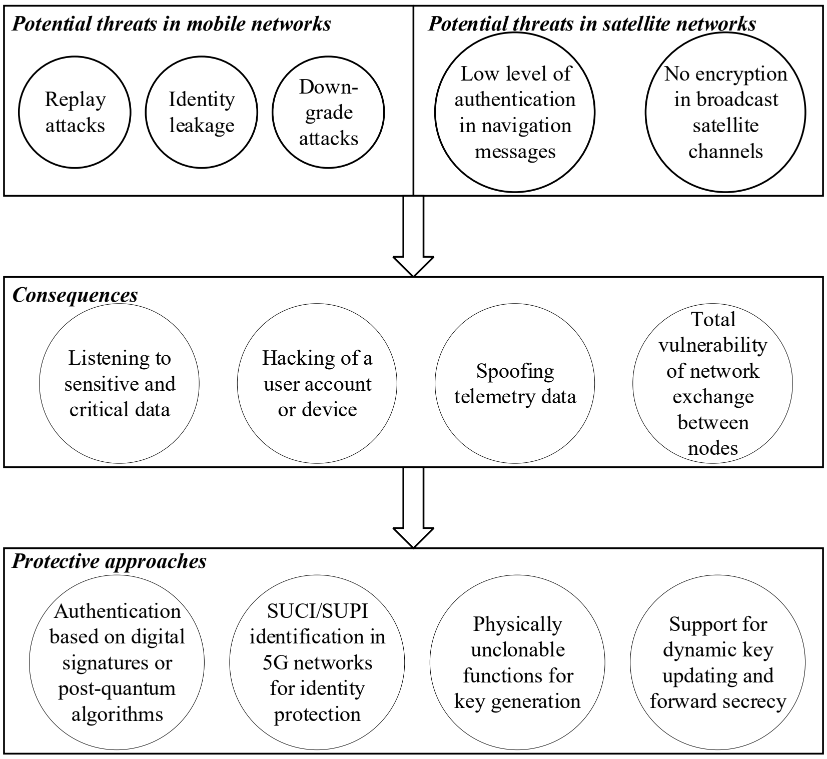

Potential threats in mobile networks
Replay attacks
Identity leakage
Down-grade attacks
Potential threats in satellite networks
Low level of authentication in navigation messages
No encryption in broadcast satellite channels
Consequences
Listening to sensitive and critical data
Hacking of a user account or device
Spoofing telemetry data
Total vulnerability of network exchange between nodes
Protective approaches
Authentication based on digital signatures or post-quantum algorithms
SUCI/SUPI identification in 5G networks for identity protection
Physically unclonable functions for key generation
Support for dynamic key updating and forward secrecy

Figure 8. Graphical interpretation of cyber threats in cryptographic protocols and authentication and methods of resisting them.

4.5. Problems of Symmetric and Asymmetric Cryptography

Symmetric cryptographic algorithms, such as AES and ZUC, are widely used in mobile networks, including those based on LTE and 5G technologies, to protect network traffic. Such algorithms are characterised by high performance and low resource consumption, which is necessary when used in mobile devices and networks with a large number of connected devices. However, their main limitation is the risk of key compromise, since one common key is used for encryption and decryption, and the key exchange process can be a target of cyberattacks. In addition, symmetric systems do not provide the impossibility of refusing to act, and in networks with a significant number of devices, they require additional research in terms of their scalability, which is critical for satellite or cloud mobile architectures [58–60].

Asymmetric cryptographic algorithms, such as RSA, ECDSA, and ECC, separate public and private keys, allowing for digital signatures and secure key exchange without prior joint encryption. Such algorithms are the cryptographic basis of many authentication mechanisms in 5G mobile networks. The main limitation of such algorithms is the significant computational load, which becomes critical in systems with autonomous power supply [58,61]. In many practical cases, mobile devices are not able to effectively implement asymmetric cryptographic operations without additional hardware acceleration, which leads to increased power consumption. In addition, classical asymmetric algorithms, such as RSA and ECC, are not resistant to quantum attacks, which necessitates the transition to PQC algorithms, which are even more complex in terms of computational load.

4.6. Quantum Challenges and Post-Quantum Cryptography

The significant increase in the power of quantum computing has increased the relevance of cyber threats to the cryptographic security of information and communication networks, including mobile and satellite networks. Public-key cryptographic algorithms (RSA and ECC) can be cracked using Shor's algorithm, calling into question the confidentiality of communications. In response, two main strategies for combating quantum cyber threats have been developed: implementing cryptographic algorithms that are resistant to quantum attacks (PQC) [62–64], and using a combination of classical and PQC algorithms in hybrid mode [65,66].

It is worth noting that to date, the results of practical testing of PQC algorithms are already known, confirming their effectiveness and potential for further scaling. Such examples include Hybrid Mode Quantum-safe Technology, which was tested in the conditions of SoftBank Corp. and SandboxAQ (Japan) [67], as well as the integration of PQC algorithms into 5G telecommunications networks, which was conducted in the conditions of SK Telecom (Republic of Korea) [68]. These studies and similar ones demonstrate the potential ability of PQC algorithms to integrate into existing network infrastructure, which is confirmed by analytical studies [69].

In satellite networks, the processes of authenticating TTC (Telemetry, Tracking and Command) signals and encrypting telemetry data are especially important; therefore, the development and implementation of PQC algorithms also play a key role in ensuring the cryptographic resilience of satellite channels at all functional levels [70].

It should be noted, however, that quantum computing poses a significant threat to existing information and communication systems. However, the rapid development of PQC algorithms, particularly those focusing on hybrid implementation, has already demonstrated their effectiveness and practicality in mobile and satellite networks.

5. Evaluation of Existing Research Results

5.1. Systematic Analysis of the Results of Scientific and Applied Research

The analysis and logical synthesis of the results of scientific and applied research and development is one of the key stages in understanding the current state and future prospects of cybersecurity technologies for mobile and satellite communication networks, taking into account quantum challenges. A comprehensive study and analysis of relevant scientific sources allows for identifying the effectiveness of specific algorithms, practical limitations, the level of integration into infrastructure and existing challenges in adapting post-quantum solutions. For this purpose, the present study employed a structured methodology to analyse relevant scientific research results that meet the following criteria: validity and thematic relevance of the source, citation frequency of the scientific work, industry orientation of the research, degree of applied impact, reliability of obtained results and publication date. The results of the critical analysis and logical systematisation of known research findings regarding the current state and prospects of cybersecurity development for information and communication networks, including the use of PQC algorithms, are shown in Table 3.

Table 3. Results of critical analysis and logical systematisation of known research results on the current state and prospects of development of cyber defence of infocommunication networks.

The subject of the study	Technologies and approaches used	Scientific and applied effect obtained	References
Approaches to the utilisation of potential post-quantum key encapsulation mechanisms and digital signature algorithms to	Public-key infrastructures (PKI), IoT, PQC	It has been proven that a rational combination of several DSAs yields the most energy-, latency-, and memory-efficient public key infrastructure, and	[71]

modern low-power IoT infrastructure		that isogeny-based, code-based, and lattice-based algorithms can be efficiently implemented on low-power IoT edge devices equipped with off-the-shelf Cortex-M4 microcontrollers while still ensuring acceptable battery life	
GNSS spoofing detection technologies using RF interference and fingerprinting	Application of machine learning based on RF fingerprinting and CNN for identification of fake signals	It has been proven that the methods of fingerprinting proposed by the authors can increase the detection accuracy of existing methods from 95.68 % to 99.7 % and can be combined with other methods to improve the overall performance of detection systems	[43]
A systematic analysis of methods for detecting cyberthreats such as jamming and spoofing in GNSS	Comparative analysis and systematic generalisation of methods based on indicators using direction of arrival (DoA), time of arrival (ToA) and National Marine Electronics Association (NMEA) messages analysis	The selected methods are organized and classified based on specific parameters and characteristics, with particular emphasis on the latest developments in the field	[42]
Technologies and approaches to GNSS spoofing detection based on ML classification algorithms.	Using signal pre-processing based on wavelet transform and SVM/CNN models for the classification of abnormal signal behaviour	A data-driven classifier has been proposed, combining a parallelised deep learning model with a clustering algorithm to estimate spoofing signal parameters. Experiments show it outperforms existing methods, particularly at moderate to high signal-to-noise levels	[72]
Detecting the reaction of a commercial 5G radio system to jamming and determining the jamming signal strength required to disrupt 5G communications	5G, multiple-input multiple-output antenna operating at the 3.6 GHz frequency band	The authors proved that the 5G radio system has been able to adapt to the interference by lowering the modulation and coding order until a breaking point was reached, at which the interference signal overwhelmed the user equipment signal in the uplink, resulting in a 5G connection failure.	[73]
A flexible dual-layer QKD-PQC Architecture for secure and stable site-to-site communication	Quantum Key Distribution (QKD) and Post-Quantum Cryptography (PQC)	The authors developed a modular, hybrid, and adaptive protocol that combines QKD with PQC, enabling uninterrupted quantum-safe key exchanges even in challenging network	[74]

		environments where traditional QKD methods often fail	
An approach to the transformational transition from classical to PQC in 5G-enabled IoT networks, taking into account current solutions, challenges and development prospects.	5G, IoT, PQC, QKD	The authors provided a comprehensive survey of a structured roadmap for quantum-secured communication in 5G-enabled IoT systems, encompassing current research developments, enabling technologies, security threats, and the latest quantum-based solutions and initiatives	[75]
The practicality of implementing post-quantum cryptography on resource-constrained devices commonly found in mobile and IoT networks	ARM-based platforms, PQC, IoT	The authors analysed and evaluated the performance and message sizes of selected post-quantum key exchange schemes on various ARM-based platforms.	[76]
Applied evaluation of PQK encapsulation for enhancing security in 5G/6G core networks	5G, 6G, PQK, PQC	This study details the integration process, emphasizing the latency characteristics of various PQC encapsulations during the initial handshakes between virtual network functions and their impact on packet size and relevance within 5G environments. The findings reveal only a minimal increase in UE connection setup time and a modest rise in data usage, suggesting that the security advantages of incorporating PQC into 5G and 6G core services significantly outweigh the associated performance trade-offs.	[32]
An approach to PQC blockchain framework for service orchestration across multi-cloud networks	PQC, blockchain, cloud technologies	This paper investigates managing network services across multiple administrative domains using blockchain networks secured by PQC. Employing a PQC algorithm leveraging Toom-Cook parallelization at various security levels demonstrates that Quorum achieves lower average write times compared to Ethereum and Hyperledger	[77]

Approaches to standardisation and performance evaluation of PQC algorithms	PQC, information and communications technology	This research reviewed the global efforts in designing and standardising quantum-safe cryptography algorithms and analysed the performance of key candidates. It has been highlighted that most quantum-safe algorithms require more CPU, memory, and larger keys, and aim to assess their overall feasibility.	[78]
A novel proof-of-concept semiconductor implementation that meets the power consumption, resource efficiency, and PQC security requirements for Industrial IoT applications.	PQC, industrial IoT (IIOT)	This work introduces a novel semiconductor proof-of-concept that addresses resource usage, power efficiency, and PQC security requirements for IIoT applications. The study details the RTL architecture of the CRYSTALS-Dilithium IP and develops a System-on-Chip integrating a RISC-V CPU with this IP to evaluate PQC feasibility on resource-constrained IIoT hardware.	[79]
An approach to the practical deployment of PQC algorithms in wireless communication security	PQC, PQC–AES hybrid schemes, wireless communication networks	This paper presents a novel framework for standalone and hybrid PQC–AES public-key encryption protocols. Results show improved balance between security and performance compared to traditional methods, supported by a thorough security analysis confirming their robustness against various attacks.	[80]

It is important to emphasize that the results of applied scientific research analysed in Table 3 represent well-validated approaches and the corresponding achieved effects in the field of PQC implementation. However, they do not constitute an exhaustive list of existing approaches and solutions in this domain. Rather, they serve as an illustration of the current state and development trends of PQC technologies for mobile and satellite networks. These results make it possible to identify consistent trends in the evolution of methods and means for creating and implementing PQC in these networks, which are systematically manifested in the following directions:

– deployment of PQC algorithms on computationally resource-constrained devices (e.g., IoT and ARM platforms), with a focus on energy efficiency, key size, and performance;

– use of hybrid cryptographic approaches and schemes (PQC-AES) for comprehensive optimisation of cybersecurity based on security and performance indicators;

– application of PQC in 5G and 6G mobile technologies, taking into account delays in key exchange processes, packet size and practical feasibility of implementation;

– orchestration of cryptographic services in cloud and multi-administrative environments using PQC-enhanced blockchain solutions;

– studying the possibility of standardising PQC algorithms with an assessment of their effectiveness in real-world applications;

– improving the protection of satellite navigation systems using machine learning algorithms and post-quantum methods to counter cyberattacks such as spoofing and jamming;

– development of adaptive QKD-PQC protocols for secure cross-level and inter-node communication in complex network conditions.

Thus, these scientific papers (see Table 3) reflect current achievements and outline key areas for further research in the field of post-quantum protection of information and communication technologies.

5.2. Current Trends in Cyberattacks

The urgency of finding scientifically sound solutions and their corresponding implementation in the form of effective cryptographic solutions for cybersecurity of mobile and satellite infocommunication technologies, in particular with the use of PQC and hybrid algorithms, is due to the significant dynamics and variability of cyberattacks. The main trends in cyberattacks include the following [81–83]:

– a significant increase in the number of jamming and spoofing attacks on GNSS networks, which is mainly due to the general availability of mass-produced products on the market and the ease of use of low-cost electronic devices;

– intellectualization' of cyberattacks, which is manifested in the active development of adaptive overshadowing and targeted MITM in radio channels at the physical level of information and communication networks;

– mobile infrastructure demonstrates relatively low cybersecurity performance during the exchange of service messages between the device and the network, due to the inheritance of new generation standards (5G/6G) of certain architectural components from older network standards;

– the increasing complexity of the hardware and software architecture of next-generation mobile and satellite networks is leading to the emergence of new potential points of intrusion, such as botnet attacks on edge devices and supply chain exploits for massive DDoS attacks.

Thus, the above-mentioned trends and evolutionary types of cyberattacks demonstrate that today, attacks are dynamically scaling their scope from purely technical to complex cyber-physical combinations. This requires multi-level protection: from adaptive protection at the physical level of networks to secure cyber-resistant hardware and software architecture of information and communication networks.

5.3. Identify Research Gaps in Existing Approaches

Based on the analysis and logical generalisation of the state-of-the-art and prospects for the development of cryptographic methods and means of cybersecurity of mobile and satellite networks, which are given in the previous sections of the article, in particular in Table 3, it is established that although there is a significant dynamics of highly effective solutions in the field of PQC and hybrid algorithms, there are also certain research limitations and gaps that require additional developments, in particular:

– the lack of a unified and standardised framework for cybersecurity of mobile networks, due to the fact that most mobile operators implement fragmented security measures rather than adhere to systematic integrated approaches, which, in addition to the deterioration of integrated cybersecurity, complicates the interoperability of the technologies used and cross-system interaction;

– limitation of energy and computing resources of infocommunication network nodes, which leads to practical difficulty or impossibility of deploying highly effective cryptographic cybersecurity algorithms in real-world conditions;

– the need to create specialised models of cybersecurity for satellite communications networks that take into account the complexity of hardware and software architecture and topology, as well as complex scenarios of cyberattacks on the space, ground, and user segments of these types of information and communication networks.

Thus, it can be stated that the above limitations and research gaps create a fundamental barrier to comprehensive cyber defence of mobile and satellite networks and, at the same time, prove the priority and importance of relevant scientific and applied research in the near future.

6. Discussions and Suggestions for Future Research

Considering the scale and variability of modern cyberattacks, the dynamics of quantum computing development, the complexity of the architecture of mobile and satellite infocommunication networks, as well as the identified research gaps in modern methods, means and algorithms for their cyber defence, the prospects for further research to improve the efficiency of infocommunication technologies are of great importance. The main generalised directions of scientific and applied research in this area include the integration of quantum-resistant cryptographic mechanisms, the development of cryptographic algorithms for energy-limited devices that are light in terms of computational load, and the construction of adaptive cybersecurity frameworks that take into account the multi-level structure of modern networks that can be integrated into existing information technologies for various applications.

One of the key trends is the development and practical implementation of hybrid cybersecurity models that combine PQC algorithms with classical encryption methods. This is due to the fact that such hybrid solutions allow reducing the computational load and energy consumption without losing resistance to cyberattacks. This is especially important for IoT-class devices used both in the mobile environment [84–86] and in satellite systems [87]. Equally important is the expansion of methods for detecting and responding to radio frequency attacks, including the use of AI and ML algorithms.

Thus, through a comprehensive analysis and logical synthesis of known scientific and information and analytical sources, a generalised architecture of promising research has been proposed, taking into account potential cyber technologies and the expected applied effect, as shown in graphical form in Figure 9.

Thus, as can be seen from Figure 9, in order to overcome the identified gaps in the current state of cyber defence of mobile and satellite communication systems, which in turn will increase the integrated efficiency, reliability and sustainability of networked information communication processes, it is advisable to focus on:

– development of standardised cybersecurity architectures for satellite and mobile systems;

– modelling of complex cyber-physical attack scenarios, taking into account all levels of infrastructure and their cross-level interaction;

– integration of PQC mechanisms into critical infocommunication nodes;

– implementation of adaptive monitoring of cyberthreats using ML and AI analytics;

– study of power consumption and time delays in PQC scenarios during large-scale deployment of new generation telecommunication networks.

In summary, an interdisciplinary approach based on the use of cryptography, quantum computing, infocommunications, artificial intelligence and machine learning technologies will contribute to the desired applied effect in creating and implementing new classes of highly efficient, reliable and scalable cyber defence systems.

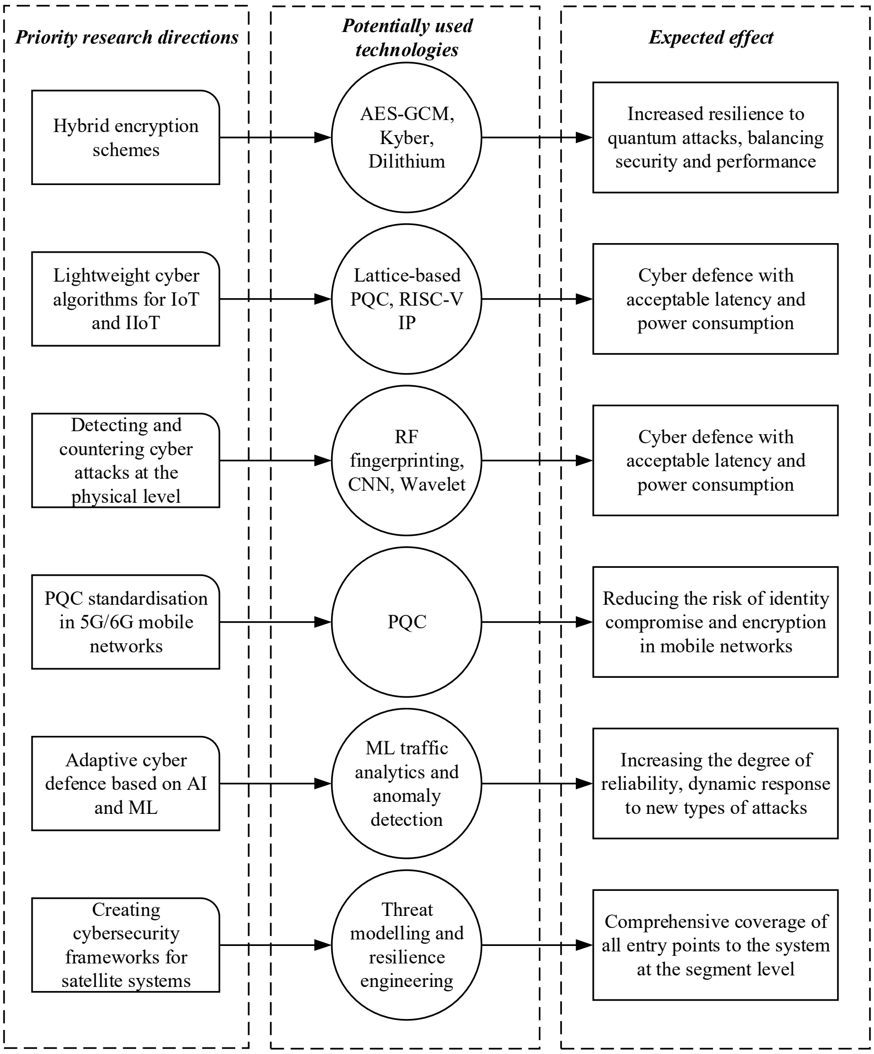

Priority research directions
Potentially used technologies
Expected effect
Hybrid encryption schemes
AES-GCM, Kyber, Dilithium
Increased resilience to quantum attacks, balancing security and performance
Lightweight cyber algorithms for IoT and IIoT
Lattice-based PQC, RISC-V IP
Cyber defence with acceptable latency and power consumption
Detecting and countering cyber attacks at the physical level
RF fingerprinting, CNN, Wavelet
Cyber defence with acceptable latency and power consumption
PQC standardisation in 5G/6G mobile networks
PQC
Reducing the risk of identity compromise and encryption in mobile networks
Adaptive cyber defence based on AI and ML
ML traffic analytics and anomaly detection
Increasing the degree of reliability, dynamic response to new types of attacks
Creating cybersecurity frameworks for satellite systems
Threat modelling and resilience engineering
Comprehensive coverage of all entry points to the system at the segment level

Figure 9. Graphical interpretation of the conceptual approach to improving the cybersecurity of information and communication networks, taking into account post-quantum threats.

7. Conclusions

The research conducted in this article allowed solving the relevant scientific and applied issue of formulating prospects for the development of methods and means to increase the effectiveness of approaches to cyber defence of information and communication networks. The results of the research allowed for drawing detailed conclusions about the current state and prospects for the development of cybersecurity of mobile and satellite information and communication networks, namely:

1. It has been established that existing cybersecurity solutions demonstrate limited effectiveness and require additional scientific and applied research in the context of a comprehensive consideration of the scaling factors of classical and quantum cyberthreats. An analysis of the architecture of modern information and communication systems has revealed their multilevel vulnerability.

2. The relevance and potential problems of implementing PQC algorithms in the limited computational and energy resources of the information and communication infrastructure have been confirmed and localised. It has been established that hybrid cryptographic models, which are combinations of classical and PQC algorithms, are currently the most appropriate solution for ensuring the balance between cybersecurity, energy efficiency and performance. In addition, the expediency of integrating intelligent systems for detecting radio-timed attacks, in particular, based on RF fingerprinting and machine learning algorithms, has been substantiated.

3. Based on the analysis and logical generalisation of modern scientific research and practical developments, it is established that modern approaches to providing cybersecurity for infocommunication systems of mobile and satellite communications need further development in the context of system integration based on the logical model of physical devices – cryptographic protocols – network infrastructure.

4. As a result of the analytical studies, promising areas for further research have been formulated, which include standardisation of mechanisms and approaches to cybersecurity of satellite networks, construction of models of adaptive and reliable response to cyber threats, development of protocols with built-in PQC algorithms, as well as testing of these solutions in real information and communication networks. Implementation of the proposed approaches will significantly increase the resilience, reliability and integral efficiency of critical information infrastructure in the current conditions of global digitalisation.

Author Contributions: Conceptualization, I.L., G.D.; methodology, I.L., I.G.; validation, I.L., G.D.; formal analysis, D.M.; investigation, I.L., I.G., D.M., G.D.; data curation, I.G.; writing—original draft preparation, I.L., G.D.; writing—review and editing, I.L., I.G., D.M.; visualization, D.M.; supervision, I.L.; All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding

Institutional Review Board Statement: Not applicable

Informed Consent Statement: Not applicable

Data Availability Statement: The raw data supporting the conclusions of this article will be made available by the authors on request.

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

References

1. IATA: IATA Releases 2024 Safety Report. Available online: https://www.iata.org/en/pressroom/2025-releases/2025-02-26-01/ (accessed on 02 July 2025).
2. IATA: EASA and IATA Publish Comprehensive Plan to Mitigate the Risks of GNSS Interference. Available online: https://www.iata.org/en/pressroom/2025-releases/2025-06-18-01/ (accessed on 03 July 2025).
3. Blatnik, A.; Batagelj, B. Evaluating GNSS Receiver Resilience: A Study on Simulation Environment Repeatability. *Electronics* **2025**, *14*, 1797. https://doi.org/10.3390/electronics14091797.
4. SeRo Systems: Detecting and Monitoring GPS Jamming and Spoofing in the Airspace. Available online: https://www.sero-systems.de/case-studies/tracking-the-threat? (accessed on 03 July 2025).
5. NIST: Post-Quantum Cryptography. Available online: https://csrc.nist.gov/projects/post-quantum-cryptography (accessed on 04 July 2025).
6. NIST: Status Report on the Fourth Round of the NIST Post-Quantum Cryptography Standardization Process. Available online: https://csrc.nist.gov/pubs/ir/8545/final (accessed on 04 July 2025).
7. ITU: SG17: Security. Available online: https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/default.aspx (accessed on 05 July 2025).
8. ITU: X.1303: Common alerting protocol. Available online: https://www.itu.int/rec/T-REC-X.1303-200709-I/en (accessed on 05 July 2025).
9. ENISA: State of cybersecurity in the EU. Available online: https://www.enisa.europa.eu/ (accessed on 07 July 2025).
10. 3GPP: A Global Initiative. Available online: https://www.3gpp.org/ftp//Specs/archive/33_series/33.501/ (accessed on 07 July 2025).

11. 3GPP: Portal. Available online: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3622 (accessed on 07 July 2025).
12. Ghanbarzadeh, A.; Soleimani, M.; Soleimani, H. GNSS/GPS Spoofing and Jamming Identification Using Machine Learning and Deep Learning. *arXiv:2501.02352* **2025**, 1–9. https://doi.org/10.48550/arXiv.2501.02352.
13. Tedeschi, P.; Sciancalepore, S.; Di Pietro, R. Satellite-based communications security: A survey of threats, solutions, and research challenges. *Computer Networks* **2022**, *216*, 1–18. https://doi.org/10.1016/j.comnet.2022.109246.
14. Williams, L.; Khan, H.; Burnap, P. The Evolution of Digital Security by Design Using Temporal Network Analysis. *Informatics* **2025**, *12*, 8. https://doi.org/10.3390/informatics12010008.
15. Trim, P.R.J.; Lee, Y.-I. Advances in Cybersecurity: Challenges and Solutions. *Appl. Sci.* **2024**, *14*, 4300. https://doi.org/10.3390/app14104300.
16. Brezavšček, A.; Baggia, A. Recent Trends in Information and Cyber Security Maturity Assessment: A Systematic Literature Review. *Systems* **2025**, *13*, 52. https://doi.org/10.3390/systems13010052.
17. Kaur, J.; Ramkumar, K.R. The recent trends in cyber security: A review. *Journal of King Saud University - Computer and Information Sciences* **2022**, *34 (8)*, 5766–5781. https://doi.org/10.1016/j.jksuci.2021.01.018.
18. Tarhan, K. Historical Development of Cybersecurity Studies: A Literature Review and Its Place in Security Studies. *Przegląd Strategiczny* **2022**, *15*, 393–414. https://doi.org/10.14746/ps.2022.1.23.
19. Li, Y.; Liu, Q. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports* **2021**, 7, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126.
20. Choi, J.; Lee, J. Secure and Scalable Internet of Things Model Using Post-Quantum MACsec. *Appl. Sci.* **2024**, *14*, 4215. https://doi.org/10.3390/app14104215.
21. Hoque, S.; Aydeger, A.; Zeydan, E. Exploring Post Quantum Cryptography with Quantum Key Distribution for Sustainable Mobile Network Architecture Design. arXiv:2404.10602 **2024**, 1–8. https://doi.org/10.48550/arXiv.2404.10602.
22. Mahmood, S.; Chadhar, M.; Firmin, S. Addressing Cybersecurity Challenges in Times of Crisis: Extending the Sociotechnical Systems Perspective. *Appl. Sci.* **2024**, *14*, 11610. https://doi.org/10.3390/app142411610.
23. Saeed, S.; Altamimi, S.A.; Alkayyal, N.A.; Alshehri, E.; Alabbad, D.A. Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. *Sensors* **2023**, *23*, 6666. https://doi.org/10.3390/s23156666.
24. Alaeifar, P.; Pal, S.; Jadidi, Z.; Hussain, M.; Foo, E. Current approaches and future directions for Cyber Threat Intelligence sharing: A survey. *Journal of Information Security and Applications* **2024**, *83*, 1–30. https://doi.org/10.1016/j.jisa.2024.103786.
25. Dritsas, E.; Trigka, M. A Survey on Cybersecurity in IoT. *Future Internet* **2025**, *17*, 30. https://doi.org/10.3390/fi17010030.
26. Han, D.; Liu, Y.; Zhang, F.; Lu, Y. Game-theoretic private blockchain design in edge computing networks. *Digital Communications and Networks* **2024**, *10 (6)*, 1622–1634. https://doi.org/10.1016/j.dcan.2023.12.001.
27. Gkonis, P.K.; Giannopoulos, A.; Nomikos, N.; Trakadas, P.; Sarakis, L.; Masip-Bruin, X. A Survey on Architectural Approaches for 6G Networks: Implementation Challenges, Current Trends, and Future Directions. *Telecom* **2025**, *6*, 27. https://doi.org/10.3390/telecom6020027.
28. Lee, W.; Suh, E.S.; Kwak, W.Y.; Han, H. Comparative Analysis of 5G Mobile Communication Network Architectures. *Appl. Sci.* **2020**, *10*, 2478. https://doi.org/10.3390/app10072478.

29. Aziz, F.M.; Shamma, J.S.; Stüber, G.L. Resilience of LTE networks against smart jamming attacks: Wideband model. In 2015 IEEE 26th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Hong Kong, China, 30 August – 02 September 2015, pp. 1344-1348. https://doi.org/10.1109/PIMRC.2015.7343507.
30. Winter, A.; Morrison, A.; Hasler, O.; Sokolova, N. Exploitation of 5G, LTE, and Automatic Identification System Signals for Fallback Unmanned Aerial Vehicle Navigation. *Eng. Proc.* **2025**, *88*, 49. https://doi.org/10.3390/engproc2025088049.
31. Boodai, J.; Alqahtani, A.; Frikha, M. Review of Physical Layer Security in 5G Wireless Networks. *Appl. Sci.* **2023**, *13*, 7277. https://doi.org/10.3390/app13127277.
32. Scalise, P.; Garcia, R.; Boeding, M.; Hempel, M.; Sharif, H. An Applied Analysis of Securing 5G/6G Core Networks with Post-Quantum Key Encapsulation Methods. *Electronics* **2024**, *13*, 4258. https://doi.org/10.3390/electronics13214258.
33. Vega-Sánchez, J.D.; Urquiza-Aguiar, L.; Paredes Paredes, M.C.; Moya Osorio, D.P. Survey on Physical Layer Security for 5G Wireless Networks. *arXiv:2006.08044* **2020**, 1–15. https://doi.org/10.48550/arXiv.2006.08044.
34. Kara, M.; Karampidis, K.; Panagiotakis, S.; Hammoudeh, M.; Felemban, M.; Papadourakis, G. Lightweight and Efficient Post Quantum Key Encapsulation Mechanism Based on Q-Problem. *Electronics* **2025**, *14*, 728. https://doi.org/10.3390/electronics14040728.
35. Ehsan, M.A.; Alayed, W.; Rehman, A.U.; Hassan, W.U.; Zeeshan, A. Post-Quantum KEMs for IoT: A Study of Kyber and NTRU. *Symmetry* **2025**, *17*, 881. https://doi.org/10.3390/sym17060881.
36. Chen, Y.; Ma, X.; Wu, C. The concept, technical architecture, applications and impacts of satellite internet: A systematic literature review. *Heliyon* **2024**, *10 (13)*, e33793, https://doi.org/10.1016/j.heliyon.2024.e33793.
37. Gao, S.; Cao, W.; Fan, L.; Liu, J. MBSE for Satellite Communication System Architecting. *IEEE Access* **2019**, *7*, 164051–164067. https://doi.org/10.1109/ACCESS.2019.2952889.
38. Kang, M.; Park, S.; Lee, Y. A Survey on Satellite Communication System Security. *Sensors* **2024**, *24*, 2897. https://doi.org/10.3390/s24092897.
39. Abdelsalam, N.; Al-Kuwari, S.; Erbad, A. Physical layer security in satellite communication: State-of-the-art and open problems. *IET Commun.* **2025**, *19*, e12830. https://doi.org/10.1049/cmu2.12830.
40. Salim, S.; Moustafa, N.; Reisslein, M.. 2025. Cybersecurity of Satellite Communications Systems: A Comprehensive Survey of the Space, Ground, and Links Segments. *Commun. Surveys Tuts.* **2025**, *27 (1)*, 372–425. https://doi.org/10.1109/COMST.2024.3408277.
41. Lichtman, M.; Jover, R.P.; Labib, M.; Rao, R.; Marojevic, V.; Reed, J.H.. LTE/LTE-a jamming, spoofing, and sniffing: threat assessment and mitigation. *Comm. Mag.* **2016**, *54 (4)*, 54–61. https://doi.org/10.1109/MCOM.2016.7452266.
42. Radoš, K.; Brkić, M.; Begušić, D. Recent Advances on Jamming and Spoofing Detection in GNSS. *Sensors* **2024**, *24*, 4210. https://doi.org/10.3390/s24134210.
43. Gallardo, F.; Pérez-Yuste, A.; Konovaltsev, A. Satellite Fingerprinting Methods for GNSS Spoofing Detection. *Sensors* **2024**, *24*, 7698. https://doi.org/10.3390/s24237698.
44. Meng, L.; Yang, L.; Yang, W.; Zhang, L. A Survey of GNSS Spoofing and Anti-Spoofing Technology. *Remote Sens.* **2022**, *14*, 4826. https://doi.org/10.3390/rs14194826.
45. Yu, C.; Chen, S.; Wang, F.; Wei, Z. Improving 4G/5G air interface security: A survey of existing attacks on different LTE layers. *Computer Networks* **2021**, *201*, 108532. https://doi.org/10.1016/j.comnet.2021.108532.

doi:10.20944/preprints202507.2242.v1

46. Lichtman, M.; Rao, R.; Marojevic, V.; Reed, J.; Jover, R.P. 5G NR Jamming, Spoofing, and Sniffing: Threat Assessment and Mitigation. In 2018 IEEE International Conference on Communications Workshops (ICC Workshops), Kansas City, MO, USA, 20–24 May 2018, pp. 1–6. https://doi.org/10.1109/ICCW.2018.8403769.
47. Harvanek, M.; Bolcek, J.; Kufa, J.; Polak, L.; Simka, M.; Marsalek, R. Survey on 5G Physical Layer Security Threats and Countermeasures. *Sensors* **2024**, *24*, 5523. https://doi.org/10.3390/s24175523.
48. Borhani-Darian, P.; Li, H.; Wu, P.; Closas, P. Deep neural network approach to detect GNSS spoofing attacks. In Proceedings of the 33rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+2020), Online, 22-25 September 2020, pp. 3241–3252. https://doi.org/10.33012/2020.17537.
49. Al-Shareeda, M.A.; Manickam, S. Man-in-the-Middle Attacks in Mobile Ad Hoc Networks (MANETs): Analysis and Evaluation. *Symmetry* **2022**, *14*, 1543. https://doi.org/10.3390/sym14081543.
50. Anthi, E.; Williams, L.; Ieropoulos, V.; Spyridopoulos, T. Investigating Radio Frequency Vulnerabilities in the Internet of Things (IoT). *IoT* **2024**, *5*, 356-380. https://doi.org/10.3390/iot5020018.
51. Osanaiye, O.; Alfa, A.S.; Hancke, G.P. A Statistical Approach to Detect Jamming Attacks in Wireless Sensor Networks. *Sensors* **2018**, *18*, 1691. https://doi.org/10.3390/s18061691.
52. Capotă, C.; Popescu, M.; Bădulă, E.-M.; Halunga, S.; Fratu, O.; Popescu, M. Intelligent Jammer on Mobile Network LTE Technology: A Study Case in Bucharest. *Appl. Sci.* **2023**, *13*, 12286. https://doi.org/10.3390/app132212286.
53. Li, X.; Chen, L.; Lu, Z.; Wang, F.; Liu, W.; Xiao, W.; Liu, P. Overview of Jamming Technology for Satellite Navigation. *Machines* **2023**, *11*, 768. https://doi.org/10.3390/machines11070768.
54. Rijnsdorp, J.; van Zwol, A.; Snijders, M. Satellite Navigation Signal Interference Detection and Machine Learning-Based Classification Techniques towards Product Implementation. *Eng. Proc.* **2023**, *54*, 60. https://doi.org/10.3390/ENC2023-15449.
55. Ahn, J.; Hussain, R.; Kang, K.; Son, J. Exploring Encryption Algorithms and Network Protocols: A Comprehensive Survey of Threats and Vulnerabilities. *IEEE Communications Surveys & Tutorials* **2025**. https://doi.org/10.1109/COMST.2025.3526605.
56. Tsantikidou, K.; Sklavos, N. Threats, Attacks, and Cryptography Frameworks of Cybersecurity in Critical Infrastructures. *Cryptography* **2024**, *8*, 7. https://doi.org/10.3390/cryptography8010007.
57. Hernández-Álvarez, L.; Bullón Pérez, J.J.; Batista, F.K.; Queiruga-Dios, A. Security Threats and Cryptographic Protocols for Medical Wearables. *Mathematics* **2022**, *10*, 886. https://doi.org/10.3390/math10060886.
58. Althamir, M.; Alabdulhay, A.; Yasin, M.M. A Systematic Literature Review on Symmetric and Asymmetric Encryption Comparison Key Size. In 2023 3rd International Conference on Smart Data Intelligence (ICSMDI), Trichy, India, 30–31 March 2023, pp. 110–117. https://doi.org/10.1109/ICSMDI57622.2023.00027.
59. Huang, C.; Zhang, Z.; Li, M.; Zhu, L.; Zhu, Z.; Yang, X. A mutual authentication and key update protocol in satellite communication network. *Automatika* **2020**, *61 (3)*, 334–344. https://doi.org/10.1080/00051144.2020.1757966.
60. Ahmadi, M.; Kaur, J.; Rani Nayak, D.; Nutan, R.; Taw, S.; Afaq, Y. A Review of Various Symmetric Encryption Algorithms for Multiple Applications. In Proceedings of the KILBY 100 7th International Conference on Computing Sciences 2023 (ICCS 2023), Phagwara, India, 5 May 2023, pp. 1–6. http://dx.doi.org/10.2139/ssrn.4491217.
61. Cheng, Y.; Liu, Y.; Zhang, Z.; Li, Y. An Asymmetric Encryption-Based Key Distribution Method for Wireless Sensor Networks. *Sensors* **2023**, *23*, 6460. https://doi.org/10.3390/s23146460.

62. Cherkaoui Dekkaki, K.; Tasic, I.; Cano, M.-D. Exploring Post-Quantum Cryptography: Review and Directions for the Transition Process. *Technologies* **2024**, *12*, 241. https://doi.org/10.3390/technologies12120241.
63. Zhang, M.; Wang, J.; Lai, J.; Dong, M.; Zhu, Z.; Ma, R.; Yang, J. Research on Development Progress and Test Evaluation of Post-Quantum Cryptography. *Entropy* **2025**, *27*, 212. https://doi.org/10.3390/e27020212.
64. Dam, D.-T.; Tran, T.-H.; Hoang, V.-P.; Pham, C.-K.; Hoang, T.-T. A Survey of Post-Quantum Cryptography: Start of a New Race. *Cryptography* **2023**, *7*, 40. https://doi.org/10.3390/cryptography7030040.
65. Demir, E.D.; Bilgin, B.; Onbasli, M.C. Performance Analysis and Industry Deployment of Post-Quantum Cryptography Algorithms. *arXiv:2503.12952* **2025**, 1–6. https://doi.org/10.48550/arXiv.2503.12952.
66. Ricci, S.; Dobias, P.; Malina, L.; Hajny, J.; Jedlicka, P. Hybrid Keys in Practice: Combining Classical, Quantum and Post-Quantum Cryptography. *IEEE Access* **2024**, *12*, 23206–23219. https://doi.org/10.1109/ACCESS.2024.3364520.
67. SoftBank R&D: SoftBank Corp. and SandboxAQ Jointly Verify Hybrid Mode Quantum-safe Technology. Available online: https://www.softbank.jp/en/corp/technology/research/story-event/008/ (accessed on 12 July 2025).
68. PostQuantum: Telecom's Quantum-Safe Imperative: Challenges in Adopting Post-Quantum Cryptography. Available online: https://postquantum.com/post-quantum/telecom-pqc-challenges/ (accessed on 12 July 2025).
69. NIST: Post-Quantum Cryptography and 5G Security: Tutorial. Available online: https://www.nist.gov/publications/post-quantum-cryptography-and-5g-security-tutorial (accessed on 12 July 2025).
70. Rani, A.; Ai, X.; Gupta, A.; Adhikari, R.S.; Malaney, R. Combined Quantum and Post-Quantum Security for Earth-Satellite Channels. *arXiv:2502.14240* **2025**, 1–9. https://doi.org/10.48550/arXiv.2502.14240.
71. Schöffel, M.; Lauer, F.; Rheinländer, C.C.; Wehn, N. Secure IoT in the Era of Quantum Computers—Where Are the Bottlenecks? *Sensors* **2022**, *22*, 2484. https://doi.org/10.3390/s22072484.
72. Borhani-Darian, P.; Li, H.; Wu, P.; Closas, P. Detecting GNSS spoofing using deep learning. *EURASIP J. Adv. Signal Process.* **2024**, *14*, 1–19. https://doi.org/10.1186/s13634-023-01103-1.
73. Birutis, A.; Mykkeltveit, A. Practical Jamming of a Commercial 5G Radio System at 3.6 GHz. *Procedia Computer Science* **2022**, *205*, 58-67. https://doi.org/10.1016/j.procs.2022.09.007.
74. Santo, A.D.; Tiberti, W.; Cassioli, D. An Adaptive Dual-Stack QKD-PQC Framework for Secure and Reliable Inter-Site Communication. In Joint National Conference on Cybersecurity (ITASEC & SERICS 2025), Bologna, Italy, 03–08 February 2025, pp. 1–12. URL: https://ceur-ws.org/Vol-3962/paper56.pdf
75. Chawla, D.; Mehra, P.S. A roadmap from classical cryptography to post-quantum resistant cryptography for 5G-enabled IoT: Challenges, opportunities and solutions. *Internet of Things* **2023**, *24*, 100950, https://doi.org/10.1016/j.iot.2023.100950.
76. Malina, L.; Popelova, L.; Dzurenda, P.; Hajny, J.; Martinasek, Z. On Feasibility of Post-Quantum Cryptography on Small Devices. *IFAC-PapersOnLine* **2018**, *51 (6)*, 462-467. https://doi.org/10.1016/j.ifacol.2018.07.104.
77. Zeydan, E.; Baranda, J.; Mangues-Bafalluy, J. Post-Quantum Blockchain-Based Secure Service Orchestration in Multi-Cloud Networks. *IEEE Access* **2022**, *10*, 129520–129530. https://doi.org/10.1109/ACCESS.2022.3228823.
78. Kumar, M. Post-quantum cryptography Algorithm's standardization and performance analysis. *Array* **2022**, *15*, 100242. https://doi.org/10.1016/j.array.2022.100242.

79. Astarloa, A.; Lázaro, J.; Gárate, J.I. CRYSTALS-Dilithium post-quantum cyber-secure SoC for wired communications in critical systems. *Internet of Things* **2025**, *33*, 101656, https://doi.org/10.1016/j.iot.2025.101656.
80. Ojetunde, B.; Kurihara, T.; Yano, K.; Sakano, T.; Yokoyama, H. A Practical Implementation of Post-Quantum Cryptography for Secure Wireless Communication. *Network* **2025**, *5*, 20. https://doi.org/10.3390/network5020020.
81. Wani, M.S.; Rademacher, M.; Horstmann, T.; Kretschmer, M. Security Vulnerabilities in 5G Non-Stand-Alone Networks: A Systematic Analysis and Attack Taxonomy. *J. Cybersecur. Priv.* **2024**, *4*, 23-40. https://doi.org/10.3390/jcp4010002.
82. Erni, S.; Kotuliak, M.; Leu, P.; Roeschlin, M.; Capkun, S. AdaptOver: Adaptive Overshadowing Attacks in Cellular Networks. *arXiv:2106.05039* **2021**, 1–13. https://doi.org/10.48550/arXiv.2106.05039.
83. PatentPC: 5G & Cybersecurity: Network Threats Stats. Available online: https://patentpc.com/blog/5g-cybersecurity-network-threat-stats (accessed on 20 July 2025).
84. Laktionov, I.; Diachenko, G.; Koval, V.; Yevstratiev, M. Computer-Oriented Model for Network Aggregation of Measurement Data in IoT Monitoring of Soil and Climatic Parameters of Agricultural Crop Production Enterprises. *Baltic J. Modern Computing* **2023**, *11 (3)*, 500–522. https://doi.org/10.22364/bjmc.2023.11.3.09.
85. Laktionov, I.; Diachenko, G.; Kashtan, V.; Vizniuk, A.; Gorev, V.; Khabarlak, K.; Shedlovska, Y. A Comprehensive Review of Recent Approaches and Hardware-Software Technologies for Digitalisation and Intellectualisation of Open-Field Crop Production: Ukrainian Case Study in the Global Context. *Computers and Electronics in Agriculture* **2024**, *225*, 1–31. https://doi.org/10.1016/j.compag.2024.109326
86. Laktionov, I.S.; Vovna, O.V.; Kabanets, M.M.; Sheina, H.O.; Getman, I.A. Information model of the computer-integrated technology for wireless monitoring of the state of microclimate of industrial agricultural greenhouses. *Instrumentation Mesure Metrologie* **2021**, *20 (6)*, 289 – 300. https://doi.org/doi.org/10.18280/i2m.200601.
87. Kashtan, V.Yu.; Hnatushenko, V.V.; Laktionov, I.S.; Diachenko, H.H. Intelligent Sentinel satellite image processing technology for land cover mapping. *Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu* **2024**, *5*, 143–150. https://doi.org/10.33271/nvngu/2024-5/143.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.