IoT

MDPI

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, UA49005 Dnipro, Ukraine; moroz.d.m@nmu.one
[2] Department of Electric Drive, Faculty of Electrical Engineering, Dnipro University of Technology, UA49005 Dnipro, Ukraine; diachenko.g@nmu.one
[3] Department of Computer Information Technologies, Donbas State Engineering Academy, UA84313 Kramatorsk, Ukraine; getman_irina@ukr.net
[4] Department of Digital Technologies and Project Decision Analysis, Technical University "Metinvest Polytechnic" LLC, Pivdenne Shose 80, 69008 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

Academic Editor: Firoz Khan

Received: 29 August 2025
Revised: 28 September 2025
Accepted: 13 October 2025
Published: 16 October 2025

Citation: Laktionov, I.; Diachenko, G.; Moroz, D.; Getman, I. A Comprehensive Review of Cybersecurity Threats to Wireless Infocommunications in the Quantum-Age Cryptography. *IoT* **2025**, *6*, 61. https://doi.org/10.3390/iot6040061

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] emphasise 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 PQC algorithms into 5G infrastructures [11].

In addition to the initiatives of NIST, ENISA and 3GPP, other international organisations play an important role in the development and implementation of post-quantum cryptography standards. In particular, the European Telecommunications Standards Institute (ETSI) is responsible for coordinating the activities of the ETSI ISG-QSC special group. This group makes recommendations to telecommunications operators and equipment manufacturers regarding the gradual migration to PQC and the implementation of hybrid schemes [12]. The International Organisation for Standardisation (ISO) is developing technical specifications and standards for the secure use of PQC in industrial and critical infrastructures through its ISO/IEC JTC 1/SC 27 sub-committee [13]. Working groups

within the Internet Engineering Task Force (IETF) also propose methods for integrating the CRYSTALS—Kyber and Dilithium algorithms into secure data transport mechanisms [14]. Thus, the global PQC standardisation process is interdisciplinary in nature, combining international initiatives to increase the likelihood of creating unified standards that improve system interoperability and accelerate the practical implementation of post-quantum solutions in the field of information and communications technology.

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 [15] proposed a deep learning-based method for detecting GNSS spoofing, achieving an accuracy of up to 99%. In [16], the security challenges of satellite communication are examined, emphasising the need for cryptographic solutions resilient to quantum attacks. The study in [17] 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

The historical evolution of security in these systems demonstrates a gradual transition from basic authentication mechanisms to the integration of PQC 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 [17–22], is shown in Figure 1.

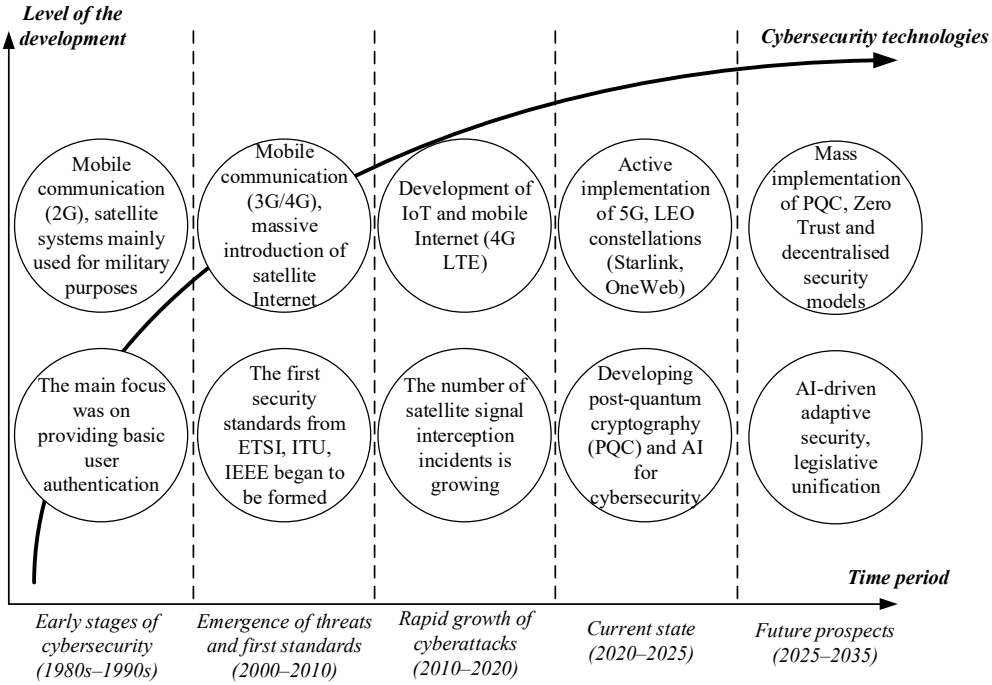


Figure 1. Graphical interpretation of historical, current and future trends in cybersecurity.

A logical systematisation of recent scientific works confirms that cybersecurity for wireless infocommunication networks has evolved into a multidisciplinary field. It now integrates classical and physical network protection methods, innovative cryptography based on post-quantum and AI-driven adaptive approaches, and adaptive regulatory frameworks for countering cyber threats.

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

With the rapid growth and rising complexity of mobile and satellite infocommunication networks, cybersecurity is becoming critically important. Threats have evolved from traditional DDoS attacks to more advanced challenges, including quantum-based risks and spoofing. This shift requires new security measures at both the physical device level and the levels of network protocols and software. In response, researchers and standards developers are addressing several key priorities: protection against electronic warfare, the use of PQC, and autonomous threat detection with machine learning (ML) and AI. A graphical summary of these issues, approaches, and expected outcomes, derived from the analysis of relevant studies [23–29], is presented in Figure 2.

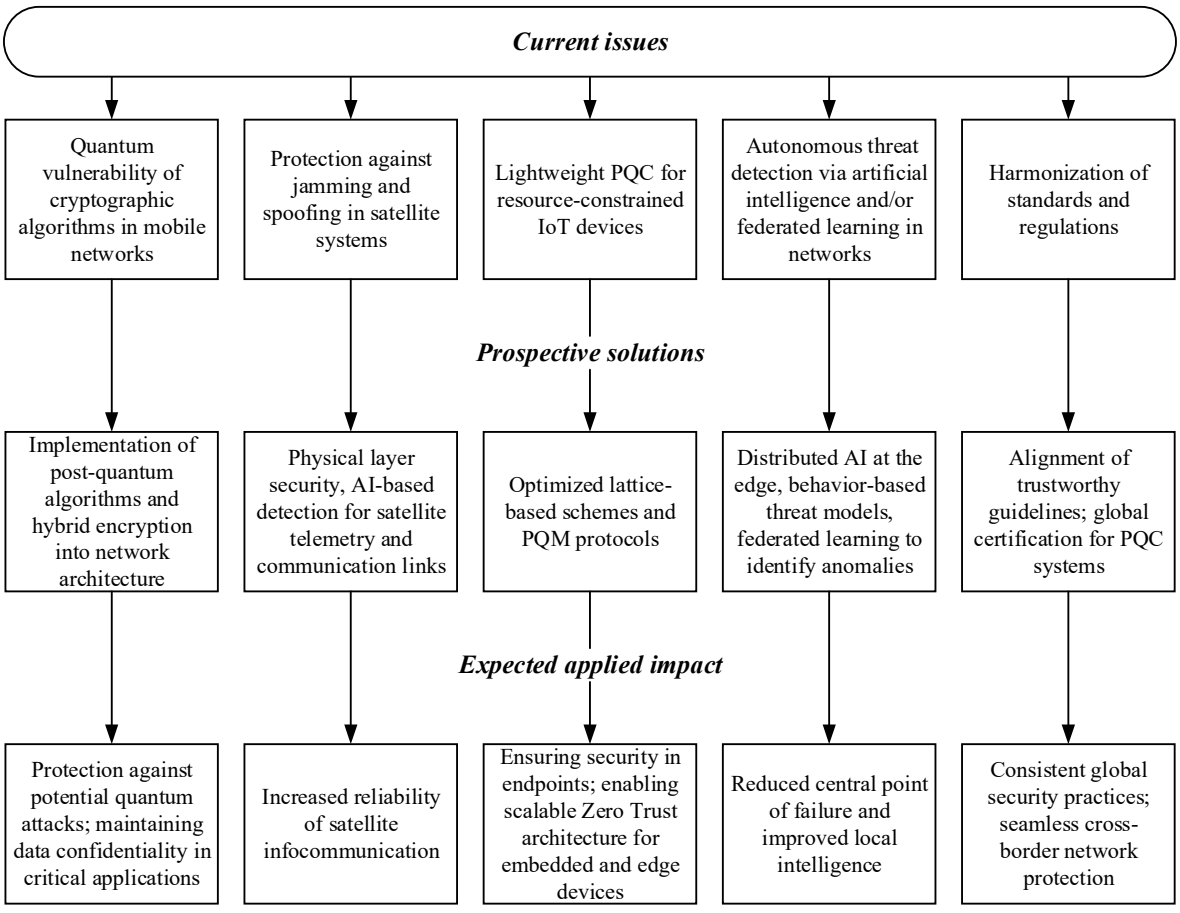


Figure 2. Graphical interpretation of current issues in cybersecurity, prospective solutions and expected applied impact of their solving. Source: authors' own development based on analysis and synthesis of scientific sources [23–29].

Thus, from the analysis of the block diagram presented in Figure 2, it is evident that modern cybersecurity approaches for infocommunication networks are multifaceted, combining quantum cryptography, ML, AI, and regulatory frameworks. Addressing these

issues will not only strengthen network security but also increase the trustworthiness of digital technologies in 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. This is achieved through a comparative analysis and logical systematisation of current research on cyber threats to mobile and satellite networks, with particular attention to the implications of quantum computing technologies. Unlike previous studies, this article focuses specifically on analysing cyber threats across the architectural layers of large-scale infocommunication networks. These include the physical layer, weaknesses in cryptographic protocols and authentication mechanisms, and the potential use of post-quantum security methods. In contrast to earlier reviews that mainly addressed general aspects of PQC, we focus on the practical challenges of implementing PQC in satellite networks and resource-constrained mobile systems.

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.

The research presented in this article is devoted to a comprehensive analysis and systematisation of modern approaches, methods and means for ensuring cybersecurity in mobile and satellite infocommunication technologies. The study takes into account both current conditions and the future impact of quantum computing. 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.

2. Methodology

2.1. Information Sources and Search Strategy

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.

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 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.

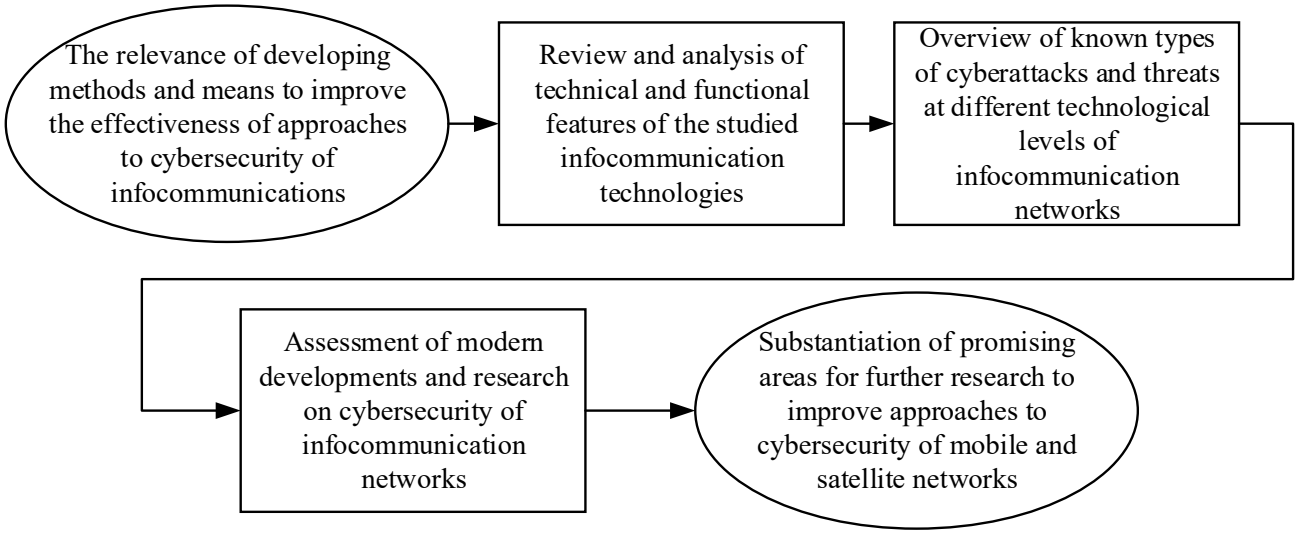


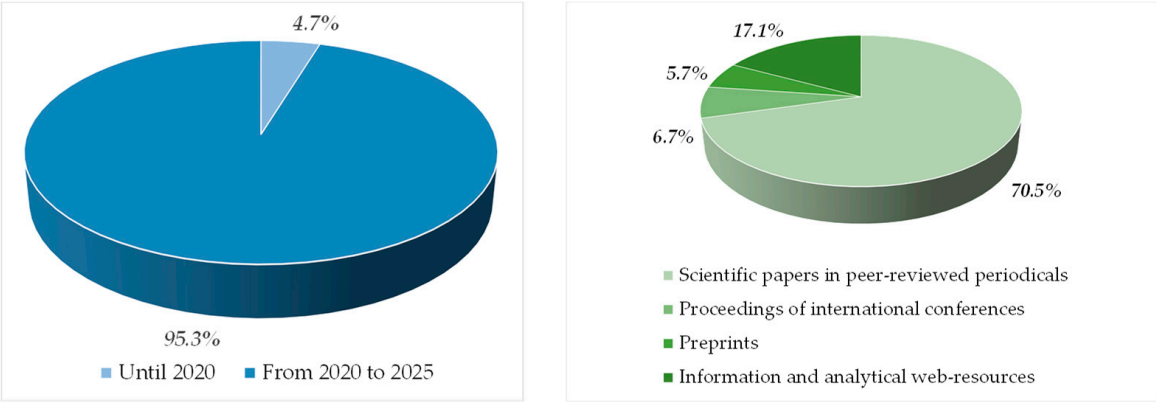
Figure 3. Generalised logical structure of the article's research.

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



(**a**) Years of publications (**b**) Types of publications

Figure 4. (**a**) Years of publications; (**b**) types of publications. Graphical interpretation of the analysed literature sources. Source: authors' own development based on bibliometric data from Table 1 and references cited.

The obtained 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.

3. Technical and Functional Features of the Studied Infocommunication Technologies

3.1. Distinctive Features of Mobile Communication

As noted in the introduction section, mobile communication systems play an important role in many practical domains. This subsection highlights their functional features and cybersecurity aspects. 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 [30,31], as summarised in Figure 5. Key characteristics of modern mobile networks include global coverage, topology reconfiguration, and mobility support. These features ensure reliable and continuous data transmission even under dynamic conditions.

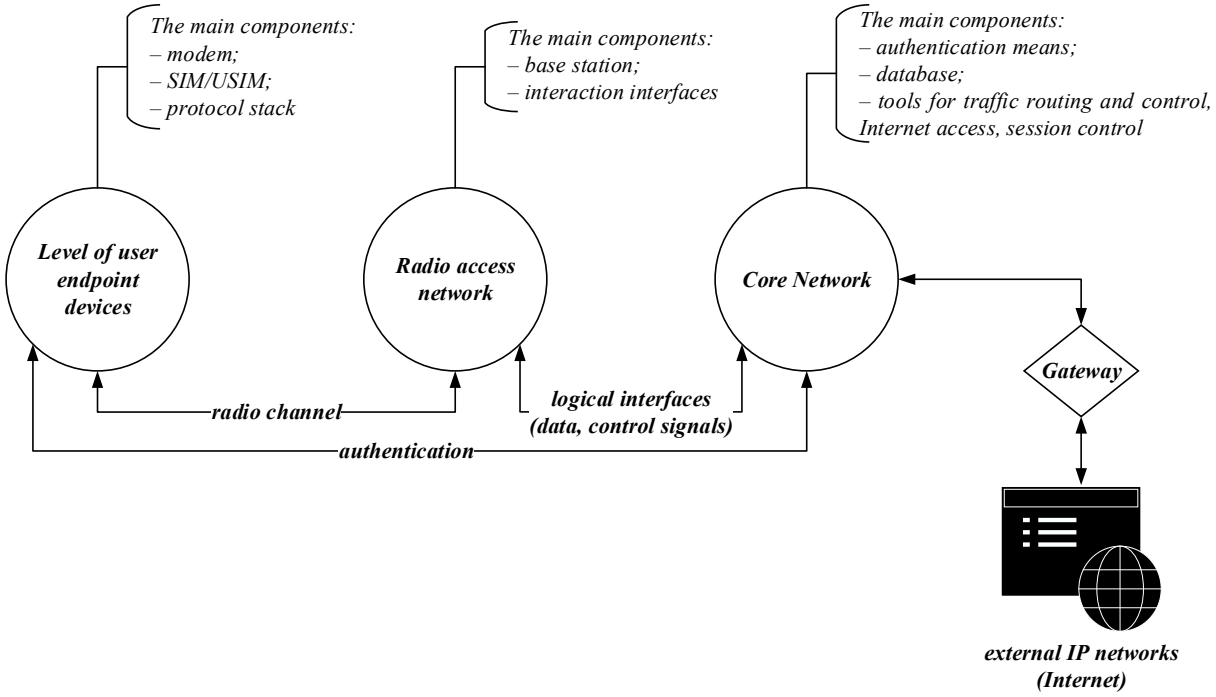


Figure 5. Generalised mobile infocommunications architecture.

From the perspective of mobile network cybersecurity, it is important to emphasise 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, signalling-level attacks, lack of full end-to-end encryption, replay attacks on authentication and others [32–34].

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 [35].

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 [36–38].

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

As discussed in Section 1.1, satellite communication systems play a critical role in many sectors. This subsection focuses on their architectural features and cybersecurity aspects. Unlike mobile networks, the architecture of satellite communication systems is shaped

by the use of orbital platforms, which determine the spatial scalability of their structural and functional design. In general, the hierarchical structure of satellite communication systems includes space, ground and user segments [39,40], as illustrated in the graphical interpretation in Figure 6.

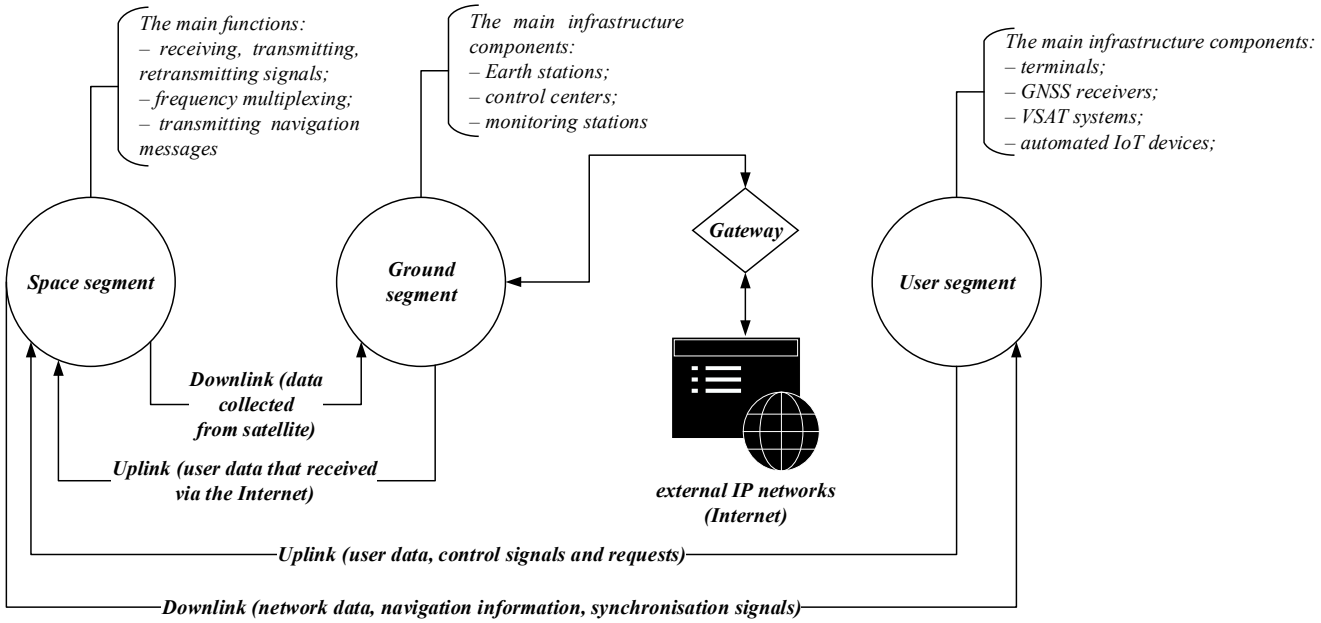


Figure 6. Generalised satellite infocommunications architecture.

From the perspective of satellite network cybersecurity, it is important to emphasise that their modern architecture is highly susceptible to cyber threats at all levels [41,42], 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 [43] 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 [44–47], as shown in Table 2.

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 information overload or interception, while the signalling layer may be targeted to create false messages or alter connection parameters. The authentication layer is a weak point for traffic protection and is particularly vulnerable to attacks based on quantum algorithms.

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

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 results reported in scientific articles [45,48–51], a generalised logical block-diagram was developed to illustrate the characteristics, consequences, and potential approaches for cyber defence of the physical layer in mobile and satellite communication networks, as shown in Figure 7.

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 [52,53].

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 [54,55]. 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 [56,57]. 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.

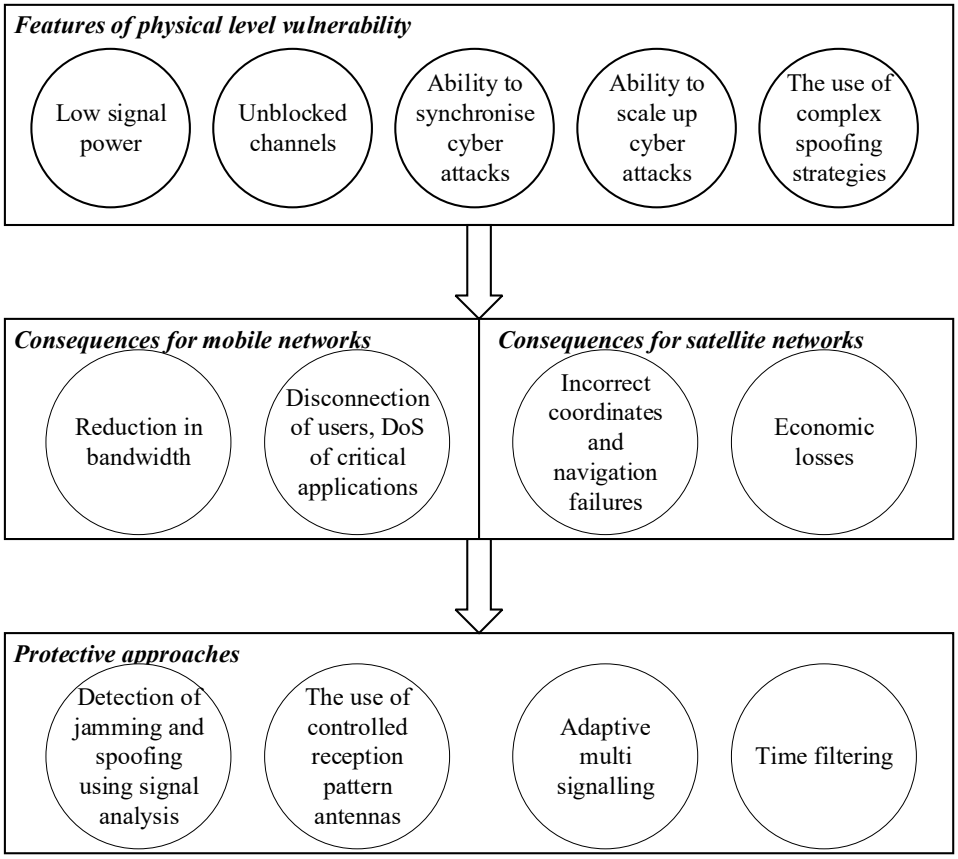


Figure 7. Graphical interpretation of cyber threats and methods of resisting them at the physical level.

4.4. IoT-Specific Cyber Threats

Compared to mobile and satellite networks, the information and communication vulnerabilities of IoT systems and networks are specific. One of the most serious risks in particular is the formation of IoT botnets, such as Mirai. In a typical scenario, these botnets use massively connected low-power devices to organise DDoS attacks on critical services [58,59]. Another common threat is unprotected or outdated firmware, which prevents the timely application of security updates and can lead to vulnerabilities being exploited over the long term [60]. In addition, the large-scale exploitation of devices in distributed infrastructures poses a problem. Attackers who have gained control of a significant number of edge devices and functional nodes in decentralised IoT system architectures can manipulate monitoring data and information messages or disrupt control system operations. These specific IoT threats require further research into the synthesis and implementation of individual protection approaches. This includes implementing secure firmware update mechanisms, using lightweight cryptographic algorithms and monitoring anomalous activity in large, spatially distributed arrays of devices.

4.5. 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 [61–63]. 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.

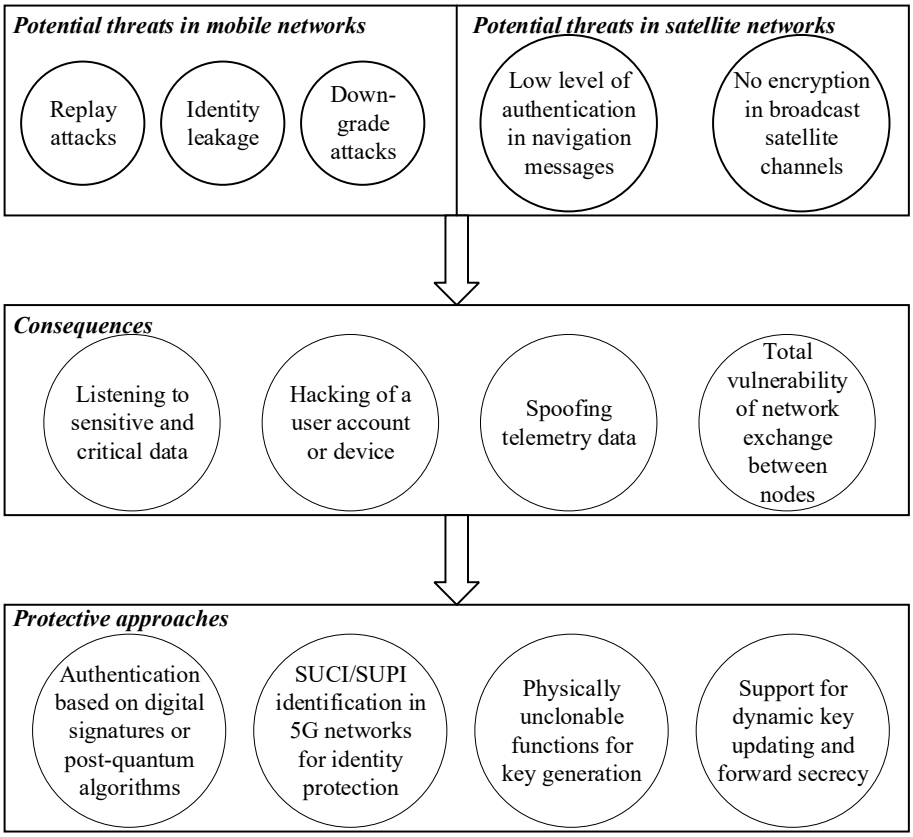


Figure 8. Graphical interpretation of cyber threats in cryptographic protocols and authentication and methods of resisting them.

Based on the above analysis, a generalised framework for the taxonomy of cyberattacks in mobile and satellite information and communication networks was proposed, as shown in Figure 9.

4.6. 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 [64–66].

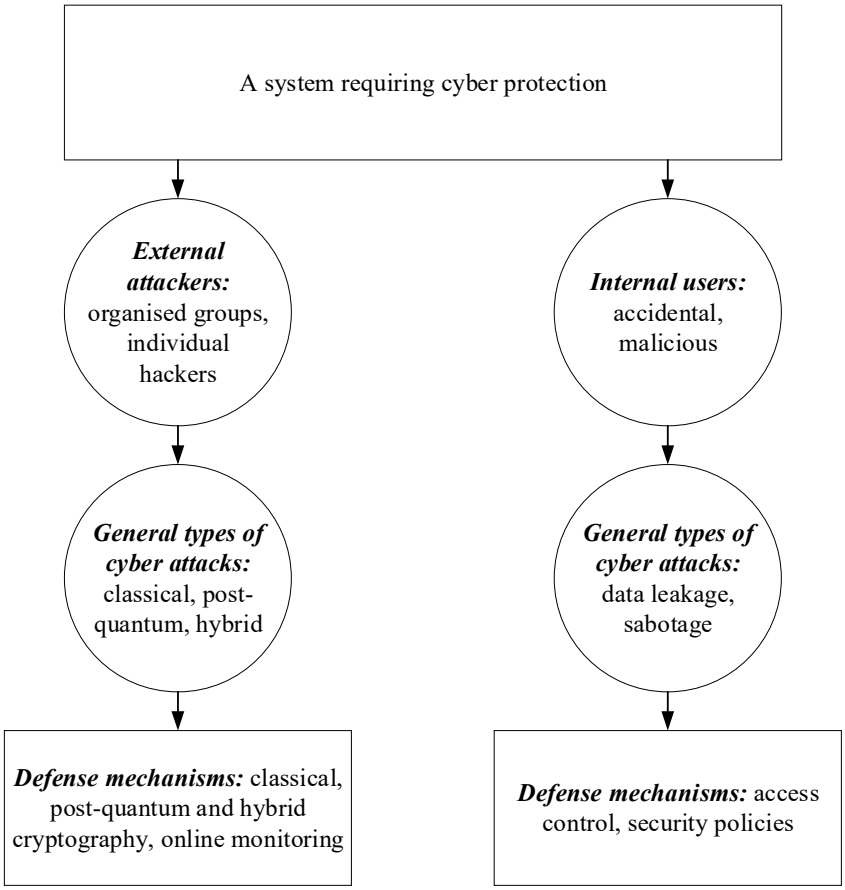


Figure 9. Generalised framework for the taxonomy of cyberattacks in mobile and satellite infocommunication networks.

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 [64,67]. 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.

4.7. Quantum Challenges and Post-Quantum Cryptography in Practical Cases

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) [68–70], and using a combination of classical and PQC algorithms in hybrid mode [71,72].

Practical testing of PQC algorithms has already produced results confirming their effectiveness and potential for large-scale deployment. Notable examples include Hybrid Mode Quantum-safe Technology tested by SoftBank Corp. and SandboxAQ (Tokyo,

Japan) [73], as well as the integration of PQC algorithms into 5G telecommunications networks conducted by SK Telecom (Seoul, Republic of Korea) [74]. These and similar studies demonstrate that PQC algorithms can be integrated into existing network infrastructures, a finding also supported by analytical research [75]. In addition, NIST conducted pilot tests of the integration of CRYSTALS—Kyber and CRYSTALS—Dilithium into transport layer security protocols for protecting web traffic, confirming their compatibility with modern browsers [76].

Hybrid cryptographic approaches that combine classical algorithms with PQC are recommended to ensure security during the transition period before full PQC implementation. This approach maintains compatibility with existing systems while protecting against potential quantum attacks. The main advantages of hybrid schemes are resilience against the failure of individual algorithms and gradual infrastructure adaptation, which is especially important for resource-constrained platforms. However, their larger key sizes and higher computational complexity require optimisation, for example, through hardware acceleration [71–73].

In satellite networks, authentication of telemetry, tracking, and command (TTC) signals and encryption of telemetry data are particularly critical. Consequently, the development and implementation of PQC algorithms play a key role in ensuring cryptographic resilience across all functional levels of satellite channels. Effective PQC deployment in satellite networks requires consideration of a structured threat model and attacker taxonomy. The main threats include: quantum attackers using algorithms such as Shor's algorithm; state actors capable of complex operations such as intercepting telemetry or conducting man-in-the-middle (MITM) attacks on ground stations; and insider threats exploiting access to infrastructure to compromise keys or data. This threat model underscores the need for hybrid PQC approaches and optimised implementations to defend against diverse types of attackers [77–79].

One of the key risks in the transition to PQC in real-world applications lies in the hardware limitations of existing infocommunication infrastructures. For example, lattice-based schemes such as Kyber and Dilithium typically require significantly larger key sizes and more complex arithmetic, which may not be efficiently supported by legacy hardware accelerators originally designed for RSA or ECC [80]. On resource-constrained hardware (Microcontroller Units (MCUs) and portable field-programmable gate arrays (FPGAs)), limited memory and cache architectures amplify code-size and constant-time countermeasure overheads. Additionally, larger key or signature sizes increase handshake latency and may cause fragmentation. At the embedded software level, constrained mobile devices with embedded microcontrollers face challenges due to higher memory consumption and longer execution times, potentially leading to vulnerabilities such as denial of service or accelerated battery depletion. Real-world examples further illustrate these challenges: NIST PQC standardisation process is supported on some types of microcontrollers through supporting authenticated ciphers and hashing algorithms to include benchmarking of signature schemes and key encapsulation methods [81]. These specific examples highlight that the transition to PQC is not merely a theoretical challenge but also entails significant practical risks for integration and implementation.

When analysing the cyber threats posed by quantum computing, it is important to distinguish between two scenarios. The first is real-time decryption, which involves the possibility of intercepting and instantly decrypting data during transmission. This is extremely dangerous for critical infrastructure and sensitive processes. The second is the 'store now, decrypt later' model, in which encrypted traffic accumulates over a long period of time. This traffic awaits the emergence of quantum computing capabilities that can break the algorithms used today. This model is particularly dangerous for data that has long-

term value [82]. These scenarios differ significantly in terms of risk assessment: real-time decryption requires existing quantum resources, whereas the 'store now, decrypt later' model creates a guaranteed, albeit delayed, vulnerability for all data transmitted today. This underlines the importance of implementing post-quantum and hybrid cryptographic solutions before practical quantum computers become available.

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 us to identify 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 modern low-power IoT infrastructure	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 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	[83]
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	[46]

Table 3. *Cont.*

The Subject of the Study	Technologies and Approaches Used	Scientific and Applied Effect Obtained	References
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	[84]
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.	[85]
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 post-quantum key exchanges even in challenging network environments where traditional QKD methods often fail	[86]
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	[87]
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.	[88]
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	[89]

Table 3. *Cont.*

The Subject of the Study	Technologies and Approaches Used	Scientific and Applied Effect Obtained	References
Approaches to standardisation and performance evaluation of PQC algorithms	PQC, information and communications technology	This research reviewed the global efforts in designing and standardising PQC algorithms and analysed the performance of key candidates. It has been highlighted that most PQC algorithms require more CPU, memory, and larger keys, and aim to assess their overall feasibility.	[90]
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.	[91]
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.	[92]
Approaches for preventing fault attacks on S-Boxes of AES Block Ciphers	AES, S-boxes, nonlinear cellular automata	The S-boxes are constructed using synthesised nonlinear cellular automata, and the proposed approach ensures detection of double-byte faults as well as correction of single-byte faults.	[93]
An efficient implementation of a post-quantum MLWR-based public key encryption (PKE) scheme leveraging NTT.	PKE, MLWR, PQC	The proposed approach achieves a balance between security and efficiency, with key generation, encryption, and decryption requiring 1422, 1040, and 2647 CPU cycles, respectively, and corresponding execution times of approximately 68.965, 34.483 microseconds.	[94]

In addition to the results in Table 3, an analysis of effective PQC algorithms was carried out, as shown in Table 4. This table was compiled by analysing and summarising information from scientific sources [91,95–98].

It is important to emphasise that the results of applied scientific research analysed in Tables 3 and 4 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;
- focusing on developing methods and means to prevent poisoning attacks, in which malicious data are deliberately introduced into datasets to reduce the accuracy of ML models or alter their behaviour, thereby directly affecting the operation of satellite and mobile systems and potentially leading to incorrect results.

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.

Table 4. Results of the comparative analysis of prominent PQC algorithms.

Algorithm	Type/Security Level	Methodological Basis	Public/Private Key Size, Bytes	Approximate Encryption/Decryption Time, ms
Kyber-512	Lattice-based KEM/AES-128	Learning With Errors	800/1632	0.1/0.3
Kyber-768	Lattice-based KEM/AES-192	Learning With Errors	1184/2400	0.2/0.5
BIKE	Code-based KEM/AES-128	McEliece-type codes	1541/3113	0.5/0.8
Dilithium	Lattice-based Signature/AES-128	Module-LWE and Module-SIS	1312/2528	0.3/0.4
Falcon-1024	NIST Security Level 5/AES-256	NTRU grids and the Fast Fourier Sampling method	1793/2305	not applicable

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 [99–101]:

- 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;
- migration to PQC involves several risks. Downgrade attacks pose a significant threat during the transition period, particularly in hybrid schemes. Vulnerabilities to side-channel attacks are critical for resource-constrained platforms, where hardware limitations complicate protection. Such attacks can force the system to use less secure algorithms, which significantly increases the risk of data compromise. This necessitates thorough testing of PQC implementations and the development of side-attack-resistant mechanisms to ensure security during migration. Thus, a comprehensive approach to migration, combining careful planning, testing, and implementation of attack-resistant approaches, is key to ensuring system reliability and security during the transition to post-quantum cryptography, as shown below in Figure 10.
- research into mechanisms for optimising digital signature algorithms through simplified structures and the elimination of deviation selection. These approaches reduce computational complexity and enable adaptation of PQC algorithms for hardware acceleration.

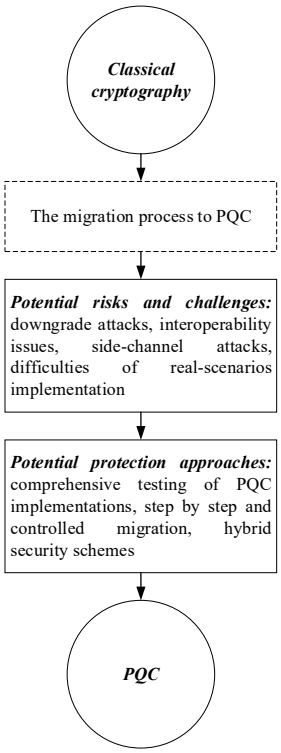


Figure 10. Block diagram of the migration approach to PQC.

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 PQC 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.

Although PQC is currently considered essential for ensuring the resilience of mobile, satellite and IoT networks against quantum attacks, there are a number of challenges associated with its practical deployment. The problem of compatibility with legacy systems is widespread in telecommunications and critical infrastructure. Devices and software complexes designed for asymmetric cryptographic algorithms such as RSA or ECC often do not support the larger key sizes and more complex operations required by PQC. This makes it difficult to integrate new algorithms into existing systems without incurring significant costs for modernising the equipment. Another important challenge is the practical implementation of migration strategies. Current practice shows that the transition to PQC

is a rather lengthy process, which is why hybrid cryptographic schemes are becoming relevant. At the same time, during the transition period, there are risks of downgrade attacks and side channels, which require additional testing and certification measures. Regulatory and standardisation uncertainty is also a significant limiting factor. Despite the active involvement of NIST and ENISA, global PQC standards have yet to be agreed upon. This creates barriers to the widespread adoption of security solutions by telecommunications companies and public sector organisations, which must meet certification requirements. These challenges can be overcome through a comprehensive approach, including the development of adaptive protocols for the phased integration of PQC into existing systems, international coordination on standards and regulatory requirements, and the creation of hardware accelerators to minimise power consumption and delays in devices with limited resources.

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 [102–104] and in satellite systems [105]. Equally important is the expansion of methods for detecting and responding to radio frequency attacks, including the use of AI and ML algorithms. Hardware acceleration and optimisation of code algorithms, as shown in Table 4, appear promising. Further research could focus on developing specialised versions of PQC algorithms that minimise power consumption and delays while ensuring compatibility with devices currently used in mobile and satellite networks.

One of the main aspects of developing and implementing PQC algorithms in real-world scenarios is key management, which is particularly relevant for platforms with limited computing resources. For effective key exchange, hybrid protocols that ensure compatibility and reduce latency are promising. One practical approach could be hardware acceleration based on RISC-V architecture. Therefore, further research should focus on lightweight key exchange protocols and attack-resistant storage mechanisms. Key management in post-quantum technologies poses a number of challenges that go far beyond the choice of algorithms. At the protocol level, traditional authentication procedures, such as transport layer security (TLS), require hardware and software adaptation to support larger public keys generated by lattice-based schemes such as Kyber. Hybrid key exchange mechanisms are currently a promising area of development and are being evaluated in real-world implementations to provide both classical and quantum protection during the transition period. In resource-constrained platforms, secure storage of long-term keys is equally important. Due to the limited amount of non-volatile memory and the lack of specialised security modules, lightweight approaches and adaptive secure boot chains are being explored. Therefore, current research emphasises the need for further development of robust key management mechanisms to achieve end-to-end quantum security.

Moreover, research into integrating fault detection methods with PQC mechanisms to enhance system resilience against side-channel and combined attacks is promising. In the context of the research development of this article, it is important to investigate multi-level countermeasures that combine hardware and software protection to minimise the risk of compromise even in the presence of multiple attack vectors simultaneously. When assessing the energy efficiency of promising cryptographic solutions for mobile and satellite infocommunications, accurate power measurement methods based on signal activity analysis from VCD and SAIF files are recommended. This approach will facilitate the selection of optimal cryptographic solutions in terms of not only security but also energy and computational efficiency for resource-constrained devices.

Future research on PQC should also focus, in particular, on practical cases with limited computing capabilities of mobile platforms. Recent studies show that lattice-based schemes such as Kyber can achieve key encapsulation with execution times of less than fractions of a millisecond on ARM processors while maintaining moderate memory requirements (see Table 4). Similarly, signature schemes such as Dilithium are being evaluated for authentication protocols (see Table 4). In turn, current initiatives such as NIST provide real-world environments for testing these algorithms. Including such performance data and practical examples in future research can help identify trade-offs in algorithms and guide the selection of lightweight PQC algorithms for resource-constrained devices.

In addition to the strictly cryptographic aspects, a key area of analysis is the risks associated with actively developing and applying AI and ML algorithms. Such multi-level, intellectualised cyberattacks are becoming increasingly relevant due to the active use of AI and ML algorithms to detect traffic anomalies. Data poisoning or specially formed signals can mislead models, reducing the accuracy with which attacks are classified or enabling malicious activity to be concealed. This gives rise to a new class of vulnerabilities, whereby the target of the attack is not network protocols or cryptography, but rather the analysis and automated decision-making algorithms themselves. These risks require integrated solutions, such as the development of cascade impact models to predict the cross-sector consequences of attacks, as well as the implementation of AI methods that are resistant to adversarial attacks, such as robust machine learning and explainable AI. This should be a key focus of future research in the field of cyber protection of information and communication networks.

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 11.

Thus, as can be seen from Figure 11, 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;
- optimisation of digital signature algorithms, which will increase resistance to lateral attacks.

When developing cyber defence strategies, it is important to pay particular attention to making a realistic assessment of the life cycle of the cryptographic algorithms being used. The growth in computing power in traditional data centres, coupled with the use of specialised hardware acceleration, may gradually reduce the effective security margin. The use of AI for cryptanalysis creates a new risk. For example, ML models are capable of detecting statistical regularities or repetitive patterns in encrypted messages. Therefore, the assessment of the long-term cybersecurity of algorithms must be flexible. According to experts, the cryptographic algorithms currently in use will remain suitable in the medium term. However, in the long term, it is advisable to plan for a transition to post-quantum or hybrid algorithms. It is also important to continuously monitor new developments in the field of AI cryptanalysis.

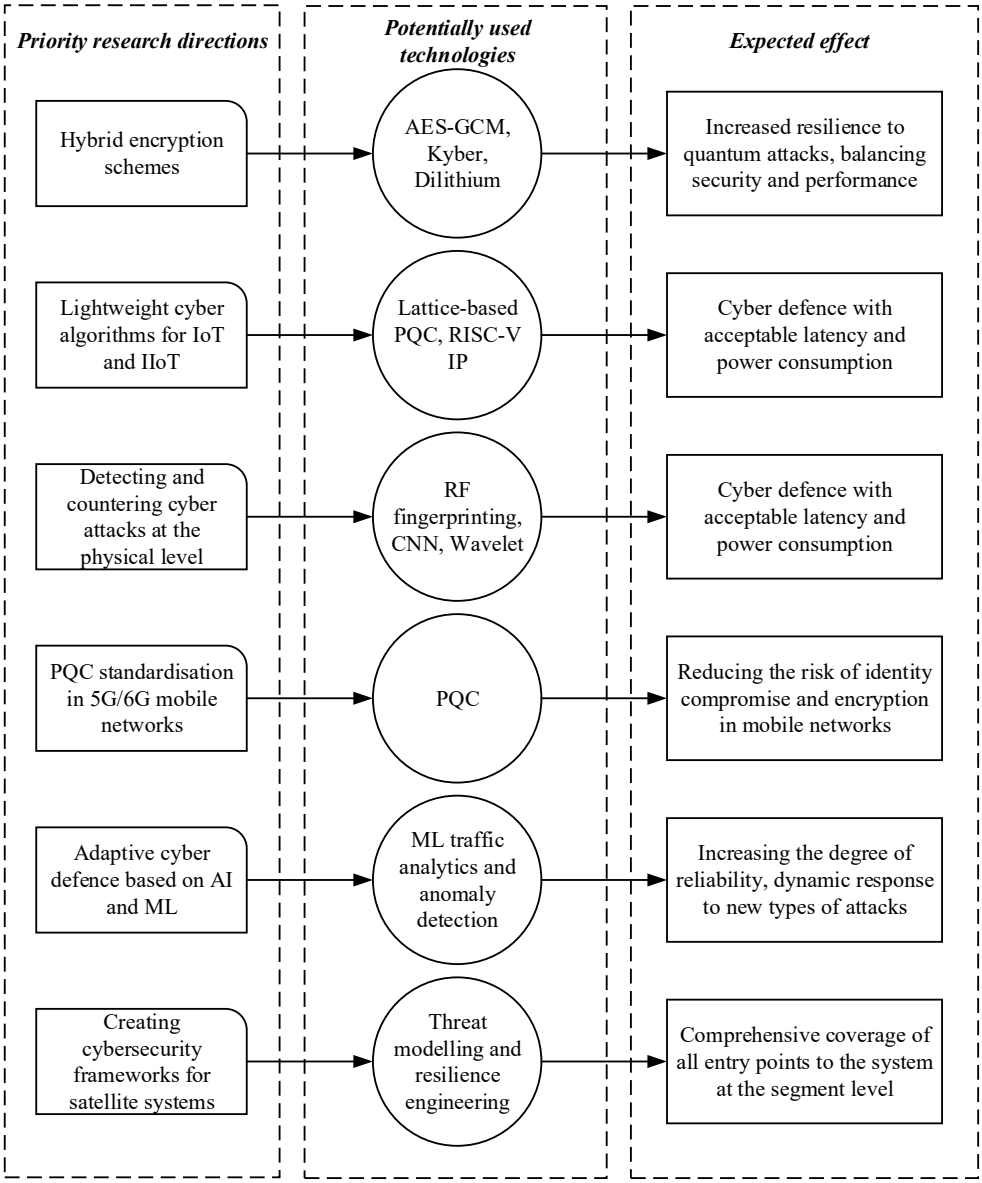


Figure 11. Graphical interpretation of the conceptual approach to improving the cybersecurity of information and communication networks, taking into account post-quantum threats.

It is important to acknowledge certain limitations of this study, which will be addressed through research in the priority areas identified above. This article focused on low-resource mobile platforms and satellite networks, which may limit the applicability of the results to other systems, such as cloud infrastructures with high computing resources. Although new attacks, such as data poisoning in ML systems, have been considered, a detailed analysis of their impact on PQC implementations requires further empirical research, particularly in the context of hybrid schemes.

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.

7. Conclusions

The research conducted in this article allowed us to solve 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. In contrast to earlier review papers that concentrated on general aspects of post-quantum cryptography, our study emphasises the practical challenges of implementing PQC in satellite networks and low-resource mobile platforms. The research also incorporates a structured threat model and attacker taxonomy, providing a holistic approach to cybersecurity in the context of quantum threats. The results of the research allowed for drawing detailed conclusions about the current state and future 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. and G.D.; methodology, I.L. and I.G.; validation, I.L. and G.D.; formal analysis, D.M.; investigation, I.L., I.G., D.M. and G.D.; data curation, I.G.; writing—original draft preparation, I.L. and G.D.; writing—review and editing, I.L., I.G. and D.M.; visualisation, D.M.; supervision, I.L. All authors have read and agreed to the published version of the manuscript.

Funding: This article was carried out as part of the scientific project 2025.06/0047 'Information technologies of cryptographic protection and data authentication for mobile and satellite communication systems'. This project is funded by the National Research Foundation of Ukraine.

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

Conflicts of Interest: Author "Iryna Getman" was employed by the company Technical University "Metinvest Polytechnic" LLC. The author declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict 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 2 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 3 July 2025).
3. Blatnik, A.; Batagelj, B. Evaluating GNSS Receiver Resilience: A Study on Simulation Environment Repeatability. *Electronics* **2025**, *14*, 1797. [CrossRef]
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 3 July 2025).
5. NIST. Post-Quantum Cryptography. Available online: https://csrc.nist.gov/projects/post-quantum-cryptography (accessed on 4 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 4 July 2025).
7. ITU. SG17: Security. Available online: https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/default.aspx (accessed on 5 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 5 July 2025).
9. ENISA. State of Cybersecurity in the EU. Available online: https://www.enisa.europa.eu/ (accessed on 7 July 2025).
10. 3GPP. A Global Initiative. Available online: https://www.3gpp.org/ftp//Specs/archive/33_series/33.501/ (accessed on 7 July 2025).
11. 3GPP. Portal. Available online: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3622 (accessed on 7 July 2025).
12. ETSI. Quantum-Safe Cryptography. Available online: https://www.etsi.org/technologies/quantum-safe-cryptography (accessed on 24 September 2025).
13. ISO: ISO/IEC JTC 1/SC 27. Information Security, Cybersecurity and Privacy Protection. Available online: https://www.iso.org/committee/45306.html (accessed on 24 September 2025).
14. IETF. Guidance for Migration to Post-Quantum Cryptography. Available online: https://www.ietf.org/archive/id/draft-kwiatkowski-pquip-pqc-migration-00.html (accessed on 24 September 2025).
15. Ghanbarzadeh, A.; Soleimani, M.; Soleimani, H. GNSS/GPS Spoofing and Jamming Identification Using Machine Learning and Deep Learning. *arXiv* **2025**, arXiv:2501.02352. [CrossRef]
16. Tedeschi, P.; Sciancalepore, S.; Di Pietro, R. Satellite-based communications security: A survey of threats, solutions, and research challenges. *Comput. Netw.* **2022**, *216*, 109246. [CrossRef]
17. Williams, L.; Khan, H.; Burnap, P. The Evolution of Digital Security by Design Using Temporal Network Analysis. *Informatics* **2025**, *12*, 8. [CrossRef]
18. Trim, P.R.J.; Lee, Y.-I. Advances in Cybersecurity: Challenges and Solutions. *Appl. Sci.* **2024**, *14*, 4300. [CrossRef]
19. Brezavšček, A.; Baggia, A. Recent Trends in Information and Cyber Security Maturity Assessment: A Systematic Literature Review. *Systems* **2025**, *13*, 52. [CrossRef]
20. Kaur, J.; Ramkumar, K.R. The recent trends in cyber security: A review. *J. King Saud. Univ.—Comput. Inf. Sci.* **2022**, *34*, 5766–5781. [CrossRef]
21. Tarhan, K. Historical Development of Cybersecurity Studies: A Literature Review and Its Place in Security Studies. *Przegląd Strateg.* **2022**, *15*, 393–414. [CrossRef]
22. Li, Y.; Liu, Q. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Rep.* **2021**, *7*, 8176–8186. [CrossRef]
23. Choi, J.; Lee, J. Secure and Scalable Internet of Things Model Using Post-Quantum MACsec. *Appl. Sci.* **2024**, *14*, 4215. [CrossRef]
24. Hoque, S.; Aydeger, A.; Zeydan, E. Exploring Post Quantum Cryptography with Quantum Key Distribution for Sustainable Mobile Network Architecture Design. *arXiv* **2024**, arXiv:2404.10602. [CrossRef]
25. Mahmood, S.; Chadhar, M.; Firmin, S. Addressing Cybersecurity Challenges in Times of Crisis: Extending the Sociotechnical Systems Perspective. *Appl. Sci.* **2024**, *14*, 11610. [CrossRef]
26. 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. [CrossRef] [PubMed]
27. Alaeifar, P.; Pal, S.; Jadidi, Z.; Hussain, M.; Foo, E. Current approaches and future directions for Cyber Threat Intelligence sharing: A survey. *J. Inf. Secur. Appl.* **2024**, *83*, 103786. [CrossRef]
28. Dritsas, E.; Trigka, M. A Survey on Cybersecurity in IoT. *Future Internet* **2025**, *17*, 30. [CrossRef]

29. Han, D.; Liu, Y.; Zhang, F.; Lu, Y. Game-theoretic private blockchain design in edge computing networks. *Digit. Commun. Netw.* **2024**, *10*, 1622–1634. [CrossRef]
30. 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. [CrossRef]
31. Lee, W.; Suh, E.S.; Kwak, W.Y.; Han, H. Comparative Analysis of 5G Mobile Communication Network Architectures. *Appl. Sci.* **2020**, *10*, 2478. [CrossRef]
32. Aziz, F.M.; Shamma, J.S.; Stüber, G.L. Resilience of LTE networks against smart jamming attacks: Wideband model. In Proceedings of the 2015 IEEE 26th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Hong Kong, China, 30 August–2 September 2015; pp. 1344–1348. [CrossRef]
33. 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. [CrossRef]
34. Boodai, J.; Alqahtani, A.; Frikha, M. Review of Physical Layer Security in 5G Wireless Networks. *Appl. Sci.* **2023**, *13*, 7277. [CrossRef]
35. 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. [CrossRef]
36. 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* **2020**, arXiv:2006.08044. [CrossRef]
37. 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. [CrossRef]
38. 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. [CrossRef]
39. Chen, Y.; Ma, X.; Wu, C. The concept, technical architecture, applications and impacts of satellite internet: A systematic literature review. *Heliyon* **2024**, *10*, e33793. [CrossRef]
40. Gao, S.; Cao, W.; Fan, L.; Liu, J. MBSE for Satellite Communication System Architecting. *IEEE Access* **2019**, *7*, 164051–164067. [CrossRef]
41. Kang, M.; Park, S.; Lee, Y. A Survey on Satellite Communication System Security. *Sensors* **2024**, *24*, 2897. [CrossRef]
42. 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. [CrossRef]
43. Salim, S.; Moustafa, N.; Reisslein, M. 2025. Cybersecurity of Satellite Communications Systems: A Comprehensive Survey of the Space, Ground, and Links Segments. *Commun. Surv. Tuts.* **2025**, *27*, 372–425. [CrossRef]
44. 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*, 54–61. [CrossRef]
45. Radoš, K.; Brkić, M.; Begušić, D. Recent Advances on Jamming and Spoofing Detection in GNSS. *Sensors* **2024**, *24*, 4210. [CrossRef] [PubMed]
46. Gallardo, F.; Pérez-Yuste, A.; Konovaltsev, A. Satellite Fingerprinting Methods for GNSS Spoofing Detection. *Sensors* **2024**, *24*, 7698. [CrossRef] [PubMed]
47. Meng, L.; Yang, L.; Yang, W.; Zhang, L. A Survey of GNSS Spoofing and Anti-Spoofing Technology. *Remote Sens.* **2022**, *14*, 4826. [CrossRef]
48. Yu, C.; Chen, S.; Wang, F.; Wei, Z. Improving 4G/5G air interface security: A survey of existing attacks on different LTE layers. *Comput. Netw.* **2021**, *201*, 108532. [CrossRef]
49. Lichtman, M.; Rao, R.; Marojevic, V.; Reed, J.; Jover, R.P. 5G NR Jamming, Spoofing, and Sniffing: Threat Assessment and Mitigation. In Proceedings of the 2018 IEEE International Conference on Communications Workshops (ICC Workshops), Kansas City, MO, USA, 20–24 May 2018; pp. 1–6. [CrossRef]
50. 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. [CrossRef]
51. 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. [CrossRef]
52. Al-Shareeda, M.A.; Manickam, S. Man-in-the-Middle Attacks in Mobile Ad Hoc Networks (MANETs): Analysis and Evaluation. *Symmetry* **2022**, *14*, 1543. [CrossRef]
53. Anthi, E.; Williams, L.; Ieropoulos, V.; Spyridopoulos, T. Investigating Radio Frequency Vulnerabilities in the Internet of Things (IoT). *IoT* **2024**, *5*, 356–380. [CrossRef]

54. Osanaiye, O.; Alfa, A.S.; Hancke, G.P. A Statistical Approach to Detect Jamming Attacks in Wireless Sensor Networks. *Sensors* **2018**, *18*, 1691. [CrossRef]
55. 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. [CrossRef]
56. 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. [CrossRef]
57. 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. [CrossRef]
58. Gelgi, M.; Guan, Y.; Arunachala, S.; Samba Siva Rao, M.; Dragoni, N. Systematic Literature Review of IoT Botnet DDOS Attacks and Evaluation of Detection Techniques. *Sensors* **2024**, *24*, 3571. [CrossRef]
59. Wazzan, M.; Algazzawi, D.; Bamasaq, O.; Albeshri, A.; Cheng, L. Internet of Things Botnet Detection Approaches: Analysis and Recommendations for Future Research. *Appl. Sci.* **2021**, *11*, 5713. [CrossRef]
60. Catuogno, L.; Galdi, C. Secure Firmware Update: Challenges and Solutions. *Cryptography* **2023**, *7*, 30. [CrossRef]
61. Ahn, J.; Hussain, R.; Kang, K.; Son, J. Exploring Encryption Algorithms and Network Protocols: A Comprehensive Survey of Threats and Vulnerabilities. *IEEE Commun. Surv. Tutor.* **2025**. [CrossRef]
62. Tsantikidou, K.; Sklavos, N. Threats, Attacks, and Cryptography Frameworks of Cybersecurity in Critical Infrastructures. *Cryptography* **2024**, *8*, 7. [CrossRef]
63. 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. [CrossRef]
64. Althamir, M.; Alabdulhay, A.; Yasin, M.M. A Systematic Literature Review on Symmetric and Asymmetric Encryption Comparison Key Size. In Proceedings of the 2023 3rd International Conference on Smart Data Intelligence (ICSMDI), Trichy, India, 30–31 March 2023; pp. 110–117. [CrossRef]
65. 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*, 334–344. [CrossRef]
66. 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. [CrossRef]
67. Cheng, Y.; Liu, Y.; Zhang, Z.; Li, Y. An Asymmetric Encryption-Based Key Distribution Method for Wireless Sensor Networks. *Sensors* **2023**, *23*, 6460. [CrossRef]
68. Cherkaoui Dekkaki, K.; Tasic, I.; Cano, M.-D. Exploring Post-Quantum Cryptography: Review and Directions for the Transition Process. *Technologies* **2024**, *12*, 241. [CrossRef]
69. 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. [CrossRef]
70. 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. [CrossRef]
71. Demir, E.D.; Bilgin, B.; Onbasli, M.C. Performance Analysis and Industry Deployment of Post-Quantum Cryptography Algorithms. *arXiv* **2025**, arXiv:2503.12952. [CrossRef]
72. 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. [CrossRef]
73. 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).
74. 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).
75. 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).
76. NIST: NIST Releases First 3 Finalized Post-Quantum Encryption Standards. Available online: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards (accessed on 15 August 2025).
77. Rani, A.; Ai, X.; Gupta, A.; Adhikari, R.S.; Malaney, R. Combined Quantum and Post-Quantum Security for Earth-Satellite Channels. *arXiv* **2025**, arXiv:2502.14240. [CrossRef]
78. Kearney, J.J.; Perez-Delgado, C.A. Vulnerability of blockchain technologies to quantum attacks. *Array* **2021**, *10*, 100065. [CrossRef]

79. Ansong, S.; Rankothge, W.; Sadeghi, S.; Mohammadian, H.; Bin Rashid, F.; Ghorbani, A. Role of cybersecurity for a secure global communication eco-system: A comprehensive cyber risk assessment for satellite communications. *Comput. Secur.* **2025**, *149*, 104156. [CrossRef]
80. Pote, P.; Bansode, R. Performance Evaluation of Post-Quantum Cryptography: A Comprehensive Framework for Experimental Analysis. *J. Inf. Syst. Eng. Manag.* **2025**, *10*, 548–556. [CrossRef]
81. NIST. Feasibility and Performance of PQC Algorithms on Microcontrollers. Available online: https://csrc.nist.gov/CSRC/media/Events/Second-PQC-Standardization-Conference/documents/accepted-papers/kaps-feasibility-performance-pqc.pdf (accessed on 20 August 2025).
82. Gladis Kurian, M.; Chen, Y. Ascon on FPGA: Post-Quantum Safe Authenticated Encryption with Replay Protection for IoT. *Electronics* **2025**, *14*, 2668. [CrossRef]
83. 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. [CrossRef]
84. Borhani-Darian, P.; Li, H.; Wu, P.; Closas, P. Detecting GNSS spoofing using deep learning. *EURASIP J. Adv. Signal Process.* **2024**, *2024*, 14. [CrossRef]
85. Birutis, A.; Mykkeltveit, A. Practical Jamming of a Commercial 5G Radio System at 3.6 GHz. *Procedia Comput. Sci.* **2022**, *205*, 58–67. [CrossRef]
86. Santo, A.D.; Tiberti, W.; Cassioli, D. An Adaptive Dual-Stack QKD-PQC Framework for Secure and Reliable Inter-Site Communication. In Proceedings of the Joint National Conference on Cybersecurity (ITASEC & SERICS 2025), Bologna, Italy, 3–8 February 2025; pp. 1–12. Available online: https://ceur-ws.org/Vol-3962/paper56.pdf (accessed on 27 August 2025).
87. Chawla, D.; Mehra, P.S. A roadmap from classical cryptography to post-quantum resistant cryptography for 5G-enabled IoT: Challenges, opportunities and solutions. *Internet Things* **2023**, *24*, 100950. [CrossRef]
88. Malina, L.; Popelova, L.; Dzurenda, P.; Hajny, J.; Martinasek, Z. On Feasibility of Post-Quantum Cryptography on Small Devices. *IFAC-Pap.* **2018**, *51*, 462–467. [CrossRef]
89. Zeydan, E.; Baranda, J.; Mangues-Bafalluy, J. Post-Quantum Blockchain-Based Secure Service Orchestration in Multi-Cloud Networks. *IEEE Access* **2022**, *10*, 129520–129530. [CrossRef]
90. Kumar, M. Post-quantum cryptography Algorithm's standardization and performance analysis. *Array* **2022**, *15*, 100242. [CrossRef]
91. Astarloa, A.; Lázaro, J.; Gárate, J.I. CRYSTALS-Dilithium post-quantum cyber-secure SoC for wired communications in critical systems. *Internet Things* **2025**, *33*, 101656. [CrossRef]
92. 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. [CrossRef]
93. Maiti, S.; Mehta, D.; Chowdhury, D.R. Preventing Fault Attacks on S-Boxes of AES-Like Block Ciphers. In *Cyber Warfare, Security and Space Research, Proceedings of the SpacSec 2021, Communications in Computer and Information Science*; Joshi, S., Bairwa, A.K., Nandal, A., Radenkovic, M., Avsar, C., Eds.; Springer: Cham, Switzerland, 2021; Volume 1599. [CrossRef]
94. Pandit, A.A.; Mishra, A. Efficient implementation of post quantum MLWR-based PKE scheme using NTT. *Comput. Electr. Eng.* **2024**, *118*, 109358. [CrossRef]
95. Bhasin, S.; D'Anvers, J.-P.; Heinz, D.; Pöppelmann, T.; Van Beirendonck, M. Attacking and Defending Masked Polynomial Comparison for Lattice-Based Cryptography. *IACR Trans. Cryptogr. Hardw. Embed. Syst.* **2021**, *3*, 334–359. [CrossRef]
96. Khan, Q.; Purification, S.; Chang, S.-Y. Post-Quantum Key Exchange and Subscriber Identity Encryption in 5G Using ML-KEM (Kyber). *Information* **2025**, *16*, 617. [CrossRef]
97. Huang, Z.; Wang, H.; Cao, B.; He, D.; Wang, J. A comprehensive side-channel leakage assessment of CRYSTALS-Kyber in IIoT. *Internet Things* **2024**, *27*, 101331. [CrossRef]
98. Iavich, M.; Kuchukhidze, T. Investigating CRYSTALS-Kyber Vulnerabilities: Attack Analysis and Mitigation. *Cryptography* **2024**, *8*, 15. [CrossRef]
99. 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. [CrossRef]
100. Erni, S.; Kotuliak, M.; Leu, P.; Roeschlin, M.; Capkun, S. AdaptOver: Adaptive Overshadowing Attacks in Cellular Networks. *arXiv* **2021**, arXiv:2106.05039. [CrossRef]
101. PatentPC. 5G & Cybersecurity: Network Threats Stats. Available online: https://patentpc.com/blog/5g-cybersecurity-network-threat-stats (accessed on 20 July 2025).
102. 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. *Balt. J. Mod. Comput.* **2023**, *11*, 500–522. [CrossRef]
103. 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. *Comput. Electron. Agric.* **2024**, *225*, 109326. [CrossRef]

104. 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. *Instrum. Mes. Metrol.* **2021**, *20*, 289–300. [CrossRef]
105. Kashtan, V.Y.; Hnatushenko, V.V.; Laktionov, I.S.; Diachenko, H.H. Intelligent Sentinel satellite image processing technology for land cover mapping. *Nauk. Visnyk Natsionalnoho Hirnychoho Universytetu* **2024**, *5*, 143–150. [CrossRef]