SECURITY & DEFENCE QUARTERLY
https://securityanddefence.pl/

Algorithms and methods for cybersecurity of critical infrastructures in quantum computing: A scoping literature review

Monika Wolfmayr[1], Ummar Ahmed[2]

[1]monika.wolfmayr@jamk.fi

[1] https://orcid.org/0000-0002-3548-8240

[2] https://orcid.org/0009-0000-0470-9736

[1,2]Institute of Information Technology, Jamk University of Applied Science, Piippukatu 2, 40100, Jyväskylä, Finland

Abstract

Information technology is vital in handling critical infrastructures, such as power grids, water supplies, healthcare, transportation networks, and infrastructures in space. Quantum computing has potential to revolutionise critical infrastructures by enabling faster optimisation, simulation, and data analysis for complex systems. The adoption of quantum technologies demands the reconsideration of cybersecurity protocols to mitigate quantum-era threats. Along with the technological progress in quantum computing, there is a risk of cyberattacks leading to research questions, asking: what new quantum computing algorithms are being designed to secure critical infrastructures; how they compare to conventional methods; how quantum computing algorithms are being designed to enhance the reliability of critical infrastructures; and what quantum computing methods are emerging for ensuring the stability and accuracy of computations critical to infrastructure management? This work focuses on answering these research questions by presenting a scoping review conducted by considering 420 research articles. The scoping review shows the possibilities that can be achieved by implementing various algorithms and methods for cybersecurity. The study encircles many categories, such as optimisation, security, networking, algorithms, protocols, communication, power systems, and space science, and shows that quantum computing can enhance their protection. This study discusses techniques for the cybersecurity of critical infrastructures in quantum computing and presents results on infrastructure analysis. We targeted various research phrases regarding the research questions mentioned about algorithms and methods for cybersecurity of critical infrastructure in quantum computing. This work calls for the reader to consider the various ways to protect critical infrastructures from different threats, including cyberattacks.

Keywords:

quantum computing, cybersecurity, quantum algorithms, quantum computing applications, critical infrastructures

Article info
Received: 06 November 2025
Revised: 19 May 2026
Accepted: 20 May 2026
Available online: 07 July 2026

Citation: Wolfmayr, M. and Ahmed, U. (2026) 'Algorithms and methods for cybersecurity of critical infrastructures in quantum computing: A scoping literature review', *Security and Defence Quarterly*, 54(2), pp. 20–33. doi: 10.35467/sdq/222239.

© 2026 M. Wolfmayr and U. Ahmed. published by War Studies University, Poland.
This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).

Introduction

Information technology (IT) is evolving due to the new discipline of quantum computing. In quantum computing, critical infrastructure serves as the foundation for applications requiring extremely secure communication and unprecedented processing capacity. The Quantum Approximate Optimisation Algorithm (QAOA) is examined and compared, and its use in locating important nodes in vital infrastructure is examined in a case study. The idealised quantum computer simulation outlines possible future solutions while exposing real-world difficulties and constraints (Silva and Droguett, 2024). The investigation of QAOA's use in critical infrastructure analysis is consistent with developments in security protocols, including a recently suggested authentication mechanism that is secure, lightweight, and energy-efficient. Through session key formation and anonymity, this system improves user privacy while providing multi-factor authentication that is resistant to both traditional and quantum attacks. Its advantage in computing, communication, and power efficiency is further demonstrated by a security analysis, which enhances the reliable solutions required to secure quantum-driven infrastructures (Momeni *et al.*, 2023). The practicality of integrating traditional and quantum technologies into a single network has been proved by the successful integration of quantum communication into the current telecommunications infrastructure. This development demonstrates how prepared Quantum Key Distribution (QKD) systems and contemporary networking techniques are for practical use cases and real-world deployments, as confirmed by deployment in production settings (IEEE, 2021). This research expands the use of quantum technologies to a new field with the Quantum Improved Weather Forecast framework, building on the integration of sophisticated quantum systems into practical infrastructure. The framework seeks to increase weather forecast accuracy and disaster preparedness by fusing quantum machine learning (ML) with conventional techniques, showcasing the revolutionary potential of quantum computing in a variety of domains (Suhas and Divya, 2023).

The process started with research questions intended to investigate algorithms and methods for critical infrastructure cybersecurity. Databases such as IEEE Xplore, Science Direct, and Google Scholar were used to collect pertinent data for this scoping study. A seamless and economical transition to quantum-safe cryptography is made possible by an integrated network design that blends classical and quantum communications (Aguado *et al.*, 2019). Building on this, the study introduces a secure framework for distributing virtual network functions (VNFs) across data centres, leveraging QKD and software-defined networking (SDN) to bolster security in the evolving landscape of software-defined networks (Aguado *et al.*, 2017a). By examining post-quantum cryptography options, this integrated approach also analyses Multimedia Internet KEYing–Sakai-Kasahara Key Encryption's (MIKEY–SAKKE) susceptibility to quantum computing. By highlighting the trade-offs between security and performance, the study strengthens the network architecture's resilience in the post-quantum age (Verchyk and Sepulveda, 2021). Electricity grids are vital hubs for energy supply and must be adequately protected to ensure their security. The challenges of deploying QKD systems to safeguard critical infrastructure are explored, with a real-world demonstration of their application within an electricity grid's network (Evans *et al.*, 2021). It is suggested that cyber-physical systems (CPS) use quantum cryptography to communicate securely, and it is investigated how quantum computing might improve these systems' efficiency (Tosh *et al.*, 2020). The following research questions are addressed throughout the scoping review:

> **RQ1**: What are new quantum methods and algorithms being designed to secure critical infrastructures, and how do they compare to conventional methods?

RQ2: How are quantum computing algorithms being designed to enhance the reliability of critical infrastructures?

RQ3: What kind of quantum methods are emerging for ensuring the stability and accuracy of computations critical to manage infrastructures?

This work aims at presenting current developments in quantum computing algorithms for securing the reliable functioning of critical infrastructures. The systematic literature review of this work contributes to the understanding in how quantum computing and cyber security methods must be combined for guarding critical infrastructures. The results of this scoping review highlight the interdisciplinary nature of the field when addressing their application for safety of critical infrastructures.

The technique afforded in Section 2 is followed by our paper; the technique comprises actions such as presenting the study background, developing the research questions, and outlining the procedures for data collection, identification, screening, and paper inclusion. Section 3 presents the findings of this scoping review, systematically organised into categories and subcategories, with particular emphasis on the ways in which quantum computing threatens conventional systems. After that, the discussion is covered in Section 4, and finally Section 5 summarise all conclusions of the scoping review.

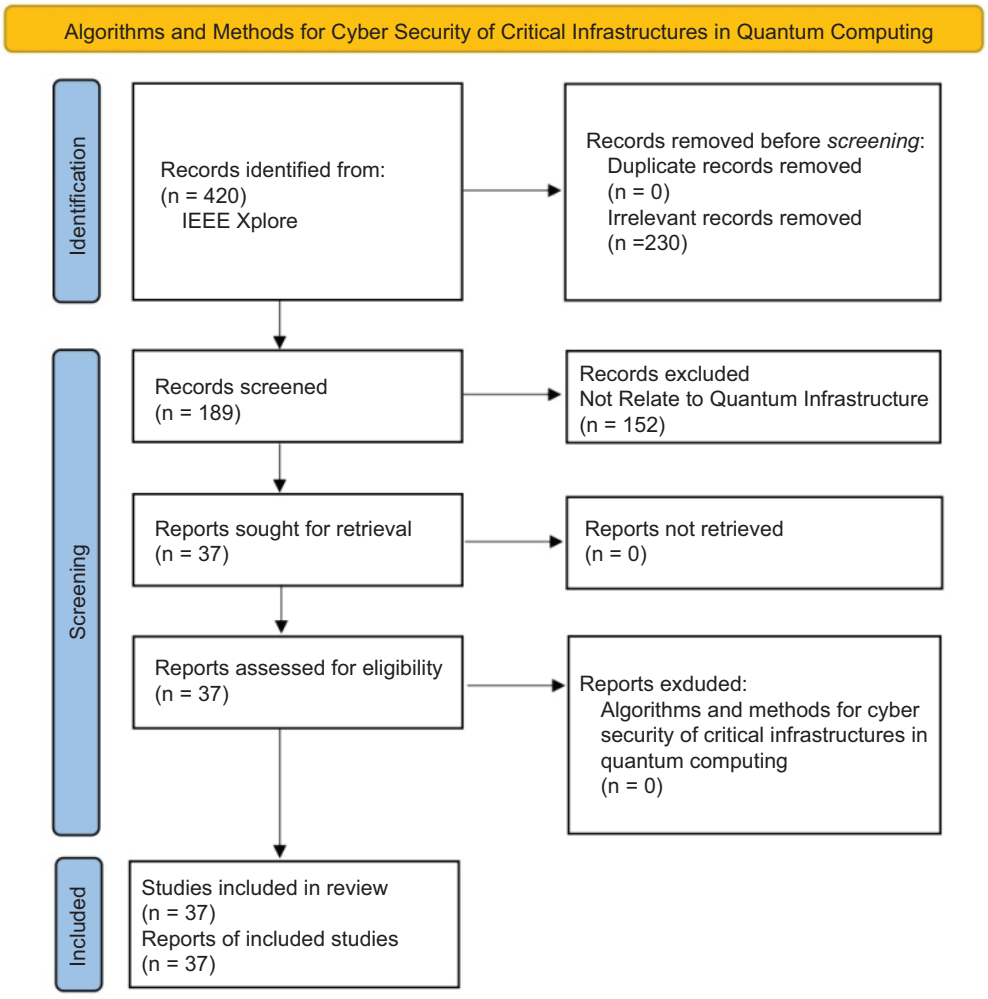
Methodology

The systematic scoping review conducted in this work aims mainly at algorithms and methods for the cybersecurity of critical infrastructures in quantum computing (QC) and details of their direct applications. The stages of the scoping review described by Arksey and O'Malley (2005) and Levac *et al.* (2010) were used in this study.

The study began by defining the scope of the topic and initiation of target research phrases regarding the research questions about the algorithms and methods for cybersecurity of critical infrastructures in quantum computing. IEEE Xplore, Science Direct, and Google Scholar were used and quantum critical infrastructures, quantum cybersecurity, quantum cybersecurity threats, quantum cybersecurity methods, quantum cybersecurity algorithms, quantum computing techniques, and quantum secure infrastructure analysis were shortlisted to initiate the scoping review, as described in Figure 1. The research was most relevant to the topic and it was compiled based on the results collected from different databases. In addition to this, the research was limited to journals only to obtain the most precise data. An effort was made to ensure that highly effective algorithms and methods were included in the research. Consequently, journals published from 2010 onwards were selected as the minimum timeframe for consideration. Furthermore, it was decided to limit the search to the first 420 relevant results using IEEE Xplore and first ten pages for Google Scholar.

Hence, any search results with quantum studies' irrelevant domains, for instance environmental monitoring and prediction, physics, natural disasters, etc., were easily left out using mentioned criteria. Along with these environmental and monitoring prediction and physics categories, collaboration of quantum studies was discovered with cloud computing, smart grids, system optimisation, network optimisation, cryptography, security, secure communication, networking, energy efficiency, algorithms, energy systems, protocols, distributed systems, communication, power systems, space science, and blockchain. All these are well-known domains, but research was limited and continued with optimisation, security, networking, algorithms, protocols, communication, power systems, and space science. All these categories and their references are presented in Table 1.

Figure 1. PRISMA flowchart of the scoping review.



Results

In this review, we grouped the research papers into algorithms and methods, and applications. The applications included areas such as networking, protocols, communication, power systems, and space science. The categorisation obtained is outlined in Table 1.

Algorithms and methods

Algorithms and methods form the foundation for understanding the interplay between quantum and classical computing. By examining approaches that harness quantum mechanics besides those constrained by conventional architectures, it becomes possible to assess both advancements enabled by quantum techniques and vulnerabilities emerging within traditional systems.

Algorithms threading quantum-based systems

Recent advancements in quantum combinatorial optimisation have been reviewed with a focus on QAOA, a promising approach in the field. A case study was executed to identify

Table 1. Research papers

Categories	References
Algorithms and methods	Aguado *et al.*, 2017a, 2017b, 2019; Alam, 2017; Aleksic *et al.*, 2013; Althobaiti and Dohler, 2021; Ansar *et al.*, 2023; Autry *et al.*, 2023; Evans *et al.*, 2019, 2021; Jagan *et al.*, 2023; Javed *et al.*, 2024; Jenefa *et al.*, 2023; Kebapci *et al.*, 2022, 2023; Khan *et al.*, 2020; Kitayama *et al.*, 2011; Raddo *et al.*, 2019; Rajeh, 2022; Silva and Droguett, 2024; Suhas and Divya, 2023; Tosh *et al.*, 2020; Verchyk and Sepulveda, 2021; Yavuz *et al.*, 2022; Zeydan *et al.*, 2022
Networking	Borah, 2023; Emu *et al.*, 2023; IEEE, 2021; Kalinin and Krundyshev, 2021
Protocols	Momeni *et al.*, 2023; Niehus *et al.*, 2023; Qu *et al.*, 2023
Application to space science, communication and power systems	Alomari and Kumar, 2023; Li *et al.*, 2010; Liu *et al.*, 2010

the key nodes in critical infrastructure using simulated, noise-free quantum computer. The findings demonstrate that applying quantum techniques to solve combinatorial optimisation issues in real-world settings has certain practical difficulties and constraints (Silva and Droguett, 2024). Current cryptography systems are seriously threatened by quantum computing, necessitating the development of new security measures. Aguado *et al.* (2019) show how classical communications and QKD can be combined into a single, production-ready network. The method allows for a gradual transition to quantum-secure networks without significant disruptions or upfront costs by utilising software-defined architectures and quantum-safe algorithms. The feasibility of this approach for connecting current security with future quantum-safe systems is demonstrated by its practical application on a functioning network. Unlike conventional approaches that rely on solvable mathematical problems, QKD employs quantum mechanics to generate cryptographic keys that are secure against computing advancements. Security issues are raised by the increasing threat of adversarial attacks to generative artificial intelligence (AI) anomaly detection systems with the development of quantum computing. In order to address the shortcomings of current models, Jenefa *et al.* (2023) suggest a revolutionary strategy that combines sophisticated generative AI approaches with quantum-resistant algorithms. This dynamic solution increases resistance against adversarial threats based on quantum technology by adjusting to new assault techniques. A possible route to safe anomaly detection systems in the quantum era is provided by experimental results that validate their efficacy. Internet of Things (IoT) communication is made possible by narrow-band IoT (NB-IoT), but quantum computing poses threats to cybersecurity. Althobaiti and Dohler (2021) present a location-aware cryptographic system that leverages lattices for effective, portable, and quantum-resistant security, using geographic location as an identity. In contrast to current protocols, this approach ensures safe authentication, avoids location spoofing, avoids the requirement for simulation (SIM) cards and public key infrastructure (PKI), and is resistant to quantum and collusion attacks. It provides a strong solution for post-quantum IoT security and is applicable to networks other than NB-IoT. In order to assess strategies for the practical and economical deployment of quantum-encrypted communication, Aleksic *et al.* (2013) investigate the integration of QKD into passive optical access networks. Raddo *et al.* (2019) describe the creation of an open-access QKD testbed in Eindhoven (the Netherlands) with the goal of confirming technological certification, security proofs, and business applications. It aims to establish an open environment for

end-to-end validation of QKD systems, in contrast to the closed QKD testbeds that are already in place. In order to improve end-user security and encourage the integration of QKD into the existing networks, the testbed investigates a quantum-to-the-home network for on-demand quantum encryption services.

Algorithms threading conventional systems

The security threats that quantum computing poses to IoT and AI-based systems, which handle private information, are addressed by Yavuz *et al.* (2022). The multi-party computation quantum network core (MPC-QNC) framework combines post-quantum cryptography, QKD, and AI to ensure secure, efficient, and privacy-preserving distributed systems. Key applications include trustworthy post-quantum machine learning (TPQ-ML), a secure federated learning system, and hybrid distributed quantum-safe public key infrastructure (HDQPKI), a quantum-safe PKI. VNFs across data centres also pose security challenges as networks adopt software to reduce costs. In order to enable secure and economical VNF distribution, Aguado *et al.* (2017a) present a secure approach that combines QKD with network functions virtualisation (NFV) and SDN. The approach demonstrates quantum communication performance in distributed settings via a time-shared optical network. QKD ensures secure communication, with numerous protocols developed to enhance utility and address channel vulnerabilities. Key QKD techniques are thoroughly examined for security in Khan *et al.* (2020), addressing their theoretical underpinnings, real-world uses, and simulated outcomes. Additionally, identity-based encryption (IBE) is well suited for mission-critical applications, as it uses identifiers to encrypt data without requiring user certificates or prior setup. For scalable and secure multimedia communications, MIKEY-SAKKE uses IBE; nevertheless, it also uses cryptographic techniques that are susceptible to quantum assaults. Verchyk and Sepulveda (2021) place National Institute of Standards and Technology's (NIST) post-quantum candidates, assess MIKEY-SAKKE's performance on limited devices, and define needs for post-quantum cryptography to replace smoothly the existing techniques. The results indicate that various combinations of post-quantum algorithms present trade-offs in speed, key size, and efficiency, as no NIST finalist fully meets all the requirements for a plug-and-play quantum-secure MIKEY-SAKKE. Implementing QKD systems for critical infrastructure also faces challenges, such as hardware interoperability, scalability, and optical loss. In order to address these concerns, Evans *et al.* (2021) provide findings from a field test of three QKD systems on an actual utility fibre network. For Cyber-Physical Systems (CPS) to remain highly efficient and prevent downtime, strong security is necessary. Current methods such as Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA) are vulnerable to quantum computing threats. Quantum cryptography offers a robust alternative, resistant to such attacks. Tosh *et al.* (2020) address the effects of implementing quantum cryptography in CPS and emphasise how quantum computers can improve security by processing and communication without being constrained by scalability. Modern power grids rely on trustworthy synchrophasor measurements. The existing methods for detecting malicious data in power systems have limitations, such as failing to identify manipulated data or depending on physical device security. To ensure data provenance and prevent manipulation, Javed *et al.* (2024) propose a protocol based on quantum principles and physically unclonable functions (PUFs), whose effectiveness is validated through security and performance analyses using IBM's Qiskit platform. It is lightweight, with minimal computational, communication, and storage demands, and provides strong protection against cyberattacks in the quantum era. The supervisory control and data acquisition (SCADA) systems monitor real-time data, control processes, and communicate with devices, but increasing connectivity exposes them to cyberthreats, including quantum-based attacks. To mitigate these risks, Rajeh (2022) proposes a

quantum-cryptography method combining hash-based signatures and QKD for secure key generation and authentication, significantly enhancing SCADA security against quantum and conventional threats. For secure data transmission in underwater networks, Burak Kebapçı and his team presents a BB84-based real-time QKD system, integrating Field-Programmable Gate Arrays (FPGA), on-board microprocessors, and optical front-ends for photon counting. Real-time monitoring, external uninterruptible power supply (UPS), and a laser alignment tool for manual setup confirmation are included (Kebapci *et al.*, 2022). Optical access networks offer high data proportions but pose security challenges, particularly in time-division multiplexing passive optical networks (TDM-PONs), where shared signals threaten privacy. Physical-layer encryption, such as QKD, can secure communication, while application-layer methods rely on safe key distribution. With quantum computing advancing, technologies, such as autonomous driving, require renewed security measures, and mobile networks should adopt quantum-resistant security algorithms (QRSAs) for safe connectivity. Zeydan *et al.* (2022) investigate how to improve data security in vehicle-to-everything services by utilising the Service & Computation Orchestrator (SCO) framework. Zeydan *et al.* (2022) illustrate how various computer techniques function under various central processing units' (CPU) loads using number theory research unit (NTRU) as a quantum-resistant security algorithm (QRSA). The study also examines current standards and future directions for post-quantum security in mobile networks. As edge-based AI demands faster processing and lower latency, secure decentralised data-sharing becomes crucial. Autry *et al.* (2023) propose the decentralised Open IoT Security Protocol (dOISP), employing quantum-safe cryptosystems for secure communication. Networks can improve edge-based AI security and efficiency by integrating dOISP, particularly in large-scale settings (Autry *et al.*, 2023). Kitayama *et al.* (2011) accepts emerging security threats in photonic networks, particularly risks to user data confidentiality and network control. Kitayama *et al.* (2011) propose a secure photonic network with QKD to protect control signals and user data, using generalized multiprotocol label switching (GMPLS) controllers and key management agents (KMAs) for provisioning of a secure path. A deployment roadmap addresses business- and mission-critical applications, highlighting the need for advanced cybersecurity, as traditional measures lose effectiveness. In order to improve defence cybersecurity, Ansar *et al.* (2023) investigate cutting-edge technologies, such as AI, machine learning, blockchain, and quantum computing. Machine learning improves accuracy, while AI can automate threat detection. Data security is guaranteed by blockchain, and although quantum computing is still in its infancy, it has the potential to both challenge and provide new encryption standards. Ansar *et al.* (2023) also examine how these technologies affect defence cybersecurity policy and practice. Mobile commerce (M-commerce) faces rising demands for security and privacy, especially in sensitive transactions. With merchants using Wi-Fi hotspots for online trading, secure communication is crucial. The McEliece cryptosystem, a post-quantum method, is proposed to enhance data encryption and privacy. It provides unbreakable security for mobile transactions (Alam, 2017). A real-time underwater QKD system built on the BB84 protocol and utilising FPGA technology is presented by Kebapci *et al.* (2023). An FPGA and an onboard computer (OBC) with optical front-ends that can count photons in real time are part of the system. For more than a 7-meter link, it was successfully tested for secure key distribution at a rate of 100 qubits per second. In addition, the system has an alignment indicator and visible laser for manual alignment checking. Computers attached to the system monitor its characteristics. Jagan *et al.* (2023) investigate the application of deep learning to develop a machine learning model for thwarting cyberthreats. The model uses a convolutional neural network (CNN) with variational autoencoders (VAEs) to analyse network traffic and system behaviour for threat detection. Results show high accuracy, supporting its use in automated monitoring and response. The study also enables advances in autonomous cybersecurity, global threat intelligence, and quantum-resistant encryption. SDN and NFV make networks more

dynamic and cost-efficient but introduce vulnerabilities in data transfer. QKD ensures high security by generating symmetric keys resistant to cryptographic attacks. In order to secure a control layer in SDN and NFV settings, Aguado *et al.* (2017a) suggest integrating QKD with current protocols. It demonstrates QKD combined with conventional keys for secure SDN–cloud communication. The quantum-improved weather forecast (QWF) framework enhances prediction accuracy by integrating traditional methods with quantum machine learning. In order to improve forecasts, lower mistakes, and better prepare for extreme weather events and ultimately save lives and safeguard infrastructure, QWF uses quantum algorithms, such as quantum support vector machines (QSVM) and neural networks (Suhas and Divya, 2023).

Networking

The integration of quantum communications into current telecommunication networks is demonstrated by the Madrid Quantum Communication Infrastructure. With successful installations and use cases in manufacturing facilities, the project exhibits a high degree of technological readiness by fusing QKD systems with contemporary networking (IEEE, 2021). The proliferation of mobile devices and a wide range of apps make it difficult for network operators to effectively manage resources. By establishing several virtual networks on a single infrastructure, network slicing provides an answer. Nevertheless, network slicing optimisation is still difficult. In order to improve network slicing efficiency in self-organising networks (SONs), Borah (2023) suggests utilising quantum computing. The method enhances resource allocation by utilising quantum-inspired optimisation algorithms, such as quantum annealing and quantum evolutionary algorithms. Network slices are also modified by a quantum-assisted self-organising process in response to traffic patterns. Simulations demonstrate that this quantum-based strategy performs better than traditional techniques, providing higher service quality and efficiency. Advances in digitalisation and info telecommunications technology over the last 10 years have given cybercriminals more chances. By adapting to communication contexts, polymorphic threats are rendering conventional network defence techniques obsolete. Kalinin and Krundyshev (2021) investigate the ways in which SDN and computational intelligence (CI) can enhance network security and performance. Comprehensive protection against cyber threats is provided by methods such as machine learning, artificial neural networks (ANN), swarm intelligence, and quantum machine learning that are efficient in processing large datasets, and identifying routing anomalies, polymorphic attacks, and false data injections. By connecting both real and virtual worlds, the Metaverse improves Internet of Sense (IoS) communication and makes senses, such as taste and smell, possible. For the infrastructure that supports this, resource allocation must be done efficiently. In order to maximise resource allocation in data marketplaces, Emu *et al.* (2023) suggest a stochastic integer programming (SIP) model with reservation and on-demand plans. Furthermore, the model reduces computing complexity by using Quantum Neural Networks (QNN) to estimate demand with less input. The strategy is to enhance real-time management in the virtual world, boost service sales, and reduce the cost of Metaverse resources.

Protocols

Security and cloud resource issues can come up as 6G connectivity in the Internet of Vehicles (IoV) expands, resulting in more users and data. Qu *et al.* (2023) suggest a Quantum Efficient Privacy Protection (QEPP) protocol for private, secure edge-to-cloud transfer that makes use of quantum communication. To improve cloud performance and

data processing speed, it uses an improved quantum Grover algorithm, effective coding, and quantum error correction. In addition to meeting essential requirements, such as accuracy, speed, and security, the QEPP guarantees privacy protection. Cyberattacks pose a threat to IoT, impeding its integration into vital infrastructures. In order to protect user privacy and anonymity, Momeni *et al.* (2023) suggest a session key establishment authentication procedure that is lightweight, safe, and energy-efficient. For increased durability, the protocol incorporates multi-factor authentication. According to a security study, it can withstand attacks from both traditional and quantum computers. Additionally, protocol performs better than current systems in terms of communication, computing, and power usage. Moreover Niehus *et al.* (2023) focus on the Bennett–Brassard 1984 (BB84) protocol-based QKD system, in which data is transmitted to an optical ground station from a small quantum satellite in low Earth orbit. Creating a testbed and simulator for a hardware-in-the-loop quantum photonic ground station is the goal.

Application to space science, communication, and power systems

Without requiring system changes, the advanced metering infrastructure (AMI) is intended to support future smart grid features and improve the existing smart metering capabilities. Distribution automation, service restoration, and network monitoring are just a few of the areas that gain from AMI's improved information gathering and dissemination between consumers and utility providers. The benefits of a carefully thought-out AMI for electrical grid operations and planning are covered in Liu *et al.* (2010). The goal of reactive power optimisation (RPO) is to minimise power loss, manage voltage, and enhance network performance. The handling of discrete variables and non-linear functions in RPO is the subject of a recent study, with algorithm convergence being a major obstacle. In order to prevent premature convergence, Li *et al.* (2010) suggest an enhanced quantum discrete particle swarm optimisation (PSO) technique that combines it with chaotic optimisation. The method accelerates convergence and improves global search. Simulation results from real-world power networks and the Institute of Electrical and Electronics Engineers' (IEEE) systems demonstrate that this approach provides significant global search capabilities and a faster proportion of convergence. Space technologies can be disrupted by space weather phenomena, such as geomagnetic storms and solar flares. Conventional detection techniques frequently lack accuracy and speed. Using quantum computing, Alomari and Kumar (2023) suggest a Hybrid Classical-Quantum Neural Network (HCQNN) that can identify space weather occurrences with 99.9% accuracy. By providing early warnings, the method lessens the effects on both economy and society while increasing the resilience of space-based systems. It demonstrates how quantum computing can enhance space weather forecasting and detection.

Discussion

The security of critical infrastructure is increasingly being shaped by quantum and post-quantum approaches. The findings suggest that algorithms, such as QAOA, post-quantum cryptographic methods, and hybrid quantum, and classical networks are moving beyond theory and are starting to offer real ways to protect systems against both current and future threats (Momeni *et al.*, 2023; Silva and Droguett, 2024). Techniques that focus on optimisation and authentication appear especially useful for improving resilience and reliability. Communication methods, such as QKD, are already being tested in real settings, which show that gradual adoption is possible (Evans *et al.*, 2021).

At the same time, the review points out a number of challenges. Many quantum algorithms still only exist in simulations or small test systems, and their use in large or complex infrastructures is limited by hardware and expenses (Silva and Droguett, 2024). Post-quantum cryptography is a more practical option in the short term, but open questions still exist about efficiency, scalability, and security (Momeni *et al.*, 2023). Another issue is that most of the research looks at separate areas, such as networking, cryptography, or optimisation, without combining them into a complete model of infrastructure protection (Aguado *et al.*, 2017b).

The results suggest that future security needs a mix of approaches. Classical defences should not be abandoned but instead combined with quantum-resistant algorithms and, where possible, quantum-based methods. Algorithms alone are not enough. Progress also depends on standards, cooperation between sectors, and investment in systems that can handle quantum communication and computation (Evans *et al.*, 2021; Verchyk and Sepulveda, 2021).

Looking forward, research should aim to close the gap between theory and practice. Work is needed on scaling QAOA for infrastructure optimisation, creating efficient hybrid communication protocols, and designing adaptive systems that use both AI and quantum-resistant methods (Momeni *et al.*, 2023; Silva and Droguett, 2024). It is also important to study non-technical factors, such as regulations, standards for interoperability, and policies for risk management, so that new algorithms can be applied in practice (Aguado *et al.*, 2019).

Quantum algorithms and methods have the potential to change how we protect critical infrastructures, but this role is still developing. The field carries a lot of promises but also many uncertainties. Interdisciplinary research and practical demonstrations are essential to make sure that the benefits of quantum computing are achieved without creating new risks for vital systems (Evans *et al.*, 2021).

Conclusions

In order to address our research questions, we investigated how new quantum techniques and algorithms are being developed to safeguard critical infrastructure and how they stack up against traditional approaches (RQ1). Because of the development of cyber techniques and the potential for exploitation of the security of critical infrastructures in quantum computing, this issue is crucial for research right now. There ought to be a few potential solutions to get around these weaknesses. We therefore inquired as to how quantum computing algorithms are being developed to improve the dependability of vital infrastructures (RQ2) and what quantum techniques are developing to guarantee the accuracy and stability of calculations that are essential for infrastructure management (RQ3). In the cyber world, modern systems share information with each other and are becoming more interdependent. This data is essential to infrastructure operations, but there is a chance that it could be hacked. By using different algorithms and techniques to secure vital infrastructure in quantum computing, this risk can be reduced. Recent advancements in quantum combinatorial optimisation, using the QAOA, highlight challenges and limitations in applying quantum methods to real-world problems, as observed in a case study on critical infrastructure. The MPC-QNC architecture, which integrates post-quantum cryptography, QKD, and AI, was presented to ensure distributed systems that are secure, efficient, and protect privacy. Another approach uses software-defined architectures and quantum-safe algorithms to enable a gradual shift to quantum-secure networks without major disruptions or upfront expenses. The study proposes a novel

approach that blends quantum-resistant algorithms with advanced generative AI techniques. By adapting to novel attack strategies, this dynamic approach strengthens defences against adversarial threats based on quantum technologies. Optimising network slicing is a challenging procedure. The use of quantum computing has been explored as a means of increasing network slicing efficiency in SONs. With the use of quantum-inspired optimisation methods, including quantum annealing and quantum evolutionary algorithms, the technique improves resource allocation. This study is not exhaustive. Numerous secure quantum authentication methods, scalable quantum security solutions, robust quantum infrastructure, etc. are the subjects of future investigations.

Funding

The Regional Council of Central Finland under the grant No. KSL/237/04.03.04.00/2023 and the European Union's Renewing and Competent Finland 2021–2027 Just Transition Fund under the Finnish Future Farm project R-00791.

Author Contributions

Conceptualisation, M.W.; methodology, M.W., U.A.; validation, U.A.; formal analysis, U.A.; investigation, U.A.; resources, U.A.; data curation, U.A.; writing—original draft preparation, M.W., U.A.; writing—review and editing, M.W., U.A.; supervision, M.W.; project administration, M.W.; funding acquisition, M.W. Both authors read and agreed to the published version of the manuscript.

Data Availability Statement

Not applicable.

Disclosure Statement

No potential conflict of interest was reported by the authors.

References

Aguado, A., Hugues-Salas, E., Haigh, P.A., Marhuenda, J., Price, A.B., Sibson, P., *et al.* (2017a) 'Secure NFV orchestration over an SDN-controlled optical network with time-shared quantum key distribution resources', *Journal of Lightwave Technology*, 35(8), pp. 1357–1362. doi: 10.1109/jlt.2016.2646921.

Aguado, A., Lopez, V., Lopez, D., Peev, M., Poppe, A., Pastor, A., *et al.* (2019) 'The engineering of software-defined quantum key distribution networks', *IEEE Communications Magazine*, 57(7), pp. 20–26. doi: 10.1109/mcom.2019.1800763.

Aguado, A., Lopez, V., Martinez-Mateo, J., Szyrkowiec, T., Autenrieth, A., Peev, M., *et al.* (2017b) 'Hybrid conventional and quantum security for software defined and virtualized networks', *Journal of Optical Communications and Networking*, 9(10), pp. 819–825. doi: 10.1364/jocn.9.000819.

Alam, M.S. (2017) 'Secure M-commerce data using post quantum cryptography', in *2017 IEEE international conference on power, control, signals and instrumentation engineering (ICPCSI)*, Chennai, India, pp. 649–654. doi: 10.1109/icpcsi.2017.8391793.

Aleksic, S., Winkler, D., Franzl, G., Poppe, A., Schrenk, B. and Hipp, F. (2013) 'Quantum key distribution over optical access networks', in *Proceedings of the 2013 18th European conference on network and optical communications & 2013 8th conference on optical cabling and infrastructure (NOC-OC&I),* Graz, Austria, pp. 11–18, doi: 10.1109/NOC-OCI.2013.6582861.

Alomari, A. and Kumar, P. (2023) 'Hybrid classical-quantum neural network for improving space weather detection and early warning alerts', in *2023 IEEE conference on computational and applied artificial intelligence (CCAAW)*, Cleveland, OH, USA, pp. 1–6. doi: 10.1109/ccaaw57883.2023.10219316.

Althobaiti, O.S. and Dohler, M. (2021) 'Quantum-resistant cryptography for the internet of things based on location-based lattices', *IEEE Access*, 9, pp. 133185–133203. doi: 10.1109/access.2021.3115087.

Ansar, S.A., Aggarwal, S., Arya, S., Sayeed, M.A., Soni, N. and Pathak, P.C. (2023) 'Elevating cybersecurity in defence: A collaborative and technologically driven approach', in *2023 6th international conference on contemporary computing and informatics* (IC3I), Gautam Buddha Nagar, India, pp. 403-408, doi: 10.1109/ic3i59117.2023.10397948.

Arksey, H. and O'Malley, L. (2005) 'Scoping studies: Towards a methodological framework', *International Journal of Social Research Methodology*, 8(1), pp. 19–32. doi: 10.1080/1364557032000119616.

Autry, C.P., Henderson, W., Magal, M., and Roscoe, A.W. (2023) 'Leveraging the decentralised open IoT security protocol ((d)OISP)™: Facilitating edge-based artificial intelligence in large-scale network infrastructures', in *2021 International conference on electrical, computer and energy technologies (ICECET)*, Cape Town, South Africa, pp. 1–8. doi: 10.1109/icecet58911.2023.10389601.

Borah, A.R. (2023) 'Enhancing network slicing efficiency in self-organizing networks using quantum computing', in *2023 International conference on smart electronics and communication (ICOSEC)*, Trichy, India, pp. 722–726. doi: 10.1109/icosec58147.2023.10276206.

Emu, M., Choudhury, S. and Salomaa, K. (2023) 'Quantum neural networks driven stochastic resource optimization for metaverse data marketplace', in *2023 IEEE 9th international conference on network softwarization (NetSoft)*, Madrid, Spain, pp. 242–246. doi: 10.1109/netsoft57336.2023.10175433.

Evans, P.G., Alshowkan, M., Earl, D., Mulkey, D.D., Newell, R., Peterson, G., *et al.* (2021) 'Trusted node QKD at an electrical utility', *IEEE Access*, 9, pp. 105220–105229. doi: 10.1109/ACCESS.2021.3070222.

Evans, P., Peterson, G., Morgan, T., Jones, K., Morrison, S., Newell, R. *et al.* (2019) 'Demonstration of a quantum key distribution trusted node on an electric utility fiber network', in *2022 IEEE photonics conference (IPC)*, San Antonio, TX, USA, pp. 1–2. doi: 10.1109/ipcon.2019.8908470.

Jagan, S., Pokhariyal, R., Mahajan, K., Deva Sudha, P. and Dutta, A. (2023) 'Machine learning with deep learning approach for cyber security threats prevention model', in *2023 international conference on innovative computing, intelligent communication and smart electrical systems (ICSES)*, Chennai, India, pp. 1–5. doi: 10.1109/icses60034.2023.10465570.

Javed, K., Khan, M.A., Ullah, M., Aman, M.N. and Sikdar, B. (2024) 'Securing synchrophasors using data provenance in the quantum era', *IEEE Open Journal of the Communications Society*, 5, pp. 1594–1608. doi: 10.1109/ojcoms.2024.3372524.

Jenefa, A., Ebenezer, V., Isaac, A.J., Marshell, J., Pradeepa, P. and Naveen, V. (2023) 'Adversarial attacks on generative AI anomaly detection in the quantum era', in *2023 7th international conference on electronics, communication and aerospace technology (ICECA)*, Coimbatore, India, pp. 1833–1840. doi: 10.1109/iceca58529.2023.10395092.

Kalinin, M.O. and Krundyshev, V. (2021) 'Computational intelligence technologies stack for protecting the critical digital infrastructures against security intrusions', in *2021 fifth world conference on smart trends in systems security and sustainability (WorldS4)*, London, United Kingdom, pp. 118–122. doi: 10.1109/worlds451998.2021.9514004.

Kebapci, B., Levent, V.E., Ergin, S., Mutlu, G., Baglica, I., Tosun, A., *et al.* (2023) 'FPGA-based implementation of an underwater quantum key distribution system with BB84 protocol', *IEEE Photonics Journal*, 15(4), pp. 1–10. doi: 10.1109/JPHOT.2023.3287493.

Kebapci, B., Mutlu, G., Baglica, I., Tosun, A., Ergin, S., Levent, V.E., *et al.* (2022) 'Real-time implementation of an underwater quantum key distribution system', in *2022 Underwater communications and networking conference (UComms)*, pp. 1–5. doi: 10.1109/ucomms56954.2022.9905688.

Khan, E., Meraj, S. and Khan, M.M. (2020) 'Security analysis of QKD protocols: Simulation & comparison', in *2020 17th international Bhurban conference on applied sciences and technology (IBCAST)*, Islamabad, Pakistan, pp. 383–388. doi: 10.1109/ibcast47879.2020.9044522.

Kitayama, K., Sasaki, M., Araki, S., Tsubokawa, M., Tomita, A., Inoue, K., *et al.* (2011) 'A novel conceptual model of secure photonic networks', in *2011 International conference on transparent optical networks (ICTON)*, Stockholm, Sweden, pp. 1–4. doi: 10.1109/icton.2011.5970925.

Levac, D., Colquhoun, H. and O'Brien, K.K. (2010) 'Scoping studies: advancing the methodology', *Implementation Science*, 5(1), p. 69. doi: 10.1186/1748-5908-5-69.

Li, N.S., Zhao, N.D., Zhang, N.X. and Wang, N.C. (2010) 'Reactive power optimization based on an improved quantum discrete PSO algorithm', in *2010 5th international conference on critical infrastructure (CRIS)*, Beijing, pp. 1–5. doi: 10.1109/cris.2010.5617552.

Liu, E., Chan, M.L., Huang, C.W., Wang, N.C. and Lu, C.N. (2010) 'Electricity grid operation and planning related benefits of advanced metering infrastructure', in *2010 5th International Conference on Critical Infrastructure (CRIS)*, Beijing, China. doi: 10.1109/CRIS.2010.5617583.

Lopez, D., Brito, J. P., Pastor, A., Martin, V., Sánchez, C., Rincon, D. and Lopez, V. (2012) 'Madrid Quantum Communication Infrastructure: a testbed for assessing QKD technologies into real production networks', in *2021 optical fiber communications conference and exhibition (OFC)*, San Francisco, CA, USA, pp. 1–4. doi: 10.1364/OFC.2021.Th2A.4.

Momeni, M.R., Jabbari, A. and Fung, C. (2023) 'An energy-efficient multiple-factor authentication protocol for critical infrastructure IoT systems', in *2023 International conference on computer science and network technology (CSNet)*, Montreal, QC, Canada, pp. 238–242. doi: 10.1109/csnet59123.2023.10339700.

Niehus, M., Silva, J.M., Simão, J., Serrador, A. and Mendes, M.J.G.C. (2023) 'Towards a hardware-in-the-loop quantum optical ground station simulator and testbed', in *2023 International conference on space optical systems and applications (ICSOS)*, Vancouver, BC, Canada, pp. 217–222. doi: 10.1109/icsos59710.2023.10491227.

Qu, Z., Chen, Z., Ning, X. and Tiwari, P. (2023) 'QEPP: A quantum efficient privacy protection protocol in 6G-quantum internet of vehicles', *IEEE Transactions on Intelligent Vehicles*, 9(1), pp. 905–916. doi: 10.1109/tiv.2023.3304852.

Raddo, T.R., Rommel, S., Land, V., Okonkwo, C. and Monroy, I.T. (2019) 'Quantum data encryption as a service on demand: Eindhoven QKD network testbed', in *2019 21st international conference on transparent optical networks (ICTON)*, Angers, France, pp. 1–5. doi: 10.1109/icton.2019.8840238.

Rajeh, W. (2022) 'An integrated authentication scheme for supervisory control and data acquisition system based on quantum key distribution', in *2022 International conference on communication and information technology (ICCIT)*, Tabuk, Saudi Arabia, pp. 374–378. doi: 10.1109/iccit52419.2022.9711639.

Silva, G.S.M. and Droguett, E.L. (2024) 'Quantum Computing Optimization: Application and Benchmark in Critical Infrastructure Assessment', in *2024 annual reliability and maintainability symposium (RAMS)*, Albuquerque, NM, USA, pp. 1–7. doi: 10.1109/RAMS51492.2024.10457821.

Suhas, S. and Divya, S. (2023) 'Quantum-improved weather forecasting: Integrating quantum machine learning for precise prediction and disaster mitigation', in *2023 international conference on quantum technologies,*

communications, computing, hardware and embedded systems security (iQ-CCHESS), Kottayam, India, pp. 1–7. doi: 10.1109/iq-cchess56596.2023.10391714.

Tosh, D., Galindo, O., Kreinovich, V. and Kosheleva, O. (2020) 'Towards security of cyber-physical systems using quantum computing algorithms', in *2020 IEEE 15th international conference of system of systems engineering (SoSE)*, Budapest, Hungary. doi: 10.1109/sose50414.2020.9130525.

Verchyk, D. and Sepulveda, J. (2021) 'Towards post-quantum enhanced identity-based encryption', in *2021 24th Euromicro conference on digital system design (DSD)*, Palermo, Italy, pp. 502–509. doi: 10.1109/dsd53832.2021.00081.

Yavuz, A.A., Nouma, S.E., Hoang, T.M., Earl, D. and Packard, S. (2022) 'Distributed cyber-infrastructures and artificial intelligence in hybrid post-quantum era', in *2022 IEEE 4th international conference on trust, privacy and security in intelligent systems, and applications (TPS-ISA)*, Atlanta, GA, USA, pp. 29–38. doi: 10.1109/tps-isa56441.2022.00014.

Zeydan, E., Turk, Y., Aksoy, B. and Tasbag, Y.Y. (2022) 'Post-quantum era in V2X security: Convergence of orchestration and parallel computation', *IEEE Communications Standards Magazine*, 6(1), pp. 76–82. doi: 10.1109/mcomstd.0001.2100060.