World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

Quantum-safe: Cybersecurity in the age of Quantum-Powered AI

Bibhu Dash [1,*] and Sameeh Ullah [2]

[1] *School of Computer and Information Sciences, University of the Cumberlands, Williamsburg, KY USA.*
[2] *School of Information Technology, Illinois State University, Normal, IL USA.*

World Journal of Advanced Research and Reviews, 2024, 21(01), 1555–1563

Publication history: Received on 14 November 2023; revised on 27 December 2023; accepted on 29 December 2023

Article DOI: https://doi.org/10.30574/wjarr.2024.21.1.2640

Abstract

There is a lot of talk about how the cyber world will change and perceive itself as quantum computing takes center stage in the computing industry in a decade. While some are enthusiastic about the advancement of quantum technology, others remain skeptical about its application in cyberspace. But there is no doubt the interaction of artificial intelligence (AI) and quantum computing offers cybersecurity both tremendous benefits and difficulties as we navigate the digital terrain. This article explores the complex interrelationship between these two state-of-the-art technologies and how it affects information system security. In this article, we look at the possible risks that the fusion of AI and quantum computing could bring, as well as the creative ways that experts are attempting to strengthen our cyber protections, current research and future directions.

Keywords: Quantum Computing; Cybersecurity; AI; QKD; FIDO2

1. Introduction

With an annual growth rate of 15%, the problem of cybersecurity is becoming increasingly pervasive [1]. The increasing digitization and system dependency of society has increased the complexity of the cyber risk and data privacy issue. Many organizations and tech startups are researching strategies to develop a cyber-resistant environment. But it is not possible yet since hackers utilize the same technology that we employ to protect our systems and data to steal our information and commit fraud. However, numerous researchers believe that the evolution of quantum computing will solve the problem of digital risks and usher in a new era of cyber defense.

The concept of quantum computing is relatively new and currently has very few choices for implementation. It might take a few years to a decade to develop a quantum computer that is accurate, functional and enterprise ready. Although 170 businesses worldwide have already begun utilizing IBM's 27 quantum systems, these are currently being used for research purposes as opposed to operational or useful ones [2]. However, there is a lot of conjecture and research around how quantum computing will alter the cybersecurity landscape. Artificial intelligence and quantum computing have been gradually integrated into more aspects of our lives to discover solutions to complex problems, and cybersecurity is one of them. Although these technologies have many advantages, their combination also adds new levels of complexity to the field of cybersecurity. This paper aims to dissect the complex nature of this issue and investigate methods for preserving future digital ecosystems in a dynamic environment.

2. AI and Cybersecurity

The cyber security industry has been significantly impacted by artificial intelligence (AI). Artificial intelligence has improved threat identification, incident response, recommendations, and vulnerability assessment, which has changed

* Corresponding author: Bibhu Dash.

cybersecurity procedures [3]. As a branch of artificial intelligence, machine learning algorithms have demonstrated the capacity to examine enormous datasets and identify trends that may point to potential security risks. However, adversaries can mount increasingly sophisticated attacks using the same technology that fortifies our defenses. A new level of complexity has been introduced by adversarial machine learning, necessitating the development of strong defenses that can respond to ever-changing threats[2].

3. Quantum Computing and Its Implications

Quantum computing is a branch of quantum information science that employs the ability to generate and use quantum bits, or qubits [3]. Quantum networking, quantum sensing, and quantum simulation are all part of it. Two key characteristics of qubits, in contrast to classical computers, have a profound impact on how quantum computers store and process data:

- Superposition: a particle's capacity to exist in more than one state simultaneously.
- Entanglement: the capacity of two particles to communicate despite their great distance from one another.

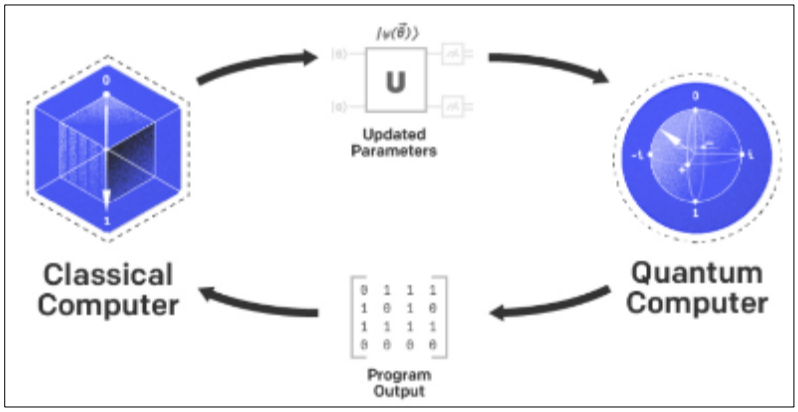

Figure 1 Bit and Qbit representation of classic and quantum computing models[4]

With its potential to do complicated calculations at rates impossible by classical computers, quantum computing presents a unique set of difficulties to traditional cryptography systems (see Table 1). Shor's technique, for example, is capable of breaking standard public-key cryptography schemes such as RSA and ECC [3, 5]. This worry is driving the desire for cryptography approaches that can survive the processing capabilities of quantum computers. Monroe et al. demonstrate gates which are basic quantum logic operation as shown in equations 1-5.

$|0\rangle|\downarrow\rangle \rightarrow |0\rangle|\downarrow\rangle$ (1)

$|0\rangle|\uparrow\rangle \rightarrow |0\rangle|\uparrow\rangle$ (2)

$|1\rangle|\downarrow\rangle \rightarrow |1\rangle|\uparrow\rangle$ (3)

$|1\rangle|\uparrow\rangle \rightarrow |1\rangle|\downarrow\rangle$ (4)

$\{|11\rangle|\uparrow\uparrow\rangle \rightarrow |01\rangle|\downarrow\uparrow\rangle\}$ (5)

Table 1 Operative differences between classical vs. quantum computing.

Classical Computing with AI	Quantum Computing with AI
Usage is in large scale and multipurpose	Usage is limited and mechanics-based computers
Information stored in bits	Information stored in quantum bits.
Discrete number of possible states: 0 or 1	There is infinite and continuous number of possible states.

Calculations are deterministic, repetitive type and slow	Calculations are probabilistic with multiple output options to the same input.
Data processing is carried out by linear logic and mostly sequential	Data processing is carried out by quantum logic and mostly parallel instances
Operations are stated mainly by Boolean algebra.	Operations are stated by linear algebra over Hilbert space.
Circuit behaviors are defined by classical physics	Circuit behaviors are defined by quantum mechanics

As quantum computing develops, there are numerous opportunities to enhance cybersecurity. From the creation of quantum-resistant cryptographic algorithms to unbreakable encryption via QKD, the incorporation of quantum technology provides a promising future. In order to fully realize the potential of quantum computing to improve cybersecurity in the digital era, interdisciplinary research projects and collaboration will be necessary. The opportunities for quantum computing are much more and highlighted below:

3.1. Quantum Key Distribution (QKD) for Unbreakable Encryption

Quantum Key Distribution (QKD) is a ground-breaking method of secure communication that is made possible by quantum computing. Theoretically impervious to eavesdropping, QKD facilitates the exchange of cryptographic keys through the use of notions from quantum physics. A quantum-safe substitute for conventional encryption techniques, communication channel security is provided by the employment of entangled particles in key distribution [6].

3.2. Post-Quantum Cryptography

Although traditional cryptography approaches are threatened by the advent of quantum computers, new cryptography techniques that are immune to quantum attacks are also made possible. The study of algorithms that can withstand the processing power of quantum computers is known as PQC. Among the promising post-quantum data-security techniques being researched are lattice-based, hash-based, and code-based encryption [7].

3.3. Enhanced Threat Detection through QML

Machine learning algorithms could be significantly accelerated by quantum computing, leading to quicker and more effective danger identification. Utilizing the computational benefits of quantum computers, quantum machine learning(QML) processes and analyzes large amounts of data, enhancing the capacity to identify and address cyber threats quickly [8].

3.4. Secure Multi-Party Computation (SMPC) for Collaborative Security

Quantum computing enables numerous parties to collaborate to compute a function over their inputs while retaining the privacy of these inputs, allowing for Secure Multi-Party Computation (SMPC). This technique has applications in collaborative security scenarios where sensitive material must be examined without revealing personal information [9].

3.5. Quantum-Safe Protocols

To secure the security of digital communication in the post-quantum future, quantum-resistant cryptographic methods are being developed. These protocols, including NTRUEncrypt and Hash-Based Message Authentication Code (HMAC), provide novel solutions to the vulnerabilities created by quantum computers [10].

3.6. Collaborative Research Initiatives

Cooperation between government, business, and academia is required to fully realize the potential of quantum computing for cybersecurity. Through efforts such as the National Institute of Standards and Technology's (NIST) Post-Quantum Cryptography Standardization initiative as shown in Figure 2 [11], experts collaborate to develop quantum-safe standards for cryptographic algorithms.

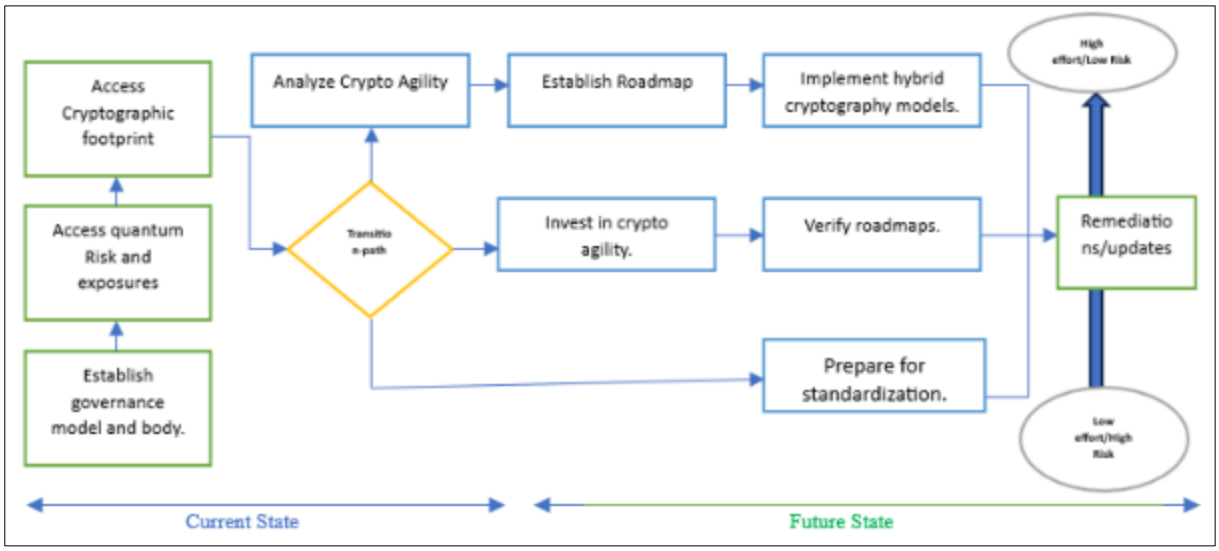

Figure 2 Describes the current and future (NIST Standards) quantum-resilient future.

4. Challenges of Quantum Computing for Cyber World

The science of cybersecurity confronts many challenges as quantum computing evolves and as it also has enormous potential to increase computational skills. In the age of quantum computing, understanding, and resolving these difficulties is critical if digital system security is to be ensured. The following are some key challenges and impediments:

4.1. Breaking Current Cryptographic Systems

Effective problem solving is possible with quantum computers, even for problems that are currently unsolvable for classical computers. For example, Shor's approach poses a threat to popular public-key encryption systems like RSA and ECC since it can factor large numbers exponentially faster than the best-known classical algorithms [12].

4.2. Quantum-Resistant Cryptography Development

While the development of quantum computers is progressing, there is uncertainty about when large-scale, practical quantum computers will be available. This timeline uncertainty poses challenges for the timely deployment of quantum-resistant cryptographic solutions [6, 13].

4.3. Stored Encrypted Data Vulnerability

Current approaches for encrypting data may not be secure against quantum computers. If data gets into the wrong hands, even encrypted and stored data today may be susceptible to quantum attacks in the future [14].

4.4. Transition Period Vulnerabilities (classic to quantum)

Hacker assaults could potentially compromise hybrid cryptography systems during the shift from conventional to quantum-safe systems. Securing this transition will need careful planning and implementation [14].

4.5. Quantum Key Distribution Challenges

Although Quantum Key Distribution (QKD) offers a viable means of facilitating secure key exchange, its widespread implementation presents logistical and resource-related issues due to its substantial physical infrastructure requirements [15].

4.6. Quantum-Safe Standardization

There is no widely recognized standard for post-quantum cryptography yet. The development and application of quantum-resistant cryptography standards is a challenging process that calls for cooperation between standardization organizations, business, and academic institutions [16].

4.7. Algorithmic Vulnerabilities

When used with quantum algorithms, several algorithms that are thought to be secure against classical algorithms may start to show weaknesses. This covers the algorithms utilized in digital signatures and hash functions.

4.8. Cost of Quantum-Safe Cryptography

The implementation and operation of quantum-resistant cryptographic algorithms may require additional resources due to their computational demands [17]. Devices and systems with little resources may so encounter problems.

4.9. Quantum-Specific Attacks

There could be an increase in attack vectors that take use of quantum phenomena as quantum computers become more common. It needs a thorough understanding of cybersecurity concepts and quantum mechanics to defend against these new dangers [18].

4.10. Interdisciplinary Skill Gap

Multidisciplinary knowledge is required when cybersecurity and quantum computing intersect. Building a qualified workforce is hampered by the current lack of experts with a thorough understanding of both cybersecurity and quantum physics.

5. The Confluence of AI and Quantum Computing

A new age in cybersecurity is being steered by the combination of AI and quantum computing. Utilizing the computational benefits of quantum computers, QML techniques (AI) process and analyze data ten times faster than their classical counterparts. This convergence creates new risks that require innovative mitigation techniques, even if it could solve challenging cybersecurity issues. The convergence of cybersecurity and quantum computing demands interdisciplinary expertise. It is currently challenging to build a trained workforce due to the lack of experts with a deep understanding of both cybersecurity and quantum physics.

Figure 3 Changing future of Enterprise Cybernetics with Quantum-powered AI

6. AI boost with rise of Quantum Computing

Quantum computing is often hailed as the next big thing in artificial intelligence. Numerous possibilities can be processed simultaneously by quantum computers. This could speed up AI algorithms and enable them to handle more datasets more quickly, leading to the development of stronger AI models. A recent analysis by the Boston Consulting Group estimates that the market potential for quantum prospects in generative, foundational, and horizontal AI is between $50 billion and $100 billion, with the ability to affect almost every industry [14, 15]. Benefits of quantum computing in AI are detailed in below.

6.1. Accelerated Machine Learning Algorithms (QML)

There exists optimism that quantum computing will greatly accelerate some machine learning techniques. Quantum computers can investigate several options at once thanks to quantum parallelism, which speeds up the training and optimization of machine learning models [14, 19].

Compared to their conventional counterparts, quantum machine learning (QML) algorithms process and analyze big datasets more quickly by taking advantage of the special capabilities of quantum computing. complicated correlations and patterns can be found using QML, which helps create AI models that are more complicated and accurate [19, 20].

6.2. Optimization Problems

Solving difficult optimization issues, such figuring out a machine learning model's ideal parameter, is a common task for artificial intelligence applications. When it comes to optimization challenges, quantum computers are especially well-suited since they have the ability to identify solutions faster than traditional techniques [20].

6.3. Enhanced Feature Selection

Machine learning feature selection procedures can be enhanced by quantum computing. Larger solution spaces can be explored by quantum algorithms, which makes it easier to find pertinent features and reduce dimensionality more effectively.

6.4. Quantum Neural Networks

By utilizing the principles of quantum computing, quantum neural networks (QNNs) are able to perform tasks that classical neural networks could find challenging. QNNs may enhance the capacity of AI systems to represent intricate relationships and patterns in data [21].

6.5. Improved Random Sampling

Random sampling, a crucial process in many AI algorithms, is an area in which quantum computers shine. Tasks like Monte Carlo simulations, which are frequently used in AI applications like reinforcement learning and optimization issues, might benefit from this capability [22].

6.6. Simulating Quantum Systems

Compared to classical computers, quantum computers are better at simulating quantum systems [2]. This is especially important for AI applications in chemistry, materials science, and drug development because these fields have high processing demands when simulating quantum systems accurately.

6.7. Enhanced Data Analysis

The ability of quantum computing to process and analyze massive datasets in parallel can improve data analysis tasks[4]. This is critical for AI applications that handle large volumes of data, such as computer vision and natural language processing.

6.8. Cryptography for Secure AI

Artificial intelligence can be safeguarded by quantum computing, as it facilitates the development of cryptographic algorithms that are immune to quantum errors. Quantum-safe encryption is important for secure AI applications in the future since AI systems often depend on secure communication and data privacy[22].

6.9. Hybrid Quantum-Classical Systems

Combining the advantages of classical and quantum computing can enhance AI capabilities in hybrid systems. Utilizing the advantages of both paradigms, quantum computers can be applied to specific tasks inside a broader classical AI framework [23].

7. Solutions and Mitigations

In order to secure data in the post-quantum age, developing cryptographic algorithms that are immune to quantum errors is crucial. Moreover, explainable AI can increase transparency in cybersecurity systems by making AI model

conclusions easier for human operators to understand and accept [23]. To develop cutting-edge solutions, it is essential to establish interdisciplinary research initiatives that unite specialists in cybersecurity, AI, and quantum computing.

With the emergence of Quantum computing, there is a race to develop security infrastructure solutions that Quantum computers cannot penetrate. Google has now devised a quantum-resilient method of implementing the FIDO2 security key (Passkeys) standard, an increasingly popular alternative to passwords. Unlike passwords, these are external, physical devices used just for authentication, such as USB sticks (see Figure 4) [24].

Figure 4 Representation of a FIDO2 key or Passkey using in classic computers.

Google also intends to utilize a hybrid strategy that combines a security key approach and a post-quantum cryptography algorithm known as Dilithium, which has been accepted for standardization by the National Institute of Standards and Technology (NIST). Dilithium is intended to operate on the hardware of a standard security key, which has limited memory and computing capacity [24, 25]

8. Threats, Challenges and Future Directions

Quantum neural networks may process information in ways that classical neural networks cannot, and quantum machine learning may be able to classify larger datasets in less time. Although the technologies used in artificial intelligence today are complex and useful for a variety of purposes, quantum computing is a novel approach that has the potential to make substantial strides in the field [25]. Conversely, the path towards practical quantum computing is arduous and protracted. Quantum computing is often heralded as the next great advancement in artificial intelligence and numerous options can be handled simultaneously by quantum computers, but the question is here with what level of challenges [26]. Quantum could speed up AI algorithms and make it possible for them to handle more datasets more quickly, which would eventually result in stronger AI models. But with the advancement of AI and quantum computing, new risks emerge. Adversarial attacks utilizing quantum machine learning models, quantum attacks on classical cryptography systems, and the potential compromising of AI-driven cybersecurity systems are a few of the challenges that need to be addressed [27]. In order to design robust cybersecurity systems, researchers need to be aware of these potential threats.

The future of cybersecurity in the era of artificial intelligence and quantum computing is still unknown as the technology landscape changes [21, 25, 28]. The future of secure digital communication will be shaped in large part by the creation of quantum-safe standards, cyber-safe device practices, continuous research in explainable AI, and the training of a skilled workforce able to navigate this challenging environment.

9. Conclusion

Unprecedented cybersecurity risks and opportunities are presented by the convergence of AI and quantum computing. The combination of these technologies strengthens our defenses against cyberattacks, but it also introduces new hazards that call for constant innovation in the field. The scientific community may clear the way for a more safe and dependable digital future by tackling these challenges. The growing application of quantum computing will lead to a number of technical issues with data processing and transmission to quantum computers, algorithm implementation in quantum computers, and verification and return of quantum computing findings. It's time to look into how the world is using AI and quantum computing to improve living conditions despite several technical concerns. Furthermore, we are prepared to welcome you to quantum cybersecurity when the time comes to make wise, secure decisions.

Compliance with ethical standards

Disclosure of conflict of interest

The authors declare that they have no conflict of interest.

References

[1] Fox, J. (2023, December 8). Top cybersecurity statistics for 2024. Pentest as a Service. https://www.cobalt.io/blog/cybersecurity-statistics-2024

[2] Brijwani, G. N., Ajmire, P. E., & Thawani, P. V. (2023). Future of Quantum Computing in Cyber Security. In *Handbook of Research on Quantum Computing for Smart Environments* (pp. 267-298). IGI Global.

[3] Rangan, K. K., Abou Halloun, J., Oyama, H., Cherney, S., Assoumani, I. A., Jairazbhoy, N., ... & Ng, S. K. (2022). Quantum computing and resilient design perspectives for cybersecurity of feedback systems. IFAC-PapersOnLine, 55(7), 703-708.

[4] Said, D. (2023). Quantum Computing and Machine Learning for Cybersecurity: Distributed Denial of Service (DDoS) Attack Detection on Smart Micro-Grid. Energies, 16(8), 3572.

[5] Watchorn, M. S., & QIS, Q. (2022). Quantum Chemistry for Detecting Cybersecurity Threats to Information Systems.

[6] Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, 175-179.

[7] Ding, J., Xie, Y., Yang, B.-Y., & Chen, X. (2019). Quantum-safe cryptography: A survey. Frontiers of Information Technology & Electronic Engineering, 20(11), 1485-1503.

[8] Rebentrost, P., Mohseni, M., & Lloyd, S. (2014). Quantum support vector machine for big data classification. Physical Review Letters, 113(13), 130503.

[9] Broadbent, A., Fitzsimons, J. F., & Kashefi, E. (2009). Universal blind quantum computation. Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science, 517-526.

[10] Hoffstein, J., Pipher, J., & Silverman, J. H. (2019). NTRUEncrypt: Digital signatures and public-key cryptosystems. Springer.

[11] National Institute of Standards and Technology (NIST). (2021). Post-Quantum Cryptography Standardization. Retrieved from https://csrc.nist.gov/projects/post-quantum-cryptography.

[12] Ghosh, U., Das, D., & Chatterjee, P. (2023). A comprehensive tutorial on cybersecurity in quantum computing paradigm. Authorea Preprints.

[13] Ford, P. (2023). The quantum cybersecurity threat may arrive sooner than you think. Computer, 56(2), 134-136.

[14] Yadav, S. P., Singh, R., Yadav, V., Al-Turjman, F., & Kumar, S. A. (Eds.). (2023). Quantum-Safe Cryptography Algorithms and Approaches: Impacts of Quantum Computing on Cybersecurity. Walter de Gruyter GmbH & Co KG.

[15] Jofre, M. (2023). Seminar on Quantum Technologies for Cybersecurity: Networks and Systems.

[16] Serrano, M. A., Sanchez, L. E., Santos-Olmo, A., Garcia-Rosado, D., Blanco, C., & Fernandez-Medina, E. (2023). Towards a quantum world in cybersecurity land.

[17] Raheman, F. (2022). The future of cybersecurity in the age of quantum computers. Future Internet, 14(11), 335.

[18] Oxford Analytica. (2022). Quantum computing necessitates cybersecurity rethink. Emerald Expert Briefings, (oxan-db).

[19] Taiber, J. (2020). Unsettled topics concerning the impact of quantum technologies on automotive cybersecurity (No. EPR2020026). SAE Technical Paper.

[20] Ko, K. K., & Jung, E. S. (2021). Development of cybersecurity technology and algorithm based on quantum computing. Applied Sciences, 11(19), 9085.

[21] Dash, B., Sharma, P., & Ullah, S. (2021). Cloud Computing Security Issues, Vulnerabilities and Recommendations.

[22] Lee, M. (2021). Quantum Computing and Cybersecurity. Belfer Center for Science and International Affairs Harvard Kennedy School, Cambridge.

[23] Althobaiti, O. S., & Dohler, M. (2020). Cybersecurity challenges associated with the Internet of Things in a post-quantum world. IEEE Access, 8, 157356-157381.

[24] Brendel, J., Clermont, S., & Fischlin, M. (2023). Post-Quantum Asynchronous Remote Key Generation for FIDO2 Account Recovery. Cryptology ePrint Archive.

[25] Sharma, P., & Dash, B. (2023, March). Impact of big data analytics and ChatGPT on cybersecurity. In 2023 4th International Conference on Computing and Communication Systems (I3CS) (pp. 1-6). IEEE.

[26] Gompert, D. C., & Libicki, M. (2023). Towards a quantum internet: post-pandemic cyber security in a post-digital world. In Survival february–march 2021: A house divided (pp. 113-124). Routledge.

[27] Althobaiti, O. S., & Dohler, M. (2020). Cybersecurity challenges associated with the Internet of Things in a post-quantum world. IEEE Access, 8, 157356-157381.

[28] Rangan, K. K., Abou Halloun, J., Oyama, H., Cherney, S., Assoumani, I. A., Jairazbhoy, N., ... & Ng, S. K. (2022). Quantum computing and resilient design perspectives for cybersecurity of feedback systems. IFAC-PapersOnLine, 55(7), 703-708.