International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 9 Issue 6, Nov-Dec 2025 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Quantum Cybersecurity

Matthew N. O. Sadiku[1], Matthias Oteniya[2], Janet O. Sadiku[3]

[1,2]Roy G. Perry College of Engineering, Prairie View A&M University, Prairie View, TX, USA
[3]Juliana King University, Houston, TX, USA

ABSTRACT

The advent of quantum computing poses significant risks to cybersecurity, as it has the potential to break current encryption methods and compromise sensitive information. Experts believe that quantum computers capable of breaking current codes could be more than a decade away, but the threat necessitates immediate action in cybersecurity planning. Quantum cybersecurity is an emerging field that focuses on the development of quantum-resistant cryptographic protocols to protect against potential threats from quantum computers. It involves using quantum mechanics to improve security and the development of new, "quantum-resistant" methods to protect against threats from future quantum computers. This paper examines the use of quantum computing in cybersecurity.

KEYWORDS: *quantum computing, QC, security, cybersecurity, quantum cybersecurity.*

How to cite this paper: Matthew N. O. Sadiku | Matthias Oteniya | Janet O. Sadiku "Quantum Cybersecurity" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-9 | Issue-6, December 2025, pp.528-538, URL: www.ijtsrd.com/papers/ijtsrd99905.pdf

IJTSRD99905

INTRODUCTION

Work on quantum computing that is currently housed in research universities, government offices and major scientific companies, is progressing rapidly. Quantum computers can potentially break encryption algorithms like RSA and ECC that are widely used to secure Internet traffic, digital signatures, and other critical systems. Thus, current cryptographic standards could soon be vulnerable to attacks from quantum computers. It is predicted that sometime around 2035, quantum computers will become sufficiently powerful to compromise current widely used cryptographic standards, the foundation for online security. By 2040 or so, organized criminal groups could leverage quantum computing to disrupt financial systems, execute massive identity theft, and compromise sensitive healthcare records. In addition to the financial costs, there is the potentially catastrophic risk for society at large if attackers gain access to critical systems. Fortunately, quantum-resistant cybersecurity solutions are within reach [1].

QUANTUM COMPUTERS

A quantum computer (QC) behaves according to the laws of quantum mechanics. Thus, quantum computers are different from binary digital electronic computers based on transistors. A major difference between classical and quantum computing lies in the way they encode data. While a digital computer requires that the data be encoded into binary digits (0 or 1), quantum computers use quantum bits, which can be in superpositions of states [2]. In other words, instead of storing information in bits as conventional digital computers do, quantum computers use quantum bits, or qubits, to encode information. (Qubits are the basic units of quantum information.) In addition to ones and zeros, qubits have a third state called "superposition" that allows them to represent a one or a zero at the same time. Figure 1 shows the comparison between the bit and qubit [3]. The computing power of a QC grows exponentially with the number of qubits it uses.

Quantum computers have the potential to perform certain calculations significantly faster than any digital computers. QC consists of a quantum processor which operates at a very low temperature (a few tens of mK) and an electronic controller which reads out and controls the quantum processors, as shown in Figure 2 [4]. Several forms of physical media (optical fibers and free space) can be used to

deliver quantum information. Figure 3 shows a representation of quantum computing [5].

In quantum system, the computational space increases with the size of the system. This enables exponential parallelism which leads to faster quantum algorithms. Unlike classical computer, QC offers massive parallelism within a single piece of hardware.

A typical quantum computer is shown in Figure 4 [6]. The basic building blocks of quantum computers include quantum gates, quantum memories, quantum CPUs, quantum languages, and quantum languages [7,8]:

- *Quantum Gates:* Quantum computers require quantum gates, which are basically different from classical Boolean gates seen in a conventional computer (AND, XOR and so on). A quantum gate acts on superpositions of different basis states of qubits. The quantum gates perform unitary operations on quantum states and lead to quantum circuits. They are particularly important for quantum error correction and experimental quantum information processing. They can be realized by superconductors, linear optic tools, or quantum dots**.** Common quantum gates are CNOT and SWAP.
- *Quantum Memories:* Quantum memories store the quantum systems in a quantum register for information processing. Quantum memories are formulated by n stationary quantum states. Quantum computers are expected to have limited memory.
- *Quantum CPUs:* These use a quantum bus for the communication between the functional elements of a quantum computer. From a computing perspective, quantum CPUs can be approached through quantum adders.
- *Quantum Languages:* These enable us to create an artificial quantum computer to simulate a quantum computing environment. The programming language should follow a functional programming structure, which can compute the process as a whole entity with a proper bounded structure.
- *Quantum Algorithms:* Quantum algorithms are significantly faster than any classical algorithm in solving some problem. Most of the successful quantum algorithms use quantum Fourier transforms in them because they require less hardware. Popular quantum algorithms include Shor's algorithm (since integer factorization is faster) and Grover's search algorithm.

In ambitious attempts to realize practical quantum computers, enormous efforts are still being expended both in designing software (quantum algorithms) and hardware development (physical implementation).

OVERVIEW ON CLASSICAL CYBERSECURITY

Cybersecurity refers to a set of technologies and practices designed to protect networks and information from damage or unauthorized access. It is vital because governments, companies, and military organizations collect, process, and store a lot of data. As shown in Figure 5, cybersecurity involves multiple issues related to people, process, and technology [9]. Figure 6 shows different components of cybersecurity [10].

A typical cyber attack is an attempt by adversaries or cybercriminals to gain access to and modify their target's computer system or network. Cybercriminals or ethical hackers are modern-day digital warriors, possessing extraordinary skills and knowledge to breach even the most impregnable systems. A typical cybercriminal is shown on Figure 7 [11]. Cyber attacks are becoming more frequent, sophisticated, dangerous, and destructive. They are threatening the operation of businesses, banks, companies, and government networks. They vary from illegal crime of individual citizen (hacking) to actions of groups (terrorists) [12].

The cybersecurity is a dynamic, interdisciplinary field involving information systems, computer science, and criminology. The security objectives have been availability, authentication, confidentiality, nonrepudiation, and integrity. A security incident is an act that threatens the confidentiality, integrity, or availability of information assets and systems [13]. These are known as the pillars of information assurance.

- *Availability*: This refers to availability of information and ensuring that authorized parties can access the information when needed. Attacks targeting availability of service generally leads to denial of service.
- *Authenticity*: This ensures that the identity of an individual user or system is the identity claimed. This usually involves using username and password to validate the identity of the user. It may also take the form of what you have such as a driver's license, an RSA token, or a smart card.
- *Integrity*: Data integrity means information is authentic and complete. This assures that data, devices, and processes are free from tampering. Data should be free from injection, deletion, or

corruption. When integrity is targeted, nonrepudiation is also affected.

- *Confidentiality*: Confidentiality ensures that measures are taken to prevent sensitive information from reaching the wrong persons. Data secrecy is important especially for privacy-sensitive data such as user personal information and meter readings.
- *Nonrepudiation*: This is an assurance of the responsibility to an action. The source should not be able to deny having sent a message, while the destination should not deny having received it. This security objective is essential for accountability and liability.

Good practices for cybersecurity in construction companies should include all of these elements.

Everybody is at risk for a cyber attack. Cyber attacks vary from illegal crime of individual citizen (hacking) to actions of groups (terrorists). The following are typical examples of cyber attacks or threats [14]:

- *Malware*: This is a malicious software or code that includes traditional computer viruses, computer worms, and Trojan horse programs. Malware can infiltrate your network through the Internet, downloads, attachments, email, social media, and other platforms. Spyware is a type of malware that collects information without the victim's knowledge.
- *Phishing*: Criminals trick victims into handing over their personal information such as online passwords, social security number, and credit card numbers.
- *Denial-of-Service Attacks*: These are designed to make a network resource unavailable to its intended users. These can prevent the user from accessing email, websites, online accounts or other services.
- *Social Engineering Attacks*: A cyber criminal attempts to trick users to disclose sensitive information. A social engineer aims to convince a user through impersonation to disclose secrets such as passwords, card numbers, or social security number.
- *Man-In-the-Middle Attack*: This is a cyber attack where a malicious attacker secretly inserts him/herself into a conversation between two parties who believe they are directly communicating with each other. A common example of man-in-the-middle attacks is eavesdropping. The goal of such an attack is to steal personal information.

These and other cyber attacks or threats are shown in Figure 8 [15].

The social and financial importance of cybersecurity is increasingly being recognized by businesses, organizations, and governments. Cybersecurity involves reducing the risk of cyber attacks. Cyber risks should be managed proactively by the management. Cybersecurity technologies such as firewalls are widely available [16]. Cybersecurity is the joint responsibility of all relevant stakeholders including government, business, infrastructure owners, and users. Cybersecurity experts have shown that passwords are highly vulnerable to cyber threats, compromising personal data, credit card records, and even social security numbers. Governments and international organizations play a key role in cybersecurity issues. Securing the cyberspace is of high priority to the US Department of Homeland Security (DHS). Vendors that offer mobile security solutions include Zimperium, MobileIron Skycure, Lookout, and Wandera.

QUANTUM CYBERSECURITY

In cybersecurity, "quantum security" is pivotal due to quantum computing's potential to undermine encryption. The possibility of quantum computing eventually overcoming modern encryption safeguards is a valid concern. Quantum computers have the potential to compromise widely-used encryption methods due to their unprecedented computational abilities. This concern has prompted the National Institute of Standards and Technology (NIST) to call for the development of "quantum safe" encryption algorithms. The emerging field aims to develop quantum-resistant algorithms to protect digital communications against quantum threats [17]. Figure 9 shows potential security vulnerability causes [18].

Quantum cybersecurity is an emerging field that aims to utilize the principles of quantum mechanics to enhance data security in data centers. It leverages the strange properties of quantum mechanics to generate encryption keys that are impossible to hack with both classical and quantum computers. It is going to have huge implications for how we protect data and systems in the coming decades. Quantum cybersecurity is depicted in Figure 10 [19].

The core principle behind quantum cybersecurity is the use of quantum-resistant cryptographic protocols that can withstand attacks from both classical and quantum computers. In other words, quantum cryptography (QC) is one of the most promising applications of quantum computing in cybersecurity. QC is an umbrella term for encrypted communications that use quantum physics to keep complete privacy between all communication

channels and detect any attempts of eavesdropping. Quantum cryptographic systems aim to provide a secure communications channel between two parties: sender and recipient. Scientists are working to use quantum cryptography to ensure the security of our data beyond simple communication. Quantum cryptography is not a single technique but a field that explores different ways to secure communication using quantum mechanics. Here we consider the main two types and what each can do.

Quantum key distribution (QKD) is an area of research in quantum cybersecurity where quantum computing has had a significant impact. It is considered a form of quantum cryptography and refers to a mechanism for encrypting and decrypting messages. It uses a cryptographic protocol to generate a secret key that is shared and known among a single pair of sender and recipient. It leverages the principles of quantum mechanics to ensure the confidentiality of transmitted data. QKD systems, however, still have technological and theoretical loopholes, some of which could make it possible for eavesdroppers to intercept and decode messages.

Post-quantum cryptography (PQC) is a more advanced cryptographic algorithm. It takes a different approach to QKD. Post-quantum cryptography, sometimes referred to as quantum-resistant encryption, involves creating cryptographic protocols that can withstand potential attacks from quantum computers. It requires developing new cryptographic algorithms that are resistant to attacks from both classical and quantum computers. This field focuses on securing classical computer systems against the advanced computational capabilities of quantum computing. NIST is already working on post-quantum cryptography standardization, setting a framework for data protection against classical and quantum threats [20]. QKD is a complimentary solution to PQC, just less about software upgrades and more about hardware innovations. The transition to post-quantum cryptography will likely take several years, if not decades.

APPLICATIONS OF QUANTUM CYBERSECURITY

Quantum computing has quickly emerged as a feasible reality with vast potential applications. The prospects of employing quantum computing in cybersecurity are broad. Common areas of application include the following [21]:

- *Post-quantum cybersecurity in law firms*: Law firms have seen an alarming rise in sophisticated cyberattacks targeting, in particular, large law firms. To effectively counteract the intelligent systems employed by cybercriminals, law firms must evolve beyond conventional defense mechanisms and explore new technologies such as quantum computing. As the law continues to evolve, more sophisticated methodologies are expected to emerge, furthering the transformation of legal practice. Confidentiality is fundamental to the practice of law and is a core ethical obligation that all lawyers and law firms are bound to uphold. Although lawyers are not traditionally well-versed in digital storage technologies, the legal profession increasingly relies on digital infrastructure to manage and protect sensitive information, raising critical considerations with respect to data security and privacy.
- *Cybersecurity arms race*: The integration of quantum algorithms into the practice of law is a major change. While the progress of quantum computing holds the promise of transforming legal analytics, it also escalates the sophistication of cybersecurity threats. The legal profession shall proactively engage with these emerging technologies. This engagement is not merely an option but a requisite, driven by the fundamental ethical obligation to maintain client confidentiality and safeguard sensitive data.

BENEFITS

With quantum computers poised to break traditional cryptography, the urgency for quantum security innovations is paramount. One of the biggest prospects seen in quantum cybersecurity is its potential to create fully protected communications channels. Industries dealing with sensitive information, such as finance, government, and healthcare, stand to benefit significantly from quantum cybersecurity. Other benefits include the following [19,22-25]:

- *Quantum Advantage*: This could trigger a new phase of cyber-espionage competition, where access to CRQC resources determines which nations can read or protect the world's encrypted archives.
- *Quantum Supremacy:* This is the inflection point at which quantum computing will outpace the speed and accuracy of classical computing. With quantum supremacy, every organization in the world that stores and processes data will be wide open to a cyberattack. If this scenario is accurate, large organizations are facing a ticking time bomb if action is not taken immediately to mitigate future risk.
- *Quantum Computing Forensics*: Quantum computers will eventually become powerful

enough to crack traditional encryption, but they also open the door for new forensic tools to strengthen cyber defenses. For example, quantum algorithms could help detect malicious hackers or identify corrupted data more quickly.

- *Enhanced Threat Detection*: Traditional cyber threat detection often faces challenges in handling the complexity and volume of data generated. Quantum computing addresses this limitation by employing parallel processing through superposition. This enables quantum algorithms to analyze diverse threat scenarios concurrently, providing quicker insights into potential cyber threats.
- *Safer Communication:* Quantum encryption offers a high level of security by using quantum states to share cryptographic keys. If anyone tries to snoop on or measure these states, it immediately disturbs them, alerting the sender and receiver. This allows them to stop the transmission before any data is at risk.

CHALLENGES

The relationship between quantum computing and cyber security is one of both opportunity and threat. The development of quantum-resistant cryptographic protocols also faces challenges related to data security and privacy. Developing a skilled workforce ensures that organizations can effectively use quantum computing technologies and mitigate the associated risks. Other challenges include [19,21]:

- *High Cost*: Implementing quantum cybersecurity solutions raises important questions about cost and feasibility. The development and deployment of quantum-resistant cryptography will likely require significant investment in research and infrastructure. While QKD has been proven, it has not yet been widely deployed commercially due to cost and infrastructure challenges.
- *Endangering Critical Infrastructure*: The integration of quantum cybersecurity solutions with existing security protocols and frameworks is a complex task. Operational technology and industrial control systems often use long-lived hardware and cryptographic keys. These systems cannot be upgraded quickly. Quantum attacks could jeopardize essential sectors like energy, healthcare, and transportation if migrations lag behind.
- *Creating Geopolitical Imbalance*: The first nations or organizations to develop CRQC capability will gain a disproportionate intelligence and defense advantage. Encrypted diplomatic, military, and economic data from other nations could be exposed. That imbalance may reshape global power dynamics in cyberspace.
- *Standardization:* Governments and organizations are developing new standards and guidelines for quantum-resistant cryptography to address threats. They are treating quantum readiness as a global security priority. Their focus is on replacing vulnerable cryptographic systems before large-scale quantum computers emerge. The National Institute of Standards and Technology (NIST) is leading the charge in the United States, focusing on developing and implementing post-quantum cryptography (PQC) standards. As quantum emerges and organizations continue to explore and discover both its game-changing advantages and threats, new standards, legislation, and regulations are in the works.
- *Collaboration:* Addressing the cybersecurity implications of quantum computing requires global collaboration among governments, academia, and the private sector. International partnerships will become crucial for sharing knowledge, aligning regulations, and fostering innovation.
- *Workforce:* As with any technological upheaval, there is an acute need for skilled professionals who understand the nuances of the new landscape. The development of a workforce with expertise in quantum cybersecurity is essential to ensuring the long-term security of sensitive information. A knowledgeable workforce will be the first line of defense against emerging quantum threats. To ensure that the workforce is prepared to address the unique challenges of quantum cybersecurity, it is essential to develop new standards and certifications for quantum cybersecurity professionals.
- *Training:* Inserting the term “quantum” before any concept instantly increases its perceived complexity. Education and awareness have become focal points. It is essential to invest in training programs and courses that familiarize cybersecurity professionals with quantum computing concepts, threats, and defense mechanisms. Training programs for IT professionals now include modules on quantum threats and solutions. Businesses are investing in upskilling their teams to ensure they are equipped to handle the complexities of quantum-secure systems.
- *Scalability:* While QKD has been demonstrated in laboratory settings, scaling up these systems to accommodate real-world network architectures

and user demands remains a significant technical challenge. Also, the integration of QKD with existing classical communication infrastructure is also a complex task that requires careful consideration of compatibility and interoperability issues.

CONCLUSION

We are now living through a quantum revolution, with modern technology allowing us to fully utilize quantum phenomena. Quantum computing is not just the future of technology, but a current innovation that may drastically change the world as we know it. It has the potential to alter our perception of cybersecurity as we know it today. Quantum computing in cybersecurity is undeniably a topic that experts cannot overlook.

Organizations are increasingly recognizing the importance of preparing for a post-quantum world. Through preparation, agility, and collaboration, the world is already laying the groundwork for a quantum-safe future. To prepare, organizations should begin migrating to post-quantum cryptography, conduct cryptographic inventories, and adopt agile architectures that can integrate new standards as they are finalized. Universities and research institutions are developing new programs and courses focused on quantum cybersecurity, while industry leaders are investing in workforce development initiatives. The burden is on researchers, technologists, policymakers, and industries to ensure that as we step into the quantum age, we are well-equipped to handle its challenges. More information about quantum cybersecurity can be obtained from the books in [26-33].

REFERENCES

[1] J. Bobier et al., "How quantum computing will upend cybersecurity," October 2025, https://www.bcg.com/publications/2025/how-quantum-computing-will-upend-cybersecurity

[2] "Quantum computing," *Wikipedia,* the free encyclopedia https://en.wikipedia.org/wiki/Quantum_computing

[3] https://www.science.org.au/curious/policy-features/rethinking-cybersecurity-quantum-world

[4] B. Patra et al., "Cryo-CMOS circuits and systems for quantum computing applications," *IEEE Journal of Solid-State Circuits*, September 2017, pp.1-13.

[5] "Quantum computing and its applications," https://www.batoi.com/blogs/perspective/quantum-computing-applications-6357d329ccbad

[6] "Why organizations should prepare for quantum computing cybersecurity now," April 2023, https://www.ey.com/en_us/insights/innovation/why-organizations-should-prepare-for-quantum-computing-cybersecurity-now

[7] L. Gyongyosia and S. Imreb, "A survey on quantum computing technology," *Computer Science Review*, vol. 31, 2019, pp. 51-71.

[8] P. S. Menon and M. Ritwik, "Comprehensive but not complicated survey on quantum computing," *IERI Procedia*, vol. 10, 2014, pp. 144 – 152. Internet of things," *IET Quantum Communication,* vol. 5, no. 2, June 2024, pp. 103-112.

[9] P. Singh, "A layered approach to cybersecurity: People, processes, and technology- explored & explained," July 2021, https://www.linkedin.com/pulse/layered-approach-cybersecurity-people-processes-singh-casp-cisc-ces

[10] M. Loi et al., "Cybersecurity in health – disentangling value tensions," *Journal of Information, Communication and Ethics in Society,* June 2019, https://www.emerald.com/insight/content/doi/10.1108/JICES-12-2018-0095/full/html

[11] M. Adams, "Unlocking the benefits of ethical hacking: The importance of ethical hackers in cybersecurity," April 2023, https://www.businesstechweekly.com/cybersecurity/network-security/ethical-hacking/

[12] M. N. O. Sadiku, S. Alam, S. M. Musa, and C. M. Akujuobi, "A primer on cybersecurity," *International Journal of Advances in Scientific Research and Engineering*, vol. 3, no. 8, Sept. 2017, pp. 71-74.

[13] M. N. O. Sadiku, M. Tembely, and S. M. Musa, "Smart grid cybersecurity," *Journal of Multidisciplinary Engineering Science and Technology*, vol. 3, no. 9, September 2016, pp.5574-5576.

[14] "FCC Small Biz Cyber Planning Guide," https://transition.fcc.gov/cyber/cyberplanner.pdf

[15] "The 8 most common cybersecurity attacks to be aware of," https://edafio.com/blog/the-8-

most-common-cybersecurity-attacks-to-be-aware-of/

[16] Y. Zhang, "Cybersecurity and reliability of electric power grids in an interdependent cyber-physical environment," *Doctoral Dissertation,* University of Toledo, 2015.

[17] J. Dargan, "Quantum cybersecurity explained: Comprehensive guide," https://thequantuminsider.com/2024/03/13/quantum-cybersecurity-explained-comprehensive-guide/

[18] P. Raquel, "Opportunities and obstacles in quantum cybersecurity," https://www.linkedin.com/pulse/opportunities-obstacles-quantum-cybersecurity-p-raquel-bise-eckze

[19] "Quantum cybersecurity: Preparing for the future of data security," https://quantumzeitgeist.com/quantum-cybersecurity-preparing-for-the-future-of-data-security/

[20] K. Viezelyte, "What is quantum cybersecurity?" November 2024, https://nordpass.com/blog/quantum-computing-cybersecurity/

[21] "Post-quantum cybersecurity in law firms," October 2024, https://ggslaw.ca/post-quantum-cybersecurity-in-law-firms/

[22] L. Williams, "Will quantum computing help or hinder the fight against cybercrime?" January 2022, https://www.investmentmonitor.ai/tech/quantum-computing-cyber-security-crime/?cf-view

[23] H. Montini, "Quantum computing and cybersecurity: A threat & an ally for security solutions," January 2025, https://www.provendata.com/blog/quantum-computing-cybersecurity/

[24] "8 Quantum computing cybersecurity risks [+ protection tips]," https://www.paloaltonetworks.com/cyberpedia/what-is-quantum-computings-threat-to-cybersecurity

[25] "The dawning age of quantum computing and its cybersecurity implications," September 2023, https://blog.24by7security.com/the-dawning-age-of-quantum-computing-and-its-cybersecurity-implications

[26] R. Rawat et al. (eds.), *Quantum Computing in Cybersecurity*. Wiley, 2023.

[27] T. Ijlal, *The Quantum Computing Cybersecurity Guide: A Beginner's Guide to Understanding and Addressing Quantum Security Risks And Threats.* Independently Published, 2025.

[28] G. Blokdyk, *The Operational Excellence Library; Mastering Quantum Computing in Cybersecurity.* 5STARCooks, 2024.

[29] S. Jacob and T. Lee, *Cybersecurity in the Age of Quantum Computing: Foundations, Threats, and the Future of Secure Computing*. Independently Published, 2025.

[30] I. Priyadarshini and R. Sharma, *Quantum Computing in Cybersecurity and Artificial Intelligence (Advances in Quantum Computing).* Wiley-Scrivener, 2025.

[31] G. J. Skulmoski and A. Memari, *Quantum Cybersecurity Program Management.* Business Expert Press, 2023.

[32] B. Santacruz, *Cybersecurity in the AI & Quantum Era*. Brian Santacruz, 2024.

[33] B. A. Kumar, S. K. Kumar, and L. Xingwang (eds.), *Quantum Computing Models for Cybersecurity and Wireless Communications (Sustainable Computing and Optimization).* Wiley-Scrivener, 2025.

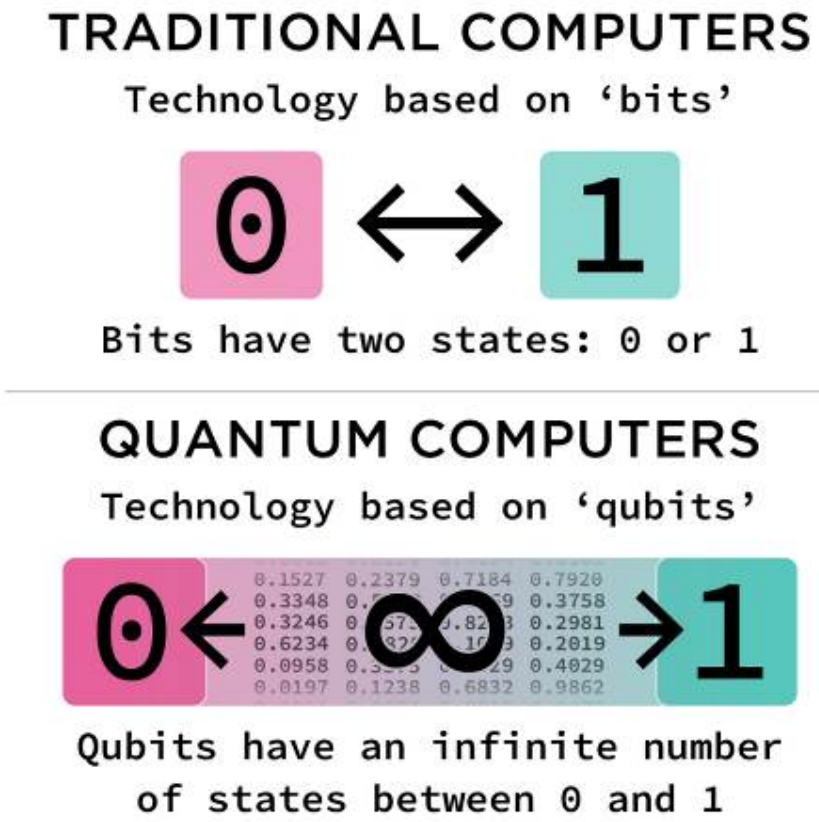

Figure 1 The bit and the qubit [3].

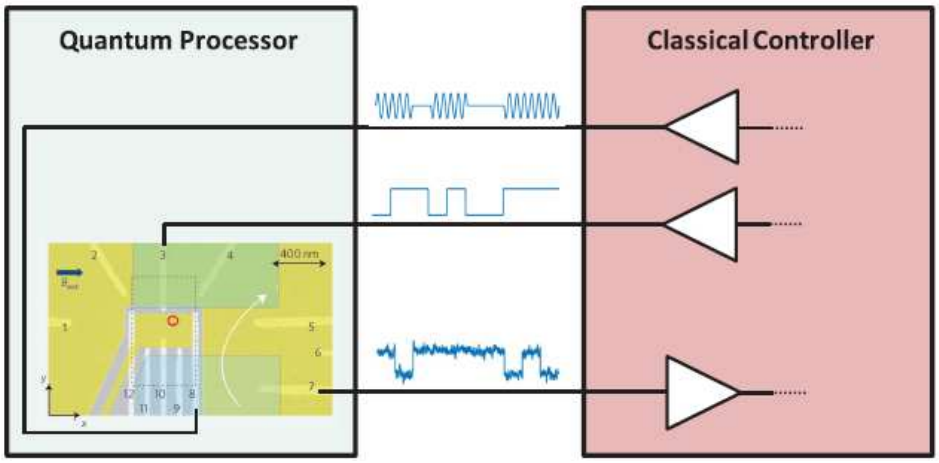

Figure 2 Quantum processor and classical electronic controller [4].

Figure 3 A representation of quantum computing [5].

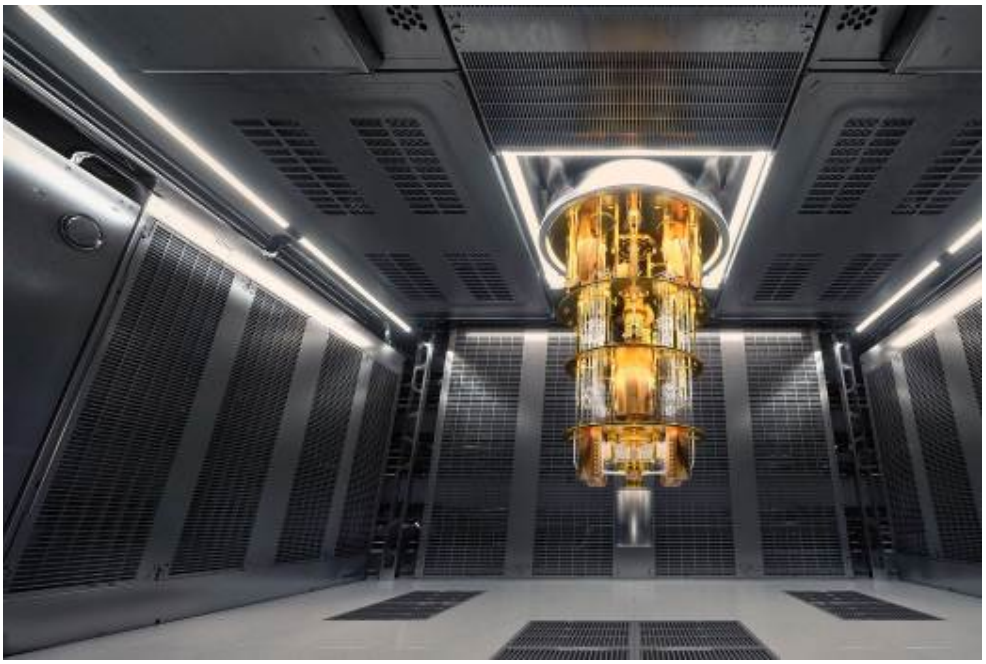

Figure 4 A typical quantum computer [6].

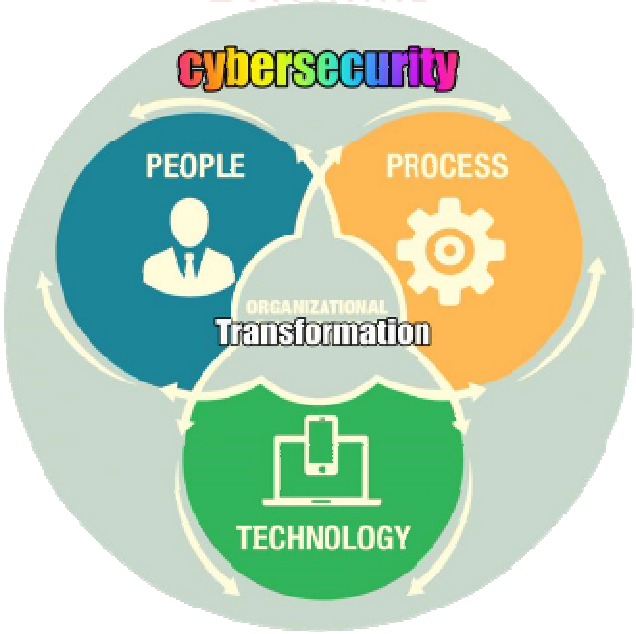

Figure 5 Cybersecurity involves multiple issues related to people, process, and technology [9].

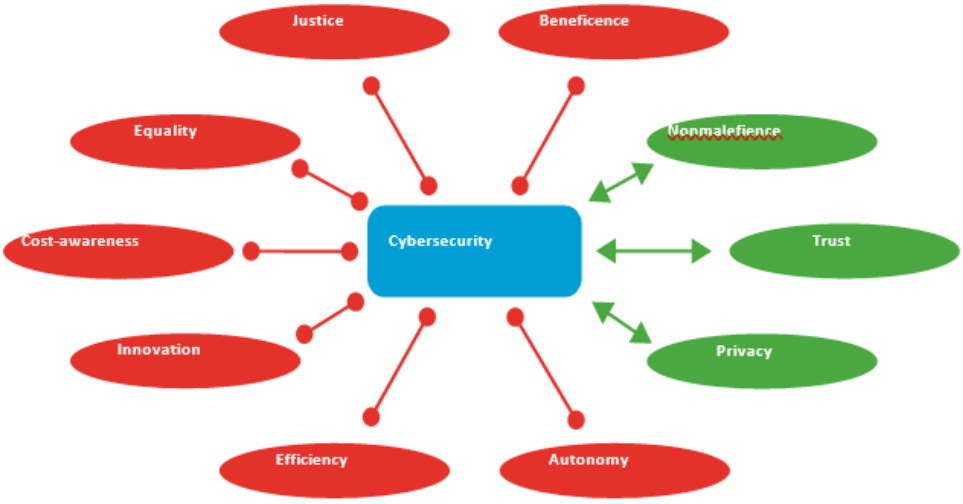

Figure 6 Different components of cybersecurity [10].(Green: supportive; red: in tension)

Figure 7 A typical cybercriminal [11].

Figure 8 Common types of cybersecurity threats [15].

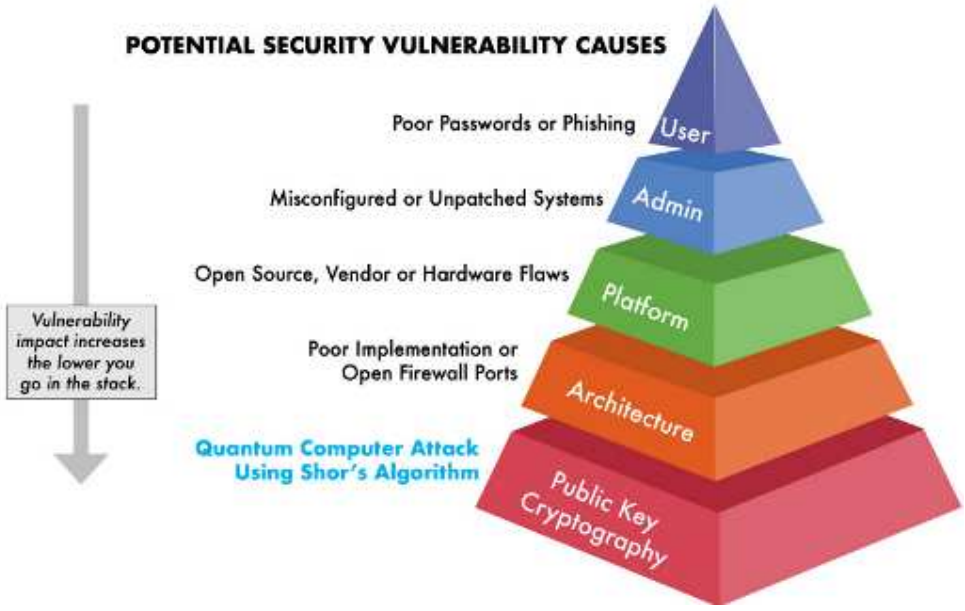

Figure 9 Potential security vulnerability causes [18].

Figure 10 Quantum cybersecurity [19].