Sri Lanka Institute of Information Technology

# Quantum Computing Impact on Cyber Security

## Individual Assignment

IE2022 - Introduction to Cyber Security

Submitted by:

| Student Registration Number | Student Name |
|---|---|
| IT20023614 | Wijesingha W.M.P.M |

Date of submission

**2021/05/28**

# Table of Contents

# Abstract

This era, people call it as Information era. Nowadays most of fields are based on information. Businesses, Banking systems, and many other larger fields need Information to increase their productivity. That is the reason cybersecurity takes a valuable place in this era. But are we safe on the internet? It is based on our security. This report talks about quantum computers, cybersecurity, Quantum theory, and principles.  and considering how quantum computing impacts cybersecurity.  Quantum technologies take a high impact on our data encryption methods. Quantum technology has a number of ways to impact encryption. In this report, I have mentioned those areas as well as uses about these technologies.

# 1. Introduction

In this world, cybersecurity is the most need to protect people's information privacy. Cybersecurity protects computer networks from threats, which could jeopardize their hardware, software, or records.

Personal information can leak and cause damages or destruction by unauthorized usage. In the future, computer technologies will continue to grow and dominate part of daily life and the economy. The position of cybersecurity and cyber-war crime will be frequent and critical.

As both hardware and software develop computing systems (and attackers) this is an area that is still in the process of evolving. The most drastic development you can imagine is perhaps a revolution in the paradigm of the computational model used. First of all, let’s consider about what is Quantum mechanics, Quantum Computing, Cyber security and How Quantum computing impact on cybersecurity.

**Quantum mechanics** is a representation of the conduct of matter and light in all its specifics, and particularly atomic events. Things on a very small scale are like nothing you witness directly. [1]

**Quantum Computing,** Normal computers store and process data as "1" and "0". We call this the "binary" method. But in quantum physics, the "superposed moment" that is common between the two rotations of an electron, the behavior of a particle, and the polarization of a proton are now used for computers. [2]

Quantum superposition is a principle of mechanics. In quantum science, two (or more) quantum positions can be combined, just as two waves can be combined in physics. Then it is considered another level. Mathematically, it is like Schrodinger's Cat's test.

Thus, in addition to "0" and "1", quantum computers use quantum superposition in both cases. That is why, once these quantum computers are processed for processing information, their data processing and the results of that processing are very fast. Even complex data can be processed in a short period of time. Simply put, a quantum computer

can perform a large number of parallel processing, or calculations at the same time. Until now, calculations have been done on a standard computer, one after the other, or as serial processing. [2]

**Cyber Security** is the defense against the leakage of information or harm to hardware, software, or electronic information by computer systems and networks and against any disturbances or misdirection of the services provided by these systems and networks. [3]

**How Quantum Computing Impact on Cybersecurity**

With the introduction of quantum computation, encryption techniques are changed. Currently, the most commonly used asymmetrical algorithms are based on complex mathematical problems, such as a big number factor, which on current most efficient supercomputers require thousands of years. The same problem could be solved in theoretical terms, in days or hours on massive quantum computers, and study at the MIT carried out more than 20 years ago by Peter Shor. [4]

The aim is to encrypt data in such a manner that no one with the data will access it unless it is the intended receiver.

And the crypt of virtually all private information transmitted through the Internet depends heavily upon a variety of phenomenon – it is very difficult to use a regular non-quantum machine to take a very large number and determine its variables.

As opposed to a multiplication that is quite fast (just multiply the digits together to connect them), it is very slow to find primary numbers multiplying each other that offer you a random, large, non-prime number that seems to work on the ordinary – even a quite strong – machine. [5]


*Figure 1*

Take this huge number. The prime numbers that multiply together to get the long number took 2000 years of the computational workflow. And for encryption, this is very helpful. [5]

Since we will use them to access private information if you have access to the two elements. Although if the variables are not found, the data is encrypted efficiently.

Cyber breaches can now, for example, be conducted more easily due to the fact that many organizations lack safeguards for their sensitive information. If quantum computers will, however, launch attacks that break up asymmetric encryption it makes the whole PKI-based encryption process that we are using to secure our confidential, outdated information. Some countries are now collecting encrypted international messages with the hopes of extracting useful secrets from that data in the future, taking advantage of the time it would take quantum computers to hack those schemes. Indeed, countries must be mindful that, once quantum cryptanalysis is possible, it would have a huge impact on international affairs by allowing decryption of all broadcast communications within the state. This may be a landmark moment for countries that heavily rely on encryption to protect military activities, diplomatic communications, and other confidential data [6]

**According to the Forbes magazine quantum computing, and prosaic quantum technology, promise to transform cybersecurity in four areas:**

1) Quantum random number generation is fundamental to cryptography.
   Conventional random numbers of generators typically use algorithms called "pseudo-random number generators," which are not really random and are therefore likely to be compromised. Companies like Quantum Dice and IDQuantique create quantum random number generators that use quantum optics to produce real allegiance sources. These devices are currently in industrial use. [7]
2) Quantum-secure communications, specifically quantum key distribution (QKD).
   The exchanging of cryptographic keys between two or more parties to enable them to exchange information secretly is at the core of secure communications. QKD makes use of quantum mechanics to allow for the fully hidden exchanging of encryption keys and can also detect the existence of an eavesdropper. QKD is currently limited to fiber propagation over tens of kilometers, with satellite proofs

of concept over thousands of kilometers. KETS Quantum Security and Toshiba are two industry leaders in this field. [7]

3) The most controversial application of QC is its potential for breaking public-key cryptography, specifically the RSA algorithm, which is at the heart of the nearly $4 trillion ecommerce industry.

   The RSA algorithm is based on the fact that the sum of two prime numbers is computationally difficult to factor. It will take trillions of years for a traditional machine to crack RSA encryption. A quantum computer with about 4,000 error-free qubits could easily beat RSA. However, this would necessitate the use of more than a million of today's noisy qubits. The world's biggest quantum computer reportedly has fewer than 100 qubits; however, IBM and Google have plans to reach 1 million qubits by 2030. A million-qubit quantum machine might only be a decade out, although the time period may be shortened. Furthermore, highly confidential financial and national security data is at risk of being hacked. A million-qubit quantum machine might only be a decade out, although the time period may be shortened. Furthermore, extremely confidential financial and national security data may be stolen today, only to be decrypted until a sufficiently powerful quantum computer becomes available. The possible challenge to public-key cryptography has prompted the invention of quantum-resistant algorithms. Post-quantum cryptography is being pioneered by companies such as PQShield. [7]

4) Machine learning has revolutionized cybersecurity, enabling novel attacks to be detected and blocked.

   When data volumes and complexity increase, so does the cost of training deep models. The emerging field of quantum machine learning can allow machine learning algorithms to be exponentially faster, more time- and energy-efficient. As a result, more powerful algorithms for detecting and beating novel cyberattack methods can emerge. [7]

# 2 Evolution of the topic

Over the last decade, a lot was done, including encryption and deep learning, to examine the usefulness of quantum computation in the cyber phone. With the ever-increasing demands for accelerated processing speed and miniaturization, traditional computers are unable to keep up with a few important parameters. Since classical computers are based on classical mechanics, their expansion is at its peak. Because of these constraints, quantum mechanics is emerging as a game-changer in the race of computing. Quantum computation is the study of quantum computers using quantum mechanics phenomena such as superposition, entanglement, tunneling, and annealing to solve problems that humans cannot solve in their lifetime.

**Timeline of Quantum Computing**

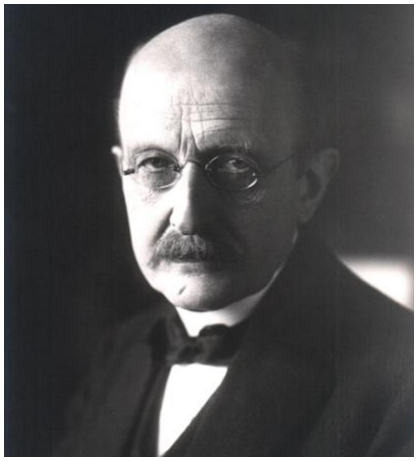

*Figure 3 Max Plank*

The invention of Max Plank and black body radiation in the late 19th century lay the groundwork for the quantum universe. A. Einstein discovered the concept of photons in 1905. Experimentation with light began in the mid-Isth century but was not widely popularized. However, when the hydrogen absorption spectrum was examined and a double-slit experiment was considered, something strange was discovered. In order to address these ludicrous results, Schrodinger proposed the wave equation in 1925. Furthermore, it was fundamental to quantum theory. [8]

1) 1935 A. Einstein, N. Rosen, and B. Podolsky Paradox

According to the EPR paradox, the wave equation is imperfect and there must be certain unknown variables, so it does not explain the whole physical universe. As a result, the Copenhagen view of the Schrodinger equation was rejected. This is also known as Quantum Entanglement. [9]

2) 1964 Bell's Inequality

Any of the variables in the theory of quantum mechanics are incomplete, according to EPR theory. In 1952, De-Broglie and Bohm completed this gap, which became known as Bohmian Mechanics. JS Bell, however, demonstrated in 1964 that both of these ideas are incompatible with the locally practical theory of classical physics. Arguments emerged regarding the disparity, which can be explained with rational conclusions. [10]

3) 1970's Quantum Information Theory

The word "Quantum Information Theory" was coined during the 1970s. The implementation of this definition was entirely the responsibility of Stephen Wisner and Charles Barnett. RS Ingarden claimed in 1975 that the Shannon theory could not be extended into quantum information theory, but that quantum information theory could be generalized to the Shannon theory. [8]

4) 1980's Richard Feynman Challenge

In May 1980, the Massachusetts Institute of Technology hosted the first Physics of Computation conference. The Nobel Laureate Richard Feynman asked the computational programmer to create a brand new breed of machines that would interact with quantum mechanics. He also developed a quantum computer's foundation and universal mode. "There' s plenty of room at the bottom" he famously said in his lecture. [11]

D. Tsui, A. Gossard, and H. Stormer were awarded the Nobel Prize in 1998 for discovering the Fractional Quantum Hall effect in 1982. They claim that quantum matter will exhibit a strong entanglement state at very low temperatures, which is microscopically distinct but identical for the local observer. [12]

5) 1990's A Huge Leap in Quantum Computing

In 1993, C.H. Barnett and colleagues demonstrated that quantum information can be transferred to distant locations using entanglement, a technique known as Quantum Teleportation. [13]

Peter Shor suggested the Las Vegas Algorithm in 1994 as a method for computing discrete logarithms and factoring integers on quantum computers. All of these issues were previously

used to build cryptosystems. [14] Peter Shor and A.Steane presented Quantum Error Correction Codes in 1995, and DiVincenzo addressed the basic physical conditions for the construction of quantum computations the year before. The science of information processing that is governed by quantum mechanics or quantum physics is known as quantum computation. [15]

6) 2001 Beginning of Implementation over Quantum Computing

   Shor's Algorithm, which factorized 15 numbers using qubits in nuclear spin, was first demonstrated in 2001 at IBM Almaden Research Center and Stanford University. [16]

7) 2010 First Commercial Quantum System.

   This year, D-Wave announced the D-Wave One, the first quantum computer. It was equipped with a 128-qubit processor. It has the ability to perform discrete optimization and single math operations. In this processor, quantum annealing was observed, but no significant speed increase was observed as compared to a classical machine.

   And, in 2013, it doubled the number of qubits, resulting in D-Wave Two, which uses roughly 512 qubits. With a 439-qubit setup, it was found to be 3600 times faster. [17]

   In 2014, scientists successfully demonstrated quantum teleportation over a distance of approximately 10 feet with minimal error.

   D-Wave unveiled the D-Wave 2x quantum computer in 2015, which has about l000 qubits. It has a total of 2,048 qubits, but about half of them are disabled and will be enabled later.

   Google researchers successfully simulate the energy of the Hydrogen H2 molecule on July 22, 2016, which will aid in the development of everything from solar cells to medicines.

   In 2016, IBM made quantum computing usable on the IBM cloud, making it possible to introduce the quantum circuit. It would cause any algorithm or experiment to be implemented on a quantum computer. [8]

**Cyber Security Evolution with (Quantum Computing).**

The continuous development of this area is critical because computer systems and attackers evolve both in hardware and software. Changing the framework of the computational model used is arguably the most dramatic transition that can be imagined. Quantum innovations seem to be on the verge of bringing humanity closer to such a transformation.

Massive quantum computers, as well as the additional computing capacity they would provide, may have disastrous implications for cyber defense. It is understood, for example, that important problems like factoring and the discrete log, whose supposed hardness ensures the security of many commonly used protocols (such as RSA, DSA, and ECDSA), can be solved efficiently (and the cryptosystems broken) if a quantum computer big enough, "fault tolerant," and universal enough is created. 35 Although this theoretical result has been understood since the 1990s, the possibility of constructing such a structure has only recently become feasible (in medium term). However, dealing with the impending threat posed by adversaries armed with quantum technology isn't the only problem in cyber security where quantum technologies will undoubtedly play a part. Quantum cyber security is a technology that investigates all facets of quantum technology's effect on the protection and privacy of communications and computations

1) The study of CISOs and other security professionals was conducted by the Neustar International Security Council (NISC). By the end of 2024, 73 percent of respondents predicted quantum innovations to have surpassed legacy technologies. Quantum computers, according to 93 percent of respondents, would “overwhelm” security technologies once they are created. Just 7% believe absolute quantum dominance would ever be achieved. [18]

2) In 2018, under the auspices of the UK's National Quantum Technologies Program, a partnership at BT's Adastral Park research base developed the world's first "ultra-secure" quantum network, essentially shielded by the laws of physics. [18]

**Cyber Security Evolution and Development.**

The ubiquity of cyber security is one of the most significant developments in the sector over the last 20 years. Red Sift, which is a part of Tech Nation's first cyber initiative, is trying to democratize cyber security by making it accessible to small enterprises as well as large corporations. Randal Pinto, co-founder of Red Sift, argues that cyber has had a moment in the last decade. Cyber defense was not a mainstream business ten years ago. The common consensus was that only big organizations should be targeted, and there was no such thing as a Chief Information Security Officer (CISO). [19]

"It was a room that hardly existed a decade ago, and what was open was bland, unscientific, and ineffective," Cybsafe creator Oz Alashe agreed. "In the last half-century, cryptography has come a long way; the invention of the RSA algorithm in the 1970s was a watershed moment. Encryption and decryption will now be done with separate keys thanks to RSA. It also totally transformed the sector.

"In the last half-century, cryptography has come a long way; the invention of the RSA algorithm in the 1970s was a watershed moment. Encryption and decryption will now be done with separate keys thanks to RSA. It also totally transformed the sector.

The dominant trend in the computer security industry for a long time was to bring further barriers – further levels of sophistication – to technology. It was argued that cyber hackers will have a tougher time getting into sophisticated networks with many barriers to entry."

It was largely used as a forensic and reactive industry," Pinto says of historical cyber defense. The remedies were costly, and they relied on recruiting contractors to look at and patch the bugs that contributed to a cyber attack. [19]

So, when we attempt to look to the future, we will leave the final words to Oz Alashe and Randal Pinto, and their forecasts and outlook for the future of cyber defense, as seen from the eyes of the organizations that are developing it.

# 3 Future developments in the area

Future quantum computers are also able to break uneven encryption solutions that base their security on integer factorization or distinct logarithms. Although cruciform algorithms are not affected by Shor's formula, the ability of quantum computing necessitates a multiplication in key sizes. for instance, massive quantum computers running Grover's formula, which uses quantum concepts to look at databases terribly quickly, could provide a quadratic improvement in brute-force attacks on cruciform coding algorithms, such as AES. to assist stand up to brute-force attacks, key sizes ought to be doubled to support the same level of protection.

Cyber Security We're thinking about how quantum computation might undermine the very foundations of today's encryption methods and have an effect on cryptography norms, and we know it's tempting to believe we have got plenty of time since quantum computing is still years away from maturity, but that's just partially true. While quantum computers are still in their early stages of development, the time to prepare was yesterday because encrypted data stolen today could end up in the hands of cyber attackers using more advanced quantum computers tomorrow. Fortunately, there is help in the form of researchers who are developing alternative methods to protect data as quantum computing advances.

We are learning more about how to use quantum-safe cryptography to help secure networks and data from present and potential attacks. It is never too early to start preparing for quantum computing and quantum-safe cryptography. Businesses can begin to understand the future effects on their confidential data now, and they can inform their security staff on quantum computing and quantum-safe cryptography.

It is more necessary than ever for society to be able to connect safely and compute effectively. Our culture has been transformed by the Internet and, gradually, the Internet of Things. If quantum technology become more commonplace in computation and communication over the next 5-10 years, we can see a flood of new possibilities. Future networks will almost definitely have both classical and quantum devices and connections, with some of them likely to be dishonest, and functionalities ranging from basic routers to servers running universal quantum algorithms. The realization of such a dynamic

network of classical and quantum connectivity requires a novel foundation that can anticipate and accommodate the complexities of real-world implementations and applications. [20]

## Preparing for The Quantum Future

We are in the midst of a quantum revolution. While the full effect of large-scale fault-tolerant quantum computers could be a decade away, quantum computers in the near future will also have significant benefits. There is a lot of money going into addressing the key issues of scaling qubit count, error correction, and algorithms. Although quantum computing can make certain current encryption protocols obsolete in terms of cybersecurity, it has the potential to significantly improve communication protection and privacy.

To be ready for the quantum revolution of tomorrow, organizations must think carefully about the longer-term dangers and advantages of quantum computation and technologies and participate in a meaningful way today.

It is more necessary than ever for society to be able to connect safely and compute effectively. Our culture has been transformed by the Internet and, gradually, the Internet of Things. If quantum technology become more commonplace in computation and communication over the next 5-10 years, we can see a flood of new possibilities. Future networks will almost definitely have both classical and quantum devices and connections, with some of them likely to be dishonest, and functionalities ranging from basic routers to servers running universal quantum algorithms. The realization of such a dynamic network of classical and quantum communication requires a novel foundation that can anticipate and accommodate the complexities of real world implementations and novel applications.

The quantum arms race has already begun. Across the globe, governments and private investors are investing billions of dollars into quantum research and development. The use of satellites to distribute quantum keys for encryption has been shown, setting the foundation for a quantum security-based global communication network. Large-scale quantum computing hardware and applications are being developed by IBM, Google, Microsoft, Amazon, and other firms. Nobody has arrived yet. Although small-scale quantum computers are currently operating, grappling with errors is a big roadblock to scaling up the technology. Qubits are very brittle as compared to bits. Quantum intelligence can be destroyed by even the tiniest disturbance from the outer universe. As a result, most modern computers must be closely insulated in enclosed

conditions with temperatures well below those of outer space. While a theoretical paradigm for quantum error correction has been established, putting it into practice in a way that is both energy and resource efficient presents major engineering challenges.

It is unclear when or whether the maximum potential of quantum computing would be available, given the current state of the field. Nonetheless, corporate executives should think about designing plans for three major areas:

**Planning for quantum security:**

Not only are current data encryption protocols vulnerable to potential quantum computers, but they are also vulnerable to ever more efficient classical computers. New encryption principles (classical or quantum) would undoubtedly emerge. Data security would take planning, capital, and quantum skills to transition to a quantum-secure architecture and supporting infrastructure. And if quantum computers are ten years out, it will be too late to evolve then. Now is the perfect moment to get started. [21]

**Identifying use cases:**

Nobody could have known how traditional computers can affect any part of our lives in so many different ways. Quantum applications are similarly difficult to predict. As a result, in order to fully realize quantum computing's promise, industry leaders and experts from various industries, such as medicine, economics, and energy, must collaborate with quantum physicists and hardware/software engineers. This would make it easier to create industry-specific quantum applications that are suited to new quantum technology or future adaptive quantum computing. Building and expanding the quantum app store would require interdisciplinary experience and preparation. [21]

**“Thinking through responsible design:**

Who will create quantum technology and have access to it, and how will consumers interact with it? The effect of AI and blockchain has highlighted the importance of considering emerging technologies' social, legal, and environmental consequences. The quantum industry is still in its infancy. This presents a once-in-a-lifetime chance to create a responsible and long-term quantum computing roadmap by incorporating inclusive approaches from the outset. [21]

The quantum technology sector's explosive rise over the last five years has been thrilling. However, the outlook remains uncertain. Fortunately, quantum theory explains why unpredictability is not really a negative thing. Indeed, two qubits may be locked together in such a way that they remain undetermined independently but are completely in alignment collectively — either both qubits are 0 or both are 1. Entanglement, or the blend of mutual

certainty and human unpredictability, is a potent fuel that powers many quantum computing algorithms. It may also be instructive in terms of how to develop a quantum industry. Businesses will boost their chances of being ready for the quantum future by preparing responsibly but still welcoming future ambiguity.

**Future of Encryption**

Quantum computers are posing a cybersecurity challenge that the IT industry has never seen before. Quantum computers, which are capable of effectively short-circuiting the cryptography we've used to shield our data until now, might theoretically break any stored data currently considered protected by modern standards – whether that's health information, financial data, consumer databases, or even vital government infrastructure.

Efforts are ongoing to secure our data against the quantum challenge, but the matter of urgency is under discussion. PQShield, a postquantum start-up cryptography firm spun out of the University of Oxford, sees that in 2020 it attempts to resolve a breakup between the size of the danger and the present cyber readiness of other firms. [22]

Kaafarani is a former engineer at Hewlett-Packard Labs who now heads a team of ten full-time quantum cryptographers from a global pool of just a hundred or so, according to him. The business is hard at work developing quantum-secure cryptography – cryptographic technologies for hardware, applications, and communications that can protect data against potential threats while also being implementable with current technology. [22] This package includes a system on chip (SoC) and software development kit that enables businesses to build encrypted communications applications using a "post-quantum" version of the Signal cryptographic protocol. PQShield's platform is designed to work for all legacy networks and those planned in the future, which means it will provide security for anything from keyless cars and other mobile vehicles to data flowing to and from cloud servers. This is important, according to Kaafarani, because post-quantum cryptography cannot be applied retrospectively, leaving data encrypted by existing

standards vulnerable to post-quantum attacks. "The end-to-end encryption we're using right now is stable," he says, "but people can intercept them and steal encrypted data."

"Once they get access to a quantum device, they will decode them, putting secrecy at risk in the future and something that is deemed classified today can be decrypted later."

Kaafarani also sees a concern with modern attitudes toward cyberattack remediation, which he compares to putting a band-aid on a recurring problem. [22]

"That's why we created PQShield: to bridge this gap and pave the way for a smooth and stable quantum transition. There is a good chance to do it right from the start here." The startup successfully closed a £5.5 million investment round led by VC firm Kindred Capital, and has now signed its first OEM client, German engineering firm Bosch. Though the deal's precise specifics are still being kept under wraps, Kaafarani believes it exemplifies the risks that companies are starting to recognize as the era of quantum computing approaches. [22]

**A $50 billion market by (2030)**

There should be a lot of competition in this area from investors as well. They became the first commercial quantum corporation by developing a quantum machine that employs the annealing technique.

We have also looked at how companies like Google are working on quantum computers. Google would be able to execute functions at least 400 times faster than using traditional methods thanks to a quantum solution.

They may be able to push their artificial intelligence goals closer to scientific exploration. According to Boston Consulting, the quantum computing industry could be worth up to $50 billion by 2030. [5]

**Quantum Information Science**

The aim of this chapter is to paint a vision of how quantum technology will be used in the future, roughly between the years 2025 and 2045. This chapter is written for the generalist who is already acquainted with wargaming. It is not meant to be a comprehensive examination of the technology, a review of the pitfalls, or a compilation of technological

roadblocks. To provide an operating picture, this manuscript assumes that engineering challenges will not prevent the technology from being activated by 2025–2045.

Any emerging technology must address a number of challenges posed by business, environmental, technical, and political pressures. [23]

# 4 Conclusion

cybersecurity is the most need to protect people's information privacy. Personal information can leak and cause damages or destruction by unauthorized usage. In the future, computer technologies will continue to grow and dominate part of daily life and the economy. As both hardware and software develop computing systems (and attackers) this is an area that is still in the process of evolving. The most drastic development you can imagine is perhaps a revolution in the paradigm of the computational model used. Quantum mechanics is a representation of the conduct of matter and light in all its specifics and particularly atomic events. If we considering about security side, it wants a large improvement to fight against quantum computing.

# References


[1] M.A. Gottlieb , Rudolf Pfeiffer, "feynmanlectures," 19 December 2020. [Online]. Available: https://www.feynmanlectures.caltech.edu/III_01.html.

[2] National Academies of Sciences, Engineering, and Medicine, Division on Engineering and Physical Sciences, Intelligence Community Studies Board, Computer Science and Telecommunications Board, Committee on Technical Assessment of the Feasibility., "Quantum Computing: Progress and Prospects," The National Academic Press, 2019.

[3] Daniel Schatz, Rabih Bashroush, Julie Wall, "Towards a Mor ds a More Representativ esentative Definition of Cyber Security e Definition of Cyber Security," *Journal of Digital Forensics Security and Law,* vol. 12, no. 2, p. 74, 2017.

[4] Walid Rjaibi, Sridhar Muppidi, Mary O'Brien, "Wielding a double-edged sword," IBM Institute for Business Value, Armonk , 2018.

[5] R. White, " Monkey Darts & Canonbury," Monkey Darts & Canonbury Publishing Ltd, 23 October 2019. [Online]. Available: https://www.monkeydarts.co.uk/bulletin/how-a-quantum-computer-could-cripple-governments-and-cause-a-financial-crisis/.

[6] A. Gouget, "Security Boulevard," 5 August 2020. [Online]. Available: https://securityboulevard.com/2020/08/quantum-computing-and-the-evolving-cybersecurity-threat/.

[7] P. Lipman, "Forbes," Forbes, 4 January 2021. [Online]. Available: https://www.forbes.com/sites/forbestechcouncil/2021/01/04/how-quantum-computing-will-transform-cybersecurity/?sh=39caa95a7d3f.

[8] Jasmeet Singh, Mohit Singh, "Evolution in Quantum Computing," College of Computing Sciences & Information Technology, Teerthanker Mahaveer University, Moradabad, India, 2016.

[9] A Einstein, B. Podolsky, N. Rosen, ""Can quantum-mechanical description of physical reality be considered complete," *Physical Review,* vol. 47, 1935.

[10] J. S. BELL, "ON THE EINSTEIN PODOLSKY ROSEN PARADOX," Physics Publishing Co., 1964.

[11] R. P. Feynma, "Simulating Physics with Computers," *International Journal of Theoretical Physics,* vol. 21, pp. 6-7, 1982.

[12] D.C. Tsui, H.L. Storm er, AC. Gossard, "Two-Dimensional Magnetotransport in the Extreme Quantum Limit," *Physical Review Latters,* vol. 48, 1982.

[13] C. Bennett, Brassard G., C. Crepeau, R. Jozsa, A Peres, and W. Wootters, ""Teleporting a n unknown quantum state via dual classical and einstein-podolsky-rosen channels," *Physical Review Latters,* vol. 70, pp. 1895- 1899, 1993.

[14] P. W. .. Shor, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring," *Annual IEEE Symposium on Fundamentals of Computer SCiences*, pp. 124-134 , 1994.

[15] D. P. DiVincenzo, "Quantum Computation," *Science*, vol. 270, no. 5234, pp. 255-26I, 1996.

[16] L.M.K. Vandersypen, M. Stephen, G. Breyta, C.S. Yanooni, Mark H. Sherwood, Isaac L. Chuang, , ""Experimental r ealization of Shor' s quantum factoring a lgorithm using nuclear magnetic resonance," *Nature*, vol. 414, pp. 883-887, 2001.

[17] Catherine C. McGeoch , Cong Wang, "Experimental Evaluation of an Adiabatic Quantum System f or Combinatorial Optimization".

[18] Alex Scroxton, "computer weekly," Tech Target, 10 December 2019. [Online]. Available: https://www.computerweekly.com/news/252475253/Rapid-evolution-of-quantum-computing-a-concern-for-CISOs.

[19] A. Logan, "Tech Nation," Tech Nation, 30 November 2019. [Online]. Available: https://technation.io/news/past-present-future-cyber-security/.

[20] Petros Wallden, Elham Kashef, "Cyber Security in the Quantum Era," *Communications of the ACM*, vol. 64, p. 120.

[21] S. Ghose, "Are You Ready for the Quantum Computing Revolution?," Harvad Business Review, 17 September 2020. [Online]. Available: https://hbr.org/2020/09/are-you-ready-for-the-quantum-computing-revolution#.

[22] H. Owen, "Tech Republic," ZDNET, A RED VENTURES COMPANY., 29 July 2020. [Online]. Available: https://www.techrepublic.com/article/the-future-of-encryption-getting-ready-for-the-quantum-computer-attack/.

[23] M. Blowers, " Quantum Information Science," *Evolution of Cyber Technologies and Operations to 2035*, pp. 91 - 92, 2015.

[24] M. A. G. a. R. Pfeiffer, "feynmanlectures," 19 December 2020. [Online]. Available: https://www.feynmanlectures.caltech.edu/III_01.html.