



# AWARENESS AND READINESS ON QUANTUM COMMUNICATION TECHNOLOGY AMONG THE REGULATORS, INDUSTRY PLAYERS AND ACADEMICIANS IN MALAYSIA

Nur Sabrina Shahrul<sup>1</sup>, Mustafa Mohd Hanefah<sup>2\*</sup>, Rosnia Masruki<sup>3</sup>, Nor Asiah Yaakub<sup>4</sup>, Noorihsan Mohamad<sup>5</sup>

<sup>1</sup> Graduate School of Muamalat, Faculty of Economics & Muamalat, Universiti Sains Islam Malaysia  
Email: nursabrinshahrul@raudah.usim.edu.my

<sup>2</sup> Faculty of Economics & Muamalat, Universiti Sains Islam Malaysia, Nilai, Negeri Sembilan  
Email: mustafa@usim.edu.my

<sup>3</sup> Faculty of Economics & Muamalat, Universiti Sains Islam Malaysia, Nilai, Negeri Sembilan  
Email: rosnia@usim.edu.my

<sup>4</sup> Faculty of Economics & Muamalat, Universiti Sains Islam Malaysia, Nilai, Negeri Sembilan  
Email: norasiah@usim.edu.my

<sup>5</sup> Department of Economics, Kulliyah of Economics and Management Sciences, International Islamic University Malaysia, Gombak, Kuala Lumpur, Malaysia  
Email: noorihsan@iium.edu.my

\* Corresponding Author

## Article Info:

### Article history:

Received date: 31.03.2024

Revised date: 22.04.2024

Accepted date: 05.05.2024

Published date: 23.06.2024

### To cite this document:

Shahrul, N. S., Hanefah, M. M., Masruki, R., Yaakub, N. A., & Mohamad, N. (2024). Awareness And Readiness On Quantum Communication Technology Among The Regulators, Industry Players And Academicians In Malaysia. *Journal of Information System and Technology Management*, 9 (35), 21-37.

## Abstract:

The Quantum Communication Technology (QCT) industry is growing aggressively at the global level, but the implementation of this technology is not yet clear in Malaysia. This qualitative study reviews the awareness and readiness among regulators, industry players and an academia on development of QCT in Malaysia. This study conducted a focus group discussion involving twelve experts representing regulators, industry players and academicians who have extensive background and knowledge in cybersecurity. This study found that most of the respondents have basic understanding on the QCT and they are also aware on the and QCT development. In this study, respondents demonstrated varying levels of awareness of Quantum Communication Technology (QCT), with 8 out of 12 having prior knowledge. The study emphasizes the need for enhanced education and promotion in Malaysia to foster QCT adoption across sectors. Themes further explore the challenges of QCT implementation, particularly the high cost and evolving cybersecurity landscape. Recommendations include government involvement, cost-benefit analyses, continuous cybersecurity improvement, and top-down support to ensure successful QCT integration, especially in the telecommunications sector, where the high-cost poses challenges. The study underscores the

DOI: 10.35631/JISTM.935002

This work is licensed under [CC BY 4.0](https://creativecommons.org/licenses/by/4.0/)

significance of education, government collaboration, and financial support for effective QCT implementation in Malaysia

**Keywords:**

Academicians, Awareness, Industry Players, Quantum Communication Technology, Regulators

**Introduction**

Quantum communication technology (QCT) is an emerging field that has the potential to revolutionize the way we communicate and transmit information. This technology has been involved by Japan over the past 30 years which the main funding agencies for these projects including Japan Science and Technology Agency (JST), the National Institute of Information and Communications Technology (NICT), the Japan Society for the Promotion of Science (JSPS), and the Cabinet Office of the Government of Japan (Yamamoto et al., 2019). QCT utilizes the principles of quantum mechanics to enable secure and efficient transmission of data (Giles, 2019) Quantum technologies offer possibilities for enhancing telecommunications systems which they can improve encryption methods and enable the secure transmission of data Krause, 2022; Martin et al., 2021).

Today, we can observe that there have been numerous cyber platform data breach occurrences, where a data breach is an unfortunate occurrence in which information was stolen by unauthorized parties without the owner of the system's knowledge or consent (Froehlich, 2022). Data loss could result in financial loss for the owner when important data is stolen, including personal information like client data, bank passwords, and so forth (Eiza et al., 2021). Data protection is a key factor in moving the country toward being digitally enabled because of the increased dependence on technology and all the risks, opportunities, and rewards that go along with it (Setiawati et al., 2020). In 2022, data breaches involving banking institutions, multimedia and broadcast organizations, and a government electoral agency affected Malaysians. Millions of people's personal data were allegedly sold online in these incidents (Loheswar, 2022).

Some of the cases include one leaking information regarding roughly thirteen million bank accounts belonging to Malaysia's largest lender Maybank. which the stolen data has been posted on a well-known database marketplace where the seller requests that potential buyers send them directly over Telegram or make use of the forum's direct messaging features to complete the transaction. Lowyat.net noted that there was also a separate listing on the same day that the seller asserted to have a personal database of Unifi's mobile users. The seller asked for US\$850 and RM3,752 for the transaction (Loheswar, 2022).

Individuals may suffer from data breaches in a variety of ways, including financial loss, identity theft, invasion of privacy, targeted scams and phishing attacks, reputational harm, and psychological effects, not just in Malaysia but across the globe (Wang & Wang, 2022). To limit the effects of data breaches and prevent further events, people and organizations must take proactive efforts, such as implementing robust security measures, updating software and systems on a regular basis, practicing good cybersecurity hygiene, and being alert to potential dangers (Vishwanath et al., 2020).

Therefore, this is where Quantum Communication Technology (QCT) comes in which it has been claimed to be better/powerful tool for secured communications (Krause, 2022; Martin et al., 2021). Quantum computing is gaining traction in the region which a larger pool of quantum engineers is also being developed in the region, with higher education institutions in Malaysia, Singapore, Vietnam, and Indonesia taking action to expand their offerings of courses on the topic (Raj, 2021). The most recent developments in QCT research for many developing nations, including electronic marketplaces, semiconductor testing, energy storage, the internet, and many other areas in nations like the US, UK, Korea, Canada, or China (Singh et al., 2020). Development of QCT in Malaysia is still unclear, however there is mini project has been conducted which is, Quantum Communication Simulator (QuCS), a program created by Associate Professor Dr. Zuriati Ahmad Zukarnain, a lecturer at the Department of Communication Technology and Networking, Faculty of Computer Science at Universiti Putra Malaysia (UPM), aims to help researchers simulate and model virtual quantum experiments (Mustafa, 2017).

From literature, this study found there is a lack of information and academic work on QCT development in Malaysia even in other countries. Therefore, these raised up questions as follow: (1) What is the awareness of QCT among the industry players and academicians? (2) What are the perceptions of industry players and academia regarding readiness to implement QCT in Malaysia? In addressing this question, we conduct focus group discussions (FGD) with Malaysian telecommunication sector players who specifically in cybersecurity department and academicians. To achieve the objective of the study, we adopted the qualitative methodology. The study aims to review the understanding of QCT among the regulators, industry players and academicians and to explore the readiness of regulators, industry players and academicians regarding the development of QCT. The needs to identify the awareness and readiness among industry players are relevant since they have direct exposure in the communication technologies scenario, thus more alert on related new technology, opportunities, threats, and other related matters. For these reasons, this study believe they have capabilities and influences in the as the main players who will get involved with the QCT development in Malaysia.

The rest of this paper is structured as follow: literature review, methodology, result, and discussion and lastly conclusion. Moreover, the contribution for the study will emerge and will be presented according to research questions, theory that underpinned and construct of the study, as well as findings that answer to the research questions.

## Literature review

### *Quantum Communication Technology*

The idea behind quantum communication technology is that qubits (quantum bits) can be sent between distant locations using photons, which is a promising use and in optical fibers, photons can travel with little attenuation and are effectively separated from disturbances, enabling long-lived superposition states (Goldner et al., 2015). To create a quantum network, which increases computing capacity and offers high security for data transfer, particularly in quantum cryptography, quantum communication allows quantum computers to link to one another (Goldner et al., 2015).

New research and development areas, such quantum communications, have emerged because of the discovery of quantum mechanics. The mystery of the quantum universe captivated

physicists, mathematicians, and computer scientists, inspiring the creation of quantum nonduality and communication protocols (Rastogi et al., 2021). Developing viable technologies that meet the strict requirements of low noise and high coherence for quantum state encoding, high bit rate and low power for the integration with classical communication networks, and scalable and low-cost production for a realistic wide deployment, is also a challenge to take into consideration (Paraíso et al., 2021).

One of the main factors driving the current active development of QCT is the growing demand for secure communications which the demand for secure communication becomes increasingly important as the number of connected devices and the volume of data increase (Bobier et al., 2023). A secure method of creating symmetric encryption keys is provided by quantum key distribution (QKD) which one of the fundamental protocols in the field of quantum communication., whose security level may be calculated using information theory. Over the past two decades, QKD has developed at an ever-increasing rate, and the most recent years have been characterized by spectacular achievements demonstrating the technology's maturity (Paraíso et al., 2021).

QCT contributes to the growth of technology. The application of quantum bits in communication technology has already outperformed the capabilities of current technologies and shown us a new direction in the advancement of technical fields (Hasan et al., 2023). A recent study discusses the application of quantum computation and communication to 6G networks which mentioning that there is a need for scientists to create quantum-resistant gear and encryption techniques to deliver 6G to the public (Ali et al., 2023). The development of efficient and effective supply chains and the coordination of standardization activities are becoming increasingly important in the standardization of quantum communication (QKD), and it appears that the majority of the involved standards developing organizations are trying to cover the entire field of QKD standardization by themselves, without paying much attention to the activities (van Deventer et al., 2022).

Aside from that, governments and companies throughout the world have invested in the development of quantum communication because they understand how important it is for security. Initiatives like the CHIPS (Creating Helpful Incentives to Produce Semiconductors) and SCIENCE Act. Act in the United States and China's commitment to quantum technology, which includes networks of quantum dots, show the strategic importance of quantum communications (Bobier et al., 2023).

### ***Development of Quantum Communication Technology***

There are several well-established international efforts in quantum research and technology, and they are expanding quickly. For instance, Canada, a global leader in the QCT has invested over \$1 billion quantum research over the last ten years, as a result, Canada has a rising effect in the commercial sector, world-class research capabilities, and significant government investments in innovation and brings Canadian in a great position to create quantum technology (Sussman et al., 2019).

While Japan has been actively engaged in national quantum information research and technology projects for the past 30 years. The National Institute of Information and Communications Technology (NICT), the Japan Society for the Promotion of Science (JSPS), the Japan Science and Technology Agency (JST), and the Cabinet Office of the Government

of Japan are the primary funding organizations for these initiatives. In the past 15 years, these authorities have invested a total of US\$250 million in the field of quantum information science and technology, in addition to industry investments. The development of prototypes such as coherent Ising machines and quantum key distribution systems as well as the opening of new research frontiers have been made possible by this financing. Japan recently unveiled new measures to promote the study of quantum information (Yamamoto et al., 2019).

Russia also seen as dominating in QCT development and research works. Quantum technologies range from sensing to quantum communications to quantum computation and simulation. Russia has made significant advances in the field of quantum research, including in the fields of semiconductor technology, lasers, and low-temperature physics. In addition to two National Technological Initiative (NTI) facilities devoted to quantum technology, Russia has developed research organizations including the Russian Quantum Center and the Kazan Quantum Center. Both public and private funds are used to support these facilities. Additionally, programs like Megagrants, which encourage foreign academics to work with Russian universities, provide funding for quantum research in Russia (Fedorov et al., 2019)

Through literature the most recent worldwide study trends in QCT area including electronic markets, semiconductor testing, energy storage, internet and US, UK, Korea, Canada, or China found as leader in the research work (Singh et al., 2020). These nations are implementing a variety of quantum cryptography projects that offer secure information communication to the high technology sector (Singh et al., 2020).

### **Methodology**

The focus of this research was on to review reviews the awareness and readiness on development of QCT in Malaysia amongst regulators, cybersecurity's industry players and academia. Hence, 12 respondents from regulators, industry player and academia were joint the FGD. The selection of these respondents due to their positions in communication technology, particularly in cybersecurity (academic and practice) which hopes to provide input in answering the research question. The major aim of the focus group discussion is to comprehend the respondent's viewpoint, ideas and experiences on the topic that has being raised.

### **Research Design**

This study is qualitative study in nature. Focus group discussion method was adopted to collect the data from the respondents. a qualitative research approach was adopted. Focus group discussion was utilized to gather data because this method enables the respondents to express their opinion in words and brainstorming the answer by discussion (Prasad, 2017). Physical face-to face focus group discussion was conducted to collect the data. Many qualitative action research projects start with in-depth respondents' interviews as part of the planning phase and frequently, the investigations are concluded with individual or focus group interviews reflecting on the process (Merriam & Tisdell, 2016). This method is chosen to conduct this study since the aim is to explore and review the awareness and readiness among regulators, industry players and an academia on development of QCT in Malaysia.

### **Instrument**

In qualitative research, subjectivity and interactivity are assumed, and the researcher is the main tool for data collection. The interdependence of the observer and the observed may lead to behavioral changes in both parties. Therefore, the question is not whether the act of

observation influences what is observed, but rather, how can the researcher recognize these effects and account for them when interpreting the data (Merriam & Tisdell, 2016). Therefore, the focus group discussion was guided by a thematic structured interview question themed as follows:

No.	Theme	Details
Q1	Awareness of QCT	To study the awareness and evaluate the depth of respondent's understanding.
Q2	Security Breaches	To study the respondent's regarding data breaches and QCT roles in becoming the solutions.
Q3	Issues and challenges	To explore the internal and external threats in implementing QCT
Q4	Telecommunication sector	To identify the readiness in implementing QCT
Q5	Recommendation to adopt QCT	To get respondent's recommendation for QCT

**Table 1: Thematic Structured Interview Question**

### Sample

The respondents in this study were recruited through purposeful sampling wherein the researcher identified and select the potential individuals with the information, experience, or viewpoints pertinent to the research topic. In this study, the researcher selects respondents among regulators, industry players and academicians who are in the IT and related cybersecurity sector since QCT is the collection of principles and techniques that enable secure communication which is much more related to cybersecurity sector. Academia and industry players were included in the discussion to identify the awareness and explore their opinion on Malaysia's readiness in implementing QCT in terms on current cybersecurity practice and research. Besides, regulators which government sector were also included because they play important roles to provide support regarding QCT development especially in terms of funds and infrastructures. In summary, academia provided insights into theoretical foundations, industry players contributed practical perspectives, and regulators ensured consideration of the broader ecosystem necessary for successful QCT adoption. The respondents are as below:

No.	Company's name	Position	Number of respondents
1.	Public University	Academia	3
2.	Government sector	Regulator	4
3.	Cyber-security specialist agency and technology company	Industry player	3
4.	Malaysian telecommunication company	Industry player	2

**Table 2: List of Respondents**

### ***Focus Group Discussion Protocol***

The focus group discussion has been conducted which consists of twelve (12) respondents, one (1) moderator and two (2) rapporteurs. There are five (5) questions which the first question assessed the awareness of QCT among respondents, the second question regarding the security breaches, third question regarding issues and challenges, fourth regarding the perspective of telecommunication sector regarding motivation to adopt QCT and what is needed for the adoption, the last one is the respondent's recommendations to develop QCT. The first, second and third main questions is to assess the respondent's awareness of QCT which the first is directly questioned about the general awareness of QCT among the respondents, second questions are awareness about security breaches which the motivation factor of QCT adoption and the awareness of issues and challenges to adopt QCT. The question is importance to understand awareness to identify the understanding the current knowledge, perceptions, and challenges related to QCT. Thus, the answers based on these questions will provides a comprehensive understanding of the current state of awareness and the factors influencing the adoption of QCT.

Therefore, for readiness will be assessed from question four and five in which it is relevant to ask about the perspective of the telecommunication sector regarding the motivation to adopt QCT and what is needed for the adoption. This is important because it provides insights into the sector's preparedness, willingness, and requirements for integrating QCT into their operations. Understanding the motivation and necessary conditions for adoption can help in assessing the current state of readiness and identifying any potential barriers or facilitators to the adoption of QCT within the telecommunication sector. The information gathered from these questions can be valuable for formulating strategies to support and promote the adoption of QCT within the telecommunication industry.

The discussion was recorded and later transcribed. There are also written answer from the respondents during the focus group discussion that were collected at the end of the session. The written answer is based on the same questioned that has been discussed during focus group discussions to let respondents add in and enhance their answer, the written answer later being combined with the verbal answer to be analysed for the pre-data analysis

### **Results**

Data gathered from focus group were analyzed using thematic analysis and being discussed accordingly. The study topics address the regulators, industry players and academia understanding of QCT and their readiness regarding to implement the technology.

#### ***Awareness of QCT and its development in Malaysia.***

According to the respondents' responses 8 out of 12 respondents said they already heard about QCT previously, additionally, one from the eight respondents emphasized that people who comes from a security background will be familiar with this technology. R10 said he heard about Quantum Technology but never heard specifically about QCT. The remaining did not answer the question. Accordingly, this study concludes that most of the respondents are aware of QCT.

The respondents also can well-explained about QCT in which 8 out of 12 respondents can elaborate on QCT. Six of the respondents: R1, R2, R3, R4. R9 and R10 alluded to this notion:

“QCT has different backgrounds, starting from engineering, physics, and IT. The intention of QCT is because of the breach of the factorial function that the algorithm shows ...” (R1).

“Communication technology that involves/uses quantum version/mechanics (globally)...” (R2)

“There are two issues in data security, data in motion, and data address. Quantum network focusing on in motion data. We are a man in the middle, sniffing traffic between point A to point B on the network. Quantum entanglement can detect if there is anybody in the middle. Intercept the communication...” (R3)

“... So, the key we will look at is a quantum algorithm, one quantum key is physics, and the other is a quantum algorithm. use the quantum concept...” (R4)

“Communication using Quantum technology to transport single photons as early research” (R6) “...it is about un-hackable communication” (R9)

“QCT is a communication technology using quantum technology, including quantum algorithms and protocols.” (R10)

Interestingly, in terms of QCT development only 4 respondents admitted they are aware of the development of QCT in Malaysia while one respondent was aware of the development at the international level but not in Malaysia. The remaining respondents either answered “no” or not answer the question. Three of the respondents: R4, R8, and R10 alluded to this notion:

“Yes, but not detail. Not aware of the recent development in Malaysia...” (R4)

“In Malaysia, yes but partially ...” (R8)

“If QKD is part of QCT, then I have been aware since 2009...” (R10)

### ***Security breaches***

During the discussion, the risk of breaking the code is acknowledged by the regulators, industry players and academicians. Most of the respondents said the security breaches can happen in the organization because of people specifically in individual faulty, lack of security awareness, low-security technology, and misconduct human error. There are also mentioned that phishing and hacking can caused the security breaches. Three of the respondents: R2, R4, and R9 alluded to this notion:

“Individual faulty and misconduct, human error.” (R2)

“...People. lack of security awareness and low-security technology to protect parameter security.” (R4)

“...But every year we actually pay hackers to come and hack us. We do. It is part of our risk assessment every year, and every year without fail a staff of 25, but for 14 years, there are still people who forget, you know, people. The human part is hard...” (R9)

In addition, the respondents also suggest some common practices if the breaches happen such as revoke the RSA (Rivest–Shamir–Adleman) key, need a proper incident response team, study the problem, and fix it accordingly and update the company policy and procedures. One of the respondents: R4 alluded to this notion:

“Perform RCA (Root Cause Analysis) and fix the issues. Back to people, processes, and technology. Improve everything...” (R4)

The respondents acknowledged that QCT is not a total solution for the breaching issue. QCT can be the solution for high level or advanced data such as national security, bank information, etc. Four of the respondents: R1, R2, R4, R8 alluded to this notion:

“...quantum is not coming to replace everything. We have to maintain everything, and the only thing is the sub of the part that is not secured that has to change...” (R1)



“...quantum computer is not replacing the classical computer. The classical will still exist, simultaneously...” (R2)

“...QCT can be a solution to parameter security but not solve the human factor for breaches.” (R4)

“...There is no single recipe for a solution. We need to do a cost or risk-benefit analysis to find the solution. So, it depends on the situation...” (R8)

In addition, all industry players agree that the issue of data security is important because during the discussion, 8 out of 12 respondents suggested that the company should undertake IT risk assessment. However, they have different idea about the frequency of IT risk assessments. Some suggested monthly, the other suggested annually. 5 respondents also suggested for a company to have Chief IT risk Officer to handle the risk. There are also suggestions to have good governance, security policies in place, awareness program and implement the access control for company to monitor security breaches to avoid the reoccurrence.

### ***Issues and challenges regarding the adoption of QCT***

Response from the respondents regarding issues and challenges of QCT adoption will be divided into two views which is external threats and internal threats. The external threats classified into 3 factors such as economic factor, technological advancement, the current standard industrial practice, and legal and regulatory requirements. For economic factor, there are concerns on the amount of investment by the government as the cost of implementation is expensive to make it available for everyone and it is important for the government and private organizations to do a cost-benefit analysis because cost and budgeting would be one of the challenges for the implementation of QCT in an organization. Three of the respondents: R1, R3, R9 alluded to this notion:

“...The obstacle is actually the money.” (R1)

“It is going to be very expensive to make it available to everyone” (R3)

“... But again, at the end of the day as a private organization, the cost-benefit analysis is very important.” (R9)

For technology advancement factor, the technology advancements can lead to data breaches due to several interconnected reason such as increased connectivity and digitization which as technology grows, more device and systems become interconnected, creating vast network of data exchange. Thus, as technology evolves, so do cyberattacks which hackers will continuously develop new techniques, tools, and strategies to bypass security measures and breach data which in other words, the hackers will take advantage on vulnerabilities in software, hardware, and network infrastructure to infiltrate systems and steal valuable data (Farrelly, 2023). One of the respondents, alluded to this notion:

“These data breaches are super easy now. We must come out with whatever way of securing it... Israel spy makes it very easy; they install spyware on your phone to intervene. They basically tell the information where the encryption is already passed. Decrypt it from your body. That is the easiest way to do it basically.” (R3).

For third factor which is the current standard industrial practice, legal and regulatory requirements, most of the respondents agreed that government involvement is important

especially in relation to policy enforcement and financial. One of the respondents said that the current standard industrial practice is very low, and the bearable cost depends on what the organization wants to protect. Therefore, the remaining of the respondents did not give any feedback regarding this factor. One of the respondents: R3 alluded to this notion:

“The price depends on what you want to protect. The central bank has a lot of resources and money so it can hire a lot of people which is very good, but other companies must rely on profitability. The government has to give the budget because it is part of the economy...” (R3) Nevertheless, the enforcement from the government is a must because if the government did not enforce, none of the agency will take an action because all companies are waiting government to inject some money. Four of the respondents: R1, R4, R5, R9 alluded to this notion:

“If the government does not push things, nobody will because the agencies or all companies are waiting for the government to inject some money...” (R1)

“We are not investing unless there is a specific requirement from regulatory...” (R4)

“...if this regulation does not exist, it will be difficult to implement because it cannot be validated.” (R5)

“If the policy is from the top, everybody in certain industries must follow it...” (R9)

While for internal traits the respondents mentioned that top management commitment and acceptance of new technology as internal challenges. For the top management commitment issue, one of the respondents mentioned that if the top management does not see the importance of investing in QCT, it will not proceed. Other respondents also add that if looking from the bottom-up will be difficult. However, if it is top-down will be easier. Therefore, one of the respondents mentioned that any technology that offers better security can be accepted by the cybersecurity team which in line with technology evolvments.

### ***Perspective Of Telecommunication Sector Regarding Motivation To Adopt QCT***

This part discusses on findings the readiness to adopt QCT which could be divided to motivation, requirements, and benchmarking. One of the respondents mentioned that the motivation for the telco sector to invest in QCT is driven by how the company value the security in which it is crucial if the communication is categorized as secret and top secret. Therefore, the motivation will also be to fulfill the demand in having secure communication. Two of the respondents: R1, R4 alluded to this notion:

“Not valuable unless politicians like top management...” (R1)

“To provide secure communication to certain highly confidential groups (demand from users) ...” (R4)

Additionally, it is mentioned that it is not easy to simply invest in QCT because the private sector or even the government will consider revenue and that is mostly how they value the business. Other respondents added that it is not viable for the internal team unless it comes from a regulatory requirement. Hence, the industry players acknowledge that QCT adoption is quite pricey to invest in because the key elements of QCT, such as photon sources, detectors, and entanglement generation equipment, are expensive and often require specialized expertise (McKinsey & Company, 2021). One of the respondents: R4 alluded to this notion:

“Not ready to fully fledge. But consider exploring a pilot project to adopt QCT...” (R4)

QCT need to be integrated to implement fundamental physical capabilities of transmission and detection, ensuring optimal performance. Historically, quantum networks have been deployed as separate infrastructures, but there is a growing need to integrate them into existing telecommunications infrastructures in a way that optimizes their performance (Martin et al., 2021). Respondents R3 mentioned that if QCT want to be integrated with other system and process, the policy should come out with a special niche that the user uses because the public not going to use it immediately or directly, but they want to see a more secure and reliable communication with their banking, and their asset information. Other respondents added that the QCT integration with other systems and process depends on the manufacturing capability to integrate QCT technology into existing infrastructure and there is no problem in the telco industry as the communications between peers to peer is already secured because every communication, end-to-end communication is encrypted.

Additionally, two (2) of the respondents also suggested the need to have specific training and upgrade the skills needed to operate and maintain the QCT. There were 7 respondents suggested a need to benchmark multiple countries for example Europe, China, and the US instead of one country for QCT adoption in Malaysia whereas every country's approach is different. Some countries approach QCT through the initiative of R&D starting from research meanwhile some other countries are based on the initiative of the policy itself. Other respondents then added that the European Union is the best for benchmarking because Europe came out with the initiative for all the countries, using money from the EU and it creates competition moving to another platform as it is driven by the industry-to-consumer. Not only the industry can get benefit but also the government will also benefit from it which the country's technology development will be progressing well. In addition, some of the respondents also emphasizes the R & D technologies project performed by US, UK, and German to be referred for QT adoption in Malaysia. Three of the respondents: R1, R7, R8 alluded to this notion:

“Every country's approach is different; some are through the initiative of R&D starting from the research...” (R1)

“Yes benchmark, R&D within universities or government even industry. See US, UK, and German.” (R7)

“We Need to follow / benchmark multiple countries instead of 1” (R8)

### ***The Readiness Of Industry Players With QCT***

The insights gathered from the Focus Group Discussion shed light on the critical imperatives for advancing quantum communication technology (QCT) and its integration into existing frameworks. The respondents articulated a consensus on the necessity of bolstering educational initiatives and emphasized the pivotal role of government in fostering integration, policy development, and international collaboration. Furthermore, the imperative of raising societal awareness, particularly at the academic level, was underscored as a vital component in the journey towards QCT integration and adoption.

In light of the Focus Group Discussion, it is evident that a multifaceted approach is essential for the advancement of quantum communication technology (QCT). The respondents unanimously stressed the imperative of enhancing educational efforts, while also highlighting the pivotal role of government in facilitating integration with existing infrastructure, conducting pilot projects, formulating strategic policies, fostering international collaborations,

and allocating substantial budgets to support QCT development. Additionally, the need to cultivate societal awareness, particularly at the academic level, was underscored, with recommendations encompassing interactive platforms such as talks, forums, training programs, accelerators, and funding initiatives. Three of the respondents: R5, R8 and R10 alluded to this notion:

“I would like to suggest exposure to quantum computing and security at degree level and industry level through talk, forum, training, accelerator programs and funding” (R5)

“Regulatory requirement can increase and speed up adoption of QCT and government needs to increase awareness” (R8)

“QCT require a big budget. Therefore, support from the government and its agencies is needed. Due to the cost also, QCT might be used only for highly classified data such as secret and top secret. QCT policy must be put under Dasar Kriptografi Negara. Qualified agencies must be appointed by the government to set up and drive the policy.” (R10).

## Discussion

The discussion will be based on the five main themes that were previously mentioned in the methodology section. These themes including awareness of Quantum Computing Technology (QCT), security breaches, issues and challenges related to QCT development, readiness of the telecommunications sector, and recommendations for QCT adoption. In general, most of the respondents aware about QCT and as for the readiness, the telecommunications industry is motivated to invest but there are a few constraints they need to consider.

### *Theme 1: Awareness of QCT*

The first theme of the study focuses on the level of awareness among respondents regarding Quantum Communication Technology (QCT). While most respondents demonstrated some level of familiarity with QCT, the extent of their knowledge regarding its development in Malaysia and internationally varied. Out of the 12 respondents, 8 reported having prior knowledge of QCT. Notably, one of these respondents, who possessed a security background, emphasized that individuals with similar expertise are likely to have a greater understanding of QCT. This indicates that a significant number of respondents are aware of QCT, and its relevance to security and related fields such as in cybersecurity background. Besides, only 4 respondents admitted they are aware of the development of QCT in Malaysia, and one respondent was aware of the development at the international level but not in Malaysia. The remaining respondents either answered "no" or did not answer the question. This suggests that while some respondents are aware of QCT, there is still room for improvement in terms of understanding its development and adoption in Malaysia compared to other countries.

Therefore, the first theme of this study indicates that most respondents are aware of QCT, but there is a need for further education and promotion of the technology in Malaysia to ensure its development and adoption in various sectors, such as national defence, aerospace, finance, and others (Latest Market Analysis, 2023). As the market for quantum communication devices is growing, it is crucial for Malaysia to stay ahead of the competition by adopting and integrating QCT into its information and communication technology (ICT) infrastructure (Latest Market Analysis, 2023).

### ***Theme 2: Security Breaches***

During the discussion, the respondents acknowledged the risks associated with security breaches and the limitations of Quantum Communication Technology (QCT) in addressing certain aspects of data security. Therefore, there is a need to emphasize on the continuous improvement in security awareness, technology, and governance to address the human factor and other challenges related to security breaches. Additionally, the respondents acknowledged the value of IT risk assessments and the role of a Chief IT risk Officer in managing and mitigating risks associated with data security. Thus, there is a need to assemble a team of experts to conduct a comprehensive data breach and prepare for proper framework in managing any cybersecurity issues.

QCT provides secure communication but is not a complete solution for all security risks. A comprehensive risk management strategy in implementing QCT is necessary, including continuous improvement in security awareness, technology, and governance, and assembling an expert team to manage cybersecurity issues. By adopting a holistic approach, organizations can better protect themselves against the evolving threat landscape posed by hackers' advancements.

### ***Theme 3: Issues, And Challenges of QCT***

The discussion highlights the challenges associated with Quantum Communication Technology (QCT) implementation, including the high cost, the need for cost-benefit analyses, and the continuous evolution of technology leading to increased cyber threats. It also emphasizes the importance of government enforcement and top management support for successful QCT integration. The high cost of QCT implementation is a concern, especially for small companies relying on return on investment (ROI) to sustain their operations. Government and private organizations are the important stakeholder who should conduct cost-benefit analyses to assess the viability of QCT implementation.

The rapid evolution of technology, including increased connectivity and digitization, creates a fertile ground for cyberattacks. As technology advances, hackers continuously develop new techniques to exploit vulnerabilities in software, hardware, and network infrastructure, posing a significant threat to data security which lead to the urgency of continuous improvement of cyber security. Thus, the current standard industrial practice is perceived to be low, and the price of protection depends on what an organization seeks to safeguard. Government enforcement is deemed essential to drive action, as companies are reliant on government investment.

Apart from that, the commitment and acceptance of new technology by top management are identified as internal challenges. The importance of top-down support for QCT implementation should be emphasized, as it can facilitate the acceptance of new technologies, particularly those offering enhanced security. Without the support from the top management of companies, the QCT development cannot be progressively developed which the support should be from both government and private sectors (companies).

There is a need for specific strategies to address the challenges of implementing QCT. These include conducting thorough cost-benefit analyses by both governments and private enterprises to assess the feasibility of QCT deployment, given its significant costs. Additionally, it is crucial to continuously improve cybersecurity measures due to the evolving technology

landscape and increasing cyber threats. Furthermore, government involvement is essential to drive action and investment in QCT implementation. Finally, gaining support and approval for innovative technology from executive leaders is vital for successful QCT integration across industries.

#### ***Theme 4: The Readiness Of Telecommunication Sector***

The telecommunication sector is inclined to invest in Quantum Communication Technology (QCT) due to its secure transmission capabilities. However, the high cost of QCT limits its application to high-value or top-secret data, posing a significant challenge for industry players, as revenue is a primary consideration for both private and government organizations. The integration of QCT with existing systems and processes depends on manufacturing capability, and specific training and skills upgrades are necessary for effective QCT operation and maintenance. Furthermore, benchmarking with countries such as Europe, China, and the US is recommended before QCT adoption in Malaysia, with the European Union being the preferred benchmarking option. Internal challenges include top management commitment and acceptance of new technology, emphasizing the need for top-down support to facilitate the acceptance of new technologies, particularly those offering enhanced security.

There are several key considerations for successful Quantum Communication Technology (QCT) adoption. Firstly, addressing the significant cost of QCT adoption is crucial for industry players, requiring careful consideration of revenue implications. Secondly, prioritizing specific training and skills upgrades is necessary for effective QCT operation and maintenance. Thirdly, conducting benchmarking with leading countries, such as Europe, China, and the US, is recommended to inform QCT adoption in Malaysia. Finally, emphasizing top management commitment and acceptance of new technology, along with the need for top-down support, is essential to facilitate successful QCT implementation. By addressing these considerations, organizations can better prepare for and integrate QCT into their operations.

#### ***Theme 5: The Recommendations To Adopt QCT***

The findings suggest that education and awareness of QCT should be enhanced, particularly among degree-level students. The government should play a pivotal role in integrating QCT with existing infrastructure, conducting pilot projects, creating policies, collaborating with other countries, and incorporating QCT implementation into regulatory requirements. The cost of QCT adoption is a significant challenge for industry players, necessitating careful consideration of revenue implications. Specific training and skills upgrades are necessary for effective QCT operation and maintenance. Benchmarking with leading countries is recommended before QCT adoption in Malaysia. Top management commitment and acceptance of new technology, along with the need for top-down support, is crucial to facilitate successful QCT implementation. The government funding is required as QCT implementation requires a substantial budget.

#### **Conclusion**

In conclusion, the study extensively explored the awareness and readiness of Quantum Communication Technology (QCT) in Malaysia, shedding light on critical factors influencing its successful integration across various sectors. The research unveiled a generally positive awareness of QCT, particularly among those with a security and cybersecurity background. However, there is a pressing need for further education and promotion within Malaysia to ensure widespread understanding and adoption across diverse sectors. Addressing the

limitations of QCT in data security, the study emphasized the continual improvement of security awareness, technology, and governance. A comprehensive risk management strategy, incorporating expert teams and IT risk assessments, was underscored to navigate the evolving cybersecurity threat landscape. Identifying challenges such as high implementation costs and the rapid evolution of technology, the study recommended government enforcement, top management support, and specific strategies, including thorough cost-benefit analyses. While the telecommunication sector expresses interest in QCT's secure transmission capabilities, the high cost presents a challenge, requiring considerations such as cost implications, prioritized training, benchmarking, and top-down support for successful adoption. The study further proposed enhancing education and awareness, particularly among degree-level students, with critical government involvement for integration, pilot projects, policy creation, international collaboration, and securing funding. In essence, achieving successful QCT implementation in Malaysia necessitates collaborative efforts involving education, industry players, government support, and strategic planning to overcome challenges and capitalize on the transformative potential of this technology.

### Acknowledgement

This research was supported by the Ministry of Higher Education (MOHE) through Long Term Research Grant Scheme.

### Bibliography

- Ali, M. Z., Abohmra, A., Usman, M., Zahid, A., Heidari, H., Imran, M. A., & Abbasi, Q. H. (2023). Quantum for 6G communication: A perspective. *IET Quantum Communication*. <https://doi.org/10.1049/qtc2.12060>
- Bobier, J.-F., Naudet-Baulieu, C., Langione, M., Thorson, B., Šnajdr, J., & Deutscher, S. (2023, March 22). *Are You Ready for Quantum Communications?* <https://www.bcg.com/publications/2023/are-you-ready-for-quantum-communications>
- Eiza, M., Okeke, R. I., Dempsey, J., & Ta, V.-T. (2021). Keep Calm and Carry on with Cybersecurity @Home: A Framework for Securing Homeworking IT Environment. *International Journal on Cyber Situational Awareness*, 5(1). <https://doi.org/10.22619/ijcsa.2020.100131>
- Farrelly, J. (2023, July 10). *High-Profile Company Data Breaches 2023*. Electric. <https://www.electric.ai/blog/recent-big-company-data-breaches>
- Fedorov, A. K., Akimov, A. V., Biamonte, J. D., Kavokin, A. V., Khalili, F. Y., Kiktenko, E. O., Kolachevsky, N. N., Kurochkin, Y. V., Lvovsky, A. I., Rubtsov, A. N., Shlyapnikov, G. V., Straupe, S. S., Ustinov, A. V., & Zheltikov, A. M. (2019). Quantum technologies in Russia. In *Quantum Science and Technology* (Vol. 4, Issue 4). Institute of Physics Publishing. <https://doi.org/10.1088/2058-9565/ab4472>
- Froehlich, A. (2022, July). *data breach*. TechTarget. <https://www.techtarget.com/searchsecurity/definition/data-breach>
- Giles, M. (2019, February 14). *Explainer: What is quantum communication? | MIT Technology Review*. MIT Technology Review. <https://www.technologyreview.com/2019/02/14/103409/what-is-quantum-communications/>
- Goldner, P., Ferrier, A., & Guillot-Noël, O. (2015). Rare Earth-Doped Crystals for Quantum Information Processing. *Handbook on the Physics and Chemistry of Rare Earths*, 46, 1–78. <https://doi.org/10.1016/B978-0-444-63260-9.00267-4>

- Hasan, S. R., Chowdhury, M. Z., Saiam, M., & Jang, Y. M. (2023). Quantum Communication Systems: Vision, Protocols, Applications, and Challenges. In *IEEE Access* (Vol. 11). <https://doi.org/10.1109/ACCESS.2023.3244395>
- Krause, J. (2022, March 29). *What are quantum computing and quantum communication? - IPPI*. <https://www.ippi.org.il/what-are-quantum-computing-and-quantum-communication/>
- Latest Market Analysis. (2023, September 12). *Quantum Communication Market Stay Ahead of the Competition by Upcoming Years 2031*. <https://www.linkedin.com/pulse/quantum-communication-market-stay-ahead-competition>
- Martin, V., Brito, J. P., Escribano, C., Menchetti, M., White, C., Lord, A., Wissel, F., Gunkel, M., Gavignet, P., Genay, N., Le Moul, O., Abellán, C., Manzalini, A., Pastor-Perales, A., López, V., & López, D. (2021a). Quantum technologies in the telecommunications industry. *EPJ Quantum Technology*, 8(1). <https://doi.org/10.1140/epjqt/s40507-021-00108-9>
- Martin, V., Brito, J. P., Escribano, C., Menchetti, M., White, C., Lord, A., Wissel, F., Gunkel, M., Gavignet, P., Genay, N., Le Moul, O., Abellán, C., Manzalini, A., Pastor-Perales, A., López, V., & López, D. (2021b). Quantum technologies in the telecommunications industry. *EPJ Quantum Technology*, 8(1). <https://doi.org/10.1140/epjqt/s40507-021-00108-9>
- McKinsey & Company. (2021, December 21). *Shaping the long race in quantum communication and quantum sensing*.
- Merriam, S. B., & Tisdell, E. J. (2016). *Qualitative Research: A guide to design and implementation* (Fourth). Jossey-Bass.
- Mustafa, Z. (2017, July 19). *Facilitating low-cost quantum experiments*. <https://www.nst.com.my/education/2017/07/258717/facilitating-low-cost-quantum-experiments>
- Paraíso, T. K., Woodward, R. I., Marangon, D. G., Lovic, V., Yuan, Z., & Shields, A. J. (2021). Advanced Laser Technology for Quantum Communications (Tutorial Review). In *Advanced Quantum Technologies* (Vol. 4, Issue 10). <https://doi.org/10.1002/qute.202100062>
- Prasad, M. (2017, September 11). *How to Conduct a Successful Focus Group Discussion*. Humans of Data. <https://humansofdata.atlan.com/2017/09/conduct-successful-focus-group-discussion/>
- R. Loheswar. (2022, December 31). *Major data breaches in Malaysia in the past 24 months / Malay Mail*. Malaymail. <https://www.malaymail.com/news/malaysia/2022/12/31/major-data-breaches-in-malaysia-in-the-past-24-months/47722>
- Raj, A. (2021, August 4). *Will there be enough quantum engineers in APAC? - Tech Wire Asia*. <https://techwireasia.com/2021/08/will-apac-have-sufficient-quantum-engineers-as-quantum-computing-gains-traction/>
- Rastogi, T., Hassija, V., & Saxena, V. (2021). Quantum communication: Concept, applications, and future outlook. *ACM International Conference Proceeding Series*. <https://doi.org/10.1145/3474124.3474131>
- Setiawati, D., Hakim, H. A., & Yoga, F. A. H. (2020). Optimizing Personal Data Protection in Indonesia: Lesson Learned from China, South Korea, and Singapore. *Indonesian Comparative Law Review*, 2(2). <https://doi.org/10.18196/iclr.2219>



- Singh, S. K., Azzaoui, A. El, Salim, M. M., & Park, J. H. (2020). Quantum Communication Technology for Future ICT - Review. *Journal of Information Processing Systems*, 16(6), 1459–1478. <https://doi.org/10.3745/JIPS.03.0154>
- Sussman, B., Corkum, P., Blais, A., Cory, D., & Damascelli, A. (2019). Quantum Canada. *Quantum Science and Technology*, 4(2). <https://doi.org/10.1088/2058-9565/ab029d>
- van Deventer, O., Spethmann, N., Loeffler, M., Amoretti, M., van den Brink, R., Bruno, N., Comi, P., Farrugia, N., Gramegna, M., Jenet, A., Kassenberg, B., Kozlowski, W., Länger, T., Lindstrom, T., Martin, V., Neumann, N., Papadopoulos, H., Pascazio, S., Peev, M., ... Wilhelm-Mauch, F. K. (2022). Towards European standards for quantum technologies. In *EPJ Quantum Technology* (Vol. 9, Issue 1). <https://doi.org/10.1140/epjqt/s40507-022-00150-1>
- Vishwanath, A., Neo, L. S., Goh, P., Lee, S., Khader, M., Ong, G., & Chin, J. (2020). Cyber hygiene: The concept, its measure, and its initial tests. *Decision Support Systems*, 128. <https://doi.org/10.1016/j.dss.2019.113160>
- Wang, Y., & Wang, L. (2022). Internet Financial Data Security and Economic Risk Prevention for Android Application Privacy Leakage Detection. *Computational Intelligence and Neuroscience*, 2022. <https://doi.org/10.1155/2022/6782281>
- Yamamoto, Y., Sasaki, M., & Takesue, H. (2019). Quantum information science and technology in Japan. In *Quantum Science and Technology* (Vol. 4, Issue 2). Institute of Physics Publishing. <https://doi.org/10.1088/2058-9565/ab0077>