DEVELOPMENT OF QUANTUM COMMUNICATIONS TECHNOLOGY (QCT) IN MALAYSIA: NATIONAL SECURITY, FRAMEWORK AND POLICY

Nurul Huda, Mustafa Mohd Hanefah, Rosnia Masruki and Nor Asiah Yaakub

Faculty of Economics and Muamalat, Universiti Sains Islam Malaysia, Malaysia

mustafa@usim.edu.my
rosnia@usim.edu.my
norasiah@usim.edu.my

*Corresponding Author: mustafa@usim.edu.my

Abstract**:** *The transfer of information from one single device to another has been more secure in recent years through to the development of quantum communication technology (QCT) in a variety of technological uses. Preparing for this new, emerging sector is important since information communication technology (ICT) in the future will certainly depend on QCT, which is built on quantum physics laws to secure the transfer of information. Future quantum technology will not only optimize computers and the internet but also change the way we communicate. This study discusses the importance and impact of QCT in the context of national security, framework, and policy. Furthermore, this paper also discusses the latest research trends of QCT in several countries including the United States, Canada, and China that Malaysia can learn from. In addition to that, this paper traces the development of QCT policy in other countries along with the existing development of security policy and framework in Malaysia. Finally, this paper discusses the importance of QCT with recommendations.*

Keywords: Communication Technology, National Security, Policy

1. Introduction

1.1 Quantum Communication Technology (QCT)

In quantum technology, the four foundations of quantum mechanics are (1) quantum computing; (2) quantum cryptography; (3) quantum imaging; and (4) quantum sensors. Quantum computing was initially introduced in 1980 by mathematician Yuri Manin when discussing the concept of quantum computation in the manuscript of his work (Singh et. al., 2020). Later, physicist Feynman observed that quantum computers vary from conventional computers in several additional ways (Feynman, 1982). In many cases, contrary to what would be achievable in a classical environment, quantum physics enables a large increase in communication efficiency (Brassard, 2001).

Soon, quantum computers will take the role of traditional computers in our daily lives. This industry is developing rapidly especially with the work being done to create quantum computers by giant tech companies like Google and IBM. A quantum computer hosted in the cloud can also make the work easier (Singh et. al., 2020). As these technologies are now the most appropriate, recent studies have concentrated more on quantum teleportation and quantum

internet. Quantum key distribution (QKD), which relies on the principles of quantum mechanics, is the most widely used quantum Internet application. It is used to protect interactions between the sender and recipient. Future quantum Internet will be highly confidential manner as a result of QKD's security, which also allows several quantum devices to be gathered to the cloud to transmit incredibly large quantities of computational power (Ezratty, 2001; Nanxi, 2021).

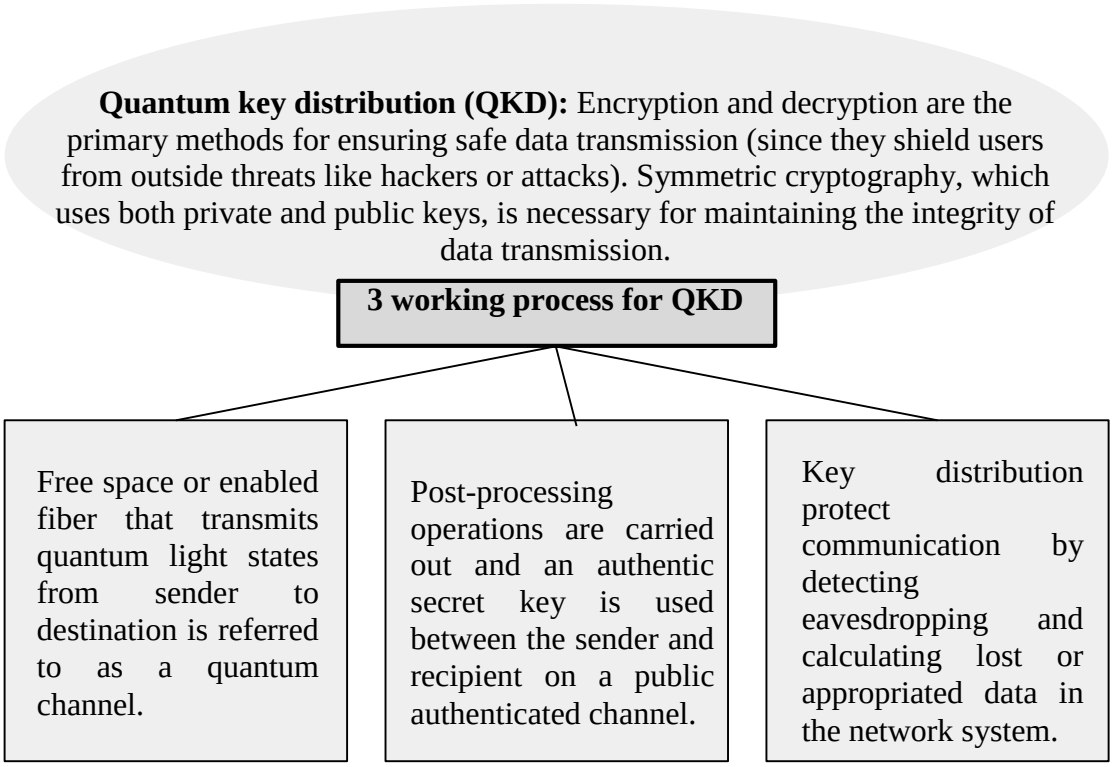

Figure 1. QKD and the three working processes

Key distribution is hence the foundation to secure communication within the network. In order to ensure safe communication in the systems, it transmits the key procedure between the sender and the recipient of the communication. According to Ezratty (2001), traditional key distribution techniques face a number of difficulties, such as security threats from shoddy random number generators, CPU power requirements, uncontrolled unidentified breaches, and more. QKD is used to overcome these difficulties and it uses quantum characteristics to transmit the secret information. In the global research trends of QCT, there are countries that are actively involved and participating in the development of QCT:

- **United States:** In accordance with the National Quantum Initiative Act, the United States has allocated 1.2 billion dollars in the direction of quantum research. The Act's main goal is to establish centers for development research. The research centers intend to engage with government, business, and academia to advance the field of quantum technology more quickly.

- **Canada:** In the last ten years, Canada has spent more than 1 billion dollars on research and development related to QCT. Quantum information processing, metrology, communications, cryptography, and networks are the main areas of research. With a financing of 80.9 million dollars, the Canadian government is actively exploring QKD in cooperation with the Canadian Space Agency to improve safer and more encrypted communications in space and safeguard digital communication.

- **China:** China is at the forefront of research into quantum technology in Asia. China creates sensors that can see through fog and corners as well as computers that are computationally more powerful than current ones. The National Development and Reform Commission and the China Academy of Science invested 490 million dollars in the research area of focus for creating QKD's industrial applications between 2011 and 2015. Since 2016, the main areas of study that have received support from both the federal and local governments have been quantum computation, metrology, and communication.

2. Impact on the Policy

In order to secure data transfer, the ICT of the future will certainly depend on QCT, which has its foundation in quantum physics laws. As such, it is essential that we remain prepared for this new, developing field. Future quantum technology will not only improve computers and ICT but also change the way people communicate. QCT is seen as the future form of communication, replacing the traditional Internet.

As these technologies are now the most appropriate, recent studies have concentrated more on quantum teleportation and quantum internet. QKD, which relies on the principles of quantum mechanics, is the most widely used quantum Internet application (Ezratty, 2001). It is used to protect interactions between the sender and recipient. Future quantum Internet will be highly confidential manner as a result of QKD's security, which also allows several quantum devices to be gathered to the cloud to transmit incredibly large quantities of computational power.

The Wikileaks scandal involving the leaking of sensitive United States information points out the main issue: when a country's important infrastructure (in this case: defense and diplomatic cables) can threaten national security (Sonny, 2011: Leigh & Harding, 2011). Further, according to Leigh & Harding (2011), important information concerning military, cyber security, and defense operations could be jeopardized if it falls into the wrong hands, endangering national and public safety. The reason is obvious that everything that we all experience has hazards and threats, whether they are intentional or accidental, physical or otherwise. In this regard, technical errors or carelessness in the management of the internet could have fatal consequences. Malaysia should be concerned about this issue. To relate, a secure, peaceful, and successful nation can be achieved with the help of cyber security programs, in this case, QCT national security, framework, and policy.

3. Development of security policy in Malaysia

The country's development and economic growth depends on the maintenance of harmony and safety both inside the nation and in the regions that surround it. With the intention of defending the nation against foreign invasion and upholding law and order in Malaysia, a

list of cybersecurity programs, national security, and policy was set up. Having said that, in order to prevent cyber security crime, measures have been taken to encourage and maintain a closer relationship between the government and the general people.

It is notable that the Malaysia Plan specifically mentions the safeguarding of crucial national information infrastructure and emphasizes this protection. The harm of cyber activity frequently threatens a nation's core foundations thus Malaysia acknowledges cyber security as a national priority. There are policies and frameworks that have been done to protect national security for example in the case of cyber security protection, the Government of Malaysia established the National Cyber Security (NCSP) strategy in 2006 as a national strategy. This policy is for the protection of the country's critical information infrastructure, albeit it places more emphasis on a narrower definition of cyber security. The timeline of the development of security policy in Malaysia is as follows:

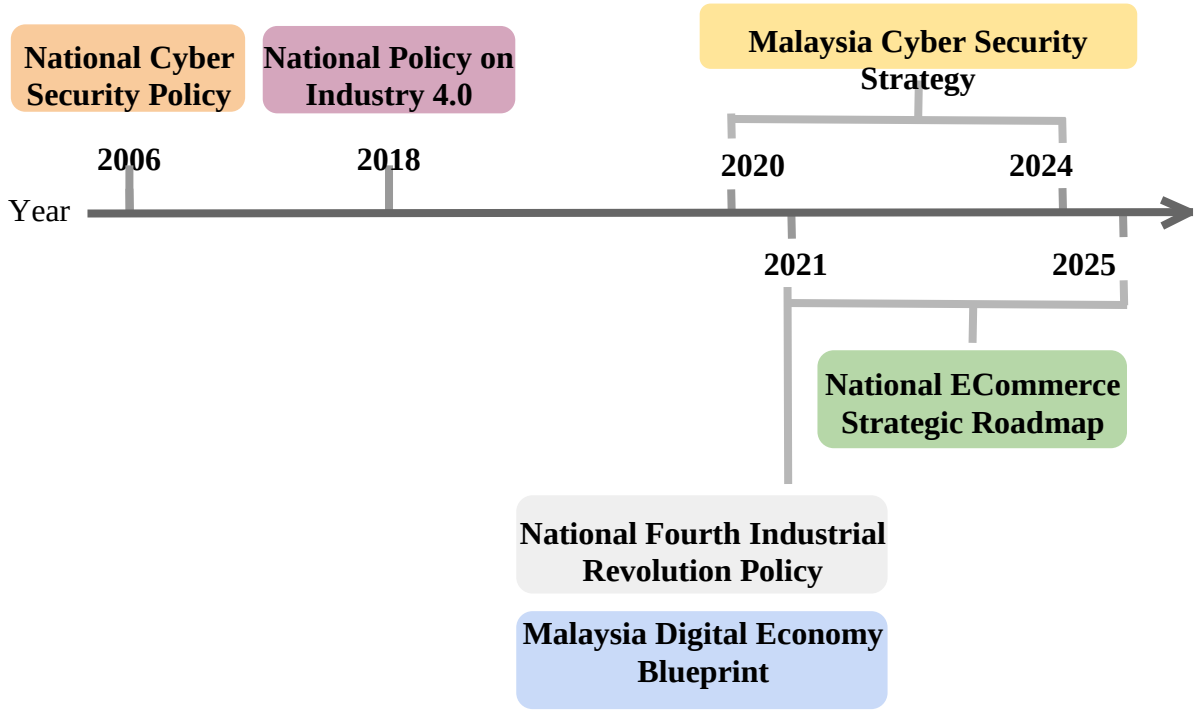

Figure 2. Development of security policy in Malaysia

- *National Cyber Security Policy (NCSP), 2006*: The NCSP defines Critical Information Infrastructure as the assets (real and virtual), systems, and functions that are vital to the nation that their failure or destruction would severely weaken Malaysia's national economic power, national reputation, national defense, and capacity to run the government. The goal: national vital information infrastructure of Malaysia must be safe and robust, that is, resistant to threats and attacks on its systems.

- *National Policy on Industry 4.0, 2018*: One of the eleven areas of technological innovation and convergence is cybersecurity which is crucial to protecting Industry 4.0 applications' information systems and production lines from threats that exist. As one of the "strategic

enablers," this policy also emphasizes cybersecurity protection in the regulatory framework. Data integrity, security, and analysis are important areas of focus for ensuring uninterrupted data flow across value chains. Additionally, this policy is formed to assist the government in identifying the most important challenges for initiatives, ministries, and agencies when planning efficient programs and offering regulatory support.

- *National Fourth Industrial Revolution (4IR) Policy, 2021*: The element of corporations, society, and government is highlighted by this policy. To foster trust in society (Strategy 11), the policy recognizes the significance of modernizing the legislative framework regulating personal data protection and cyber security.

- *Malaysia Digital Economy Blueprint, 2021*: This blueprint emphasizes the increasing cyber security uptake among businesses, eCommerce, data sharing, and all levels of society (which includes the reinforcement of cyber security outreach) as one of the identified key thrusts and strategies.

- *National E-Commerce Strategic Roadmap (NESR), 2021-2025*: This roadmap emphasizes the digitalization phase in the eCommerce sector and it emphasizes 15 comprehensive programs developed in collaboration with the National Cyber Security Agency and many other Ministries and agencies.

- *Malaysia Cyber Security Strategy (2020-2024)*: This strategy aims to achieve its vision by fortifying local capabilities to predict, detect, deter, and respond to cyber threats by strengthening our cyber security governance, nurturing competent people, supporting best practice processes, and deploying effective technologies. It also aims to improve the platforms, routes, and channels for government agencies, corporations, and the general public to share information on cyber security and cyber risks. This strategy is designed to cater to cyber security focusing not only on national security but also to support the digital economy as one of the government's agenda.

In fact, nearly every aspect of its development especially for Malaysia as a developing country has adopted the internet in every aspect of the spectrum. Greater acceptance and usage of ICT become strategically more important, as is explicitly stated in every Malaysia Plan. However, this particular focus has not been supported by a specific piece of legislation or framework that covers QCT (in specific). Therefore, with the rapid development and competitiveness of QCT, it is valid to have a strategic policy (specifically for QCT) to protect important data in the early stage as Malaysia is yet to actively adopt quantum technology compared to other advanced countries.

4. Why QCT is Important for Security

The exchange of information from one device to another has been safer in recent years because of the development of QCT. It serves as a traditional commercial medium where a variety of Internet of Things (IoT) devices get interconnected with ICT and can transfer information via quantum technologies (Singh et. al., 2020).

Future networks' digital communications will have to deal with a number of challenges, such as massive amounts of data, low latency, high-broadband deployment, security, and privacy. The above-mentioned challenges can be resolved via quantum communication,

quantum sensing, and quantum computers. In all, the most important requirement for future smart, advanced applications is the secure transfer of data. But to accomplish that, we'll require a much safer and secure network called the quantum Internet. Today, nations all around the world, including China, Canada, and the United States, are looking into QCT. With the help of the quantum internet, it will be possible to create a secure network where quantum-designed machines and gadgets can securely communicate and exchange information.

Security is about avoiding harm that results from other people's unethical acts (Schneier, 2003). In turn, national security involves preventing negative outcomes that might harm a nation in every aspect of its development. National security is thus a broad and varied notion that encompasses everything from economic strength to social welfare, to political stability and efficient government. This idea of security may still be broadly applicable and needs to be further understood in order to adjust to changing situations, particularly in light of the nation's increasing dependency on the Internet.

According to Sonny (2011), similar to many other developed and developing countries, Malaysia has positioned itself to make e-government and e-commerce the primary drivers of the economy. People believe that the Internet is the key enabler of governance in both the public and commercial sectors. The challenge is that a governance system would face more hazards the more it was dependent on the Internet. It is therefore to fix this dilemma, this paper proposed to include QCT in Malaysia's national security framework and policy.

5. Conclusion

A Government of Malaysia would face additional risks the more it was dependent upon the Internet and ICT if there is no cyber security protection. Information online is at risk and the nation's important data infrastructure (such as communications) will become vulnerable, destroying national security, if the system's security fails to be reliable enough to safeguard the system. The policy recommendation to include QCT in the national policy in this study could be seen as a component of a larger plan to protect and safeguard Malaysia's national security.

Acknowledgments

This research forms part of the Long-Term Research Grant Scheme (LRGS) project with Universiti Malaya (UM), Universiti Malaysia Perlis (UniMap) and Universiti Islam Anatarabangsa (UIA).

References

Brassard, G. (2001). Quantum Communication Complexity (A Survey). *Journal of Quantum Physics*, 2316-. https://doi.org/10.48550/arXiv.quant-ph/0101005

Ezratty, O. (2001). Understanding Quantum Technologies. *Le Lab Quantique 4th Edition*.

Feynman, R. P. (1982). Simulating physics with computers. *International Journal of Theoretical Physics*, *21*, 467-488. https://doi.org/10.1007/BF02650179

Leigh, D. & Harding, L. (2011). Wikileaks: Inside Julian Assange's war on secrecy. Guardian Books: US.

Malaysia Cyber Security Strategy (2020-2024). National Security Council, Prime Minister Department, Malaysia

Malaysia Digital Economy Blueprint (2021). Economic Planning Unit, Prime Minister Department, Malaysia

Nanxi, Z. (2021). Quantum Entanglement and Its Application in Quantum Communication. *Journal of Physics: Conference Series*. https://doi.org/10.1088/1742-6596/1827/1/012120

National Cyber Security Policy (2006). Ministry of Science, Technology and Innovation, Malaysia.

National E-Commerce Strategic Roadmap (2021-2025). Malaysia Digital Economy Cooperation.

National Fourth Industrial Revolution Policy (2021). Economic Planning Unit, Prime Minister Department, Malaysia

National Policy on Industry 4.0 (2018). Ministry of International Trade and Industry, Malaysia

Schneier Bruce (2003). Beyond Fear: Sensible Security Thinking in an Uncertain World. Books by Copernicus, New York

Singh, S. K., Azzaoui, A. E., Salim, M. M., & Park, J. H. (2020). Quantum Communication Technology for Future ICT – Review. *Journal of Information Processing Systems (JIPS), 16*(6), 1459-1478. https://doi.org/10.3745/JIPS.03.0154

Sonny, Z. (2011). National Security In Malaysia's Digital Economy: Redefinition, Reaction And Legal Reform. *Journal of Applied Sciences Research*, *7*(15), 2316-2325. https://doi.org/ISSN 1819-544X