Quantum and Military Communication Security

An Analysis of the Opportunities, Risks, Implementation Challenges, and Prospects of Quantum Computing in Military Communication

Author: Eddo Dijkstra
University of Twente
P.O. Box 217, 7500AE Enschede
The Netherlands

ABSTRACT,
This paper explores the implications of quantum computing on military communication security, including the relevant opportunities, risks, challenges, and prospects. Although quantum-related technologies like quantum key distribution (QKD) and post-quantum cryptography (PQC) provide improved encryption methods to protect against quantum threats, they also pose risks because they might compromise current systems. The study uses Technology Readiness Level (TRL) and Horowitz's adoption-capacity theory to assess the strategic, financial, and organisational factors influencing the adoption of these technologies. This paper also examines three QKD and PQC projects that help with the quantum transition process, as well as relevant stakeholders in this process, such as decision-makers, IT teams, Big Tech, NATO, and the government. The results, derived from qualitative research methods like interviews and desk research, show the necessity of developing and implementing quantum-enhanced and quantum-resistant systems to protect military communications. Additionally, it is important that countries work together to speed up development and that there are investments in training and education programmes to get skilled talent.

Graduation Committee Members:
Dr. M.L. Ehrenhard, University of Twente
Dr. J.U. Dahlke, University of Twente

Keywords
Quantum Computing, Military Communication, Cybersecurity, Quantum Key Distribution, Post-Quantum Cryptography, Technology Readiness Level, Adoption-Capacity Theory

1. INTRODUCTION

In recent years, there has been a huge increase in the use of quantum computing, and although this technology is not yet 'mature' (Gschwendtner et al., 2024), it is going to affect many sectors, including the military industry and the communication systems used here (TU Delft, 2020). Due to rising tensions in the world and the rapid advancement of technologies (Ero & Atwood, 2024; Roser, 2023), the security of these communications is critical. Traditional cryptographic methods, which once provided strong security, are now facing vulnerabilities that are exposed by these new capabilities of quantum computing (Baseri et al., 2024). This emerging scenario offers both opportunities and challenges for defence actors worldwide, which makes the study of quantum computing's impact on military communications security a timely and important topic.

Secure communication is the backbone of military operations, because without, "troops and assets will not be able to stay informed, coordinate actions, synchronize operations, and make quick judgments in challenging circumstances" (Spectra Group, 2023). The arrival of quantum computing offers superb opportunities to improve communication security, with technologies such as quantum key distribution (QKD) using quantum principles to protect information. However, it simultaneously threatens to break conventional cryptosystems with quantum algorithms, which serves as a reminder of the urgent need for the military industry to adopt quantum-resistant cryptographic solutions, such as post-quantum cryptography (PQC). The military's existing value networks and communication infrastructures need to evolve to integrate these advanced technologies before they have passed their developmental stage and their impact becomes uncontrollable. So, by looking at both the opportunities & risks that quantum computing brings about, the challenges of transitioning to systems that make use of quantum computing, and the relevant stakeholders in this transition, this research will show quantum computing's dual role in enhancing and threatening secure military communications.

This study is academically relevant in the fields of global (cyber)security, cryptography, technological innovation, defence studies, and strategic management. From a practical perspective, the study is useful for military organisations and the defence industry. It provides information to understand how quantum computing will transform communications and also shows the urgent need for developing and deploying these quantum-resistant technologies. Moreover, there is currently not a lot of information on stakeholders that are relevant in this transition in military systems, which gives this research more importance.

This study will answer the following research question:

"What are the implications of quantum computing for the security of military communications?"

The following objectives will help with answering this question:

1. The possible effects of quantum computing on existing military communication systems will be examined. This includes looking at how quantum technologies could enhance and harm current secure communication methods.
2. The effectiveness of quantum-enhanced and quantum-resistant technologies will be evaluated. The study will explore QKD and PQC as solutions to the threats posed by quantum computing.
3. The challenges of transitioning to quantum-secure systems will be looked at. This means uncovering the practical difficulties of adopting quantum technologies in a military setting, which includes the stakeholders that help with this transition.
4. And recommendations for military stakeholders based on two technology adoption frameworks will be provided. The research will give useful insights that could potentially help military organisations and defence industries protect their communication networks against quantum threats.

This thesis is organised as follows: Chapters 2, 3, and 4 are the theoretical sections. Chapter 2, 'Quantum Computing', dives into quantum computing itself and its most fundamental principles, which include superposition and entanglement. It also goes more into quantum cryptography and the two key approaches, QKD and PQC, that are currently under development to protect data against quantum threats. Chapter 3, 'Military Communications', gives information about the importance of military communications and looks at current ways that the military is communicating in a secure way, with also a part dedicated to the evolution of these technologies to see how they have adapted to emerging threats and innovations. Chapter 4, 'Technology Adoption Frameworks', defines two military technology adoption frameworks, technology readiness level and adoption-capacity theory. Chapter 5, 'Methodology', details the research procedure, describing the qualitative research design and data collection methods. Chapter 6, 'Results', presents the results of the study and delves into the opportunities that quantum computing offers, as well as the associated risks and challenges. Moreover, it looks at some current relevant projects and stakeholders that are important in the transition to quantum technology. Chapter 7, 'Discussion', looks at the implications of the findings, comparing them with existing literature and also makes a recommendation for the relevant (military) stakeholders. Finally, Chapter 8, 'Conclusion', closes the thesis by summarising the main findings and addressing the central research question, while also reflecting on the limitations of the study and offering suggestions for future research.

2. QUANTUM COMPUTING

2.1 Principles of Quantum Computing

Quantum computing uses the unique properties of quantum mechanics to perform computations in ways that are currently not possible for classical computers (Nofer et al., 2023). Before talking about its differences, first an overview of the two most fundamental principles underlying quantum computing.

2.1.1 Superposition

Quantum computers use quantum bits (qubits), which are the basic unit of quantum information (Dejpasand & Ghamsari, 2023). Unlike classical bits, which can be either 0 or 1, a quantum system has the ability to be in multiple states at the same time, also known as superposition (Choi, 2023). This means that a qubit can be in a state representing 0, 1, or any combination of these states simultaneously (Choi, 2023). This capability is crucial because it allows quantum computers to perform many calculations in parallel, which greatly enhances their computational power (FasterCapital, 2024). For example, a quantum computer with 300 qubits can represent more states simultaneously than there are atoms in the observable universe (Vereniging Officieren Verbindingsdienst, 2019).

2.1.2 Entanglement

Another key principle is entanglement, in which two qubits or more become interconnected such that the state of one qubit

directly influences the state of another, no matter how far apart they are (Choi, 2023). This interconnection, which is used in quantum computing to link qubits together in complex ways, enabling highly efficient and secure communication, means that the measurement of one qubit immediately determines the state of the other (Choi, 2023).

2.2 Quantum Cryptography

Quantum technology uses the aforementioned principles to achieve large advancements in various fields. One of the fields this study will focus on is quantum cryptography, which uses quantum entanglement and superposition to create highly secure communication channels that are theoretically immune to eavesdropping. This is linked to quantum computing, which enables the development of advanced cryptographic protocols, real-time encryption and decryption processes, and stronger security frameworks that are resistant to both classical and quantum attacks.

Two key approaches to theoretically quantum-secure or quantum-resistant data protection that are currently under active development are QKD and PQC.

2.2.1 Quantum Key Distribution

QKD uses the principles of quantum mechanics–specifically quantum entanglement and the no-cloning theorem–to enable the secure exchange of cryptographic keys between two parties, by ensuring that any attempt at eavesdropping will disturb the quantum state, alerting the communicating parties, which should therefore mean theoretically unbreakable encryption (Neumann et al., 2021). To expand on the previous sentence, the no-cloning theorem gives QKD a big advantage, as it states that it is impossible to copy an arbitrary unknown quantum state (Wooters & Zurek, 1982). Any eavesdropping attempt alters the quantum states and introduces detectable errors, which allows the communicating parties to discard the compromised key (Choi, 2023).

There are two primary approaches to QKD. First off, there is the prepare-and-measure protocol, which includes the BB84 protocol, where one party prepares qubits in one of several possible states and then sends them to the other party, who measures them on a chosen basis. This is secure since an eavesdropper's measurement will introduce errors, that can then be detected (Neumann et al., 2021). The second protocol is entanglement-based, and it includes the E91 protocol. Here, entangled photon pairs are distributed between the communicating parties. Measurement outcomes on these entangled pairs are correlated in a way that is secure against eavesdropping. This is because, yet again, any interception attempts disturb the entanglement, which shows that there is an eavesdropper (Neumann et al., 2021).

QKD has been mainly demonstrated over fibre optic cables, as well as open air (Parker, 2021). However, it also works over long distances using satellites, which involves the transmission of quantum keys between ground stations via satellites (Polnik et al., 2020). This method has been successfully demonstrated in a number of experiments, including the Micius satellite, that was part of the Chinese Academy of Sciences' 'QUESS' initiative, which demonstrated that secure key exchange is possible between locations across thousands of kilometres (Bedington et al., 2017). Another project that demonstrates secure communications via quantum cryptography from space is QKDSat, developed by the European Space Agency and private partner Arqit, which leads an industrial consortium with key players in this industry, such as British Telecom (European Space Agency, 2020). The European Space Agency is carrying out this project to ensure that Europe remains at the forefront of cybersecurity and quantum secure communications, increasing its autonomy in this strategic field.

The European Union too has invested in this QKD technology, for instance, through the European Quantum Communication Infrastructure (EuroQCI) initiative, which aims to deploy QKD networks across Europe (European Union, 2024). The previously mentioned QKDSat programme has no links to EuroQCI, as some non-EU member states are involved in this project (Foust, 2023). More on the advantages of QKD and satellite-based QKD is in Section 6.1 'Opportunities'.

2.2.2 Post-Quantum Cryptography

PQC refers to the cryptographic algorithms that are designed to be secure against both classical and quantum computer attacks (UNIDIR — the UN Institute for Disarmament Research, 2023). Unlike QKD, PQC can be implemented on existing digital infrastructure without the need for specialised quantum hardware (TNO et al., 2023). Its algorithms are based on mathematical problems that are difficult to solve for quantum computers (*Falcon Algorithm Co-developed With Thales Selected by the NIST as a New Standard in Post-Quantum Cryptography*, 2022). These algorithms are currently in the process of standardisation by organisations such as the National Institute of Standards and Technology (NIST), with more information on this in Section 6.2.2 'Challenges of Transitioning'.

A current fear in the military world is 'Harvest now, decrypt later', where encrypted data is now being collected with the intent to decrypt it at a later time by making use of advancements in computing power, which are most likely brought about through quantum computers (Krelina, 2021). More on this specific issue is in Section 6.2.1 'Risks'. PQC handles this problem as it aims to develop cryptographic algorithms that are resistant to attacks by quantum computers (Ajala et al., 2024). For this reason, recent studies have emphasised the urgent need for military organisations, such as NATO, to switch to quantum-safe alternatives, like PQC, to protect against quantum threats (Brandmeier et al., 2021).

3. MILITARY COMMUNICATIONS

3.1 Importance of Secure Communications

There are several reasons why secure communications are important for the military. To keep up with the high tempo of operations and be resilient against adversaries with electronic warfare capabilities, it is important that the communications architecture can operate at pace over long distances and is reliable and secure (Spectra Group, 2023). This way military units can work effectively, even in complex and dynamic environments. And within the United States military, the Department of Defense Information Network (DODIN) serves as the backbone for command, control, communications, and data exchange (Nakasone, 2019). The United States Cyber Command (USCYBERCOM) defends the DODIN and facilitates almost every phase of operations for the United States military (U.S. Cyber Command, 2013). Secure communications within this network are crucial as any breach or disruption could harm the command, control, coordination, and data integrity of all military functions. So, ensuring the security of DODIN ensures that military operations can go on without interruption, which is important to maintain operational effectiveness and resilience. Moreover, USCYBERCOM insists on the importance of continuous and proactive cyber operations to protect national security, rather than reactive measures. This is made possible by secure communication channels, which give military cyber forces the ability to anticipate and counter threats before they can cause any harm (Nakasone, 2019). However, these

communication methods were not always this security-oriented and have changed a lot over the years, as can be read in the next subsection, 'Evolution of Military Communications'.

3.1.1 Evolution of Military Communications

The application of quantum technology would mark another era in the ever-evolving field of military communications. Looking at this domain from the United States' perspective, an early military communication method that was used in the 18th century was verbal commands, often supplemented by hand and arm signals to control formations during battle (Lipscomb, 2017). This method was direct but limited by distance and noise. Another visual way of communicating, besides using hands and arms, were flags and guidons, which gave identity to military units and helped them distinguish themselves from each other (Lipscomb, 2017). Written orders were also used and were delivered by runners on foot or horseback, who delivered and distributed directives and battle orders (Lipscomb, 2017). These written messages were used more for field orders, with flags being used for tactical manoeuvres. Another early method was the use of musical instruments, like the fife, drums, and bugles (Lipscomb, 2017). Drums were particularly effective because of the audibility of the beats over long distances and their ability to build morale among troops through battle songs (Norris, 2012). Homing pigeons played an important role too as they could carry messages over long distances, although this method had limitations, like the potential loss of the pigeon or interception of the message (Q-Leap Edu Quantum Communications, 2021).

With the arrival of the industrial revolution in the last half of the 18th century came new technological advancements that brought some drastic changes to army communications (Zapotoczny, 2006). For instance, the invention of the telegraph allowed for instant transmission of messages over long distances (Carey, 1983). At the end of the 19th century, the telegraph was made wireless, and this allowed for the transmission of Morse code and voice signals (radio) without the need for physical wires (Lipscomb, 2017). However, one problem was the ease with which the wireless telegraph could be intercepted, so the army kept looking for better and safer ways to communicate. This they found in telephones, which do not transmit signals in dots and dashes like the telegraph but send signals of different pitches, allowing the person at the opposite end to hear the spoken voice (Richardson, 2015). This provided a more reliable and clearer means of communication compared to telegraphs. Still, field phones were utilised during World War I and World War II because mountains and stormy weather had a great effect on these radio signals (Lipscomb, 2017). They were used until the late 20th century, when radio communications became more secure, making the field phones obsolete (Lipscomb, 2017).

Now the military is working with modern innovations, such as satellite communications, internet and cellular technology, and digital communication platforms. More on these in the next Section, 3.2 'Current Military Communication Systems'.

3.2 Current Military Communication Systems

The first example of current military communication systems, which is the primary way of communication, is through satellite systems, also known as satellite communications (Lipscomb, 2017). They offer secure communication, even in remote and hostile areas, because of their global coverage and reliability (Dhaka, 2024). Thanks to this technology, voice and encrypted data can now be transmitted in real time during military operations. Communication over long distances without the need for physical infrastructure is now possible through satellite radios and satellite telephones (Lipscomb, 2017).

Another current way of communicating is with the internet, email systems, and cellular technology (Lipscomb, 2017). Mobile devices allow flexible and reliable communication options in various operational environments, and also enhance communication efficiency and record-keeping (Henderson, 2022). Government-secured cell phones are issued to military personnel. In the case of the United States military, they work together with Samsung, and they deliver commercial off-the-shelf mobile devices that are enhanced with customised software (Samsung U.S. Newsroom, 2023).

Also still widely used are (tactical) radio networks, especially for short-to-medium-range communications (Lipscomb, 2017). These networks make use of frequency hopping, which means rapidly changing the carrier frequency during transmission, making it difficult for adversaries to intercept or jam the communication, thus securing the voice and data communication (Rothman, 2019).

But despite all these advanced technological systems, traditional methods like hand and arm signals, flags, and signal lights are still used in some specific tactical situations, especially when radio silence is needed or if electronic communication is compromised (Lipscomb, 2017).

And to ensure the security of these communications, there are a number of technologies and protocols employed. For instance, the methods of encryption can be divided into two categories. Symmetric encryption uses the same key for both encryption and decryption, which is highly secure, as both the sender and receiver must have the key (Ubaidullah & Makki, 2016). Asymmetric encryption uses two keys: public for encryption and private for decryption. The public key can be shared with anyone, but the private key is kept secret (Stohrer & Lugrin, 2023).

4. TECHNOLOGY ADOPTION FRAMEWORKS

Two frameworks will be used to analyse the adoption of quantum technologies within military communication systems. This is relevant for the parts on risks, challenges of transitioning, and prospects.

The first framework, Technology Readiness Level (TRL), was originally conceived by NASA in the late 20th century to measure how far a technology was from being deployed in space (Héder, 2017). Over time, this framework was also adopted by the United States Department of Defense and the European Union. Nowadays, it is a nine-level scale, with TRL 1 where the basic principles are observed and TRL 9 where the actual system is proven in operational environments (European Commission, 2013). The higher the TRL, the more mature the technology. In military context, the Department of Defense makes use of TRLs to determine the readiness of new technologies for integration into weapon systems and other critical defence infrastructures (Héder, 2017). For military communication systems, this framework can be used to assess the readiness of quantum technologies, such as QKD and PQC, as well as the first useful quantum computer. By using this framework, there will be a systematic approach to adopting new military technologies. The risk of deploying immature technologies will be minimised if it is required that these (new) technologies have to meet specific readiness levels before they are integrated. Furthermore, the TRL framework also helps with funding decisions, resource allocation, and strategic and risk mitigation planning (Salvador-Carulla et al., 2024). Technologies that have a lower TRL, but are deemed potentially useful, might receive initial funding. But as they advance through the TRL stages and are nearing deployment, they increasingly attract more resource investments

for the actual integration (Olechowski et al., 2020). For this study, the TRLs for the military quantum technologies, that Krelina (2021) developed, will be used.

And the second framework is the adoption-capacity theory that was introduced by Michael C. Horowitz in his book "The Diffusion of Military Power: Causes and Consequences for International Politics" (Horowitz, 2010). He emphasises that the successful adoption of major military innovations (MMIs) depends on two key factors: financial capital and organisational capacity, which are also the independent variables here. Financial capital refers to the financial resources that are required to adopt new military technologies (Horowitz, 2010, p. 31). Innovations that are not just military-exclusive but also useful in civilian contexts need less funding than those that are purely military (Horowitz, 2010, p. 31). And the higher the financial intensity, the slower the innovation spreads and the less likely a state will try to adopt it (Horowitz, 2010, p. 32). Organisational capacity refers to the ability of military organisations to adapt and integrate MMIs (Horowitz, 2010, p. 33). This includes elements such as training, education, and doctrine (Horowitz, 2010, p. 33). Once again, the higher the required organisational capacity, the slower the spread of the innovation and the less likely it is that a state will try to adopt it (Horowitz, 2010, p. 39). Horowitz has identified three determinants of organisational capacity. Firstly, the critical task focus, which is about the military being specific of its objectives, where a broader focus more likely leads to the adoption of innovations (Horowitz, 2010, p. 35). Secondly, the experimentation resources, which is about the commitment to test with disruptive innovations, with an increase in the likelihood of successful adoption if more resources are allocated towards experimentation (Horowitz, 2010, p. 37). And lastly, the organisational age, where older organisations are generally less flexible and less willing to introduce innovations (Horowitz, 2010, p. 37). The two independent variables influence the dependent variable, diffusion, which is defined as follows by Horowitz (2010, p. 19): "the process by which an innovation is communicated through certain channels over time among the members of a social system." In the military context, this refers to the spread of military innovations into the armed forces of different countries and states. MMIs in this theory, according to Horowitz (2010, p. 22), are "major changes in the conduct of warfare, relevant to leading military organizations, designed to increase the efficiency with which capabilities are converted to power."

Horowitz's adoption-capacity theory will complement the TRL framework as it provides a broader perspective on the adoption process. Where the TRL focuses on the maturity of the technology itself, the theory by Horowitz addresses the external factors that influence whether a technology will be adopted. And while TRLs ensure that only mature technologies are deployed, the adoption-capacity theory says that even ready technologies might not be adopted if the financial and organisational conditions are not right. These frameworks together give a strong analysis of the challenges and prospects for the adoption of quantum technologies within military communication systems, which is useful for relevant stakeholders, like military strategists and decision-makers. This means that both the technological and organisational factors are considered.

5. METHODOLOGY

5.1 Research Design

This study made use of a qualitative research design to investigate the implications of quantum computing for the security of military communications. This means that non-numerical data was collected and analysed, such as interviews and text documents, to understand concepts and to get more in-depth insights into the research problem (McCombes, 2023). This research also made use of the inductive approach, which is a reasoning method that analyses specific evidence to form general inferences (Bisht, 2024). This method is useful because quantum technology, and especially its impact on the security of military communications, is still a new and under-explored field. It allows themes to emerge from the collected data, which were collected through both primary data (interviews) and secondary data (desk research). To analyse this data, a thematic analysis was used, which means that the collected data was coded to identify broad themes and patterns. To ensure the credibility of the research design, triangulation was applied. This meant that the data from the interviews were compared with the data from the desk research, thus ensuring that the conclusions were supported by multiple sources of evidence (Stewart, 2023). And by using multiple data sources, some weaknesses in the data can be compensated for by the strengths of other data, thus increasing the validity and reliability of the results (Hales, 2005).

5.2 Data Collection

5.2.1 Desk Research

Because interviewing relevant actors for this study was difficult due to the topic's classified characteristic, some information had to be found through secondary data. This secondary data was collected through desk research, which includes scientific papers found through academic databases like Scopus and Google Scholar, from which, for example, the two technology adoption frameworks and some of the stakeholders were defined. But also online articles from trustworthy web pages such as McKinsey & Company and Defense Advancement or reports from relevant organisations like NATO, the Dutch General Intelligence and Security Service, and the Dutch Ministry of Defence.

5.2.2 Interviews

Two semi-structured interviews were conducted with two members of Quantum Delta NL, a project that aims to put the Netherlands on the map as a leading centre for quantum technology (*Home | Quantum Delta NL*, 2019), as well as a cybersecurity expert at Thales, a company known for its solutions, services, and products for companies, organisations, and governments in the markets of defence and (cyber)security (*About Thales*, n.d.). This means that the questions were within a predetermined thematic framework but were not set in order or in phrasing. It allowed for more flexibility and was more open-ended as the interviewees were asked to clarify or elaborate on some answers they gave (George, 2023). The aims of these interviews were to get valuable insights into the general information on quantum technology, the latest advancements in this area, its potential benefits and risks, the prospects of these technologies, and relevant stakeholders in the transition to quantum technology. Because it was difficult to interview people directly from the Dutch Defence, as a lot of information related to quantum is very classified, the criteria for becoming a relevant interviewee were toned down quite a bit. The criteria now were that the person had to have knowledge about quantum technology and its possible advantages and disadvantages in terms of secure communication and had to know who the key players in this field were. And some questions that were asked during these interviews were: 1. What breakthroughs in quantum technology do you expect in the coming years? 2. Can you also comment on the future of quantum communications/cryptography, and how might these affect the current security of communications? 3. What are the benefits of adopting quantum technology? 4. What are the advantages of PQC? Moreover, these interviews were both in-person and online through Microsoft Teams and were recorded with the consent of both interviewees to be later

transcribed and analysed. So, ethical considerations, like informed consent and confidentiality, were strictly adhered to.

5.3 Data Analysis

A thematic analysis was used to identify patterns and themes within the qualitatively collected data from both the interviews and desk research, following the six-step method developed by Braun and Clarke (2006). This approach was selected because it is both structured and flexible, which allowed a thorough examination of the data while tailoring it to the specific requirements of this study. Firstly, familiarisation with the data collected from the desk research and the transcribed interviews, which were thoroughly read and listened to. Secondly, the key pieces of information were highlighted, and specific codes were assigned to these data segments. This coding was done by marking the text with different colours through Apple Preview or Microsoft Word, which made the coding structure more organised. Thirdly, these codes were written down in a Word document and then grouped into broader themes that summarised the overarching patterns in the data. An example of such a theme was 'Opportunities of quantum computing', which included the codes 'Improved security' and 'Geopolitical advantage'. Another theme was 'Risks and challenges', which contained the codes 'Implementation costs' and 'Technological uncertainty'. Fourthly, the themes mentioned above were reviewed to ensure that they were clear, relevant, and accurately represented the data. Broad themes, such as 'Risks and challenges', were split in order to capture more subtle differences within the data. Fifthly, after the review, the themes were now clearly defined with detailed descriptions, outlining what they captured and why they were interesting for this study. And lastly, the themes were compiled into a coherent narrative and now addressed the research question and key findings.

6. RESULTS

6.1 Opportunities

In general, quantum communication holds the potential to establish highly secure communication channels that are immune to existing hacking techniques (T. Klaver & B. Tel, personal communication, June 19, 2024). This is because, unlike classical communication channels, which can be intercepted and decrypted, quantum communication channels make use of the aforementioned properties of quantum entanglement and superposition. It thus provides immediate detection of the breach, as any attempt to intercept the communication disrupts the quantum state.

Additionally, quantum computing allows for faster data transmission, which is crucial during operations with a high tempo (Dynes et al., 2016). And besides being faster, it can also process large amounts of data simultaneously, which improves the effectiveness and efficiency of military communication systems (*Big Data Boosting A.I.*, 2018).

As cyber warfare becomes more prevalent, protecting military communication networks from cyberattacks is critical (cybersecurity expert, personal communication, June 2, 2024). Quantum computing can provide the advanced algorithms and cryptographic methods that are resilient against these future threats posed by enemies who possess quantum technology.

Possessing these advanced quantum abilities can give a country an enormous geopolitical advantage by ensuring that their nation's military communication remains secure while (potentially) compromising the communication of adversaries (T. Klaver & B. Tel, personal communication, June 19, 2024). This quantum-enabled country can decide to not only protect their own communication, but also share their knowledge on quantum technology with allies who have not yet adopted quantum-secure technologies.

More specifically, quantum computing offers advancements in encryption methods and, thus, in security (cybersecurity expert, personal communication, June 2, 2024). As previously noted, traditional encryption methods, like asymmetric encryption, rely on complex mathematical problems that take a long time for current computers to solve. Quantum computers, on the other hand, can solve these problems much faster and potentially decrypt sensitive information. PQC responds to this by using new mathematical principles that are not easy to solve for quantum computers, which ensure the security of encrypted communications even when quantum computing becomes more widespread.

QKD also provides a highly secure method for exchanging encryption keys, ensuring that any attempt at eavesdropping on the key change process can be detected immediately, as it alters the state of the qubits being exchanged (cybersecurity expert, personal communication, June 2, 2024).

Both PQC and QKD, in combination with current technology, can improve the security of communication systems. To make this more concrete, the Defense Advanced Research Projects Agency (DARPA) will be looked at. This is a key agency of the United States Department of Defense and is responsible for the development of and investments in emerging technologies for military use and national security (Congressional Research Service, 2021). The Quantum-Augment Network (QuANET) programme, one of DARPA's recent initiatives, aims to enhance military communications by combining the best aspects of both quantum and classical communication technologies, which they can accomplish using QKD and PQC (DARPA, 2023). They saw a lack of cohesion in today's quantum implementations, resulting in systems that cannot work together, hence the reason for QuANET (DARPA, 2023). By combining current and near-future quantum networking hardware and protocols with classical infrastructure, they believe that "they can achieve the efficient security and covertness properties of quantum networks with the pervasiveness of classical networks" (DARPA, 2023).

6.2 Risks, Challenges, and Prospects

6.2.1 Risks

Besides the aforementioned opportunities, quantum computing in military communications may present vulnerabilities. First off, there are a couple of security risks. For example, PQC methods, which themselves do not make use of quantum technology, are still being developed and standardised (cybersecurity expert, personal communication, June 2, 2024). So while PQC methods are designed to withstand quantum attacks, their novelty means they have not been as extensively tested as traditional encryption methods. Therefore, there is a risk that early implementations might contain vulnerabilities, which poses a risk to the military if it adopts these methods prematurely. This potential risk is reinforced by the fact that the United States military has implemented incomplete technology before. For instance, during Operation Just Cause (1989-1990), the first-time use of manpackable tactical satellite radios was problematic, as the ultra-high frequency signals were easily detected and jammed by the enemy (Raines, 1996). However, safer high-frequency radios were still in development, thus showing the premature use and implementation of this technology. The TRL framework can help with analysing these risks, as the technological risk decreases as technologies progress to higher TRLs due to the decreased technical difficulties (Mankins, 2009). These risks include the aforementioned potential security vulnerabilities but also implementation challenges due to the technology's immaturity.

For instance, certain PQC methods and initial quantum communication systems require more developmental steps before being ready for deployment, thus posing a major risk if implemented too early.

Not switching to quantum computers as soon as the technology becomes available is also a risk. This is because of the Harvest Now, Decrypt Later strategy, which means that sensitive military communications intercepted today could be at risk in the future. Adversaries can intercept and store encrypted communications now to decrypt them later when more powerful quantum computers become available, even if present quantum computers are unable to break current encryption (cybersecurity expert, personal communication, June 2, 2024).

This second risk of adapting as quickly as possible conflicts with the first-mentioned risk of premature implementation. So this shows how difficult quantum is. This leads to the next point, which is that the full consequences of quantum computing are not yet entirely understood and unexpected consequences could arise. As with any disruptive technology, there are unknown risks associated with the widespread adoption of quantum computing (Daher, 2021).

Moreover, as mentioned in the 'Opportunities' section, quantum computers can crack current encryption methods. This also has a downside, as it makes the existing secure communication systems vulnerable to interception and decryption by enemies (Forbes Technology Council, 2022). The same goes for QKD, which is theoretically impenetrable during transmission, but attacks can focus on the final receiver where the hardware or software still contains bugs or verification problems (Krelina, 2021). And the countries lacking quantum computing abilities, and who are not allies with countries that have knowledge of quantum technology, are at a strategic disadvantage in warfare, as adversaries with this technology can outmanoeuvre and out-strategise them (cybersecurity expert, personal communication, June 2, 2024).

6.2.2 Challenges of Transitioning

While there are huge potential benefits, there are also challenges to implementing quantum technologies into current military communication systems. As will be seen below, these challenges include the technical, strategic, financial, and organisational domains. Firstly, there are technical challenges involved in the transition to quantum-resistant encryption methods and quantum communication technologies. Large changes to the current infrastructure are required because this technology is different from classical computing systems, which are resource-intensive and complex processes (cybersecurity expert, personal communication, June 2, 2024). Additionally, this integration is further complicated by the fact that military equipment like naval ships, which also make use of communication systems, often remains in service for decades (cybersecurity expert, personal communication, June 2, 2024). This is because ships and other long-term assets need to be designed with future technological advancements in mind, which is difficult given the rapid pace of quantum technology development (NATO Science for Peace and Security Programme, 2023). But even with this fast rate of development, technologies like QKD and PQC are still in mid-to-late TRL stages according to Krelina (2021). So, for this reason, there are even more research and development efforts required to bring these technologies to a maturity level where they can be reliably integrated into the existing military infrastructure.

Secondly, a reason that these quantum technologies, and especially PQC, are not yet at the highest TRL and widely used by the military is that the new cryptographic methods need to be standardised and extensively tested to ensure reliability and security (cybersecurity expert, personal communication, June 2, 2024). It is hard to adopt these technologies uniformly if there is a lack of standardisation. This process is ongoing and thus poses a barrier to immediate adoption. An example of a method in this standardisation process is Falcon, which is a PQC scheme that Thales helped develop (*Falcon Algorithm Co-developed With Thales Selected by the NIST as a New Standard in Post-Quantum Cryptography*, 2022). It was selected by NIST (National Institute of Standards and Technology), which is committed to standardisation in science (About NIST, 2022), because of its strong security and high bandwidth efficiency. However, before this scheme was chosen in 2022, five years had already passed, and now it is in the phase of being fully defined. This shows that this standardisation process takes many years, which is something to keep in mind in terms of strategy.

Thirdly, there are a lot of financial resources needed for researching, developing, and deploying quantum technologies (IQM Quantum Computers et al., 2024). As shown by Horowitz's adoption-capacity theory (2010), this financial capital plays a big part in the adoption of major military innovations. Here, the high financial intensity of quantum technology means that adoption is limited to states or military organisations with the largest budgets, creating global differences in military capabilities and a barrier to widespread diffusion. Additionally, there is an organisational challenge, because besides investing in the technologies themselves, there is a need for highly specialised talent to manage these technologies. This is currently in short supply and requires major investments in education and training (T. Klaver & B. Tel, personal communication, June 19, 2024). Another challenge related to the organisational capacity is that there are some difficulties with stakeholder management. Integrating quantum technologies into military communications is a technical, strategic, and organisational challenge as it involves multiple stakeholders, including military, governmental, and private sector entities (T. Klaver & B. Tel, personal communication, June 19, 2024). Cooperation and alignment among these groups is crucial for successful implementation of technologies (Mishra & Mishra, 2013).

Lastly, a complexity of this implementation, which is linked to the 'Risks' section, is that the intricacy of quantum technologies and their integration into existing systems may introduce new vulnerabilities. This is because it is challenging to integrate these new principles without introducing new weaknesses, which makes the transitioning process even more difficult (T. Klaver & B. Tel, personal communication, June 19, 2024).

6.2.3 Prospects

The prospects below for the implementation of quantum computing in military communications are based on the TRLs of quantum technologies from Krelina (2021), the adoption-capacity theory by Horowitz (2010), and information from the interviews.

In the near term, so for the next decade, the developments below are expected in the area of quantum-secured military communications. There will first be implementations of quantum-safe encryption methods and initial experiments with quantum communication systems (cybersecurity expert, personal communication, June 2, 2024). Both PQC and QKD have a relatively high general TRL, standing at 7-8, with both having an expected horizon of 2025 (Krelina, 2021). Since this is a general TRL, it can take some extra years to overcome all technological obstacles and meet all military requirements. There will also be large investments allocated to continue research and development efforts aimed at overcoming current technical

obstacles and enhancing the reliability of quantum technologies. Examples of this large financial capital include the €500 million-plus award given by the French defence agency to French startups that build universal quantum computers (Swayne, 2024b), or the fact that the United States, the European Union, and China spent respectively $1.8 billion, $1.2 billion, and $15.3 billion on quantum technology in 2022 (Bogobowicz et al., 2023). The first useful quantum computer has a TRL of 4-5 with an expected horizon of 2030 (Krelina, 2021).

For the longer-term, so for approximately ten-plus years, the expectations are that quantum computing will be a standard component of military communication systems (T. Klaver & B. Tel, personal communication, June 19, 2024). This should be the case as technologies mature and standardisation efforts pay off, indicating that they have achieved TRL 9 and are widely diffused. Horowitz's theory, however, indicates that there will be variations in this adoption. Geopolitical dynamics will shift, with the nations now leading in quantum technology, such as the United States, China, and Russia, having an even bigger advantage over countries that do not have the capability to use quantum-secured military communication, because of their financial and organisational advantages (Horowitz, 2010; Smith, 2022). These leading states will therefore benefit from first-mover advantages and will become strategically superior (Horowitz, 2010). Moreover, there are also expectations for a quantum communication network, which as of right now only has a TRL of 1-3 and an expected horizon of 2035 (Krelina, 2021). This is an advanced system that makes use of quantum technologies and quantum entanglement to enable highly secure and efficient communication, data transfer, and synchronisation between quantum computers, sensors, and other network devices (Krelina, 2021). So this shows the role of organisational capacity in successful technology adoption, as the complexity of this network calls the need for a lot of experimentation and adaptation within military organisations.

6.3 Projects

Listed below are several QKD and PQC initiatives funded by the NATO Science for Peace and Security Programme, which are important in the transition to the quantum era and show the organisation's commitment to protecting communication (NATO Science for Peace and Security Programme, 2023). The 'SEQUEL' project is related to QKD, the 'Quantum-safe Authenticated Group Key Establishment' project is related to PQC, and the 'Secure Communication via Classical and Quantum Technologies' project is an example of the combination of both methods and research communities.

6.3.1 SEQUEL Project

The SEQUEL (Secure Quantum Communication Undersea Link) project was a multi-year project from 2018 to 2022 in which a prototypical QKD link between Italy and Malta was developed by making use of existing telecommunications infrastructure (National Research Council of Italy et al., 2021).

Its main objective was to establish a secure communication link between Italy and Malta using QKD technology. However, on a bigger scale its objectives were to test the practical application of QKD over a submarine optical fibre link, improve the technology for future use, and provide a template for future industrial-grade systems and products for quantum networks.

The following aspects appear upon closer examination of this project's strategy and implementation. Firstly, the project was cost-effective since it made use of existing submarine telecommunications infrastructure that connects Italy and Malta. Secondly, it involved a number of institutions, such as the National Research Council of Italy, the Istituto Nazionale di Ricerca Metrologica, and the University of Malta. This collaboration promoted international cooperation and the sharing of expertise between the two countries. Thirdly, the developed QKD stations were small, portable, relatively low-cost, and able to be set up in other locations with similar environments. Lastly, and maybe most groundbreaking as this was the first of its kind, was that the performance of the QKD system was evaluated under real-world conditions and not through a simulation. This provided useful data and established a standard for future projects.

And besides the military applications, this QKD system can also be used by commercial entities such as data centres, financial institutions, and telecommunication firms that are interested in secure communications and who want to protect themselves against cyber threats. Therefore, it has a dual use, benefitting both the civilian and defence sectors.

6.3.2 Quantum-safe AGKE

The Quantum-Safe Authenticated Group Key Establishment (AGKE) project, which ran from 2018 to 2022, was about implementing a protocol that authenticates all users and devices involved and establishes a common secret key between them (Slovak University of Technology et al., 2021). The project involved collaboration between Slovak, Maltese, Spanish, and American universities to develop a secure AGKE solution that could withstand attacks from adversaries with large quantum-computing resources and will allow groups of users to exchange information and collaborate securely over open networks.

The protocol was successfully implemented in the C programming language and a live demonstration was shown involving five nations. It also provides countermeasures against practical real-world attacks, including support for a hardware security module responsible for cryptographic computations involving secret data.

Zooming in on the used strategy for and the implementation of this project, the first thing that can be seen is that the project once again brought together institutions from different countries all over the world, promoting international cooperation and knowledge exchange. The project also brought together expertise from different fields, such as computer science, engineering, and mathematics, to provide a well-thought-out quantum-safe AGKE solution. Moreover, young researchers received education and training throughout the entire project, which should ensure a new influx of much-needed talent.

Impact-wise, the results contributed to the standardisation efforts of quantum-safe cryptography, in particular the PQC standardisation process by NIST. The project's models, solutions, and success inspire further work and can lead to improved efficiency in quantum-safe cryptography. It also increased quantum security competencies and enhanced expertise exchange between participating research communities.

6.3.3 Secure Communication via Classical and Quantum Technologies

There are currently multiple projects underway that combine QKD and PQC. The reason it has only been underway in recent years is because there was barely any collaboration between the two research communities. A project that is now running from 2023 to 2026 is the 'Secure Communication via Classical and Quantum Technologies' project (University of Alabama in Huntsville et al., 2023). This multi-year project involves collaboration between five academic institutions across four nations: the USA, Finland, Slovakia, and Spain. Its aim is to integrate PQC and QKD to develop a secure cryptographic

protocol for group communication over distributed, hybrid networks.

The University of Alabama is leading this initiative and has expertise in both QKD, through its Department of Physics and Astronomy, and PQC, through its Department of Mathematical Sciences (Nelson, 2024).

The objectives of the project are as follows. A cryptographic protocol should be designed, analysed, and implemented, combining the strengths of PQC and QKD for secure group communications. It should also bring the traditionally separate research communities of PQC and QKD closer together. Moreover, the project offers possibilities for training and educational opportunities to young scientists across both research communities.

Once more, this project brings together the knowledge of institutions with strong backgrounds in cryptography, quantum technologies, and cybersecurity. However, some of the participating institutions, like the University of Alabama in Huntsville or the Slovak University of Technology in Bratislava, also have partnerships with defence and intelligence agencies or are recognised for their excellence in cyber defence research (Canfil, 2022; ESET, 2024). This not only shows their suitability for this project but also the project's relevance to this study.

6.4 Stakeholder Analysis

An examination of the stakeholders is necessary in order to see who are responsible for this quantum development and implementation. Below is an overview of the roles and influences of the relevant internal stakeholders, which are people and departments directly part of the military and in charge of the adoption and integration of quantum technologies, and the external stakeholders, who are not necessarily military but do work with them or are affected by them. In this case, relevant refers to those actors in the transformation to quantum technologies in military communication. This analysis was made using the information from the interviews and the research by Perrier (2022), Kong et al. (2022), and other additional scientific articles.

6.4.1 Internal Stakeholders

Firstly, the most important stakeholders in the military are the decision-makers, commanders, and strategists who are part of the military leadership and command structure (De Boisbossel, 2022). In the Netherlands, this includes the Chief of Defence, who holds the highest military position and is the most senior military adviser to the Minister of Defence (Ministerie van Defensie, 2022b). For the United States, this is the Chairman of the Joint Chiefs of Staff, who is the highest-ranking military officer and principal military adviser to the President (*10 U.S. Code § 152 - Chairman: Appointment; Grade and Rank*, 2024). They are in charge of the overall direction of military operations and security protocols and have to be actively involved in the planning process to offer advice and knowledge (United States Government US Army, 2020). Additionally, the planner develops potential fixes for problems that are presented in strategic guidelines (United States Government US Army, 2020). The Netherlands Chief of Defence advises the Minister of Defence on the modernisation of the armed forces, such as whether to implement quantum technologies (Ministerie van Defensie, 2022b). However, most countries that have the technological and financial capability are interested in this new technology, and new doctrines on a quantum future have already been published (Obis, 2023).

Secondly, the tech teams, such as the IT and cybersecurity teams, who are technical experts that will manage the integration and maintenance of quantum technologies (Swayne, 2024a). They make sure that newly developed military systems are both protected against evolving cyber threats and are compatible with the existing infrastructure (Sahu et al., 2024).

Thirdly, and closely related to the stakeholders just mentioned, there are R&D departments, made up of researchers and developers who work with military organisations through special R&D programmes and are focused on advancing technology (Sennewald, 1990). These departments are important because they are at the forefront of technological advancements, and their knowledge and capabilities are reflected on the power of the military forces (Okur, 2013). As one of the interviewees works at Thales and is actively working on this quantum topic, this shows the importance of R&D teams in developing and integrating quantum-resistant technologies.

Fourthly, a signal corps, who is responsible for military communication, which includes radio, telephone, and digital communications (Maseng et al., 2010). More specifically, these corpses consist of specialists that are responsible for providing and maintaining reliable and real-time communication. They are more useful in the actual operations themselves, making them a bit different from cybersecurity teams that mostly just look at the security. The signal corps' operational feedback is important in evaluating the effectiveness and practicality of quantum communication systems.

Lastly, the finance departments play an important role, as they are responsible for budget management, purchasing services and supplies, and financial planning for the military, including new technologies like quantum computing (*Financial Manager*, 2020; Tagarev, 2010). Since transitioning to quantum is important, a lot of money is put into this area (Vincent, 2023).

6.4.2 External Stakeholders

Firstly, the government and regulatory bodies set policies related to defence and technology, which include national plans that give strategic direction or support measures for research, innovation, and diffusion (*Technology Policy*, 2024). They also play a role in providing funding, as they see the strategic importance of quantum technologies (*The State of Quantum in 2024*, 2024). International governance, which involves states and public international law, can and have already created agreements for the use of quantum technologies globally (Silbert, 2022). National governance can then look more towards the development of quantum technologies within a country, with China, the European Union, and the United States having already announced major public investments (McKinsey & Company, 2023). An example of this national governance is the AIVD (Dutch General Intelligence and Security Service), which falls under the Ministry of the Interior and Kingdom Relations. Together with TNO (Dutch Organisation for Applied Scientific Research) and CWI (National Research Institute for Mathematics and Computer Science), they have written a PQC migration handbook, which provides organisations with a roadmap on how to transform their encryption methods to PQC (TNO et al., 2023). So this shows the role of the government in setting policies and providing support for quantum technology integration.

Secondly, there are technology vendors and contractors who supply quantum technologies and related services. As quantum technology has attracted huge interest from governments in recent years, large companies such as IBM, Google, and Microsoft are now spending millions of dollars on quantum computing R&D in the race for quantum supremacy (Van Amerongen, 2021). For instance, IBM and Google will give $100 million and $50 million, respectively, to universities in Japan and

the United States to promote quantum computing research and to compete with China (Swayne, 2024c).

Thirdly, research and innovations in these technologies are driven by academic and research institutions. The big companies just mentioned work closely together with academia (e.g. the IBM Academic Initiative or Microsoft who has its own laboratory at the QuTech Research Institute at the TU Delft), but it is still important to be aware of what goes on at these institutions as the military itself (T. Klaver & B. Tel, personal communication, June 19, 2024). These partnerships also aim to attract more top scientific talent, which is one of the current problems. An example of this is the 'Quantum and Advanced Technologies Talent Building Program', funded by the Queensland Government, that aims to build a talent pipeline for the quantum ecosystem in Queensland (State of Queensland, 2023). This includes collaborations between Australian and international universities and the military, where the government of Queensland wants to have Defence as an early adopter of these technologies.

Fourthly, joint initiatives and resource sharing with other allied nations and defence bodies, such as NATO, can help with the development of these relatively new quantum technologies. For instance, NATO considers interoperability to be a cornerstone of its Allied Command Transformation, in which member and partner nations work together through testing and experimentation, in order to respond coherently and effectively to any challenges facing the Alliance (NATO Allied Command Transformation, 2024). Another example is the Joint Statement on Cooperation between the United States and Germany to strengthen collaboration in the field of quantum information and science and to overcome challenges by pooling expertise (National Quantum Initiative, 2024).

Lastly, the media plays an important role as they have the power to shape public opinion and indirectly affect government policies (Drummond, 2019). According to Drummond, funding and political will for secure military communication technologies can be influenced by media coverage and the subsequent public perception.

7. DISCUSSION

The results of this study showed the impact of quantum computing on military communication and its security. It offers huge potential for advancing encryption methods and data processing capabilities through QKD and PQC, thus protecting the communication systems against quantum-based cyber threats. However, continuous advancement of cryptographic methods is required to counter any potential security issues which are introduced by quantum computers. Besides these technical challenges, there are also financial and organisational hurdles in transitioning to these quantum-secure systems, that could impact their adoption and effectiveness in a military context. Moreover, taking all the threats into account, military organisations should not only prioritise R&D efforts in quantum-related technologies, but also the development of specialised training programmes to get the needed talents and technical expertise. Since secure communication is the backbone of military operations, the importance of this study's findings lies in their implications for national security and defence strategy. Military organisations can ensure this security of their communication systems by being aware of the threats and taking preventive measures. Moreover, the future prospects of quantum technology are valuable information for the military itself but can also be important insights for policymakers and researchers. So, the results of this study mattered because they showed how relevant both the emergence of quantum technologies and military communication security are. By identifying both potential benefits and concerns, this research improved understanding of how to successfully use quantum developments while reducing their dangers.

The findings of this study were in line with the existing literature, which sees the enormous potential of quantum computing in cryptography as well, but also its associated risks. These studies too talked about the superiority of QKD and PQC in securing communication channels that are resistant to quantum attacks. And they have similar concerns about the technological and infrastructural challenges in transitioning to these quantum technologies. However, this study focused on the security of military communication, while a lot of studies look more generally at the impact of quantum computing for the military.

The biggest limitation of this study was the small size of the interviews that were held. It was difficult to find relevant organisations or individuals willing to be interviewed due to the highly secure nature of military communications, especially in combination with quantum technology. For instance, I had a brief exploratory conversation with a representative of MINDbase in Enschede. MIND stands for Military Innovation by Doing, and this is part of the innovation centre of the Dutch Ministry of Defence (Ministerie van Defensie, 2022a). The person indicated that, unfortunately, he could not help me with this study because of the reason just mentioned. This might have affected the reliability of some of the results and perhaps did not reflect the full complexity of this topic. Also, all the people that were interviewed were Dutch, which could have led to some bias. For instance, cultural and organisational differences might have influenced the interviewees perspectives on technology adoption or security priorities (Haddad et al., 2019). Additionally, some of the findings could quickly become or are already outdated as the developments in quantum technology evolve rapidly (International Intellectual Property Law Association, 2024). Another limitation is that there are also some shortcomings in the TRLs (Olechowski et al., 2020) and Horowitz's adoption-capacity theory (Horowitz, 2010), and since much of the text relied on just these two frameworks, the impact of these shortcomings might be greater than necessary. Lastly, the research question was quite broad, meaning that not all the implications of quantum computing could be explored.

A recommendation for future research would be to expand the interview sample by also seeking sources outside the Netherlands. While an interviewee from a non-NATO country like China or Russia might give totally different perspectives, even interviewing somebody from an allied nation, such as the United States, could offer some slight new perspectives that expand on the findings in this study. Another thing that future research should aim for is also interviewing a policymaker, to gain an even broader range of perspectives. Moreover, by using more frameworks, their shortcomings will be corrected. And a better formulated research question that does not just say 'implications' could also go more in-depth into relevant areas.

8. CONCLUSION

This research aimed to answer the question: "What are the implications of quantum computing for the security of military communications?". The results indicate that quantum computing leads to both opportunities and risks for military communication systems. Quantum technologies like QKD and PQC offer advanced methods to secure communications against potential quantum attacks. However, the same quantum capabilities could also be used to break traditional cryptographic methods, which means that urgent advancements in quantum-resistant cryptographic solutions are needed.

The study uncovered some other critical insights as well. To ensure that eavesdropping attempts are detectable, QKD makes use of quantum entanglement and the no-cloning theorem to create highly secure communication systems. PQC is almost fully resistant against both classical and quantum computer attacks, as it provides cryptographic algorithms. And PQC can be easily implemented into existing infrastructures without any special hardware. This is not the case for QKD, which means there are some technical and strategic challenges that need to be fixed first. Some other opportunities were that quantum communication can establish secure channels that are immune to traditional hacking techniques, it can improve data transmission speed, and it can process large amounts of data efficiently. And nations that have these quantum capabilities could get a geopolitical advantage by ensuring their communications remain secure, while, if needed, they can comprise those of their enemies. The primary risks include prematurely implementing PQC methods that are not yet vulnerability-free or the threat of the 'Harvest Now, Decrypt Later' strategy. Challenges in transitioning to these quantum-secure systems include technical, strategic, and financial difficulties, such as the need for infrastructure change, the long lifecycle of military equipment, and the need for standardisation and thorough testing of new cryptographic methods. If things then go according to plan, in the near term, initial implementations of quantum-safe encryption are expected. And over the longer term, quantum computing is anticipated to become the standard in each (military) communication system.

The findings of this study contribute to the theoretical understanding of quantum computing's impact on cryptography and communication security in the military. It shows the dual role of quantum technologies in both enhancing and threatening secure communications, which shows the need for continuous development in cryptographic methods.

Some practical recommendations for military stakeholders should be that the adoption of QKD and PQC should be prioritised, which requires investments in R&D and infrastructure upgrades. It is also important to collaborate with other (allied) countries in this area, as this can speed up the advancement and standardisation of quantum-secure communication technologies. Finally, this technology has no use without the right people, so investments in education and training programmes to get a skilled workforce are crucial.

9. ACKNOWLEDGEMENTS

I would like to express my deepest gratitude to my supervisor, Dr. Michel Ehrenhard, for guiding me and providing helpful insights throughout the entire thesis process. I would also like to express my appreciation to the interview participants from Quantum Delta NL and Thales for sharing their expertise and insights, as this greatly enriched the findings of this study. Lastly, I appreciate everyone who supported me during this process and made this research possible.

10. REFERENCES

10 U.S. Code § 152 - Chairman: appointment; grade and rank. (2024, January 1). FindLaw. https://codes.findlaw.com/us/title-10-armed-forces/10-usc-sect-152/

About NIST. (2022, January 11). NIST. https://www.nist.gov/about-nist

About Thales. (n.d.). Thales Group. https://www.thalesgroup.com/en/global/group

Ajala, N. O. A., Arinze, N. C. A., Ofodile, N. O. C., Okoye, N. C. C., & Daraojimba, N. a. I. (2024). Exploring and reviewing the potential of quantum computing in enhancing cybersecurity encryption methods. *Magna Scientia Advanced Research and Reviews*, *10*(1), 321–329. https://doi.org/10.30574/msarr.2024.10.1.0038

Baseri, Y., Chouhan, V., & Ghorbani, A. (2024). *Cybersecurity in the Quantum Era: Assessing the Impact of Quantum Computing on Infrastructure* (Journal-Article 2404.10659v1). https://doi.org/10.48550/arXiv.2404.10659

Bedington, R., Arrazola, J. M., & Ling, A. (2017). Progress in satellite quantum key distribution. *Npj Quantum Information*, *3*(1). https://doi.org/10.1038/s41534-017-0031-5

Big data boosting A.I. (2018, November 28). Quantum Flagship. https://qt.eu/applications/big-data-boosting-ai

Bisht, R. (2024, April 12). *What is Inductive Reasoning? Definition, Types and Examples*. Researcher.LIfe. https://researcher.life/blog/article/what-is-inductive-reasoning-definition-types-examples/

Bogobowicz, M., Gao, S., Masiowski, M., Mohr, N., Soller, H., Zemmel, R., & Zesko, M. (2023, April 24). *Quantum technology sees record investments, progress on talent gap*. McKinsey & Company. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/quantum-technology-sees-record-investments-progress-on-talent-gap

Brandmeier, R. A., Heye, J., & Woywod, C. (2021). Future development of quantum computing and its relevance to NATO. *Connections the Quarterly Journal*, *20*(2), 89–109. https://doi.org/10.11610/connections.20.2.08

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Canfil, E. (2022, July 27). *Huntsville Center and the University of Alabama Huntsville team up to identify research areas in unmanned aircraft systems*. U.S. Army Engineering And Support Center. https://www.hnc.usace.army.mil/Media/News-Stories/Article/3107683/huntsville-center-and-the-university-of-alabama-huntsville-team-up-to-identify/

Carey, J. W. (1983). Technology and ideology: the case of the Telegraph. *Prospects*, *8*, 303–325. https://doi.org/10.1017/s0361233300003793

Choi, D. (2023). Quantum Technology and the Military-Revolution or Hype?: The impact of emerging quantum technologies on future warfare. *Expeditions With MCUP*, *2023*. https://doi.org/10.36304/expwmcup.2023.11

Congressional Research Service. (2021). Defense Advanced Research Projects Agency: Overview and Issues for Congress. In *FAS Project on Government Secrecy* (No. R45088). https://sgp.fas.org/crs/natsec/R45088.pdf

Daher, D. (2021, October 19). *Mitigating risks during the adoption of disruptive technologies*. https://www.linkedin.com/pulse/mitigating-risks-during-adoption-disruptive-dana-daher

DARPA. (2023, June 13). *A Network Security Revolution Enhanced by Quantum Communication*. Defense Advanced Research Projects Agency. https://www.darpa.mil/news-events/2023-06-13

De Boisboissel, G. (2022). New Technologies and Decision-Making for the Military. In *IntechOpen eBooks*. https://doi.org/10.5772/intechopen.98849

Dejpasand, M. T., & Ghamsari, M. S. (2023). Research trends in quantum computers by focusing on qubits as their building blocks. *Quantum Reports*, *5*(3), 597–608. https://doi.org/10.3390/quantum5030039

Dhaka, M. K. (2024, June 6). *Role Of Satellite Communication In Safeguarding Our Borders*. Indian Aerospace and Defence Bulletin. https://www.iadb.in/2024/06/06/role-of-satellite-communication-in-safeguarding-our-borders/

Drummond, N. (2019, September 9). *British Army Engagement – Winning the Battle for the Minds of Key Stakeholders*. UK Land Power. https://uklandpower.com/2019/09/09/british-army-engagement-winning-the-battle-for-the-minds-of-key-stakeholders/

Dynes, J. F., Tam, W. W., Plews, A., Fröhlich, B., Sharpe, A. W., Lucamarini, M., Yuan, Z., Radig, C., Straw, A., Edwards, T., & Shields, A. J. (2016). Ultra-high bandwidth quantum secured data transmission. *Scientific Reports*, *6*(1). https://doi.org/10.1038/srep35149

Ero, C., & Atwood, R. (2024, January 1). 10 Conflicts to Watch in 2024. *Foreign Policy*. https://foreignpolicy.com/2024/01/01/conflicts-2024-gaza-sudan-china-iran-myanmar-ukraine-ethiopia-sahel-haiti-armenia-azerbaijan-iran-hezbollah/

ESET. (2024, May 3). *Locked Shields 2024: ESET bolsters Slovak cyber defense during live-fire NATO exercise*. https://www.eset.com/int/about/newsroom/press-releases/company/locked-shields-2024-eset-bolsters-slovak-cyber-defense-during-live-fire-nato-exercise/

European Commission. (2013). HORIZON 2020 WORK PROGRAMME 2014 – 2015 General Annexes. In *European Union*. https://ec.europa.eu/research/participants/portal4/doc/call/h2020/common/1617621-part_19_general_annexes_v.2.0_en.pdf

European Space Agency. (2020, November 23). *Secure communication via quantum cryptography*. https://www.esa.int/Applications/Connectivity_and_Secure_Communications/Secure_communication_via_quantum_cryptography

European Union. (2024, April 18). *The European Quantum Communication Infrastructure (EUROQCI) initiative*. Shaping Europe's Digital Future. https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci

Falcon algorithm co-developed with Thales selected by the NIST as a new standard in post-quantum cryptography. (2022, July 13). Thales Group. https://www.thalesgroup.com/en/worldwide/security/press_release/falcon-algorithm-co-developed-thales-selected-nist-new-standard

FasterCapital. (2024, June 24). *Breaking Barriers: How Quantum Computing Startups are Changing the Game*. https://fastercapital.com/content/Breaking-Barriers--How-Quantum-Computing-Startups-are-Changing-the-Game.html

Financial Manager. (2020, November 9). United States Army. https://www.goarmy.com/careers-and-jobs/support-logistics/admin-financial-support/36a-financial-manager

Forbes Technology Council. (2022, November 8). 13 Risks That Come With The Growing Power Of Quantum Computing. *Forbes*. https://www.forbes.com/sites/forbestechcouncil/2022/11/08/13-risks-that-come-with-the-growing-power-of-quantum-computing/

Foust, J. (2023, January 23). *SES considering quantum cryptography satellite system*. SpaceNews. https://spacenews.com/ses-considering-quantum-cryptography-satellite-system/

George, T. (2023, June 22). *Semi-Structured Interview | Definition, Guide & Examples*. Scribbr. https://www.scribbr.com/methodology/semi-structured-interview/

Gschwendtner, M., Hijazi, H., Morgan, N., & Soller, H. (2024, February 16). *Quantum computing: The time to act is now*. McKinsey & Company. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/tech-forward/quantum-computing-the-time-to-act-is-now

Haddad, A., Doherty, R., & Purtilo, R. (2019). Respect in a diverse society. In *Elsevier eBooks* (pp. 60–76). https://doi.org/10.1016/b978-0-323-53362-1.00005-0

Hales, D. (2005). An Introduction to Triangulation. In *UNAIDS*. https://www.unaids.org/sites/default/files/sub_landing/files/10_4-Intro-to-triangulation-MEF.pdf

Héder, M. (2017). From NASA to EU: the evolution of the TRL scale in Public Sector Innovation. *The Innovation Journal*, *22*(2), 1–23. http://eprints.sztaki.hu/9204/

Henderson, J. (2022, May 13). Mobile Tech Can Maximize Uptime for Military Employees. *FedTech Magazine*. https://fedtechmagazine.com/article/2022/05/mobile-tech-can-maximize-uptime-military-employees

Home | Quantum Delta NL. (2019, November 9). Quantum Delta NL. https://quantumdelta.nl/

Horowitz, M. C. (2010). *The Diffusion of Military Power: Causes and Consequences for International Politics*. Princeton University Press.

Huttner, B., Alléaume, R., Diamanti, E., Fröwis, F., Grangier, P., Hübel, H., Martin, V., Poppe, A., Slater, J. A., Spiller, T., Tittel, W., Tranier, B., Wonfor, A., & Zbinden, H. (2022). Long-range QKD without trusted nodes is not possible with current technology. *Npj Quantum Information*, *8*(1). https://doi.org/10.1038/s41534-022-00613-4

International Intellectual Property Law Association. (2024, June 26). *Researchers Say IP Trends Indicate a Quickly Increasing Quantum Ecosystem Is "Co-Evolving," Reaching Maturity*. https://iipla.org/researchers-say-ip-trends-indicate-a-quickly-increasing-quantum-ecosystem-is-co-evolving-reaching-maturity/

IQM Quantum Computers, OpenOcean, Lakestar, & The Quantum Insider. (2024). *State of Quantum 2024: Understanding the 2023 trends and outlook for 2024* (pp. 4–5) [Report]. https://assets-global.website-files.com/6523f13a748909d3e1bbb657/65e6d35be62d08db2e7b3b71_State-of-Quantum-2024-report.pdf

Kong, I., Janssen, M., & Bharosa, N. (2022). Challenges in the Transition towards a Quantum-safe Government. *Proceedings of the 23rd Annual International Conference on Digital Government Research*, 282–292. https://doi.org/10.1145/3543434.3543644

Liao, S., Cai, W., Liu, W., Zhang, L., Li, Y., Ren, J., Yin, J., Shen, Q., Cao, Y., Li, Z., Li, F., Chen, X., Sun, L., Jia, J., Wu, J.,

Jiang, X., Wang, J., Huang, Y., Wang, Q., . . . Pan, J. (2017). Satellite-to-ground quantum key distribution. *Nature*, *549*(7670), 43–47. https://doi.org/10.1038/nature23655

Lipscomb, P. (2017). The Evolution of Communications in the Military as it Relates to Leadership. *Integrated Studies*. https://digitalcommons.murraystate.edu/bis437/90/

Locy, J. (2024, April 26). *Office of Research and Innovation Assists USC-ISI QuANET Proposal Funded by DOD DARPA for "8M*. Office of Research and Innovation at USC. https://research.usc.edu/news/2024/03/office-of-research-innovation-assists-usc-isi-quanet-proposal-funded-by-dod-darpa-for-18m/

Maseng, T., Landry, R., & Young, K. (2010). Military communications. *IEEE Communications Magazine*, *48*(10), 50–52. https://doi.org/10.1109/mcom.2010.5594676

McCombes, S. (2023, November 20). *What Is a Research Design | Types, Guide & Examples*. Scribbr. https://www.scribbr.com/methodology/qualitative-research/

McKinsey & Company. (2023). Quantum Technology Monitor. In *McKinsey & Company*. https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/quantum%20technology%20sees%20record%20investments%20progress%20on%20talent%20gap/quantum-technology-monitor-april-2023.pdf

Ministerie van Defensie. (2022a, March 3). *Minister Bijleveld onder indruk van innovaties bij MINDbase*. Defensie.nl. https://www.defensie.nl/actueel/nieuws/2021/03/03/minister-bijleveld-onder-indruk-van-innovaties-bij-mindbase

Ministerie van Defensie. (2022b, March 10). *Netherlands Chief of Defence*. Dutch Ministry of Defence. https://english.defensie.nl/organisation/central-staff/netherlands-chief-of-defence

Mishra, A., & Mishra, D. (2013). Applications of Stakeholder Theory in Information Systems and Technology. *Engineering Economics*, *24*(3), 254–266. https://doi.org/10.5755/j01.ee.24.3.4618

Nakasone, P. M. (2019). A Cyber Force for Persistent Operations. *Joint Force Quarterly*, *92*, ISSN 1070-0692. https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92.pdf

National Quantum Initiative. (2024, May 22). *The United States and Germany Sign Joint Statement to Enhance Cooperation in Quantum*. https://www.quantum.gov/the-united-states-and-germany-sign-joint-statement-to-enhance-cooperation-in-quantum/

National Research Council of Italy, University of Malta, & Istituto Nazionale di Ricerca Metrologica. (2021). Secure Quantum Communication Undersea Link. In *NATO Science for Peace and Security Programme* (No. G5485). https://www.nato.int/nato_static_fl2014/assets/pdf/2021/11/15-sps-G5485/0864-21-V3-SPS_Flyer_G5485.pdf

NATO Allied Command Transformation. (2024, May 28). *Interoperability: a Cornerstone Concept of NATO*. https://www.act.nato.int/article/interoperability-cornerstone-concept/

NATO Science for Peace and Security Programme. (2023). *Quantum Technologies and the Science for Peace and Security programme*. https://www.nato.int/nato_static_fl2014/assets/pdf/2023/11/pdf/231130-SPS-Quantum-1487-23.pdf

Nelson, R. (2024, January 25). *UAH researchers to head NATO quantum technologies security program*. 256 Today. https://256today.com/uah-researchers-to-head-nato-quantum-technologies-security-program/

Neumann, N. M. P., Van Heesch, M. P. P., De Graaf, P., Phillipson, F., & Smallegange, A. a. P. (2021). Quantum Computing for Military Applications. In *2021 International Conference on Military Communication and Information Systems (ICMCIS)* (pp. 1–8). IEEE Press. https://doi.org/10.1109/ICMCIS52405.2021.9486419

Nofer, M., Bauer, K., Hinz, O., Van Der Aalst, W., & Weinhardt, C. (2023). Quantum computing. *Business & Information Systems Engineering*, *65*(4), 361–367. https://doi.org/10.1007/s12599-023-00823-w

Norris, J. (2012). *Marching to the drums: A History of Military Drums and Drummers*. Spellmount Publishers.

Obis, A. (2023, October 23). *Army's New Intel Doctrine Prepares for a Quantum Future*. GovCIO Media & Research. https://govciomedia.com/armys-new-intel-doctrine-prepares-for-a-quantum-future/

Okur, C. (2013). *The Effect of Defense R&D on Military Capability and Technological Spillover* [MSc Thesis, Air Force Institute of Technology]. https://scholar.afit.edu/cgi/viewcontent.cgi?article=2002&context=etd

Olechowski, A. L., Eppinger, S. D., Joglekar, N., & Tomaschek, K. (2020). Technology readiness levels: Shortcomings and improvement opportunities. *Systems Engineering*, *23*(4), 395–408. https://doi.org/10.1002/sys.21533

Parker, E. (2021). *Commercial and Military Applications and Timelines for Quantum Technology*. RAND Corporation. https://www.rand.org/content/dam/rand/pubs/research_reports/RRA1400/RRA1482-4/RAND_RRA1482-4.pdf

Perrier, E. (2022). The Quantum Governance Stack: Models of Governance for Quantum Information Technologies. *Digital Society*, *1*(3). https://doi.org/10.1007/s44206-022-00019-x

Polnik, M., Mazzarella, L., Di Carlo, M., Oi, D. K., Riccardi, A., & Arulselvan, A. (2020). Scheduling of space to ground quantum key distribution. *EPJ Quantum Technology*, *7*(3). https://doi.org/10.1140/epjqt/s40507-020-0079-6

Q-Leap Edu Quantum Communications. (2021, March 24). *1-1 History of communication* [Video]. YouTube. https://www.youtube.com/watch?v=JZFK4jr3c7M

Raines, R. R. (1996). *Getting the Message Through: A Branch History of the U.S. Army Signal Corps*. https://history.army.mil/html/books/030/30-17-1/CMH_Pub_30-17-1.pdf

Richardson, A. J. (2015). The cost of a telegram: the evolution of the international regulation of the telegraph. *Accounting History*, *20*(4), 405–429. https://doi.org/10.1177/1032373215599409

Roser, M. (2023, February 22). *Technology over the long run: zoom out to see how dramatically the world can change within a lifetime*. Our World in Data. https://ourworldindata.org/technology-long-run

Rothman, T. (2019, February 26). *Random Paths to Frequency Hopping*. American Scientist.

https://www.americanscientist.org/article/random-paths-to-frequency-hopping

Sahu, K., Kumar, R., Srivastava, R. K., & Singh, A. K. (2024). Military Computing Security: Insights and Implications. *Journal of the Institution of Engineers (India): Series B*. https://doi.org/10.1007/s40031-024-01136-6

Salvador-Carulla, L., Woods, C., De Miquel, C., & Lukersmith, S. (2024). Adaptation of the Technology Readiness Levels for impact assessment in implementation sciences: The TRL-IS checklist. *Heliyon*, e29930. https://doi.org/10.1016/j.heliyon.2024.e29930

Samsung U.S. Newsroom. (2023, September 20). Samsung Galaxy S23 Tactical Edition and Galaxy XCover 6 Pro Tactical Edition: New Smartphones for Military Personnel and First Responders. *Samsung U.S. Newsroom*. https://news.samsung.com/us/samsung-galaxy-s23-tactical-edition-samsung-galaxy-xcover-6-pro-tactical-edition-help-military-personnel-make-informed-decisions-achieve-objectives-securely-share-mission-data/

Sennewald, R. W. (1990). A PRIMER ON RESEARCH AND DEVELOPMENT IN THE U.S. ARMY. In *Association of the United States Army*. https://www.ausa.org/sites/default/files/SR-1990-A-Primer-on-Research-and-Development-in-the-US-Army.pdf

Silbert, S. (2022). Don't let concern over quantum technologies limit international collaboration. *Deleted Journal*. https://doi.org/10.1126/scidip.ade6813

Slovak University of Technology, University of Malta, University of Alabama in Huntsville, & Universidad Rey Juan Carlos. (2021). Secure Communication in the Quantum Era. In *NATO Science for Peace and Security Programme* (Report No. G5448). https://www.nato.int/nato_static_fl2014/assets/pdf/2021/9/pdf/210929-SPS-Flyer-G5448.pdf

Smith, Z. L. M. (2022, February 11). Make Haste Slowly for Quantum. *CSIS*. https://www.csis.org/analysis/make-haste-slowly-quantum

Spectra Group. (2023, March 29). *Importance of Reliable & Secure Military Communications for Mission Success*. Defense Advancement. https://www.defenseadvancement.com/feature/importance-of-reliable-secure-military-communications-for-mission-success/

State of Queensland. (2023). Queensland Quantum and Advanced Technologies Strategy: Turning deep science into trailblazing industries. In *Department of Environment, Science and Innovation Queensland* [Report]. https://science.des.qld.gov.au/__data/assets/pdf_file/0028/324397/qld-quantum-advanced-technologies-strategy-2023.pdf

Stewart, L. (2023, October 5). *Why Researcher Triangulation Matters*. ATLAS.ti. https://atlasti.com/research-hub/researcher-triangulation

Stohrer, C., & Lugrin, T. (2023). Asymmetric Encryption. In *Trends in Data Protection and Encryption Technologies* (pp. 11–14). Springer, Cham. https://doi.org/10.1007/978-3-031-33386-6_3

Swayne, M. (2024a, February 12). *Rise of the Quantum CISO? A guide to prepare CISOs and technical teams for the Quantum era*. The Quantum Insider. https://thequantuminsider.com/2024/02/12/rise-of-the-quantum-ciso-a-guide-to-prepare-cisos-and-technical-teams-for-the-quantum-era/

Swayne, M. (2024b, April 11). *French Defense Agency to award startups €500 million-plus to build universal quantum computers*. The Quantum Insider. https://thequantuminsider.com/2024/03/09/french-defense-agency-to-award-startups-e500-million-plus-to-build-universal-quantum-computers/

Swayne, M. (2024c, April 20). *Companies invest total of "50 million in quantum computing research at US and Japanese universities*. The Quantum Insider. https://thequantuminsider.com/2023/05/19/ibm-and-google-join-forces-invest-150-million-in-quantum-computing-research-at-us-and-japanese-universities/

Tagarev, T. (2010). *Building Integrity and Reducing Corruption in Defence: A Compendium of Best Practices*. Geneva Centre for the Democratic Control of Armed Forces. https://www.dcaf.ch/sites/default/files/publications/documents/Compendium_Building_Integrity_and_Reducing_Corruption_in_Defence.pdf

Technology policy. (2024, June 20). OECD. https://www.oecd.org/en/topics/policy-issues/technology-policy.html

The State of Quantum in 2024: Progress Amid Cautious Optimism. (2024, June 24). Tech Tour. https://techtour.com/news/2024/the-state-of-quantum-in-2024.html

TNO, CWI, & AIVD. (2023). *The PQC Migration Handbook: Guidelines For Migrating To Post-Quantum Cryptography* (2nd ed.). https://publications.tno.nl/publication/34641918/oicFLj/attema-2023-pqc.pdf

TU Delft. (2020, December 1). *The possible dark side of quantum communication technologies*. https://www.tudelft.nl/over-tu-delft/strategie/vision-teams/quantum-internet/impact-governance/the-possible-dark-side-of-quantum-communication-technologies

Ubaidullah, M., & Makki, Q. (2016). A Review on Symmetric Key Encryption Techniques in Cryptography. *International Journal of Computer Applications*, *147*(10), 43–48. https://doi.org/10.5120/ijca2016911203

UNIDIR — the UN Institute for Disarmament Research. (2023, December 1). *Multi-Stakeholder Dialogue: Quantum Technologies - Implications for International Peace & Security* [Video]. YouTube. https://www.youtube.com/watch?v=E8JQ-xuinJE

United States Government US Army. (2020). *Joint Publication JP 5-0 Joint Planning December 2020*. Federation of American Scientists. https://irp.fas.org/doddir/dod/jp5_0.pdf

University of Alabama in Huntsville, VTT Technical Research Centre of Finland, Slovak Academy of Sciences, Slovak University of Technology, & Universidad Carlos III de Madrid. (2023). *NATO SPS Project G5985*. https://www.quantum-safe-cryptography.science/home

U.S. Cyber Command. (2013, August 28). *Our Mission and Vision*. https://www.cybercom.mil/About/Mission-and-Vision/

Van Amerongen, M. (2021, June 3). *Quantum technologies in defence & security*. NATO Review.

https://www.nato.int/docu/review/articles/2021/06/03/quantum-technologies-in-defence-security/index.html

Van Houts, M. (2024, July 12). *Quantum Delta NL krijgt €273 miljoen toegekend door het Nationaal Groeifonds voor de derde fase*. Quantum Delta NL. https://quantumdelta.nl/news/quantum-delta-nl-krijgt-eur273-miljoen-toegekend-door-het-nationaal-groeifonds-voor-de-derde-fase

Vereniging Officieren Verbindingsdienst. (2019). Kwantum Computing Binnen Defensie. In *Intercom* (Vol. 48, Issue 2, pp. 59–61). https://vovklict.nl/intercom/2019/2/27.pdf

Vincent, B. (2023, April 12). Pentagon seeks $75M for new program to accelerate quantum tech transition. *DefenseScoop*. https://defensescoop.com/2023/04/12/pentagon-seeks-75m-for-new-program-to-accelerate-quantum-tech-transition/

Wootters, W. K., & Zurek, W. H. (1982). A single quantum cannot be cloned. *Nature*, *299*(5886), 802–803. https://doi.org/10.1038/299802a0

Zapotoczny, W. (2006). *The Impact of the Industrial Revolution on Warfare* (pp. 1–7). https://www.wzaponline.com/yahoo_site_admin/assets/docs/InductrialRevolution.292125935.pdf