Master's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

Paulina Katarzyna Wesolowska

Quantum Computing and Cryptographic Risk: A Threat Assessment for Norway

Master's thesis in MISD
Supervisor: Tjerand Silde
Co-supervisor: Hans Waardal Heum
December 2025

NTNU
Norwegian University of
Science and Technology

Paulina Katarzyna Wesolowska

Quantum Computing and Cryptographic Risk: A Threat Assessment for Norway

Master's thesis in MISD
Supervisor: Tjerand Silde
Co-supervisor: Hans Waardal Heum
December 2025

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

NTNU
Norwegian University of
Science and Technology

Abstract

Quantum computing is an emerging technology grounded in quantum mechanics, where the shift from conventional physics in computing to quantum behaviour opens the door to new technological breakthroughs. Of particular concern is that a future fault-tolerant quantum computer could compromise widely deployed public-key cryptography. The intelligence, defence, and technological competitiveness benefits at stake have driven states to invest heavily in research, talent, and infrastructure to gain an edge in the ongoing "quantum race" and be the first to turn quantum breakthroughs into strategic advantage.

At the same time, preparing for the quantum threat largely means migrating to post-quantum cryptography (PQC), which replaces quantum-vulnerable algorithms with quantum-resistant ones. However, the quantum threat is often treated as either catastrophic and imminent or too uncertain and distant to act on. This pushes PQC down the priority list.

This thesis aims to bring together the different dimensions of the quantum threat and assess how quantum-enabled threats could realistically manifest within Norway's security landscape. Using an exploratory qualitative design, it synthesises policy/strategy and technical literature with open-source threat intelligence and semi-structured expert interviews to map plausible pathways from quantum capability to adversarial use. The purpose is to make the quantum threat more accessible and decision-relevant for Norway.

The findings suggest that Norway, while a small state, is not a marginal case in the quantum-security landscape. Norway's role in European energy supply and its Arctic/North Atlantic geography make it a plausible target for quantum-enabled intelligence gains. The findings support prioritising PQC migration in the most critical, long-lived systems. Preparedness also requires making the quantum threat understandable across the wider ecosystem to enable action.

Sammendrag

Kvantedatamaskiner er en fremvoksende teknologi forankret i kvantemekanikken, der skiftet fra konvensjonell fysikk i databehandling til kvantefenomener åpner for nye teknologiske gjennombrudd. Særlig bekymringsfullt er at en fremtidig feiltolerant kvantedatamaskin kan kompromittere utbredt offentlig-nøkkel-kryptografi. Gevinstene innen etterretning, forsvar og teknologisk konkurransekraft har ført til at stater investerer tungt i forskning, kompetanse og infrastruktur for å få et fortrinn i det pågående «kvantekappløpet», og være først til å utvikle og utnytte teknologien.

Samtidig innebærer forberedelser mot kvantetrusselen i stor grad migrering til post-kvantum-kryptografi (PQC), som erstatter kvantesårbare algoritmer med kvantesikre alternativer. Kvantetrusselen omtales imidlertid ofte enten som katastrofal og nært forestående, eller som for usikker og fjern til å handle på. Dette skyver PQC nedover på prioriteringslisten.

Denne oppgaven har som mål å samle de ulike dimensjonene ved kvantetrusselen og vurdere hvordan trusler muliggjort av kvanteteknologi kan manifestere seg i Norges sikkerhetslandskap. Med et eksplorativt kvalitativt design sammenstiller den styrings- og strategidokumenter og teknisk litteratur med trusselinformasjon fra åpne kilder og semi-strukturerte ekspertintervjuer for å skissere mulige veier fra utvikling av kvanteteknologi til uønsket bruk. Formålet er å gjøre kvantetrusselen mer tilgjengelig og beslutningsrelevant for Norge.

Funnene tyder på at Norge, selv som småstat, har en tydelig relevans i det kvantesikkerhetsmessige trusselbildet. Norges rolle i europeisk energiforsyning og landets geografi i Arktis/Nord-Atlanteren gjør Norge til et realistisk mål for kvantemuliggjort etterretningsvirksomhet. Funnene støtter å prioritere PQC migrering i de mest kritiske systemene med lang levetid. Beredskap forutsetter også at kvantetrusselen gjøres forståelig i et bredere aktørøkosystem for å muliggjøre handling.

Preface

This thesis marks the completion of my Master's degree in Information Security at the Norwegian University of Science and Technology (NTNU). I would like to thank my supervisors, Tjerand Silde and Hans Waardal Heum, for their guidance and support throughout the work on this thesis. I am also grateful to all interview participants for sharing their perspectives and expertise. Finally, I would like to thank all the other individuals I encountered over the past few months for sharing their perspectives and insights on this topic.

Oslo, 22nd December 2025

Paulina Wesolowska

Contents

Figures

Tables

Acronyms

AES Advanced Encryption Standard

BGP Border Gateway Protocol

DES Data Encryption Standard

ECC Elliptic Curve Cryptography

FTQC Fault-Tolerant Quantum Computer

HNDL Harvest Now, Decrypt Later

NATO North Atlantic Treaty Organization

NISQ Noisy Intermediate-Scale Quantum

NIST National Institute of Standards and Technology

NSM Norwegian National Security Authority

OT Operational Technology

PQC Post-Quantum Cryptography

QFT Quantum Fourier Transform

QPE Quantum Phase Estimation

RSA Rivest–Shamir–Adleman

TLS Transport Layer Security

Chapter 1

Introduction

2025 has been designated by the United Nations as the International Year of Quantum Science and Technology, marking the centenary of quantum mechanics [1]. A hundred years on, advances in engineering and experimental physics have moved quantum computing from theory toward practical prototypes, making it more plausible to build physical systems that exploit quantum effects for computation. This may deliver major benefits across science and technology, but it also raises questions that are directly relevant to national security.

One of the most consequential security concerns is the potential impact on modern cryptography. Public-key cryptography underpins confidentiality and trust in modern digital society, enabling secure communication as well as mechanisms such as authentication and digital signatures. When fault-tolerant, cryptographically relevant quantum computers become feasible, they could compromise widely deployed public-key cryptography and weaken core trust mechanisms, making decryption and certain forms of impersonation achievable [2–4].

Mitigating the potential cryptographic impact of quantum computing requires proactive measures, most notably transitioning to post-quantum cryptography (PQC). Yet large-scale migration is difficult to prioritise because it is complex, costly, and time-consuming, and it must often be planned under uncertainty [3, 5, 6]. A central question is therefore how to set priorities: what should be protected first, by whom, and why.

This thesis responds to that challenge by developing a structured, Norway-focused threat assessment. It brings together technical and strategic perspectives to examine relevant state actors and incentives, plausible pathways from quantum capability to malicious use, and what this implies for prioritising protective measures for Norwegian national security.

1.1 Motivation

Quantum risk is a collective challenge: effective protection requires coordinated measures and sustained effort across sectors, and in many cases must be implemented before the threat is fully observable. For such action to be possible, the

issue also needs to be understood in a way that is credible and decision-relevant. Existing research and policy discussion often address important parts of the puzzle in isolation, such as algorithmic vulnerabilities, standardisation, migration challenges, or assessments of technical feasibility. While these contributions are valuable, they do not always produce a coherent national-security picture of how quantum-enabled threats might be developed and used by state actors, or what this implies for a small but technologically advanced state such as Norway.

The motivation for this thesis is therefore to provide a high-level, integrated overview of the quantum threat landscape that is accessible and relevant to decision-makers, security practitioners, and organisations that may lack expertise in quantum physics or cryptography. Rather than focusing narrowly on a single technical or organisational issue, the thesis combines perspectives from quantum technology, cybersecurity, geopolitics, and intelligence analysis to assess how quantum capabilities might realistically be developed and used by state actors, and what this implies for Norway.

1.2 Problem Statement

This thesis presents a national-level assessment of quantum-enabled threats to Norway. Specifically, it clarifies what the quantum threat entails in a Norwegian context, assesses which state actors are most likely to develop cryptographically relevant quantum computing capabilities and how they could be used, and identifies which sectors or functions should be prioritised for protective measures.

To address this problem, the thesis is guided by the following research questions:

- RQ1: How might a quantum advantage realistically be employed in an adversarial context, based on current geopolitical dynamics and expert assessments?
- RQ2: Which state actors are most likely to develop and control cryptographically relevant quantum capabilities?
- RQ3: Which Norwegian national sectors or functions are most exposed to quantum-enabled threats, given their strategic importance and reliance on cryptographic systems?

1.3 Scope and Limitations

The scope of this thesis is focused on high-level national functions and critical sectors, rather than on specific technologies, systems, or individual organisations.

The scope is deliberately limited to state-level adversaries, with primary emphasis on China and Russia, as these states are often viewed as adversaries of the West, given their strategic competition with the EU and the United States [7–10].

This assessment aims to achieve the best understanding currently possible based on open sources and expert interviews. Both the technology and the geo-

political context are evolving rapidly, which means the threat picture may change considerably in the coming years.

Threat assessments are, by nature, snapshots in time rather than fixed predictions. It is also possible that certain aspects of this assessment are incomplete because some information is not publicly available. This includes quantum development roadmaps, targeting, system vulnerabilities, or migration activities that are either confidential or simply not disclosed in open sources.

Furthermore, one thesis could not examine every system or sector in detail, and the analysis is therefore limited to what can reasonably be assessed from available data and expert interviews. Therefore, this assessment should be understood as a contemporary attempt to evaluate the quantum threat in a realistic and practical manner, moving beyond the generic statement that "quantum computers will break encryption" and instead offering a grounded picture of how the threat is likely to manifest in practice.

1.4 Contribution of the thesis

This thesis contributes a Norway-focused, national-security assessment of how quantum-enabled threats may materialise, bridging technical discussions of cryptographic vulnerability with strategic analysis of state competition and offensive incentives. By making the quantum threat more accessible across a wider ecosystem of stakeholders, the thesis aims to strengthen risk communication and enable earlier, more coordinated protective measures.

This master's thesis also aims to contribute to the long-term resilience of digital services by conducting a comprehensive threat assessment that identifies key vulnerabilities, not only from a technical perspective but also by considering the geopolitical risks and strategic motivations of foreign states. The objective is to support the development of a secure and sustainable digital society capable of withstanding future technological disruptions. The study aligns with the broader aims of the United Nations Sustainable Development Goal (SDG) 9, which seeks to *"build resilient infrastructure, promote inclusive and sustainable industrialisation, and foster innovation"* [11]. This supports Target 9.5, which emphasises upgrading the technological capabilities of industrial sectors in all countries and encouraging innovation [11].

1.5 Structure of the Thesis

This thesis is organised into nine chapters.

Chapter 2 Theoretical and Technical Background introduces quantum computing concepts and explains the cryptographic implications.

Chapter 3 Methodology describes the document analysis, expert interviews, and the threat-assessment method used in the thesis.

Chapter 4 The Quantum Race examines the main actors and their investments shaping the global quantum development.

Chapter 5 Security Imperatives in Quantum Development describes the strategic motivation of China and Russia, and their cyber offensive operations.

Chapter 6 Post-Quantum Defence and Norwegian Initiatives covers Post Quantum Cryptography approaches, standardisation, migration challenges, and national preparedness efforts.

Chapter 7 Threat Assessment applies the framework to assess how quantum-enabled threats may emerge and what risk pathways matter most.

Chapter 8 Discussion interprets the results and discusses uncertainties in the quantum technology landscape.

Chapter 9 Conclusion summarises the main findings.

Chapter 2

Theoretical and Technical Background

This section introduces the foundational principles of quantum computing to explain how quantum algorithms, such as Shor's or Grover's algorithms, can in theory break encryption and what this could imply for confidentiality, authentication, and digital signatures in a national security context. The chapter then presents the current state of technological development and discusses the remaining challenges that must be overcome before the quantum threat can materialise in practice.

2.1 Quantum Computing and Its Cryptographic Implications

Quantum computing exploits the principles of quantum mechanics to perform calculations that are not classically feasible. The idea can be traced back to the 1980s, when physicists first proposed theoretical models showing that such calculations could be carried out by harnessing quantum-mechanical properties, such as superposition, entanglement and interference, within physical systems [2, 12].

To understand how a quantum computer uses them at a fundamental level, it is useful to start by looking at how classical computers operate. In a classical computer, every operation can be reduced to performing a set of mathematical calculations. These calculations rely on binary units, or bits, that can take the value of 1 or 0, where each bit can exist only in one of these two states at any given moment [5, 13].

A computer built on quantum mechanical principles relies on quantum bits, or qubits. When these are embedded in a physical system, a qubit can represent the values of 0 or 1 like a classical bit, but it can also exist in a superposition of 0 and 1. Two qubits can also enter an entangled state, meaning they become correlated in such a way that the value of one is tied to the value of the other. When qubits are entangled, manipulating one qubit produces a corresponding

effect on its entangled counterpart [2, 5, 13, 14].

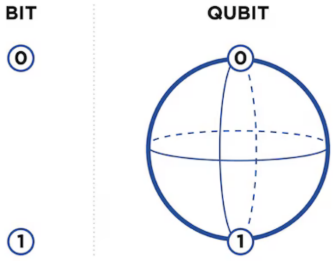


Figure 2.1: *The figure illustrates the contrast between classical bits and quantum bits (qubits) [15].*

2.1.1 Cryptographic Relevance

Quantum behaviour in computing could potentially speed up the search for decryption keys or to efficiently solve the hard mathematical problems that many cryptographic schemes rely on for security. This is particularly concerning given how much of today's digital infrastructure depends on algorithms that are vulnerable to quantum-enabled cryptanalysis. The way this advantage manifests depends on the cryptographic scheme involved, since different algorithms rely on different underlying hardness assumptions. Cryptographic methods are generally classified into two types: symmetric and asymmetric schemes.

Symmetric cryptography, used in algorithms such as the Advanced Encryption Standard (AES), relies on a single shared key for both encryption and decryption. The communicating parties must have access to the same key before any secure exchange can take place. Once the key is shared, the sender encrypts the message, and the receiver uses the same key to decrypt it. Symmetric encryption is generally fast and straightforward to use, but the sharing of a secret key through large-scale or distributed systems can introduce some security challenges, such as for example the risk that the key could be intercepted by an unintended party [3, 4, 6, 16].

Asymmetric cryptography, such as RSA encryption, Diffie-Hellman key exchange or Elliptic Curve Cryptography (ECC), solves the key distribution problem by relying on two linked keys, a public key that can be freely shared, and a private key that must remain secret. Asymmetric schemes depend on computationally hard mathematical problems that make it infeasible to derive the private key from the public one; if that assumption fails, an attacker may be able to decrypt intercepted ciphertexts, impersonate legitimate parties, and forge digital signatures [4, 6, 12, 16].

Asymmetric cryptographic algorithms are vulnerable to quantum computers because a sufficiently powerful quantum machine could solve these problems. This was shown by Shor, who demonstrated that schemes such as RSA could be broken by factoring the modulus, then recovering the secret key from the public

key. Symmetric cryptography is generally seen as more resilient, since an attacker cannot directly "solve for the key" in the same way. However, Grover's algorithm still introduces some concerns for symmetric schemes.

2.1.2 Shor's Algorithm and RSA

In 1994, Petter Shor introduced the first practical quantum algorithm that could solve a classically difficult problem. This result was a breakthrough for the field of quantum computing, not only because it implied that widely used cryptographic systems could be broken, but also because it provided the first concrete evidence that quantum computers might outperform classical machines on problems beyond quantum simulation. Shor's work transformed quantum computing from a theoretical curiosity into a scientific and technological pursuit [5, 12, 14].

Shor's algorithm deals with the demanding problem of factoring large integers, especially those that are constructed as the product of two primes, which is the foundation of RSA encryption. In the RSA scheme, the value N (given by $p \times q$, where p and q are prime numbers) is public. For an attacker, the difficult task is to recover p and q, and classical computers do not have an efficient method for factoring N when the primes are sufficiently large. This hard problem can be reformulated as a period-finding task [17]. Shor's algorithm considers the function $a^x \mod N$, where a is chosen at random such that it is smaller than N and coprime with it. The aim is to determine the smallest integer k, called the period, satisfying $a^k \equiv 1 \mod N$. Up to this point, the steps remain classical. To actually determine the period efficiently, the algorithm uses the Quantum Fourier Transform (QFT) [17, 18].

RSA's security relies on the hardness of the factorisation problem. Shor's algorithm shows theoretically that RSA can be broken by converting factorisation into a period-finding problem and solving it using the Fourier transform. The same reasoning applies to the discrete logarithm problem, which means that Diffie-Hellman key exchange and Elliptic Curve Cryptography (ECC) are also vulnerable to Shor's algorithm.

2.1.3 Grover's Algorithm and AES

Grover's algorithm, introduced in 1996 by Lov Kumar Grover, revealed a theoretical vulnerability in symmetric cryptographic systems when facing quantum computers.

Algorithms like the Advanced Encryption Standard (AES) base their security on the complexity created through multiple rounds of substitutions and permutations, combined with both linear and non-linear transformations, to obscure the relationship between plaintext, ciphertext, and key. AES can be configured with key lengths of 128, 192 or 256 bits, which determine whether the cipher performs 10, 12 or 14 rounds of processing [18, 19]. In practice, this comes down to how hard it is to brute-force the key. Brute force means guessing the correct key by trying every possible solution. The longer the key is, the more guesses are needed. For

AES, the key space is so large that even the smallest key size would take an unrealistic amount of time, far longer than anyone could practically attempt. Because of this, AES is considered safe from brute-force attacks with classical computers.

Grover's algorithm, however, provides a quadratic speed-up for searching through unsorted space. This means that the required work grows much more slowly than in the classical approach: as the problem size increases, the number of steps increases far less than proportionally [20]. Instead of checking every possible key one by one, a quantum computer can use quantum properties to evaluate many possibilities at once and reduce the number of guesses needed. When applied to AES, the key-search problem becomes a task of locating the correct key within a very large set of candidates. Grover's algorithm reduces the number of steps required to find this key by repeatedly increasing the likelihood of the correct solutions while decreasing the incorrect ones, meaning that the probability of identifying the right key grows with each iteration [6, 16, 19].

The algorithm effectively halves the security of symmetric keys. A 128-bit key would offer only about 64 bits of security in the presence of a quantum computer [19]. Even though Grover's algorithm shows that symmetric encryption can be weakened, this effect can largely be mitigated by increasing key sizes, for example by moving from AES-128 to AES-256 [12, 19]. In addition, although Grover's algorithm theoretically offers a quadratic speed-up, it must be executed sequentially, meaning it cannot take advantage of massive parallelism in the same way that classical brute-force attacks can. Classical attacks can distribute the key search across many processors simultaneously, but Grover's algorithm must be run as a single coherent quantum process and cannot be divided across multiple quantum computers in the same manner. The practical speed-up may therefore be smaller than the theoretical model suggests [12]. The long-term quantum impact on symmetric schemes is therefore considered much more limited, and the practical risk remains low given current knowledge.

2.1.4 Security Consequences

Cryptography plays a fundamental role in modern security, from securing our communications and information to verifying the integrity of messages, identities, and systems. The potential impact is emphasised by the term often used to describe it: a "quantum apocalypse". We rely on it to ensure the confidentiality of our personal information, and states rely on it to secure classified information against adversaries. It also enables modern systems to verify trust, authenticity, and integrity.

Digital signatures are used to confirm the legitimacy of a server's identity when establishing a connection through TLS certificates, and vendors use them to verify the authenticity and integrity of their hardware and software [21]. They verify that e-passports are genuinely issued by national authorities, enable secure FIDO authentication for user logins, and form the foundation of certificate authorities that vouch for websites and organisations.

Many of these signatures today rely on RSA or elliptic-curve algorithms. This means that if a cryptographically relevant quantum computer were to exist, an attacker could take a publicly available verification key, for example, the public key used to verify software updates, and use Shor's algorithm to compute the corresponding private signing key for factoring-based or elliptic-curve-based signature schemes. With that signing key, the attacker would gain full signing capability for that identity. A forged vendor signature would be indistinguishable from a legitimate one, making it possible to distribute malicious updates through trusted channels. Such a compromise could impact millions of systems if distributed at scale, or it could be used against smaller targets to stay less "noisy" and avoid quick detection. Regardless, the scale of the use of vulnerable technology for digital signatures could be catastrophic for many sectors and countries, because even if you have the strongest encryption possible on the application level, a kernel-level backdoor installed through a forged, signed update can still access data before it is encrypted.

This is just one hypothetical scenario for how an adversary could exploit a sufficiently powerful quantum computer in a large-scale attack. Once the underlying cryptographic assumptions fail, the range of potential misuse expands dramatically, from decrypting sensitive communications to compromising national security systems by tampering with critical infrastructure or accessing classified information.

2.1.5 Harvest Now, Decrypt Later

The Harvest Now, Decrypt Later (HNDL) attack describes intercepting and storing encrypted data today with the expectation that it can be decrypted in the future once cryptographically relevant quantum computers become available [5, 22]. This strategy is especially worrying for information with a long shelf life. From this perspective, sensitive data currently protected by quantum-vulnerable algorithms should already be considered effectively compromised, even if the practical consequences will not be visible until a quantum capability materialises.

This can be achieved by threat actors through passive eavesdropping on network data, which is most encrypted using Transport Layer Security (TLS) to secure communication between applications and servers. While most of the data transmitted within a TLS session is protected by symmetric encryption (such as AES), the TLS handshake that establishes the session relies on asymmetric algorithms such as RSA or ECC for key exchange [23]. If a threat actor later manages to decrypt the private RSA key, they could decrypt the recorded handshake and derive the session keys, allowing them to access traffic that was originally encrypted with a symmetric algorithm. The Transport Layer Security (TLS) protocol is governed by the Internet Engineering Task Force (IETF), which is currently working with NIST to make TLS resistant to quantum attacks. The IETF's TLS Working Group is developing hybrid post-quantum key exchange mechanisms for TLS 1.3, combining classical and post-quantum algorithms. This proposal is still under active

review as an Internet-Draft, with its current review period expiring in March 2026 [23, 24].

Threat actors can also try to redirect Internet traffic, so it flows through networks they control or gain access to a tap point at an ISP or a cable landing station to copy packets remotely [22]. Techniques such as BGP hijacking achieve this by re-routing traffic. The Border Gateway Protocol (BGP) connects the autonomous systems that make up the internet, but it is relatively easy to manipulate, allowing malicious actors to reroute internet traffic through their own networks [25]. Route manipulation is easier to detect than a pure passive tap (because it alters routing paths), but it can still be subtle as traffic may be routed via unexpected jurisdictions (for example, through China or Russia) without obvious immediate signs of tampering. Even when traffic is diverted, the act of copying is still passive: it leaves the packets intact, so there may be no immediate service disruption or obvious red flags at the application level [22].

2.2 The Contemporary Quantum Computing Landscape

As described in section 2.1, the emergence of quantum computers could have major implications for modern security. The good news is that no quantum computer capable of realising these threats currently exists. So far, there remain significant research constraints that must be overcome before a quantum computer can pose a practical cryptographic threat. Nearly 50 years of research have brought the field closer to practical realisation, yet some obstacles remain to be solved before non-classical quantum phenomena can be reliably reproduced in physical hardware.

2.2.1 Fundamental Research Challenges

Qubits are inherently susceptible to decoherence, a process by which they become entangled with their environment, introducing noise and errors [13, 26, 27]. This introduces an obstacle of finding a way to shield qubits from such noise while, at the same time, enabling them to interact effectively with external control signals requires for computations [18, 26, 28]. Quantum information has only a limited lifetime when stored in a qubit, and without mitigation, when we run an algorithm that requires many steps, the information may be lost before the algorithm finishes running [29]. Because of this, the output of a quantum algorithm cannot be considered reliable, since environmental noise can easily corrupt the result. This fragility is one of the greatest threats to the viability of quantum computing, leading some to question whether large-scale machines are achievable at all [27, 29].

Quantum error correction and fault tolerance represent proposed solutions to this problem. Quantum Error Correction refers to the protocols that can detect and correct errors on qubits, whereas fault tolerance extends this by ensuring that

the entire computation is reliable even though the error correction process itself can be noisy [29]. This distinction arises because QEC itself needs to perform additional operations on the physical qubits which also introduces new errors.

A fault tolerant quantum computer (FTQC) needs therefore to employ QEC in a way that solves more errors than it causes. These concepts, error correction and fault tolerance, make it possible to preserve quantum information long enough to obtain a reliable result. This idea is formalised with the threshold theorem, which states that the error rate of the physical hardware must be kept below a threshold, and if achieved, only then can we perform long calculations in a reliable manner [26, 29]. If we manage to reduce the errors of physical gates, then many of these physical gates and qubits can be combined into logical qubits and gates which behave more reliably because QEC is always running in the background. This theorem has been significant, and much of the progress in quantum computing has been motivated by it [29].

Because the threshold theorem requires many additional physical qubits and gates to construct logical components, the total number of physical qubits needed for fault-tolerant quantum computation at cryptographically relevant scales could reach several millions [29]. A second issue is that even if that many qubits could be built, each of them must remain below the error threshold [29]. While this may be manageable for small systems, stabilising millions of qubits simultaneously represents an extraordinary challenge.

Even with error correction in place, the quantum computer does not become perfectly stable but becomes much less noisy. This means that it may be possible to run certain useful applications, but only if the remaining noise stays below the level that the algorithm or use case can tolerate. How useful a fault-tolerant machine becomes will therefore depend on how much noise a given quantum circuit can withstand before the output becomes unreliable. The lower the noise, the more complex the computations it can perform safely [12].

2.2.2 Present Quantum Capabilities vs. Requirements for Breaking RSA

Literature emphasises that the cryptographic threat will not materialise until fault-tolerant architectures exist. Without large-scale error correction and reliable logical qubits, quantum computers cannot execute algorithms such as Shor's [12]. A commonly used benchmark to gauge the timeline of the quantum threat is the estimated number of qubits required to factor an RSA-2048 modulus. Although the threat extends far beyond RSA, RSA-2048 serves as a key reference point for assessing when quantum computers might realistically reach the scale needed to endanger widely used asymmetric cryptography.

Recent estimates suggest that approximately 1 million noisy qubits could be enough to break RSA-2048 in less than a week [30, 31]. Predicting when this will be achieved is difficult, as it depends on progress in qubit quality, error correction, and scaling technologies. It is, however, worth noting that these estimates are evolving; only a few years ago, studies placed the requirement at a minimum of 20 million noisy qubits, meaning that the projected resource costs have already shrunk significantly [30].

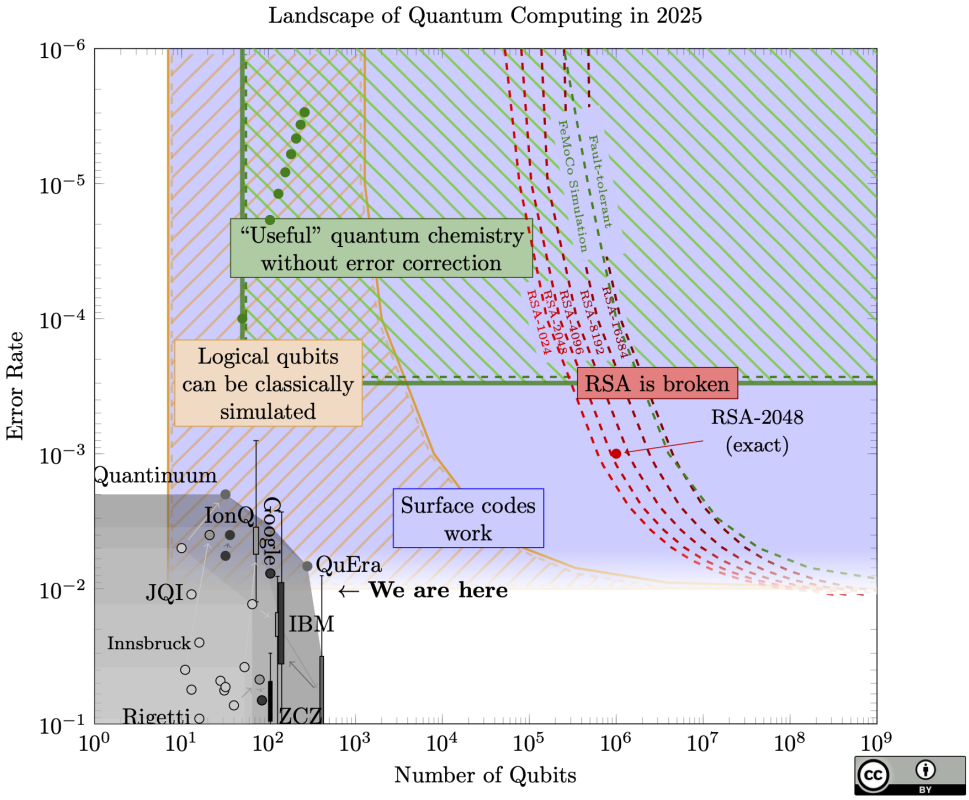


Figure 2.2: *The figure illustrates the current position of quantum computers relative to the qubit numbers and error rates required for useful applications and for breaking RSA encryption [31].*

Preskill [28] introduced the term Noisy Intermediate-Scale Quantum (NISQ) to describe the era of quantum devices with 50 to a few hundred qubits, expected to be powerful enough for meaningful experiments but still too noisy for fault tolerance. Although the term was originally a forward-looking projection, it accurately describes the current state of quantum computing today. Current machines from IBM, Google, and QuEra have around 100–500 qubits with very high error rates, and they are currently too noisy to run large-scale algorithms reliably [28, 31]. The figure 2.1 displays the current state of quantum technology. In this

regime (the orange zone), the useful operations that can be performed have so far been classically simulatable. To reach practical quantum computing, we must move into the zone where error correction becomes possible and many physical qubits can be combined into more reliable logical qubits.

Before we reach a cryptographically relevant quantum computer, many other applications of quantum computing may be achievable. There has been a lot of development in the private sector, with companies exploring a range of potential business applications for quantum computing. Much of the scientific literature in this area focuses on resource estimation to understand which applications might become achievable with which technological capabilities. Based on this analysis, it is expected that commercially useful quantum applications could be achieved well before the development of a cryptographically relevant quantum computer. The technology may thus find use across several areas first, such as data processing, optimisation and operations research, and simulating nature, for example by modelling molecules and developing new materials [12, 13].

Several quantum computers have also been made accessible to the public via cloud services [12]. IBM was one of the first to do this with the launch of the IBM Quantum Experience in 2016 [32]; and since then, other providers such as IonQ, Rigetti, Google, and others followed. Since 2025, the European Union provides access to multiple European-built quantum computers through its Quantum Flagship programme [33]. While early cloud-accessible devices had too few qubits and too much noise to outperform classical computers in any way, they have been extremely valuable for research. Public access has allowed thousands of scientists and engineers to experiment on these services and drive progress in the field [12].

With today's quantum technology, we are still not close to the level required to threaten modern cryptography. As quantum computers begin to achieve other practical advantages over classical systems, these developments may serve as markers of progress, offering a clearer sense of when a cryptographically relevant threat could realistically arise. It is, however, worth noting that these figures reflect only what is publicly visible. The full potential of quantum computing would provide significant strategic advantages to nation states; a point further explored in the next chapters. It is therefore reasonable to assume that some developments are not disclosed.

Achieving a practical, fault-tolerant quantum computer would require infrastructure far beyond what current prototypes resemble. A practical fault-tolerant quantum computer will require a system composed of roughly 50–100 quantum processing units, each requiring up to 1 million qubits. An estimated cost per quantum processing unit is 10 million USD [26]. One of the hardware platforms are the superconducting circuits, built from electronic circuits cooled to 10-20 mK inside dilution refrigerators to behave quantum mechanically [26]. The hardware pieces include coaxial wiring which carry signals into the cryostat, for which wir-

ing alone can cost about 4 million USD. A dilution refrigerator to cool qubits to millikelvin temperature costs around 1 million USD for 150 qubits [26]. Quantum computers will need to operate alongside classical systems, sharing parts of the computational workload efficiently; a model often referred to as hybrid quantum computing. This means factoring in the cost of classical control electronics, which are required for qubit operations, error correction, and system control. These figures do not even begin to account for the ongoing resources required to maintain such systems or operate large-scale quantum workloads. This includes human resources, lab facilities, and significant energy consumption; much of which stems from the heat generated by the electronics operating inside the cryostat and the heat carried through the connecting cables [29].

Given these factors, and as supported by several sources [12, 34, 35], it is a reasonable assumption that some degree of secrecy must be expected, and that any cryptographically relevant capability would likely be held by nation states, rather than commercial actors for some time.

Chapter 3

Methodology

This thesis adopts a qualitative and exploratory research design, collecting and interpreting information through document analysis, open-source threat intelligence, and expert interviews. To strengthen credibility, the thesis uses triangulation by cross-checking findings across multiple sources and methods [36]. The expert interviews supplement the gaps in documentation, clarify ambiguous areas, and offer professional interpretations of uncertainties and likely future developments. During the work on the thesis, AI-tools have been used for text assistance and spell checking. The declaration of AI use is attached at the end of the thesis.

3.1 Document Analysis

The research foundation for this thesis includes government strategies, policy documents, and national plans from Norway, the EU, China, Russia, and the United States, as well as academic literature analysing their strategic cultures and historical trajectories. These sources provide insight into how different states prioritise quantum technology development and how they frame the need to protect themselves against the cryptographic risks posed by future quantum computers. They also form the basis for assessing how far various actors have progressed in the so-called “quantum race”, and for evaluating how such capabilities may strategically be used once they emerge. The countries examined in this analysis are the United States, the European Union, China and Russia. These countries were selected based on being leading actors in the quantum race. Russia and China are frequently portrayed as strategic competitors to the West, with potential ambitions to use advanced technologies as tools in power politics and security policy. Together, these countries frame the geopolitical and technological landscape relevant for this study.

This thesis also relies on qualitative document analysis of technical sources related to quantum technology, cryptography, and digital security. These documents clarify the technical foundations of quantum computing, its implications for cryptographic systems, and the countermeasures, including the transition to post-quantum cryptography. Secondary sources were used to interpret and contextualise the technical material, helping to identify assumptions, uncertainties, and implementation challenges. Insights from the document analysis informed both the design of the interview guides and the structure of the threat assessment, particularly by highlighting areas where policy documents are incomplete and where expert interpretation is needed.

3.1.1 Threat Intelligence Sources

The study incorporates threat intelligence sources that monitor and categorise nation-state threat actors. These sources identify groups, assign them cluster names, and track their historical activity, including tactics, techniques, and procedures (TTPs), to support attribution and guide defensive measures. Such material is valuable for understanding patterns of behaviour, although it naturally contains some uncertainty. Attribution of cyber operations to a specific group or state is challenging, and naming conventions differ across intelligence vendors and public repositories. In this thesis, publicly documented state-linked threat actors associated with Russia and China were examined. The purpose was to identify recurring targeting patterns such as preferred sectors, regions, and operational objectives, and to compare these patterns with the strategic motivations described in the geopolitical and academic literature. This forms part of the broader threat assessment, helping to evaluate which sectors or countries may be of greatest interest to these states, and where future quantum capabilities should they emerge, might plausibly be applied.

3.2 Expert Interviews

Given that this study deals with a high degree of uncertainty, speculation, and technical complexity, and that threat assessments by nature require nuanced judgement, it was considered necessary to explore the topic in more depth through expert insight. For this reason, the study includes semi-structured qualitative interviews with experts in the field. This method also enables deeper exploration of the informants' own experiences and perspectives.

3.2.1 Design and Conduct of the Interviews

The informants were presented with different questions based on their professional role and area of expertise. For example, the quantum technology expect was asked about technological development and the feasibility of large-scale quantum machines, while the informant from Norway's National Security Authority (NSM) was primarily asked about national preparedness and risk assessments. The prepared interview questions are provided in Appendix A. Additional follow-up questions were asked during the interviews to clarify responses and explore themes raised by the informants, and are therefore not fully captured in the appendix. The goal was not to obtain uniform responses, but to identify patterns and differences in how experts conceptualise the quantum threat, shaped by their distinct backgrounds, practical experience, and institutional context.

The interviews were conducted primarily through Microsoft Teams, with three participants interviewed digitally. Two interviews were conducted in person. Each interview was planned to last approximately 45 minutes. The actual duration varied depending on the respondents' level of detail and engagement, ranging from 35 minutes to one hour and 15 minutes. During the interviews, audio recordings were captured and used for transcription. These recordings were deleted immediately after the transcripts were completed.

3.2.2 Respondents

The informants were selected through purposeful sampling based on their professional expertise and relevance to the research questions. Because the thesis focuses on Norway's transition to post-quantum solutions, it was essential to include experts with insight into national strategies and migration efforts. Therefore, a representative from the Norwegian National Security Authority (NSM) was interviewed, as they possess in-depth knowledge of national preparedness. To complement the national perspective, an expert from a private IT consultancy firm specialising in information security and advising Norwegian organisations on PQC readiness was also interviewed. This provided insight into how the industry interprets the quantum threat, how clients respond to it, and what challenges are seen in practice. Additionally, representatives from a Norwegian critical infrastructure organisation was included to shed light on practical considerations for sectors with long-lived systems and strict security requirements. Finally, an expert in quantum technology from a global technology company was interviewed to contribute a technical perspective on the state of quantum computing development and remaining barriers.

Table 3.1: Overview of respondents and their expertise

ID	Affiliation	Expertise	Interview Format
R1	The Norwegian National Security Authority (NSM)	Cryptography and information security	Online
R2	Global technology company	Quantum technology	Online
R3	Private IT consultancy firm	Information security	Online
R4	Public critical infrastructure	Information security	In-person
R5	Public critical infrastructure	Information security	In-person

3.2.3 Ethical and Legal Considerations

As this study concerns sensitive topics related to national security and involves a degree of speculation due to the emerging nature of the quantum threat, it was necessary to conduct ethical and legal assessments before beginning the research. These included considerations related to anonymity, informed consent and voluntary participation, and the risk of potential identification. The aim was to ensure that informants could share their views freely and without concern for unintended exposure. All names were anonymised, and participants' specific roles were described only at a general level to reduce recognisability. Organisational affiliations were also generalised, apart from NSM, where the use of the institutional name was agreed upon.

The project was reported to Sikt's data protection services, which is the national body responsible for assessing research projects that process personal data in Norway. All participants received a written consent form outlining the purpose of the study, contact information, how their role and affiliation would be presented, how the data would be stored and handled, and their right to withdraw at any time without providing a reason. All data collected in the expert interviews was stored and processed in accordance with NTNU's guidelines for the processing of personal data [37].

3.3 Threat assessment method

Because quantum-enabled threats involve significant uncertainty and limited empirical data, this thesis applies a qualitative likelihood assessment based on the standardised national scale used in Norwegian threat assessments. The categories,

described in table 3.2, are used to express the probability of the threat happening in Norway. The placement on this scale is informed by three analytical factors commonly used in intelligence analysis; **(1) capability**, describing what the relevant state actors could realistically achieve given their technological development, secrecy practices, and historical cyber offensive operations, **(2) intent**, whether the actor has strategic motivations or historical behaviour that suggests an interest in targeting Norway, and **(3) opportunity**, the degree to which Norwegian infrastructure, dependencies or vulnerabilities present exploitable openings, also considering PQC migration efforts completed and planned.

This capability–intent–opportunity (CIO) framework makes it possible to integrate technical cyber-security considerations with broader geopolitical and strategic dynamics. By combining these perspectives, the analysis provides a structured basis for assessing how serious the quantum threat is for Norway.

National standard (likelihood)	**Description**
Very likely	There is very strong reason to expect the event to occur.
Likely	There is good reason to expect the event to occur.
Possible	The event is as likely as it is unlikely.
Unlikely	There is little reason to expect the event to occur.
Very unlikely	There is very little reason to expect the event to occur.

Table 3.2: Qualitative likelihood categories [38].

Chapter 4

The Quantum Race

Quantum technology increasingly appears in national defence and strategy documents, reflecting its role as a key element of great-power competition. It represents both an economic and military asset, shaping future leadership in technology and security [9, 39]. This chapter examines the main actors and investments in the global quantum race to provide an overview of which states are most likely to achieve quantum advantage over modern cryptographic systems. The analysis is primarily based on public investments, national programmes, and research and development strategies related to quantum technologies.

4.1 The European Union

As the second quantum revolution shifts quantum science from theoretical understanding towards practical technologies capable of reshaping the physical world, nations are accelerating efforts to secure leadership in this emerging domain. The European Union is no exception. Europe played a central role in the first quantum revolution, during which many of the foundational discoveries in quantum physics were made [40, 41]. This legacy has strengthened the EU's ambition to remain at the forefront of the next wave of quantum innovation, an ambition articulated clearly in the Quantum Manifesto of 2016, which called for Europe to position itself as a leading actor in the development of quantum technologies [41].

The Manifesto became the political and strategic foundation for what followed: the Quantum Flagship, a 10-year programme launched in 2018 with a budget of EUR 1 billion for collaborative research among Member States [42]. The programme aims to integrate several R&D initiatives within quantum computing, quantum communication, and quantum sensing [9]. The goal in quantum computing is to deploy three quantum computers by 2030, across platforms such

as trapped ions, superconducting qubits, and semiconducting qubits [42].

The EU advances its ambitions through a set of interconnected initiatives. Alongside the Quantum Flagship, these include broader frameworks such as the Digital Decade objectives for technological development and digitalisation, and EuroQCI, launched in 2019 to establish a secure pan-European quantum communication network [43]. The political foundations for these efforts were reinforced through the European Declaration on Quantum Technologies (2023), while long-term priorities are articulated in the Strategic Research and Industry Agenda (SRIA 2030), developed jointly by the European Commission and the Quantum Flagship community [43]. Several broader EU policies also indirectly support quantum technology, such as the Critical Raw Materials Act, which seeks to ensure access to materials for strategic technologies, including quantum hardware [43].

Additional support for quantum projects is provided through broader EU programmes such as the Digital Europe Programme and Horizon Europe [43]. Today, more than 5,000 researchers across the EU are working on the development of quantum technologies, giving the EU the highest density of quantum research activity worldwide [42]. There is also EUR 7.2 billion planned for government funding for quantum technology research. Most of this comes primarily from the EU and France, Germany, the Netherlands and Sweden [42].

The EU aims to develop quantum technologies that reflect European values, such as privacy, transparency, and ethical governance. When combining EU-level funding with national investments, the overall financial commitment to quantum technologies is substantial, estimated at up to EUR 12 billion across Member States and EU programmes [9].

The European Union's main strength lies in its strong national institutions and research programmes across Member States. However, this also exposes one of its key weaknesses: fragmentation. Quantum research and investment have traditionally been distributed unevenly, and often pursued through separate national initiatives. The EU aims to address this lack of coordination through the proposed EU Quantum Act, expected in 2026, which seeks to bring these national efforts under a unified strategic framework [9].

4.2 Norway

Norway has generally not been viewed as a strong driver in the development of quantum technologies. The field has long been characterised by limited national initiatives, insufficient funding, and a lack of coordinated policy direction. In Norway's digitalisation strategy for 2024–2030, the government sets the goal of

making Norway the world's most digitalised country by 2030. However, quantum computing and quantum technologies receive only brief mention, with no concrete measures beyond general references to increased research efforts [44]. Quantum technology requires substantial resources as well as sustained international collaboration, making it difficult for research environments to progress without clear governmental support [43].

Until recently, Norwegian public funding for quantum-related activities was roughly NOK 70 million per year, an amount considered modest. This raised questions about how such funding should be prioritised and which areas should receive emphasis. In mid-2025, the Norwegian Government have announced a national quantum initiative to strengthen its position in the international quantum race. The plan includes an immediate investment of 43 million NOK in research infrastructure, 244 million NOK to be distributed in 2025 to four national centres for quantum technological research, and a commitment of 750 million NOK over five years to develop a Norwegian quantum industry in collaboration with academia and the private sector [45, 46].

A recurring criticism has also been the absence of national guiding principles or a coherent framework for prioritisation. As a result, there has been a strong call for the adoption of a national strategy to provide direction, establish priorities, and support the structured development of quantum technology in Norway [43]. In May 2025, the Norwegian government announced that the Research Council of Norway, Innovation Norway, and the Norwegian National Security Authority have been tasked with developing the knowledge base for a national quantum technology strategy, which is planned to be presented in 2026 [47]. Such a strategy is expected to draw inspiration from its neighbouring countries, as well as the EU and NATO.

Some experts have argued that Norway should not attempt to cover the entire quantum technology landscape, which is far too broad for a country of its size. Instead, Norway is encouraged to identify a strategic niche where it can realistically build world-class expertise, quantum sensing is mentioned as a promising candidate, and to let this specialisation guide future funding and capability development [43].

Given Norway's close alignment with both the EU and NATO, it is natural that its approach to quantum technologies will be shaped by broader European and transatlantic priorities. Norway has also tried to benefit from EU-driven quantum initiatives, taking part in funding programmes such as Digital Europe and Horizon Europe, which support quantum-related projects [43]. However, Norway is at a disadvantage compared to full EU Member States, as it cannot access several EU initiatives, such as the European Declaration on Quantum Technologies, the EuroQCI programme, and certain quantum-focused funding instruments. Even in programmes where Norway does participate, such as the Digital Europe Pro-

gramme, the Norwegian government does not provide the national co-funding required for participation. As a result, Norwegian companies, universities, and research institutes must sometimes finance the entire national share themselves, which makes participation significantly more difficult and has led to low involvement [43]. Without this support, Norway misses out on substantial EU funding that could have been obtained through stronger participation in these programmes.

In contrast, our nearest neighbours, Sweden, Finland, and Denmark, have moved further ahead in quantum technology and are making greater use of EU funding instruments in this field. Norway is collaborating with other Nordic countries through the Nordic Council of Ministers, which focuses on joint solutions where cross-country cooperation can achieve better results than individual national efforts [44]. In May 2025, the Nordic Prime Ministers issued a joint statement emphasising the need to strengthen Nordic collaboration in quantum computing, communication, and cryptography. The statement, endorsed by Norway, highlights a regional commitment to coordinate on quantum security and to ensure that supply chains related to quantum technologies adhere to standards promoting security, trust, and privacy [48]. Nordic collaboration would not only benefit Norway but also help elevate the Nordic region's overall position in quantum technology.

4.3 USA

Quantum technology in the United States is largely shaped by market-driven innovation, where private tech firms and startups play the leading role in advancing the field. The country now hosts over 150 quantum-focused companies, with around one-third dedicated specifically to quantum computing [34]. Major technology firms such as IBM and Google, together with startups like IonQ, have been central to developing early quantum computing prototypes and pushing the technology toward commercial viability [9].

The federal government plays an important coordinating role, primarily by facilitating collaboration between industry, academia, and national laboratories through initiatives such as the National Quantum Initiative Act [9, 49]. In 2016, the National Science and Technology Council (NSTC) called for a coordinated national approach to advance quantum technologies. This was followed by new federal initiatives, including the National Science Foundation's Quantum Leap programme and the Department of Energy's QuantISED initiative, which expanded quantum research across U.S. universities and national laboratories [34]. The 2018 National Quantum Initiative Act (NQIA) then formalised a unified national framework for quantum research [9, 34, 49]. The Act also established the National Quantum Coordination Office to oversee federal civilian quantum activities and

enabled institutional mechanisms such as the National Institute for Standards and Technology's (NIST) Quantum Economic Development Consortium (QED-C), designed to strengthen cooperation between government, industry, and academia. In total, federal spending on Quantum Information Science between 2021 and 2024 is estimated at approximately USD 5.1 billion [34].

The country's strong venture capital culture and well-established innovation ecosystem encourage investors to take greater technological risks, enabling rapid progress, particularly in quantum hardware development. As a result, U.S. companies like IBM and Google currently operate some of the most advanced quantum processors in the world. The American approach is characterised by open innovation and cross-sector collaboration, and as a driver of scientific and economic competitiveness [35, 50].

The United States is often portrayed as the leading actor in the quantum race, particularly in areas such as theoretical research, quantum error correction, and hybrid quantum–classical integration [35, 50]. Several recent milestones highlight this position. Google has demonstrated a 105-qubit superconducting processor with built-in error-correction features, while QuEra has produced a 256-qubit neutral-atom quantum computer. IBM has also set ambitious targets, including a roadmap toward a fault-tolerant quantum computer by 2029 with an estimated 200 logical qubits [34, 51].

This decentralised, industry-driven model gives the United States a significant advantage by enabling many parallel efforts, each pursuing different technical approaches and therefore increasing the likelihood of breakthroughs. At the same time, this diversity comes with trade-offs: knowledge, hardware, and software developed within one corporate ecosystem are not always compatible with those of others, or even disclosed, making it more difficult to scale solutions or transfer advances across platforms [34].

4.4 Russia

While Russia inherited a strong Soviet legacy in physics and sciences, the collapse of the Soviet Union in 1991 led to a dramatic decline in scientific capacity. Research funding fell by nearly 90% and many of the country's leading scientists emigrated in search of better opportunities [8, 9]. Nevertheless, Russia has publicly stated ambitions to be among the global leaders in quantum computing, backed by a government-approved roadmap, dedicated funding, and initiatives aimed at building human capital and infrastructure [52–54]. Russia has introduced mega grant programme that provide substantial funding for internationally recognised researchers to establish research groups at Russian universities [55]. Its regulatory concept also emphasises the use of grants to bring high-level for-

eign specialists into the country [56]. Furthermore, the 2025 quantum roadmap outlines concrete plans to strengthen domestic human capital by upskilling local experts in key quantum fields [52].

Russia has pursued quantum research through a number of independent initiatives since around 2010. According to Russian press reports, in 2016, the Ministry of Education and Science of the Russian Federation approved a state project to develop the country's first quantum computer, supported by an initial allocation of 750 million rubles [57]. The country's quantum technology development is led by the Russian Quantum Center (RQC) and the National University of Science and Technology (MISiS), but overall coordination is carried out by Rosatom, the state nuclear corporation [9, 55]. In this broader national framework, other state institutions also play key roles; Russian Railways (RZhD) leads the development of quantum communication infrastructure, while Rostec oversees advances in quantum sensing and metrology [55, 57].

Between 2020 and 2024, Russia implemented a state-backed initiative for quantum systems amounting to approximately $790 million USD. As part of this programme, in 2024 it unveiled two 50-qubit quantum computer prototypes, based respectively on rubidium neutral atoms and ytterbium ions [9, 58]. Rosatom stated that in 2022; Russia's technological lag in quantum computing was estimated at 10–15 years behind the global leaders. The subsequent national initiatives and roadmap were designed to significantly narrow this gap to 2–3 years by 2025, with the long-term ambition of positioning Russia as a competitive actor, and eventually a leader in quantum computing [59].

The new roadmap up to 2030 was announced in August 2025, with Rosatom designated as the responsible organisation. Among its technical targets is the creation of a 300-qubit quantum computer [52, 54]. The state budget is reported to provide 29 billion Rubles, approximately 305 million USD [52]. It is, however, worth noting that these figures do not tell the full story. Russia is a highly restrictive state, and a significant share of federal budget spending is classified and therefore not reflected in publicly available data [60]. The Rosatom Quantum Accelerator programme indicates that the current objective is to translate the quantum technologies developed during the 2020–2024 roadmap into commercially viable products and to establish an operational quantum computing service by 2030 [52].

The quantum research in Russia is primarily state-controlled and reliant on public funding, with limited participation from private startups. The *Concept for Regulating the Quantum Communications Sector in the Russian Federation up to 2030* [56] places quantum technology development and research under strong state direction, stating that its infrastructure is to be optimised and shared between organs of the unified system of public authority, while the sector's development is to be guided through comprehensive state support. It also explicitly notes that the

Concept is subject to revision *"on the basis of the level of development of quantum technologies, as well as of the decisions and actions of foreign states and territories that commit unfriendly actions in relation to the Russian Federation, legal entities and natural persons"* [56].

Due to the international sanctions and export limits imposed on Russia after its 2022 invasion of Ukraine, access to materials and components necessary for quantum computing, such as superconducting electronics, has become more limited [9]. For instance, cryocoolers, which are necessary for maintaining cryogenic temperatures in quantum systems, are primarily manufactured in the United States, Europe and Japan [9, 61]. That makes Russia dependent on Chinese suppliers and parallel import networks, as its own domestic production base remains too limited to sustain large-scale quantum hardware development [9].

Russia appears to approach quantum technologies primarily through a national security lens, with the development of quantum computing framed largely as a response to the perceived "quantum threat" and the need to protect critical national interests. Quantum technology is thus presented not only as a technological endeavour, but as a strategic project tied to sovereignty and security. Although Russia is not currently on par with leading actors such as the United States and China, its stated ambition is to narrow this gap significantly. At the same time, the roadmap's goals appear highly ambitious, and Russian experts themselves call for a more realistic assessment of the country's quantum plans, arguing that a universal quantum computer by 2030 is unlikely [62]. How far Russia will succeed in implementing these objectives remains uncertain.

4.5 China

China has made the development of quantum technology a national priority and has been investing in this field for more than three decades, with its first experimental research initiatives beginning in the 1990s [9, 63]. Estimates suggest China has so far invested over USD 15 billion in the field of quantum computing [9, 49, 64]. The early stages of China's national quantum programme have primarily focused on quantum communication, where the country holds a significant global lead and is expected to be the first area of quantum technology to reach large-scale practical application [63]. Much of this effort aims to secure communication infrastructure through quantum key distribution (QKD), motivated by an ambition to protect sensitive information from interception by foreign intelligence services [34].

China integrates quantum technology directly into its long-term national planning systems, where major science and technology priorities are set through five year-plans (FYPs) [34]. The 14th Five-Year Plan (2021–2025) placed quantum

technology as a national strategic priority, second only to artificial intelligence. In March 2025, China announced the establishment of a new government fund worth over 138 billion USD to support strategic technologies, including artificial intelligence, quantum technology, and hydrogen energy storage, although the specific share allocated to quantum remains unknown [49, 50, 65].

The coordinated system has provided the resources and institutional support needed to accelerate China's progress in quantum technologies. One example is the Jiuzhang photonic quantum computer developed at the University of Science and Technology of China (USTC) in 2020, which demonstrated performance beyond the reach of classical supercomputers. USTC built on this success with the Zuchongzhi superconducting processor in 2021, first introduced as a 66-qubit device demonstrating quantum advantage and later expanded into a 176-qubit system with significantly enhanced capabilities [34, 50]. Commercialisation efforts followed quickly after these breakthroughs. In 2024, China announced the Tianyan state-run quantum cloud platform for research, and in 2025 USTC introduced the Zuchongzhi-3 superconducting processor for commercial use [34].

Some major companies, including Alibaba, Baidu, and Huawei, as well as a handful of startups, have also contributed to the field. However, many of these private initiatives remain underfunded, and both Alibaba and Baidu have transferred their quantum research and facilities to public research institutions, which indicates an effort by the Chinese government to centralise control and oversight of quantum innovations [35].

A common observation is that China remains behind the United States in quantum computing development. While this may hold some truth, John M. Martinis, the 2025 Nobel laureate in Physics, described the gap as only "nanoseconds" [66]. In reality, it is difficult to determine the true position of China in the quantum race, since reliable data on China's quantum computing remain limited, as the level of commercial activity and investment transparency is low [9, 49, 64]. While China actively participates in international cooperation between research institutions, universities, and private companies to gain access to global resources and research infrastructure, it is more restrictive and secretive when it comes to its own findings and technological breakthroughs [35]. The U.S.–China Economic and Security Review Commission [34] reports that this lack of visibility is intentional, arguing that China is pushing aggressively toward cryptographically relevant quantum computing while obscuring key aspects of its progress.

4.6 Findings

The global quantum race is shaped by diverging political systems, strategic priorities, and technological capacities. The United States appears to currently hold

a narrow lead in quantum computing, driven by a dynamic private sector, strong research institutions, and coordinated federal investment [9, 35]. China follows closely behind with massive state funding, centralised coordination, and an integrated civil–military ecosystem that rapidly translates scientific progress into strategic capability [9, 35]. The US openness to sharing can also inadvertently expose sensitive research to foreign competitors, particularly China, which is highly active in global research networks but less forthcoming about its own findings. Consequently, China appears determined to close this technological gap as quickly as possible.

Russia, while significantly behind both China and the United States, is attempting to accelerate its development through state-led initiatives coordinated by Rosatom. Their ambitions, however, are widely viewed as highly optimistic and potentially unrealistic given Russia's economic constraints and technological lag. While Russia remains significantly behind both China and the United States in terms of technological development, it maintains close cooperation with China across technological, defence, and economic domains. This relationship could potentially allow Russia to access resources, expertise, and infrastructure that it would otherwise lack, thereby positioning it closer in the quantum race than commonly anticipated. Although there is currently no evidence of direct collaboration on fault-tolerant quantum computing, the partnership represents a plausible scenario that cannot be entirely ruled out, suggesting that Russia may gain an indirect quantum advantage through its ties with China [67]. While Russia's reliance on China has grown substantially, the dependence is largely asymmetrical. China, in contrast, is far less economically dependent on Russia and tends to calibrate its behaviour pragmatically to avoid actions that could cause significant economic or diplomatic costs. Beijing seeks to maintain its image as a responsible global actor, which limits the extent to which it fully aligns itself with Moscow [68].

Europe occupies a distinct position. The European Union's focus on quantum technology is primarily driven by its pursuit of technological sovereignty and strategic autonomy. The EU tends to take a cautious and values-driven approach to emerging technologies. Much like with AI and data protection, Europe prioritises privacy, ethics, and regulatory oversight, even if this sometimes slows the pace of innovation. This reflects a form of pre-emptive governance, where the EU seeks to anticipate challenges and guide development responsibly rather than reacting afterwards [9]. Although Europe may lag behind China in investment and the United States in pace of innovation, it seeks to develop quantum technologies consistent with its commitments to strategic autonomy, ethical integrity, and technological sovereignty.

Chapter 5

Security Imperatives in Quantum Development

This thesis hypothesises that the first state to achieve quantum advantage will likely leverage it to advance its strategic objectives, rather than treating it as a global public good. This raises a central question: what potentially adversarial strategic motivations drive countries such as China and Russia in their pursuit of quantum technologies? The following section examines these issues. This chapter focuses on the strategic logic that shapes state behaviour and on observed patterns in state-linked cyber operations, as these provide the most concrete indicators of how Norway may be targeted in practice.

5.1 Chinese Strategic Motivations

The century of humiliation, referring to the period of the 19th and 20th centuries during which the country experienced significant territorial loss and foreign actors dominated their trade and politics, contributed to the shaping of modern Chinese politics [69]. The formation of the People's Republic of China (PRC), ruled by the Chinese Communist Party (CCP), marked the beginning of an effort to re-establish China as a significant international actor [69]. The period before the Century of Humiliation is often framed as China's golden age, and the CCP's goal of returning to that status remains central to its policy [69]. In its efforts to rebuild and develop the country, the CCP has recognised the need to strengthen its technological capabilities, with control over information regarded as a central pillar of maintaining political power. The Chinese People's Liberation Army (PLA), is the largest active-duty military in the world and has been developing its cyber capabilities [70].

"Informationised warfare" (xinxihua zhanzheng) refers to the digitisation and integration of information and communication technologies (ICT) into the economy, politics, and military affairs. In such an environment, states gain access to each other's systems through information technologies, which creates new threats to national security. This is not limited to technical means such as for example spreading malware, but the information itself can also become a threat, such as if the public opinion pressures political leaders into conflict. As societies have become increasingly informationised, the state and the military are likewise required to develop informationised capabilities to maintain control and to counter threats [70].

With the fall of the Soviet Union in the 1990s, Chinese scholars describe it as a failure of the Communist party to control information and uphold its vanguard role. With the lessons learned from the Soviet experience, the CCP sees information as vital both to the national interest and to the survival of the Communist party in China [70]. Information dominance also applies in the broader competition between states. It requires the ability to gather, analyse, and exploit intelligence in a timely manner while preventing adversaries from doing the same, both to achieve national objectives and to safeguard national interests. According to Chinese scholars, these abilities will also be decisive in determining who prevails in a future war. In times of conflict, there is little opportunity to build these capacities, which is why preparation for informationised warfare must take place primarily during peacetime [70].

5.2 Russian Strategic Motivations

Russia is frequently portrayed as the principal adversary of European security and the North Atlantic Treaty Organisation (NATO), a public perception that has intensified following Russia's invasion of Ukraine in 2022 [71–73]. Russia's contemporary strategic objectives reveal a persistent ambition to reclaim the power and status once held by the Soviet Union and to transition from a regional power to a leading global actor. This aspiration is rooted in a belief that Russia possesses a historic and spiritual entitlement to great-power status, derived from its civilisational heritage, economic potential, and long-standing geopolitical influence in Eurasia. At its core, Moscow seeks to re-establish itself as the natural hegemon of Europe and the broader Eurasian space [71–73]. While this perspective is not universally shared among all Russian elites, there is a broad consensus that Russia should exert a degree of control over its geopolitical environment and maintain influence across the territories of the former Soviet bloc [71].

Russia's invasion of Ukraine reflects not only a desire to prevent Ukraine's alignment with the West and preserve influence over a closely linked neighbour, but also a deeper sense of strategic vulnerability that has defined Russia's per-

ception of the West for centuries. As Götz and Staun [71] point out, part of this sense of vulnerability stems from Russia's vast geography. The country's size and long borders make it virtually impossible to defend all its territory at once. Historically, the country has repeatedly been invaded from the West, most notably by Napoleonic France in the early nineteenth century and Nazi Germany during the Second World War. These experiences, followed by decades of confrontation with the United States and NATO during the Cold War, have entrenched a strategic worldview in which the West is perceived as Russia's primary source of threat [71].

Russia perceives the West as a fundamental obstacle to its aspiration of restoring great-power status, which it regards as a historical and civilisational right. In Moscow's view, Western influence prevents it from re-establishing dominance over the post-Soviet region, an area it considers its legitimate sphere of privileged interests [73]. After the invasion, Russia grew more worried about the expanding military cooperation between Ukraine and Western countries, such as joint exercises and training missions, through EU and NATO programmes. Putin has said that if NATO establishes a military presence in Ukraine, it will stay there permanently, which Russia sees as a major security threat. This growing cooperation has made Moscow even more fearful of an external attack and Western influence near its borders [71].

These strategic objectives are reflected not only in military and diplomatic behaviour, but also in cyber operations, where espionage, coercion, and disruption can be pursued below the threshold of armed conflict.

5.3 Offensive Cyber Operations

Since the escalation of the war in Ukraine, Russia has increasingly adopted a wartime cyber posture, marked by more frequent, coordinated, and at times destructive operations [7]. Many of the most capable threats are linked to state-attributed actors, commonly described as advanced persistent threats (APTs). Open-source threat reporting often associates several prominent Russian cyber groups with the country's intelligence and security services, including the Main Intelligence Directorate (GRU), the Foreign Intelligence Service (SVR), and the Federal Security Service (FSB) [74].

GRU-attributed activity is frequently described as more operationally aggressive, including disruptive operations and attacks on government and critical infrastructure [75–80]. In Ukraine, Russian-linked actors have repeatedly demonstrated a sustained interest in the energy sector, including attempts to disrupt electricity supply and industrial operations. Beyond Ukraine, Russian operations have also targeted Western states, where activity is more consistently associated with

intelligence collection and long-term access. By contrast, SVR-attributed operations are often discussed primarily in terms of strategic espionage [81, 82]. A well-known example is the SolarWinds supply-chain compromise in 2020, which enabled access to numerous government agencies and private companies via tampered network management software [82]. FSB-attributed activity is similarly commonly characterised as covert intrusion and intelligence collection, particularly against governmental and defence-related targets [83–88].

Overall, Russia's targeting is heavily shaped by the war in Ukraine and Russia's increasingly confrontational relationship with NATO and other Western states. In this context, disruptive operations have been especially visible in Ukrainian critical infrastructure, while espionage operations remain a persistent feature of activity directed at NATO member states, including Norway [89]. Russia has also increasingly used disruptive cyber activity against European entities, including Norway, to create insecurity and exert pressure below the threshold of of armed conflict [38].

China's cyber activity is frequently described as being dominated by espionage and long-term access operations, particularly against government institutions and technology-intensive sectors [89, 90]. A distinguishing feature in public assessments is the extent to which state-linked operations can involve a broader ecosystem of actors (including commercial entities) operating in alignment with state objectives, often associated with China's security and intelligence apparatus, including the Ministry of State Security (MSS) [90, 91]. In practice, this is reflected in the large number of distinct Chinese threat groups identified in open-source reporting. MSS functions as a central actor in China's cyber-espionage apparatus, and some reporting suggests that China's focus on large-scale cyber collection intensified after the Snowden disclosures increased Chinese awareness of U.S. intelligence capabilities [92].

China's targeting is broad: while it heavily prioritises the United States, it targets a wide range of countries and sectors, with government institutions and technology firms among the most frequently affected [89]. For a small state like Norway, this implies that being a "secondary" target does not necessarily reduce exposure: access operations aimed at larger allies, suppliers, or shared platforms can still create significant spillover risk.

This targeting can be explained by the concept of "civil-military fusion" (军民融合), where civilian and military domains are intertwined. Cheng [70] highlights three main motivations for such targeting: first, to gather human intelligence; second, to exploit specific technologies or expertise for China's own development; and third, to address commercial concerns. According to Cheng [70], the objectives of Chinese espionage operations include:

- mapping and understanding adversaries' plans, structures, capabilities, meth-

ods, locations, and vulnerabilities;
- assessing the capabilities and communication networks of military systems, especially air defence forces, and identifying weak points;
- analysing the psychology and behavioural patterns of commanders and personnel within military units;
- identifying facilities and infrastructure that could be used for military or information operations; and
- evaluating the physical and natural conditions in potential battlefields.

Overall, the pattern reflects an information-warfare approach aimed at gathering extensive data across many domains, "information about everything and everyone", so that it can be exploited whenever strategically necessary. As Cheng [70] notes, the PLA seeks to identify vulnerabilities not only of the United States but of all potential adversaries.

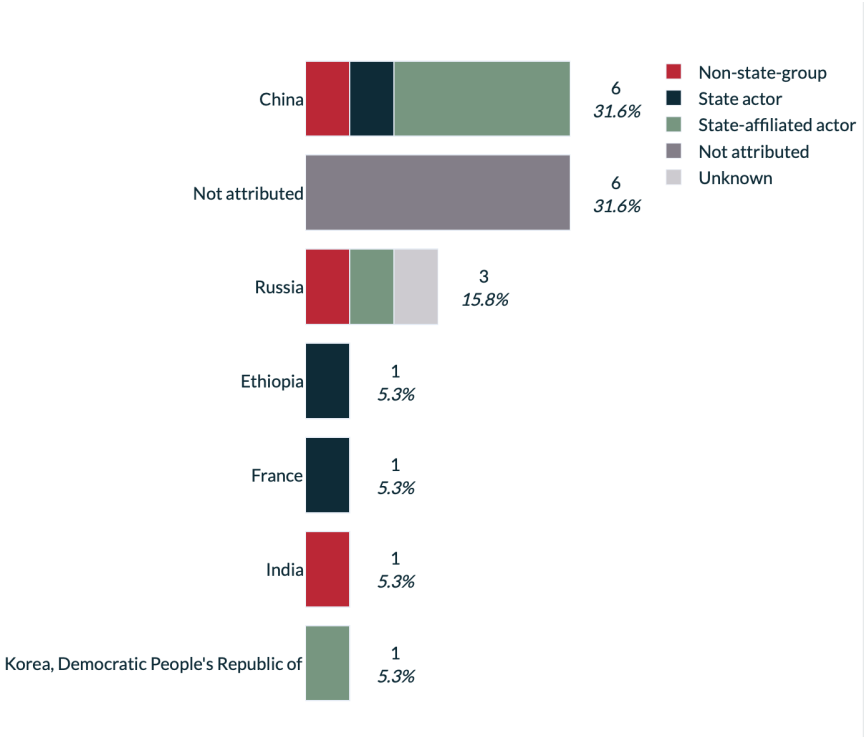


Figure 5.1: *Main countries of origin of cyber incidents against Norway* [93].

Between 2000 and 2025, publicly reported cyber incidents involving Norway in the European Repository of Cyber Incidents (EuRepoC) [93] suggest that data theft is the most frequently recorded incident type, and that China is the most common publicly attributed country of origin among the incidents that are attributed.

However, a substantial share of cases in open-source incident datasets are not attributed, and EuRepoC necessarily reflects what becomes visible through public reporting rather than the full underlying activity. This creates systematic bias: covert, state-affiliated espionage operations are designed to remain undetected and may therefore be under-represented, while smaller or less publicised incidents may never enter the dataset at all.

5.4 Norwegian Perspective

The arctic region is where Norwegian, Chinese and Russian security interests most directly intersect. Already in 2007, Vladimir Putin highlighted the Arctic as central to Russia's ambition to reclaim great-power status. Although the 1920 Svalbard Treaty granted Norway full sovereignty over the archipelago, Russia has repeatedly challenged this sovereignty, through political statements, media narratives, joint military exercises with China, and diplomatic pressure [94, 95].

Svalbard's location makes it uniquely valuable for civilian and scientific purposes. Its high-Arctic latitude allows environmental monitoring, including measurements of radioactivity. Because Svalbard is so far north, almost all satellites that orbit from pole-to-pole pass directly over it. This makes it one of the few places where they can send down data every time they go around the Earth [94]. For that reason, Svalbard has become an important site for satellite communication. The Svalbard Treaty prohibits Norway from establishing military installations on the islands, and Russia has repeatedly argued that Norway's satellite facilities breach the treaty because such capabilities could, in theory, support military operations. Norway rejects this view, and the issue remains a grey zone [94].

Svalbard also lies near two important sea passages that link the Arctic Ocean with the North Atlantic. Because these corridors are important for moving allied ships and supplies, any Russian attempt to assert control over the area could hinder NATO's ability to operate between the Arctic and the Atlantic and potentially obstruct transatlantic reinforcement in a crisis [94].

China has also shown growing interest in the Arctic region. As part of its broader ambition to become both a global and "polar" power, China has sought to expand its presence by purchasing land, investing in infrastructure, and establishing companies in the region [94–96]. For China, the Arctic offers several strategic benefits: access to natural resources, opportunities to participate in the emerging Arctic trade routes, and a way to strengthen its long-term geopolitical foothold in the High North [95].

While Svalbard illustrates how geography drives strategic competition in the High North, Norway's exposure is also tied to critical infrastructure that connects

the region to Europe, most notably energy supply. The war between Russia and Ukraine fundamentally reshaped Europe's energy landscape. Before 2022, Russia was the EU's largest energy supplier, but sanctions and reduced Russian exports forced European states to seek alternative sources. As a result, Norway had to fill part of this gap and has become the EU's largest energy supplier, now holding more than half of Europe's total reservoir capacity [10, 97]. The green transition and global climate policies mean that Norway is becoming more reliant on renewable technologies, a sector in which China is the world's dominant producer. This growing dependence on Chinese-made green technology introduces vulnerabilities into critical infrastructure and creates potential avenues for coercion, surveillance, or espionage, a dynamic described in the literature as "weaponised interdependence" [97].

Norway's expanded role as Europe's primary energy supplier, makes the Norwegian energy sector an attractive target for Russian sabotage [38], while its growing dependence on Chinese technology increases vulnerabilities that could be exploited [97]. In addition, Norway's close alignment with the United States and strong support for Ukraine further place it at strategic odds with both Russia and China.

Chapter 6

Post-Quantum Defence and Norwegian Initiatives

The acceleration of the global quantum race has raised serious concerns about the long-term viability of today's cryptographic systems. This has led to the emergence of post-quantum cryptography (PQC), a set of cryptographic schemes designed to remain secure even against quantum-capable adversaries. This section examines the current state of PQC development, the main families of algorithms proposed as replacements for quantum-vulnerable cryptography, and the mathematical foundations that make them resistant to quantum attacks. This section also explores the practical barriers to PQC adoption. Drawing on expert interviews, it provides an applied perspective on how the quantum threat is currently understood within Norwegian organisations and highlights where the greatest vulnerabilities and migration challenges are expected to arise.

6.1 Post-Quantum Cryptography (PQC)

Post-quantum cryptographic algorithms derive their security from mathematical problems that are believed to be infeasible even for quantum computers. These schemes fall into several main families, including lattice-based, code-based, hash-based, isogeny-based, and multivariate cryptography. The U.S. National Institute of Standards and Technology (NIST) began investigating PQC around 2012 and, in 2016, launched an open international standardisation project to identify new public-key encryption and digital signature schemes that would remain secure once quantum computers are strong enough to break current systems [16, 98, 99]. By the end of 2017, NIST had almost 70 prominent candidates for post-quantum cryptography [98]. In 2022, NIST announced the first set of algorithms selec-

ted for standardisation: CRYSTALS-Kyber for key establishment and CRYSTALS-Dilithium, FALCON and SPHINCS+ for digital signatures [98, 99]. By 2024, three PQC standards had been formally published as FIPS 203 (ML-KEM), FIPS 204 (ML-DSA) and FIPS 205 (SLH-DSA). In parallel, NIST has continued work on additional algorithms [98, 99]. NIST has also opened a separate process for additional digital signature schemes, for which around 40 proposals were submitted and are now being evaluated in successive rounds [99].

Lattice-based Cryptography

Lattice-based cryptography relies on mathematical objects called lattices, which arise from group theory. A lattice can be viewed as a set of regularly spaced points in an n-dimensional grid, extending infinitely in all directions [100]. Each point can be reached by taking integer linear combinations of a chosen set of basis vectors, meaning the entire structure is generated from these vectors.

The security of lattice-based cryptography relies on several computational problems believed to remain hard even for quantum computers. Two central examples are the Shortest Vector Problem (SVP) and the Closest Vector Problem (CVP) [101]. SVP asks for the shortest non-zero vector in the lattice, a task that becomes extremely difficult because cryptographic lattices are constructed in very high dimensions, where finding such a vector is computationally infeasible. CVP involves finding the lattice point closest to a given target vector, and the number of possible candidates grows exponentially with dimension, making the problem computationally infeasible [102]. An additional challenge in lattice-based cryptography comes from the learning with errors (LWE) problem. LWE deliberately adds small random noise to a system of linear equations. This added noise significantly increases the difficulty of the problem by obscuring the true values of the unknown variables, and making it hard to separate the error from the underlying data [101].

Two of the standards selected by NIST are lattice-based. ML-KEM, derived from CRYSTALS-Kyber, is a key encapsulation mechanism that enables two parties to establish a shared secret [24, 99]. ML-DSA, derived from CRYSTALS-Dilithium, is a digital signature scheme [3, 98, 99]. An additional signature standard based on FALCON, a lattice-based digital signature algorithm, is under development as draft FIPS 206, [99].

6.1.1 Code-based Cryptography

Code-based cryptography is grounded in coding theory, which studies how to detect and correct errors that occur when data is transmitted over noisy channels.

In this approach, messages are encoded using linear codes, often with extra redundancy added so that a receiver equipped with the proper decoding algorithm can recover the original message even if some errors occur. These error-correcting codes act as a one-way transformation: while encoding is straightforward, decoding a randomly chosen linear code without the secret structure is difficult even for quantum computers [14, 103]. The security of code-based crypto schemes relies mainly on problems such as Syndrome Decoding (SD) and Learning Parity with Noise (LPN) [103]. LPN is the code-based analogue of the LWE problem in lattice cryptography. In LPN, one must recover a hidden binary vector from linear equations that have been deliberately perturbed with random noise [14, 16, 104]. The SD problem involves finding the error vector that generated a given syndrome. A syndrome can be understood as the parity-check output associated with a received word [103]. The syndrome is computed by applying a parity-check matrix to a received word, which may contain errors. Because many different error patterns can lead to the same syndrome, determining which one was applied becomes extremely hard [105].

Code-based cryptography has therefore emerged as a strong candidate for post-quantum security. In 2025, NIST announced that HQC, a code-based Key Encapsulation Mechanism, whose security derives from the decisional version of the syndrome decoding problem, was selected as the next algorithm to be standardised, providing a code-based alternative to the lattice-based KEMs already selected by NIST [3, 99].

6.1.2 Hash-based Cryptography

Hash-based cryptography uses cryptographic hash functions as the basis for secure digital signatures. These schemes benefit from the fact that cryptographic hash functions have been studied and deployed for decades. Their security properties are well understood, and the community has extensive experience analysing their behaviour and potential vulnerabilities. This long history provides hash-based post-quantum cryptography with a strong empirical foundation compared with newer constructions [106].

The idea is that a hash function should be easy to compute but difficult to reverse. In practice, three core properties must hold. Preimage resistance refers to the difficulty of finding an input that produces a specific hash output. Second-preimage resistance means that, given one input, it should be infeasible to find a different input that results in the same output. Collision resistance requires that it be computationally impractical to find any two distinct inputs that hash to the same value [103, 106].

In 2024, NIST formally standardised SLH-DSA (FIPS 205), a hash-based di-

gital signature scheme derived from SPHINCS+, whose security relies on the collision resistance of the underlying hash functions [3, 99, 103].

6.1.3 Other PQC alternatives

Isogeny-based cryptography relies on isogenies, mathematical mappings that connect one elliptic curve to another. The security of these schemes comes from the difficulty of determining which specific isogeny connects two given curves [5, 103]. Despite computations on elliptic curves being efficient on a sufficiently powerful quantum computer using Shor's algorithm, finding this "missing link" is believed to be computationally infeasible, as no polynomial-time method is known for recovering it, either classically or on a quantum computer.

One candidate in NIST's Additional Digital Signature Schemes process is a symmetric-based signature scheme. FAEST is built from symmetric primitives, primarily AES and cryptographic hash functions, while still providing public-key style verification. It uses an AES key as the private signing key and publishes a public verification key derived using AES under that secret key; the signature then convinces verifiers that the signer knows the corresponding secret key without revealing it [99, 107].

Another type of post-quantum cryptosystem is multivariate cryptography, which builds its security on the hardness of solving algebraic systems made up of many variables and polynomial equations defined over finite fields [108]. Recovering the secret requires solving these equations, a task known to be extremely difficult in general. Many constructions use quadratic polynomials, leading to what is called the MQ problem. Some variants employ polynomials of higher degree, such as cubic terms, which makes the underlying problem even more complex [108, 109]. Because of this computational difficulty, multivariate schemes are viewed as strong candidates for PQC, with the structure particularly well suited for digital signatures.

6.2 National preparedness initiatives

Although Norway does not yet have a national PQC strategy, several preparatory efforts are already underway. Until a Norwegian roadmap is published, the EU's coordinated implementation roadmap functions as the primary reference point for how Norway is likely to structure its transition to post-quantum solutions.

In April 2024, The European Commission published the *Recommendations on a Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography (PQC)*, developed by the NIS Cooperation Group (NIS-CG) PQC Work

stream [110]. It is the first EU framework guiding Member States on how to transition to quantum safe cryptography. The European Commission's recommendation asks that each EU Member State develop and publish its own national PQC transition roadmap within two years, meaning by April 2026, in accordance with the principles in the Coordinated Implementation Roadmap.

Since the transition to post-quantum cryptography (PQC) is a complex process that depends on factors such as supply-chain readiness and technical prerequisites, the European Commission's recommendation divides the migration into *First Steps* and *Next Steps*, prioritising actions based on each system's quantum risk level - low, medium, and high. The risk level is determined by the time and effort required to complete the PQC transition, the expected impact if the cryptography is breached, and the quantum vulnerability of the cryptographic method used [110]. For example, if the confidentiality and authenticity of data are protected by a quantum-vulnerable cryptographic algorithm, and the data must remain secure for a long period of time, with a significant impact in case of a breach, and if the transition effort is expected to take more than eight years, then the use case is considered high-risk and should be prioritised for PQC transition over others. This is consistent with the way risk assessments and prioritisation are described in other research [12, 111].

The *First Steps* require countries to develop national awareness and communication plans, establish a timeline and implementation plan for the transition, perform quantum risk analyses, map dependencies, create cryptographic asset management systems, and engage with the NIS Cooperation Group's PQC workstream [110]. The overall goal is for the transition of high-risk use cases to be initiated by the end of 2026. By the end of 2030, all EU Member States are expected to complete the PQC transition for high-risk use cases and begin the transition for medium-risk ones, as outlined in the *Next Steps*. By this stage, quantum-safe software and firmware updates should also be enabled by default [110].

As an EEA country, Norway generally implements EU digital regulations and strategies. It is therefore reasonable to expect that Norway will develop a national PQC roadmap broadly aligned with the EU timeline, meaning that the migration of high-risk use cases should be completed by 2030. In the Norwegian context, this primarily affects the organisations that fall under the Security Act (Sikkerhetsloven). According to § 2-2, the Norwegian National Security Authority (NSM) has the cross-sector responsibility for ensuring that preventive security measures are carried out in all entities subject to the Act. Under § 1-2, this includes state, county, and municipal bodies, as well as private suppliers of goods or services related to security-graded procurements [112]. The Act also applies to entities that handle information, information systems, objects, or infrastructure that are essential to fundamental national functions *(grunnleggende nasjonale funksjoner, GNF)*, or that conduct activities critical to maintaining those functions [113].

It is also worth noting that the responsibility for preventive security ultimately lies with the individual ministries and the entities subject to the Security Act. NSM holds an advisory and supervisory role but does not have the authority to direct or manage security work within these organisations. Responsibility for implementing the necessary measures therefore rests with each entity and its responsible ministry [114]. The roadmap is a recommendation rather than a legally binding instrument and primarily outlines expectations for the transition. Existing regulatory frameworks, such as NIS2, may serve as a basis for introducing future quantum-safe requirements [115].

While EU-level guidance outlines expected priorities and timelines, the expert interviews provide important context on how Norway has approached the quantum threat in practice. Respondent R1 (NSM), stated that the agency began evaluating the long-term implications of quantum computers as early as 2015, motivated by the need to protect classified information with a security lifespan of up to 30 years. According to the Security Act § 5-6, cryptographic systems used to protect classified information must be approved by the National Security Authority, and security classifications are by default valid for up to 30 years, as stated in § 5-3 [112]. In line with this, and as confirmed in the expert interviews, protecting classified information within the defence sector and central government administration was identified as the highest priority. In 2023, NSM published its first guidance document on quantum migration, outlining how organisations can begin the transition to quantum-safe cryptography, with particular focus on the telecommunications, finance, health, energy, and petroleum sectors [116].

The transition to PQC is therefore not yet driven by law or a national strategy, but rather by expectations through the EEA framework, guidance documents, sector-specific regulations (particularly the Security Act), and by organisations that are already migrating because they recognise that the process is long and early action is advantageous. As these highest-priority environments, such as defence and government administration, have already begun addressing the quantum risk, the forthcoming national PQC roadmap is expected to build on their experience and extend guidance to other sectors.

6.2.1 Practical Migration Landscape

Overall, the interviews indicated greater confidence that entities covered by the Security Act, such as the defence sector and central government administration, are likely to meet the requirements in time. In line with this, Respondent R3 emphasised that organisations under the Security Act “will have a plan” and are expected to comply. However, the same informant noted that this optimism does not extend to the wider ecosystem.

Larger commercial organisations may struggle due to complex system landscapes, incomplete asset inventories, extensive supplier dependencies, and limited visibility into where vulnerable cryptography is used. Smaller companies may be more agile but often lack resources. The informant (R3) was particularly concerned about consumer-facing devices and embedded hardware; products that remain in use for decades and are unlikely ever to be upgraded. For these actors, the informant expected the transition to be "messy," with only a small fraction realistically able to meet future deadlines.

Operational technology (OT) systems were repeatedly highlighted by Respondents R1, R4, and R5 as one of the most challenging environments for migration to quantum-safe cryptography. OT systems differ significantly from IT systems in terms of asset lifecycles, upgradeability, and how cryptography is used. Many OT environments rely on legacy technologies that use little or no modern encryption, yet cryptographic mechanisms are still present to verify software sources, authenticate devices, or enable secure remote connectivity in multi-site industrial operations [117]. According to CISA [117], the quantum-related risks facing OT systems will vary widely across organisations due to the highly heterogeneous nature of these environments. At the same time, the potential consequences are substantial: compromise of OT systems can endanger human life and cause large-scale physical damage. While such incidents can already occur without quantum capabilities, the availability of a cryptographically capable quantum computer could lower the barrier for certain types of attacks and increase the likelihood of disruptive events affecting fundamental national functions [117].

Informants (R1, R4, R5) noted that sectors such as power generation and energy distribution still operate equipment where cryptographic components are integrated into hardware, creating uncertainty about how feasible upgrades will be within the expected timelines. At the same time, R1 and R4 highlighted that the most relevant quantum-related risk for OT is integrity, not confidentiality. Manipulated control signals such as false commands to shut down parts of the power grid represent a hypothetical threat scenario. Because such attacks require decryption, forgery, or alteration of data in real time, an adversary would need an operational quantum computer at the time of the intrusion. Therefore, the experts viewed PQC migration for OT environments as more nuanced: confidentiality protections may need earlier transition, while integrity-focused risks are less directly tied to the quantum timeline.

Despite the availability of post-quantum schemes and emerging guidance, many organisations are still not well positioned to begin migration. A frequently highlighted barrier in both the literature and the expert interviews is the lack of cryptographic agility and limited visibility into where and how cryptography is used in their systems [3, 4]. This is particularly relevant for larger organisations, which often do not have a complete and updated asset inventory and an overview of all dependencies on vulnerable cryptographic algorithms.

It seems that organisational and external factors, rather than technical ones, hinder the adoption of PQC once the technical parameters are set. Based on the expert interviews, the migration to PQC appears distant for many organisations. Informants (R3, R4) emphasised that the main barrier is not the technical difficulty, but the lack of awareness and organisational prioritisation. Decision-makers often lack the competence to assess quantum-related risk, identify where cryptography is used, and translate this into concrete backlog tasks. As the informant (R3) described, "*the technical part is manageable, but getting the task into the backlog is the real challenge*". Without strong external triggers such as major security incidents, media attention, or requirements from large vendors, quantum readiness struggles to compete with other priorities, especially in organisations already dealing with technical debt.

Chapter 7

Threat Assessment

This section synthesises the findings from the preceding analysis to evaluate how quantum-enabled threats may realistically manifest in a Norwegian context. Drawing on the technological landscape, geopolitical dynamics, and expert interviews discussed earlier, the assessment focuses on the likelihood, form, and potential targets of adversarial quantum use against Norway. The aim is not to predict a single outcome, but to outline the most plausible threat scenarios based on current knowledge and observable trends. Throughout this chapter likelihood judgements are expressed using the qualitative scale, presented in Chapter 3 (Table 3.2), ranging from *very unlikely* to *very likely*.

7.1 Integrated Assessment

This section synthesises the analysis and answers the research questions.

7.1.1 RQ1: How might a quantum advantage realistically be employed in an adversarial context, based on current geopolitical dynamics and expert assessments?

The CIO framework helps identify the most significant threat by building threat profiles. When it comes to capability, both Russia and China are investing in and developing quantum computers, though to different degrees. As outlined in Chapter 4, the ongoing quantum race is filled with uncertainty and secrecy. However, based on currently available information, both states could eventually develop a cryptographically relevant quantum computer. When that becomes a reality, there will likely be a period in which both states possess the capability to

break quantum-vulnerable public-key cryptography, although China is more likely to achieve it first.

Beijing's primary strategic focus remains on the United States and its regional rivals in Asia. In this sense, Norway represents a valuable but secondary intelligence target for China, rather than a central arena of competition. China tends to calibrate its behaviour pragmatically to avoid actions that could cause significant economic or diplomatic costs. Beijing seeks to maintain its image as a responsible global actor [68]. China has rejected the way it is portrayed in Norwegian threat assessments, emphasising in its response that it seeks "win–win" cooperation and peaceful development rather than confrontation with Norway [118]. It is thus **very likely** that China's main adversarial use of quantum computing will be intelligence and espionage, rather than destructive operations.

Given Russia's current wartime posture and its history of targeting critical infrastructure, it is more likely that Russia would employ quantum capabilities in a disruptive manner, such as attacking energy production or power grids via OT systems to create instability, or compromising satellite communications in the Arctic to weaken NATO in a potential conflict. It is thus **very likely** that Russia's main use of quantum computing in an adversarial way will be disruptive operations.

7.1.2 RQ2: Which state actors are most likely to develop and control cryptographically relevant quantum capabilities?

Based on publicly available information, it is currently difficult to determine with confidence which country will be the first to develop a cryptographically relevant quantum computer. Both the United States and China are assessed as plausible candidates, while Russia is considered less likely in the near term but cannot be excluded.

It is **possible** that China will achieve a cryptographically relevant capability before the United States, particularly in classified or military programmes that are not visible through open sources. It is equally **possible** that the first breakthrough will occur in the US. A Russian "quantum surprise" is considered **unlikely** in the short to medium term, given more limited industrial capacity, but cannot be ruled out over a longer time horizon, especially in the second wave when the technology becomes more available.

7.1.3 RQ3: Which Norwegian national sectors or functions are most exposed to quantum-enabled threats, given their strategic importance and reliance on cryptographic systems?

Russia views NATO's northern flank as a critical pressure point in its broader confrontation with the West. Norway's close alignment with NATO, its geographic proximity to Russia, and its role in Arctic security make it a natural intelligence and sabotage target for Russian services. China's approach to informationised competition is global rather than regionally bounded. Its doctrine of civil–military fusion and emphasis on comprehensive intelligence-gathering means that Norway, like many technologically advanced Western states, because Chinese strategy prioritises collecting broad-spectrum data from a wide range of actors.

These factors combine to make Norway a potential target for the strategic objectives of both China and Russia, and their increasingly close partnership may further affect areas of high strategic importance to Norway [119]. While China does conduct extensive global intelligence-gathering and Norway is a relevant target [38], it is **unlikely** that Norway would be the first or primary target for a state actor such as China or Russia. However, it is **very likely** that Norway would experience indirect or collateral effects from large-scale operations aimed at higher-priority targets such as the United States or NATO. In a future quantum-enabled intrusion, it is **possible** that Norway could be used as an access route toward larger targets, particularly due to its role as a key energy supplier to Europe, its position along transatlantic Arctic routes, and its critical satellite infrastructure. Norway may appear insignificant as a small state in global power politics, but as Palmstrøm Loen and Hove Gusdal [97] note, small states often suffer most when major powers clash, turning their surroundings into arenas of intensified great-power rivalry. For Norway, this is especially concerning given its energy sector and strategic role in the Arctic.

Historically, state-sponsored cyber operations against Norway and other NATO countries have targeted critical infrastructure. These environments also contain extensive operational technology (OT), where legacy systems, long asset lifecycles, and limited cryptographic agility create persistent vulnerabilities. The expert interviews underscored that OT systems represent one of the most challenging domains to secure in time for the quantum transition, and therefore a plausible target for any actor seeking to exploit cryptographic weaknesses without immediately revealing a breakthrough.

Norway's High North within the broader Arctic constitute Norway's most strategically important region, and both Russia and China have clear and growing interests there [96, 119]. In recent years, Russia has shown growing interest in Svalbard's strategic infrastructure. In 2022, two fibre-optic cables connecting Svalbard to mainland Norway were mysteriously damaged shortly before the invasion

of Ukraine. During the early stages of the war, the KSAT satellite network, of which the SvalSat station on Svalbard is the main hub, was also hit by a large cyberattack [94]. In the same region, there is also suspicion that the Chinese research station on Svalbard may be used for military intelligence purposes [95].

Given the threat, the sectors and technologies of greatest value include Norwegian critical infrastructure, particularly the energy sector and satellite systems. Also relevant are places with access to sensitive knowledge, universities, research environments, and communication channels involving decision-makers.

Based on these considerations, it is **likely** that a state actor with quantum cryptanalytic capabilities would prioritise Norwegian critical infrastructure, particularly energy systems and satellite infrastructure, for intelligence collection or targeted disruption.

7.2 Harvest Now, Decrypt Later as a Long-Term Risk Factor

China controls significant parts of the global internet infrastructure, including key choke points in international network traffic, which amplifies its ability to intercept data flows. China has been implicated in multiple BGP hijacking incidents. Similarly, Russia has also been involved in HNDL activities; for instance, in 2020, the Russian state telecommunications provider Rostelecom redirected traffic from over 200 networks, including Google and Facebook, to its own servers [22, 25, 120]. There is also evidence suggesting that Russia may have harvested data from fibre-optic cables [22].

Given the scale of mass interception activities attributed to Russian and Chinese actors, data collected now may carry long-term strategic value once decrypted or correlated with other information sources. The Norwegian Communications Authority (Nkom) has observed several large-scale BGP hijacking campaigns internationally [121]. In its 2024 Risk and Vulnerability Analysis for the Electronic Communications Sector, Nkom stated that, following the Russian BGP hijacking incidents, it had implemented measures to make such attacks more difficult to conduct in Norway. However, there is no publicly available documentation of any specific measures targeting the HNDL threat [122].

The Czech National Cyber and Information Security Agency (NÚKIB) [123] notes that the types of data targeted depend on the attackers' strategic priorities and objectives, and that such attacks are expected to intensify over the next five years as the implementation of post-quantum cryptography (PQC) progresses and adversaries realise they are running out of time to collect data encrypted with vulnerable algorithms.

The possibility of HNDL underscores the importance of migrating to PQC solutions as soon as possible.

7.3 Phases of Adversarial Quantum Use

The following assessment draws primarily on expert interviews and reflects how practitioners expect a quantum-enabled threat to emerge over time. In the expert interviews, all informants were asked how they believed the quantum threat would manifest in practice. The question was framed explicitly considering existing theories that suggest quantum breakthroughs may be kept secret and used strategically, in a way that makes it difficult for other states to determine whether a given effect was caused by quantum capabilities. The informants did not present fully developed theories, but their reflections converged a consistent picture. R1 and R3 stated that it seemed very natural that a state would initially try to hide such a capability and keep its quantum advantage secret.

At some point, however, use of the capability would likely become visible, for example, if a state were to employ a quantum computer to disable critical infrastructure, such as a power grid, immediately before a military operation. Another informant (R3) emphasised that major states such as the US, Russia, China, and North Korea already maintain catalogues of software vulnerabilities and offensive tools, and that a cryptographically relevant quantum computer would simply become "one more power tool" in this arsenal. In their view, the capability would be weaponised and kept secret "up to a certain point", then eventually leak or become obvious through its effects. R2 stressed that commercial and industrial quantum applications are likely to appear earlier than crypto-breaking machines. They argued that economic uses of quantum computing will probably generate visible benefits and indirect indicators of progress long before the first cryptanalytic breakthrough becomes public.

Based on these hypotheses, if we assume that a state would use quantum capabilities in the most strategic way possible, then its advantage would be temporary before more actors gain access. Is Russia likely to be the first to use this capability adversarial? This threat assessment considers that less likely. However, reframing the question: is Russia likely to use quantum computing adversarially in the second wave of quantum attacks, once more states have access and the secrecy barrier has lowered? That appears very likely. Because the time between the first and second wave could be highly uncertain, potentially months or years, and given how long PQC migration can take, critical infrastructure resources of interest to Russia may be targeted and exploited with a quantum-relevant computer in the second wave if they are not already prioritised. Even if a quantum computer is not the direct enabler of the attack, it may support or simplify operations.

Chapter 8

Discussion

This assessment has examined the threat of quantum computing, the countermeasures to that threat, the surrounding quantum race landscape, the strategic motivations for adversarial use of the technology, and the key vulnerabilities and likely targets from a technical and geopolitical perspective.

Based on the analysis, this thesis finds that initial adversarial use of quantum computing would most plausibly be state-led and indirect, supporting intelligence collection and strategic leverage over Norwegian critical infrastructure, with the potential to enable high-impact operations later. This is due to Norway's role in NATO, European energy security, and Arctic security, all of which are of strategic interest to both China and Russia. The energy and satellite sectors emerge as the most vulnerable parts of Norwegian critical infrastructure, as they rely heavily on operational technology (OT) systems that are difficult to migrate and modernise. In these environments, the primary risk is related to the integrity of data, such as manipulation or injection of false information, meaning that the threat would materialise only once a cryptographically relevant quantum computer is operational, rather than through harvest-now-decrypt-later (HNDL) attacks.

As quantum technologies become more accessible over time, their use by a broader range of actors is likely to expand the threat to the wider ecosystem. The analysis further finds that current migration efforts in Norway are *insufficient*, largely due to limited prioritisation and low awareness. Greater efforts should therefore be made to secure critical infrastructure against high-impact nation-state attacks, particularly within the energy and space sectors, while simultaneously increasing awareness within the cybersecurity community to initiate timely post-quantum migration and protect the broader ecosystem from quantum-enabled threats.

8.1 The Paradox of the Quantum Technology Landscape

This assessment finds that the advent of quantum computing will pose a genuine risk to Norwegian national security. At the same time, the surrounding landscape remains something of a paradox. While effective technical countermeasures exist, the primary challenge lies with implementing them. The threat demands proactive and coordinated action, yet it remains abstract, uncertain, and unevenly understood across sectors.

Quantum technology is emerging as a strategic field with a wide range of potential economic, scientific, and technological applications, although many concrete use cases remain under active research [12]. This has made quantum technology a highly attractive strategic asset for nation states, prompting investments of billions of dollars despite the lack of clearly defined end uses. Notably, states are committing enormous resources to a technology whose constructive applications are still not fully understood. Russia's national quantum road map, for example, explicitly includes more than one hundred hypotheses for potential applications of quantum computers to be developed by 2030 [53].

Zancanaro [39] explains these investments as being driven by a form of collective strategic anxiety among states. The possibility that rival actors may achieve hidden breakthroughs in quantum computing creates mutual mistrust and incentivises continued investment, even in the absence of clearly defined constructive applications. No state wants to risk falling behind in a technology perceived as strategically transformative, and these dynamics fuels global competition. From this perspective, the investment logic resembles a form of strategic anticipation rather than a response to clearly articulated needs. In the defence domain, similar considerations apply to states seeking to ensure resilience against future threats posed by actors that may achieve technological superiority. As a result, the emerging quantum threat landscape is characterised less by cooperation, and more by competition and secrecy.

This dynamic is also reflected beyond the state level. When reviewing the literature and discussing the topic with security professionals, there appears to be no coherent or shared narrative about the quantum threat. Instead, the field is characterised by contradiction, uncertainty, and misunderstanding.

While many actors acknowledge that quantum computing represents a potential future threat, it is often perceived as too technically distant to engage with in a concrete or operational manner. Quantum computing is grounded in concepts such as superposition and entanglement, which lie far outside the everyday expertise of most security professionals. As Richard P. Feynman remarked, *"I think I can safely say that nobody really understands quantum mechanics"*, a statement made by a physicist and Nobel laureate deeply embedded in the field. Unlike clas-

sical technologies, quantum systems do not lend themselves to intuitive analogies or straightforward visual representations. While these concepts can be simplified for explanatory purposes, as outlined in Section 2.1, beyond such simplifications they quickly become abstract, resembling something akin to black magic.

When looking at media articles, it is easy to encounter headlines claiming that quantum computing will fundamentally change the world, rival the industrial revolution in impact, or even trigger an impending "quantum apocalypse", with some suggesting it is already too late due to harvest-now–decrypt-later attacks [22]. This sounds alarming. In my own discussions with security professionals, several described having encountered quantum computing only through brief conference talks or high-level briefings, without subsequently integrating it into their risk assessments. As noted by Krågebakk [43], media narratives tend to frame quantum computing as an overwhelming and inevitable force, which can trigger a natural fight-or-flight response, leading some to disengage out of uncertainty or fear. This dynamic can hinder innovation and delay necessary preparations. If quantum technologies are to mature and be used responsibly, they must become more democratised, accessible, understandable, and usable by the broader ecosystem. Without this, the organisations responsible for migration will struggle to prioritise and operationalise quantum-safe measures, regardless of how easy the technical solutions become. As R3 noted, the main challenge is often not the technical work itself, but getting post-quantum migration tasks prioritised and placed on organisational backlogs. Respondents R4 and R5 similarly emphasised that limited awareness and unclear ownership of the issue mean organisations tend to delay action until external pressure or clearer signals emerge.

8.2 Addressing the Scepticism in Quantum Computing

The lack of a coherent narrative is further reinforced by literature that questions whether quantum computing will ever deliver on its promises. Over the past few decades, forecasts about when large-scale quantum computers will arrive have varied widely and have frequently been revised. The result is persistent uncertainty about when quantum computing will become a practical cryptographic threat. Dyakonov [27] goes as far as describing this as a sociological problem, arguing that parts of the quantum computing field operate almost like "mafia-like structures", where researchers are pushed by funding incentives into wild exaggerations bordering on scientific misconduct. Nobel Prize laureate Robert Laughlin has also expressed deep scepticism, arguing that the relevant laws of quantum mechanics are already known, and that if building such a machine were realistically possible, we would likely have seen more tangible progress by now. His argument is essentially: if you hire the smartest people in the world and they fail for 40 years, maybe the problem is not the people [27].

From this perspective, quantum computing becomes not a guaranteed future, but something closer to a scientific and political controversy. When this view was raised in the interviews, R2 explained that the uncertainty surrounding quantum computing has shifted significantly in recent years. In the early period around 2017, much of the rhetoric consisted of "perhaps," "maybe," and cautious predictions, largely because no one wanted to promise too much. R2 stated that this has changed, and that there is now a high degree of confidence that quantum computers of certain sizes will be realised.

There is, however, still considerable scepticism within the cybersecurity community, ranging from the belief that large-scale quantum computers will never materialise, to the view that they may emerge but that their ability to break cryptography is overstated. This scepticism complicates the formation of a shared sense of urgency at the management level, making it more difficult to prioritise and implement measures aimed at reducing quantum-related risks.

It is easy to take Robert Laughlin's scepticism at face value. However, history offers many examples of transformative technologies that were dismissed before their impact became clear. For instance, in 1998 Paul Krugman argued that the Internet would have "no greater impact than the fax machine" [124]. History shows that groundbreaking technologies are often dismissed long before they reshape society. Quantum computing may seem far-fetched to some, but if thousands of people have dedicated their careers to it, there must be some truth to it, right?

There is therefore a clear need for calibration in how these issues are approached in order to address the threat at hand. The primary vulnerability does not necessarily lie in the technical weaknesses of asymmetric cryptography to Shor's (or Grover's) algorithm, but rather in organisational shortcomings: a failure to acknowledge and prioritise the risk, combined with a lack of coordinated national initiatives to support and drive efforts to secure critical infrastructure. This threat assessment ultimately aims to clarify and simplify the quantum landscape for those who perceive it as vague or confusing, and to make these issues more accessible to the people responsible for making security decisions.

Chapter 9

Conclusion

This thesis set out to clarify the threat posed by a cryptographically relevant quantum computer to Norway. While much of the existing debate focuses on whether quantum computers will eventually break asymmetric cryptography, this study has approached the issue from a broader national security perspective, asking how such a capability might realistically be developed, used, and prioritised by state actors, and what this implies for Norwegian interests.

The analysis shows that the quantum threat should not be understood as a single, sudden technological "event", but as a gradual and strategic process shaped by uncertainty, secrecy, and geopolitical competition. Although large-scale, fault-tolerant quantum computers capable of breaking widely used public-key cryptography do not yet exist, the direction of global investment and research suggests that such capabilities cannot be dismissed as speculative. At the same time, the timeline remains highly uncertain, and early quantum advantages are likely to be uneven, classified, and applied selectively rather than openly demonstrated.

By examining the quantum race, this thesis finds that the United States and China remain the most plausible candidates to achieve a cryptographically relevant quantum capability first, while Russia is less likely in the near term but cannot be excluded over a longer horizon. Importantly, the assessment suggests that the first adversarial uses of quantum advantage are unlikely to be broad or indiscriminate. Instead, they are more likely to be integrated into existing intelligence and cyber operations, either to enhance espionage, support disruptive activities, or enable strategic effects without immediately revealing a technological breakthrough.

The findings indicate that Norway is unlikely to be a primary or first-order target for quantum-enabled attacks. However, Norway's role as a key energy supplier to Europe, its strategic position in the Arctic, and its satellite infrastructure mean

that it is highly exposed to indirect and collateral effects of great-power competition. In such a context, quantum-enabled capabilities may be used against Norwegian systems either as part of wider operations targeting NATO or the EU, or through supply chains, infrastructure dependencies, and intelligence collection.

The threat assessment further highlights that the most significant vulnerabilities are not confined to the defence sector, which generally benefits from higher security maturity, but rather lie within civilian critical infrastructure, particularly energy systems, satellite services, and operational technology environments. These systems are difficult to migrate, have long lifecycles, and often lack cryptographic agility, making them attractive targets for future quantum-enabled attacks.

A central conclusion of this thesis is that the quantum threat is as much an organisational and strategic challenge as it is a technical one. While post-quantum cryptographic solutions are emerging, migration efforts remain uneven and slow, especially outside the most security-sensitive sectors. Interviews and literature reviewed in this study suggest that uncertainty, scepticism, and limited understanding of quantum technology complicate prioritisation and decision-making. As a result, the primary vulnerability may lie not in cryptography itself, but in delayed action, fragmented responsibility, and insufficient communication of risk.

As quantum technology and geopolitical dynamics continue to evolve, sustained assessment, coordination, and awareness will be essential to reduce long-term national security risk.

Bibliography

[1] International Year of Quantum Science and Technology (IYQ). 'IYQ 2025: International Year of Quantum Science and Technology,' Accessed: 21st Dec. 2025. [Online]. Available: https://quantum2025.org/.

[2] Europol Innovation Lab, 'The Second Quantum Revolution – The impact of quantum computing and quantum technologies on law enforcement,' Publications Office of the European Union, Luxembourg, Observatory Report, 2023. Accessed: 1st Sep. 2025. [Online]. Available: https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_Innovation_Lab_Observatory_Report%20-%20The%20Second%20Quantum%20Revolution.pdf.

[3] TNO, CWI and AIVD. 'The PQC Migration Handbook: Guidelines for Migrating to Post-Quantum Cryptography.' Version 2 (December 2023). Developed and published as part of the Dutch National Cryptostrategy (NCS)., Accessed: 1st Sep. 2025. [Online]. Available: https://english.aivd.nl/publications/publications/2023/04/04/the-pqc-migration-handbook.

[4] W. Baker, W. Polk and M. Souppaya, 'Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms,' National Institute of Standards and Technology (NIST), Tech. Rep., 2021. Accessed: 1st Sep. 2025. [Online]. Available: https://doi.org/10.6028/NIST.CSWP.04282021.

[5] F. Muller and M. P. P. van Heesch. 'Migration to Quantum-Safe Cryptography: About Making Decisions on When, What, and How to Migrate a Quantum-Safe Situation,' Accessed: 19th Oct. 2025. [Online]. Available: https://publications.tno.nl/publication/34637213/SDdGJI/TNO-2020-migration.pdf.

[6] L. Baumgärtner, B. Klein, N. Mohr, A. Pflanzer and H. Soller. 'When- and how- to prepare for post-quantum cryptography,' Accessed: 1st Sep. 2025. [Online]. Available: https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/when%

20and%20how%20to%20prepare%20for%20post%20quantum%20cryptography/when-and-how-to-prepare-for-post-quantum-cryptography.pdf.

[7] M. Jonsson, 'Espionage by Europeans: Treason and Counterintelligence in Post-Cold War Europe,' *Intelligence and National Security*, vol. 39, no. 1, pp. 77–92, 2024. DOI: 10.1080/02684527.2023.2254020. [Online]. Available: https://doi.org/10.1080/02684527.2023.2254020.

[8] A. Jackson, 'How the Collapse of the Soviet Union Made Russia a Great Cyber Power,' *The Cyber Defense Review*, vol. 9, no. 1, pp. 99–112, 2024. Accessed: 12th Oct. 2025. [Online]. Available: https://www.jstor.org/stable/48770667.

[9] M. Ivezic. 'Quantum Geopolitics: The Global Race for Quantum Computing,' Accessed: 12th Oct. 2025. [Online]. Available: https://postquantum.com/quantum-computing/quantum-geopolitics/.

[10] J. M. Godzimirski, 'The Ukraine War, the New Geopolitics of Energy, and Norway,' Norwegian Institute of International Affairs (NUPI), Tech. Rep., 2023, https://www.nupi.no/en/publications/cristin-pub/the-ukraine-war-the-new-geopolitics-of-energy-and-norway. Accessed: 9th Dec. 2025.

[11] United Nations Department of Economic and Social Affairs. 'Goal 9: Build resilient infrastructure, promote inclusive and sustainable industrialization and foster innovation,' Accessed: 13th Oct. 2025. [Online]. Available: https://sdgs.un.org/goals/goal9.

[12] C. G. Almudever, G. Alagic, G. Burkard, X. Fu, J. C. Garcia-Escartin, A. G. Rattew, M. Roetteler, R. Wiersema and R. Xue, *Assessing the Benefits and Risks of Quantum Computers*, 2024. Accessed: 1st Sep. 2025. [Online]. Available: https://arxiv.org/abs/2401.16317.

[13] L. Kumar, M. A. K. Akhtar, M. Saxena, D. Mishra and V. Khatri, 'Quantum Computing: Unleashing the Power of Superposition and Entanglement,' *Tuijin Jishu/Journal of Propulsion Technology*, vol. 44, no. 4, 2023. Accessed: 1st Sep. 2025. [Online]. Available: https://propulsiontechjournal.com/index.php/journal/article/view/1218/846.

[14] M. E. Sabani, I. K. Savvas and G. Garani, 'Learning with Errors: A Lattice-Based Keystone of Post-Quantum Cryptography,' *Signals*, vol. 5, pp. 216–243, 2024. DOI: 10.3390/signals5020012. Accessed: 1st Sep. 2025. [Online]. Available: https://doi.org/10.3390/signals5020012.

[15] Mecalux. 'Quantum computing and its impact on logistics: What does it mean for the supply chain future.' Online blog article, Accessed: 4th Dec. 2025. [Online]. Available: https://www.mecalux.com/blog/quantum-computing-logistics.

[16] S. Li, Y. Chen, L. Chen, J. Liao, C. Kuang, K. Li, W. Liang and N. Xiong, 'Post-Quantum Security: Opportunities and Challenges,' *Sensors*, vol. 23, no. 21, 2023. DOI: 10.3390/s23218744. Accessed: 1st Sep. 2025. [Online]. Available: https://www.mdpi.com/1424-8220/23/21/8744.

[17] C. Pittet, *Mathematical aspects of shor's algorithm*, HAL document, 2014. Accessed: 1st Sep. 2025. [Online]. Available: https://cel.hal.science/cel-00963668/document.

[18] M. Hirvensalo, *Quantum Computing* (Natural Computing Series), 2nd ed. Springer-Verlag Berlin Heidelberg, 2004. DOI: 10.1007/978-3-662-09636-9. Accessed: 2nd Sep. 2025. [Online]. Available: https://doi.org/10.1007/978-3-662-09636-9.

[19] X. Bonnetain, M. Naya-Plasencia and A. Schrottenloher, 'Quantum Security Analysis of AES,' *IACR Transactions on Symmetric Cryptology*, vol. 2019, no. 2, pp. 55–93, 2019. DOI: 10.13154/tosc.v2019.i2.55-93. Accessed: 1st Sep. 2025. [Online]. Available: https://doi.org/10.13154/tosc.v2019.i2.55-93.

[20] SpinQ. 'Grover's Algorithm: How It Speeds Up Quantum Search.' Available: spinquanta.com (web), Accessed: 21st Dec. 2025.

[21] T. G. Tan, P. Szalachowski and J. Zhou. 'Challenges of Post-Quantum Digital Signing in Real-world Applications: A Survey,' Accessed: 3rd Nov. 2025. [Online]. Available: https://eprint.iacr.org/2019/1374.

[22] C. Stöcker. 'Q-Day Countdown: The HNDL Cybersecurity Crisis Europe Can't Ignore,' Spherity / Medium, Accessed: 19th Oct. 2025. [Online]. Available: https://medium.com/spherity/q-day-countdown-the-hdnl-cybersecurity-crisis-europe-cant-ignore-0694ce4a5802.

[23] R. Salz. 'Building a Quantum-Safe Internet: The IETF's Plan for TLS,' Akamai Technologies, Accessed: 19th Oct. 2025. [Online]. Available: https://www.akamai.com/blog/trends/building-quantum-safe-internet-ietf-plan-tls.

[24] D. Stebila, S. Fluhrer and S. Gueron, 'Hybrid Key Exchange in TLS 1.3,' Internet Engineering Task Force (IETF), TLS Working Group, Internet-Draft draft-ietf-tls-hybrid-design-16, 2025. Accessed: 19th Oct. 2025. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/.

[25] F. Douzet, L. Salamatian, K. Salamatian, L. Pétiniaud, K. Limonier and T. Alchus, 'Measuring the Fragmentation of the Internet: The Case of the Border Gateway Protocol (BGP) During the Ukrainian Crisis,' in *12th International Conference on Cyber Conflict (CyCon 2020) – "20/20 Vision: The Next Decade"*, 2020, pp. 1–26. Accessed: 19th Oct. 2025. [Online]. Available: https://ccdcoe.org/uploads/2020/05/CyCon_2020_9_Douzet_Petiniaud_Salamatian_Limonier_Salamatian_Alchus.pdf.

[26] M. Mohseni et al., *How to Build a Quantum Supercomputer: Scaling from Hundreds to Millions of Qubits*, arXiv:2411.10406, 2024. Accessed: 2nd Sep. 2025. [Online]. Available: https://arxiv.org/abs/2411.10406.

[27] M. I. Dyakonov, *Will We Ever Have a Quantum Computer?* (SpringerBriefs in Physics), 1st ed. Springer, Cham, 2020, pp. XI, 49, ISBN: 978-3-030-42018-5. DOI: 10.1007/978-3-030-42019-2.

[28] J. Preskill, *Quantum Computing in the NISQ era and beyond*, Institute for Quantum Information and Matter and Walter Burke Institute for Theoretical Physics, California Institute of Technology (Caltech), 2018. Accessed: 2nd Sep. 2025. [Online]. Available: https://arxiv.org/pdf/1801.00862.

[29] M. Fellous-Asiani, 'The resource cost of large scale quantum computing,' Available: theses.hal.science (PDF), Ph.D. dissertation, Université Grenoble Alpes, 2021. Accessed: 21st Sep. 2025.

[30] C. Gidney, *How to factor 2048 bit RSA integers with less than a million noisy qubits*, 2025. Accessed: 4th Oct. 2025. [Online]. Available: https://arxiv.org/abs/2505.15917.

[31] S. Jaques. 'Quantum Landscape,' Accessed: 16th Sep. 2025. [Online]. Available: https://sam-jaques.appspot.com/quantum_landscape.

[32] IBM Quantum. 'IBM Quantum Platform — Cloud-Based Quantum Computing Services,' Accessed: 3rd Dec. 2025. [Online]. Available: https://quantum.cloud.ibm.com/.

[33] Quantum Flagship. 'EU gives unprecedented access to quantum computers – accelerating next-generation technology,' Accessed: 3rd Dec. 2025. [Online]. Available: https://qt.eu/news/2025/2025-08-28_eu-gives-unprecedented-access-to-quantum-computers.

[34] J. Federici, *Vying for Quantum Supremacy: U.S.–China Competition in Quantum Technologies*, U.S.-China Economic and Security Review Commission, 2025. Accessed: 8th Dec. 2025. [Online]. Available: https://www.uscc.gov/sites/default/files/2025-11/Vying%20for%20Quantum%20Supremacy%20U.S.-China%20Competition%20in%20Quantum%20Technologies.pdf.

[35] H. Omaar and M. Makaryan, 'How Innovative Is China in Quantum?' Information Technology and Innovation Foundation, 2024. Accessed: 19th Oct. 2025. [Online]. Available: https://itif.org/publications/2024/09/09/how-innovative-is-china-in-quantum/.

[36] P. D. Leedy and J. E. Ormrod, *Practical Research: Planning and Design*, 11th. Harlow, England: Pearson Education Limited, 2015, Global Edition, ISBN: 978-1-292-09587-5.

[37] Norwegian University of Science and Technology (NTNU). 'Processing of Personal Data – Policy: The Processing of Personal Data in Research,' Accessed: 3rd Nov. 2025. [Online]. Available: https://i.ntnu.no/wiki/-/wiki/English/Processing+of+personal+data+-+policy.

[38] Norwegian Police Security Service (PST). 'National Threat Assessment 2025.' Available: PST: Nasjonal trusselvurdering 2025 (PDF), Accessed: 16th Nov. 2025.

[39] E. Zancanaro. 'The Quantum Race: How Emerging Technologies Reshape Global Security Governance,' Accessed: 12th Oct. 2025. [Online]. Available: https://www.e-ir.info/2025/09/29/the-quantum-race-how-emerging-technologies-reshape-global-security-governance/.

[40] J. P. Dowling and G. J. Milburn, 'Quantum technology: the second quantum revolution,' *Philosophical Transactions of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, vol. 361, no. 1809, pp. 1655–1674, 2003. DOI: 10.1098/rsta.2003.1227.

[41] European Commission. 'Quantum Manifesto: A New Era of Technology,' Accessed: 5th Dec. 2025. [Online]. Available: https://qt.eu/about-quantum-flagship/quantum-manifesto/.

[42] European Commission, 'Digital Decade Cardinal Points: Commission Staff Working Document,' European Commission, Commission Staff Working Document SWD(2023) 571 final, 2023, Accompanying the Communication on the 2023 State of the Digital Decade. Accessed: 5th Oct. 2025. [Online]. Available: https://www.coit.es/sites/default/files/ce_digital_decade_cardinal_points.pdf.

[43] V. Krågebakk, 'The Ecosystem Surrounding Quantum Technology: Important Considerations and Key Takeaways,' Kongsberg Gruppen, White paper, 2025. Accessed: 6th Dec. 2025. [Online]. Available: https://www.kongsberg.com/globalassets/kongsberg-discovery/news/quantum-technology/the-ecosystem-surrounding-quantum-technology-public.pdf.

[44] Ministry of Digitalisation and Public Governance (Norway). 'Fremtidens digitale Norge – Nasjonal digitaliseringsstrategi 2024–2030.' Available: regjeringen.no (PDF), Accessed: 4th Oct. 2025.

[45] Government of Norway. '43 millioner kroner til satsing på kvanteteknologi.' Press release, 2025-06-19, Accessed: 20th Dec. 2025. [Online]. Available: https://www.regjeringen.no/no/aktuelt/43-millioner-kroner-til-satsing-pa-kvanteteknologi/id3109876/.

[46] SINTEF. 'Ønsker regjeringens satsing på kvantevitenskap og teknologi velkommen,' Accessed: 5th Oct. 2025. [Online]. Available: https://www.sintef.no/siste-nytt/2025/onsker-regjeringens-satsing-pa-kvantevitenskap-og-teknologi-velkommen/.

[47] Government of Norway. 'Nå starter arbeidet med nasjonal strategi for kvanteteknologi,' Accessed: 4th Oct. 2025. [Online]. Available: https://www.regjeringen.no/no/aktuelt/na-starter-arbeidet-med-nasjonal-strategi-for-kvanteteknologi/id3100025/.

[48] Government Communications Department (Finland). 'Joint Statement by the Nordic Prime Ministers and Heads of Government on Quantum Technologies: Laying the Foundation for Future Nordic Advancements.' Published 2025-05-26, Accessed: 6th Oct. 2025. [Online]. Available: https://valtioneuvosto.fi/en/-/10616/joint-statement-by-the-nordic-prime-ministers-and-heads-of-government-on-quantum-technologies-laying-the-foundation-for-future-nordic-advancements.

[49] QURECA. 'Quantum Initiatives Worldwide 2025,' Accessed: 18th Oct. 2025. [Online]. Available: https://www.qureca.com/quantum-initiatives-worldwide/.

[50] J. Krikke. 'US–China in a defining race for quantum supremacy,' Asia Times, Accessed: 8th Dec. 2025. [Online]. Available: https://asiatimes.com/2025/07/us-china-in-a-defining-race-for-quantum-supremacy/.

[51] IBM Quantum. 'Building a large-scale fault-tolerant quantum computer,' IBM, Accessed: 8th Dec. 2025. [Online]. Available: https://www.ibm.com/quantum/blog/large-scale-ftqc.

[52] 1Prime. 'Rosatom has approved the roadmap for the development of quantum computing,' Accessed: 16th Oct. 2025. [Online]. Available: https://1prime.ru/20250801/rosatom-860207996.html.

[53] Atomic Energy. 'Russia has approved a quantum computing roadmap through 2030,' Accessed: 6th Dec. 2025. [Online]. Available: https://www.atomic-energy.ru/news/2025/08/01/158151.

[54] Rosatom. 'Rosatom Quantum Accelerator,' Accessed: 16th Oct. 2025. [Online]. Available: https://xn--80aaeb9acfuj8af4i.xn--p1ai/.

[55] A. K. Fedorov, A. V. Akimov, J. D. Biamonte, A. V. Kavokin, F. Y. Khalili, E. O. Kiktenko, N. N. Kolachevsky, Y. V. Kurochkin, A. I. Lvovsky, A. N. Rubtsov, G. V. Shlyapnikov, S. S. Straupe, A. V. Ustinov and A. M. Zheltikov, 'Quantum technologies in Russia,' *Quantum Science and Technology*, vol. 4, no. 4, p. 040 501, 2019. DOI: 10.1088/2058-9565/ab4472. Accessed: 6th Dec. 2025. [Online]. Available: https://doi.org/10.1088/2058-9565/ab4472.

[56] Government of the Russian Federation. 'Concept for Regulating the Quantum Communications Sector in the Russian Federation up to 2030.' Order of the Government of the Russian Federation No. 1856-r of 11 July 2023, Accessed: 6th Dec. 2025. [Online]. Available: http://publication.pravo.gov.ru/document/0001202307170029.

[57] TAdviser. 'A project to create a universal quantum computer has been approved in Russia,' Accessed: 6th Dec. 2025. [Online]. Available: https://tadviser.com/index.php/Article:Quantum_computers_and_networks_in_Russia.

[58] M. Swayne. 'Russia Unveils Its 50-Qubit Rubidium Neutral Atom Prototype Quantum Computer,' Accessed: 16th Oct. 2025. [Online]. Available: https://thequantuminsider.com/2024/12/29/russia-unveils-its-first-50-qubit-quantum-computer-prototype/.

[59] Rosatom. 'By 2030, a quantum industry will be formed in Russia,' Accessed: 6th Dec. 2025. [Online]. Available: https://www.ocks-rosatoma.ru/upload/magazine/sao-n13-2024/article-4.pdf.

[60] E. Ribakova and L. Risinger. 'The Russian Economy in 2025: Between Stagnation and Militarization, organization = Atlantic Council,' Accessed: 10th Dec. 2025. [Online]. Available: https://www.atlanticcouncil.org/content-series/russia-tomorrow/the-russian-economy-in-2025-between-stagnation-and-militarization/.

[61] MarketsandMarkets. 'Cryocooler Market – Key Players and Market Trends.' Available: https://www.marketsandmarkets.com/ ResearchInsight/cryocooler-market.asp, Accessed: 16th Oct. 2025.

[62] Roscongress Foundation. 'The Current State of Quantum Technologies,' Accessed: 6th Dec. 2025. [Online]. Available: https://roscongress.org/materials/sovremennoe-sostoyanie-kvantovykh-tekhnologiy/.

[63] Q. Zhang, F. Xu, L. Li, N.-L. Liu and J.-W. Pan, 'Quantum information research in China,' *Quantum Science and Technology*, vol. 4, no. 4, p. 040 503, 2019. DOI: 10.1088/2058-9565/ab4bea. [Online]. Available: https://doi.org/10.1088/2058-9565/ab4bea.

[64] McKinsey & Company, 'Quantum Technology Monitor 2025: From Concept to Reality in 2025,' McKinsey & Company, Tech. Rep., 2025. Accessed: 16th Oct. 2025. [Online]. Available: https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/the%20year%20of%20quantum%20from%20concept%20to%20reality%20in%202025/quantum-monitor-2025.pdf.

[65] Reuters. 'China to set up national venture capital guidance fund, state planner says,' Accessed: 18th Oct. 2025. [Online]. Available: https://www.reuters.com/world/china/china-set-up-national-venture-capital-guidance-fund-state-planner-says-2025-03-06/.

[66] J. Martinis. 'Nobel winner warns China is 'nanoseconds' behind the US in quantum race,' The Business Times, Accessed: 8th Dec. 2025. [Online]. Available: https://www.businesstimes.com.sg/international/global/nobel-winner-warns-china-nanoseconds-behind-us-quantum-race.

[67] H. Phillips. 'The Rising Threat of China and Russia's Deepening Technological Partnership,' Accessed: 19th Oct. 2025. [Online]. Available: https://fsi.stanford.edu/sipr/technological-partnership.

[68] A. Caruso and T. Rühlig. 'The dependence gap in Russia–China relations,' Accessed: 19th Oct. 2025. [Online]. Available: https://www.iss.europa.eu/publications/analysis/dependence-gap-russia-china-relations.

[69] N. Morgado and É. D. Druhalóczki, 'Traditional Worldviews, Strategic Culture and Revolutionary Mentality: The Case of People's Republic of China,' *China Report*, vol. 60, no. 4, pp. 361–377, 2024, DOI: 10.1177/00094455241288062.

[70] D. Cheng, *Cyber Dragon: Inside China's Information Warfare and Cyber Operations*, 1st ed. Santa Barbara, CA: Praeger, 2016, ISBN: 9781440835643. DOI: 10.5040/9798400636431.

[71] E. Gotz and J. Staun, 'Why Russia Attacked Ukraine: Strategic Culture and Radicalized Narratives,' *Contemporary Security Policy*, vol. 43, no. 3, pp. 482–497, 2022. DOI: 10.1080/13523260.2022.2082633. [Online]. Available: https://doi.org/10.1080/13523260.2022.2082633.

[72] K. B. Payne and J. S. Foster, 'Russian strategy: Expansion, crisis and conflict,' *Comparative Strategy*, vol. 36, no. 1, pp. 1–89, 2017. DOI: 10.1080/01495933.2017.1277121. [Online]. Available: https://doi.org/10.1080/01495933.2017.1277121.

[73] W. Materski, *Tsars, Soviets, Putin: A Study of Russia's Politics of History*, 1st ed. Munich: De Gruyter Oldenbourg, 2025. [Online]. Available: https://doi.org/10.1515/9783111348395.

[74] B. Smith, 'Russian intelligence services and special forces,' House of Commons Library, Tech. Rep. CBP 8430, 2018. Accessed: 20th Oct. 2025. [Online]. Available: https://researchbriefings.files.parliament.uk/documents/CBP-8430/CBP-8430.pdf.

[75] MITRE Corporation, *Group G0007: APT28 (also known as Fancy Bear)*, 2025. Accessed: 20th Oct. 2025. [Online]. Available: https://attack.mitre.org/groups/G0007/.

[76] Electronic Transactions Development Agency (ETDA), *Threat Group Cards: Sofacy, APT 28, Fancy Bear, Sednit*, 2025. Accessed: 20th Oct. 2025. [Online]. Available: https://apt.etda.or.th/cgi-bin/showcard.cgi?g=Sofacy%2C+APT+28%2C+Fancy+Bear%2C+Sednit.

[77] MITRE Corporation, *Group G1003: Ember Bear*, 2025. Accessed: 20th Oct. 2025. [Online]. Available: https://attack.mitre.org/groups/G1003/.

[78] E. T. D. A. (ETDA), *Threat Group Cards: SaintBear, Lorec53*, 2025. Accessed: 20th Oct. 2025. [Online]. Available: https://apt.etda.or.th/cgi-bin/showcard.cgi?g=SaintBear%2C%20Lorec53.

[79] MITRE Corporation. 'Group G0034: Sandworm Team,' Accessed: 20th Oct. 2025. [Online]. Available: https://attack.mitre.org/groups/G0034/.

[80] Fraunhofer FKIE (Malpedia). 'Sandworm (Threat Actor) – Malpedia,' Accessed: 20th Oct. 2025. [Online]. Available: https://malpedia.caad.fkie.fraunhofer.de/actor/sandworm.

[81] MITRE Corporation. 'Group G0016: APT29 (also known as Cozy Bear),' Accessed: 20th Oct. 2025. [Online]. Available: https://attack.mitre.org/groups/G0016/.

[82] CyberArk Blog Team. 'The Anatomy of the SolarWinds Attack Chain,' Accessed: 20th Oct. 2025. [Online]. Available: https://www.cyberark.com/resources/blog/the-anatomy-of-the-solarwinds-attack-chain.

[83] Brandefense Threat Intelligence Team. 'Gamaredon Group: A Persistent Russian Espionage Threat,' Accessed: 20th Oct. 2025. [Online]. Available: https://brandefense.io/blog/gamaredon-group-2025/.

[84] MITRE Corporation. 'Group G0047: Gamaredon Group,' Accessed: 20th Oct. 2025. [Online]. Available: https://attack.mitre.org/groups/G0047/.

[85] MITRE Corporation. 'Group G1033: Star Blizzard,' Accessed: 24th Oct. 2025. [Online]. Available: https://attack.mitre.org/groups/G1033/.

[86] Microsoft Threat Intelligence. 'New Star Blizzard spear-phishing campaign targets WhatsApp accounts,' Accessed: 24th Oct. 2025. [Online]. Available: https://www.microsoft.com/en-us/security/blog/2025/01/16/new-star-blizzard-spear-phishing-campaign-targets-whatsapp-accounts/.

[87] MITRE Corporation. 'Group G0010: Turla,' Accessed: 24th Oct. 2025. [Online]. Available: https://attack.mitre.org/groups/G0010/.

[88] D. Frank and T. Fakterman. 'Threat Group Assessment: Turla (aka Pensive Ursa),' Accessed: 24th Oct. 2025. [Online]. Available: https://unit42.paloaltonetworks.com/turla-pensive-ursa-threat-assessment/.

[89] Microsoft. 'Microsoft Digital Defense Report 2025,' Accessed: 19th Dec. 2025. [Online]. Available: https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/Microsoft-Digital-Defense-Report-2025.pdf.

[90] Cybersecurity and Infrastructure Security Agency (CISA). 'AA25-239A: Countering Chinese State-Sponsored Actors' Compromise of Networks Worldwide to Feed Global Espionage System,' Accessed: 21st Dec. 2025. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-239a.

[91] U.S. Attorney's Office, District of Columbia. 'Chinese Nationals with Ties to the PRC Government and APT27 Charged in a Computer Hacking Campaign for Profit, Targeting Numerous U.S. Companies, Institutions, and Municipalities,' Accessed: 19th Dec. 2025. [Online]. Available: https://www.justice.gov/usao-dc/pr/chinese-nationals-ties-prc-government-and-apt27-charged-computer-hacking-campaign-profit.

[92] Breached Company. 'The Silent Revolution: How China's Ministry of State Security Became the World's Most Formidable Cyber Power,' Accessed: 19th Dec. 2025. [Online]. Available: https://breached.company/the-silent-revolution-how-chinas-ministry-of-state-security-became-the-worlds-most-formidable-cyber-power/.

[93] European Repository of Cyber Incidents (EuRepoC). 'Cyber Incident Dashboard.' Viewed "Main countries of origin of cyber incidents against Norway", Accessed: 19th Dec. 2025. [Online]. Available: https://eurepoc.eu/dashboard/.

[94] B. van der Wal. 'NATO's Polar Pressure Point: The Svalbard Archipelago and the Russian Challenge,' The Arctic Institute, Accessed: 8th Dec. 2025. [Online]. Available: https://www.thearcticinstitute.org/natos-polar-pressure-point-svalbard-archipelago-russian-challenge/.

[95] K. Adler. 'Tensions rise as China, Russia, US and Europe scramble for Arctic influence,' BBC News, Accessed: 9th Dec. 2025. [Online]. Available: https://www.bbc.com/news/articles/cjwqn7z02plo.

[96] B. Steinveg, 'Small States in World Politics: Norwegian Interests and Foreign Policy Challenges in the Arctic,' *Arctic Review on Law and Politics*, vol. 15, pp. 3–24, 2024. Accessed: 8th Dec. 2025. [Online]. Available: https://arcticreview.no/index.php/arctic/article/view/5125/9609.

[97] U. Palmstrøm Loen and I. Hove Gusdal. 'A Global Energy Interconnection? Exploring China's Strategic Ambitions and Security Implications for Norway,' Norwegian Defence Research Establishment (FFI), Accessed: 9th Dec. 2025. [Online]. Available: https://www.ffi.no/en/publications-archive/a-global-energy-interconnection-exploring-chinas-strategic-ambitions-and-security-implications-for-norway.

[98] C. Boutin. 'NIST Announces First Four Quantum-Resistant Cryptographic Algorithms,' Accessed: 1st Sep. 2025. [Online]. Available: https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms.

[99] National Institute of Standards and Technology (NIST). 'The Road Ahead for Post-Quantum Cryptography.' Available: NIST: The Road Ahead for Post-Quantum Cryptography (PDF presentation), Accessed: 5th Dec. 2025.

[100] Norwegian University of Science and Technology (NTNU). 'Lattice-Based Cryptography.' Course material for TMA4160, Accessed: 23rd Aug. 2025. [Online]. Available: https://wiki.math.ntnu.no/_media/tma4160/lattice-i.pdf.

[101] A. Nadiga. 'Lattice Based Cryptography and Learning With Errors,' Accessed: 16th Sep. 2025. [Online]. Available: https://asnadiga.github.io/Documents/Post_Quantum_Crypto_and_LWE.pdf.

[102] H. Bennett, 'The Complexity of the Shortest Vector Problem,' Association for Computing Machinery, Tech. Rep. 1, 2023, pp. 37–61. DOI: 10.1145/3586165.3586172. Accessed: 23rd Aug. 2025. [Online]. Available: https://doi.org/10.1145/3586165.3586172.

[103] T. Chithralekha, K. Singh, G. Ganeshvani and M. Rajarajan, 'Post-Quantum and Code-Based Cryptography Some Prospective Research Directions,' *Cryptography*, vol. 5, no. 4, p. 38, 2021. DOI: 10.3390/cryptography5040038. Accessed: 16th Sep. 2025. [Online]. Available: https://doi.org/10.3390/cryptography5040038.

[104] A. Burton and S. Cheng. 'On Learning Parity with Noise in Different Noise Regimes,' Accessed: 16th Sep. 2025. [Online]. Available: https://www.cs.utexas.edu/~dwu4/courses/sp22/static/projects/BurtonCheng.pdf.

[105] A. Chailloux, T. Debris-Alazard and S. Etinski, 'Classical and Quantum Algorithms for Generic Syndrome Decoding Problems and Applications to the Lee Metric,' *CoRR*, vol. abs/2104.12810, 2021. Accessed: 23rd Aug. 2025. [Online]. Available: https://arxiv.org/abs/2104.12810.

[106] E. Fathalla and M. Azab, 'Beyond Classical Cryptography: A Systematic Review of Post-Quantum Hash-Based Signature Schemes, Security, and Optimizations,' *IEEE Access*, vol. 12, pp. 175 969–175 987, 2024. DOI: 10.1109/ACCESS.2024.3485602. Accessed: 16th Sep. 2025. [Online]. Available: https://doi.org/10.1109/ACCESS.2024.3485602.

[107] FAEST Team. 'FAEST Signature Algorithm,' Accessed: 19th Dec. 2025. [Online]. Available: https://faest.info/.

[108] J. Ding and B.-Y. Yang, 'Multivariate Public Key Cryptography,' in *Post-Quantum Cryptography*, D. J. Bernstein, J. Buchmann and E. Dahmen, Eds., Berlin, Heidelberg: Springer, 2009, pp. 193–241, ISBN: 978-3-540-88701-0. DOI: 10.1007/978-3-540-88702-7_6. Accessed: 16th Sep. 2025. [Online]. Available: https://doi.org/10.1007/978-3-540-88702-7_6.

[109] N. Kundu, S. K. Debnath, D. Mishra and T. Choudhury, 'Post-quantum digital signature scheme based on multivariate cubic problem,' *Journal of Information Security and Applications*, 2020. DOI: 10.1016/j.jisa.2020.102512. Accessed: 16th Sep. 2025. [Online]. Available: https://doi.org/10.1016/j.jisa.2020.102512.

[110] EU PQC Workstream, 'A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography,' European Commission, NIS Cooperation Group, Tech. Rep., 2025, Part 1, Version 1.1. Accessed: 5th Oct. 2025. [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography.

[111] I. Kong, M. Janssen and N. Bharosa, 'Challenges in the Transition towards a Quantum-safe Government,' in *Proceedings of the 23rd Annual International Conference on Digital Government Research: Intelligent Technologies, Governments and Citizens*, Association for Computing Machinery (ACM), 2022, pp. 282–292. DOI: 10.1145/3543434.3543644. Accessed: 1st Sep. 2025. [Online]. Available: https://doi.org/10.1145/3543434.3543644.

[112] Lovdata. 'Act relating to national security (Security Act).' LOV-2018-06-01-24, Accessed: 20th Dec. 2025. [Online]. Available: https://lovdata.no/dokument/NLE/lov/2018-06-01-24.

[113] Nasjonal sikkerhetsmyndighet (NSM). 'Veileder i departementenes identifisering av grunnleggende nasjonale funksjoner – Om denne veilederen,' Accessed: 3rd Nov. 2025. [Online]. Available: https://nsm.no/regelverk-og-hjelp/veiledere-og-handboker/veileder-i-departementenes-identifisering-av-grunnleggende-nasjonale-funksjoner/om-denne-veilederen/.

[114] Government of Norway. 'Nasjonal sikkerhetsmyndighet – Oppgaver og styring,' Accessed: 5th Nov. 2025. [Online]. Available: https://www.regjeringen.no/no/dokumenter/nasjonal-sikkerhetsmyndighet-oppgaver-og-styring/id3096862/.

[115] A. G. Rodriguez, 'A Quantum Cybersecurity Agenda for Europe II: Enabling Policy and Investment Options for the Quantum Transition,' European Policy Centre (EPC), Discussion Paper, 2025, Available: EPC: A Quantum Cybersecurity Agenda for Europe II (PDF). Accessed: 4th Nov. 2025.

[116] Nasjonal sikkerhetsmyndighet (NSM). 'Kvantemigrasjon veileder,' Accessed: 15th Aug. 2025. [Online]. Available: https://nsm.no/fagomrader/digital-sikkerhet/kryptosikkerhet/kvantemigrasjon/kvantemigrasjon-veileder.

[117] Cybersecurity and Infrastructure Security Agency (CISA), 'Post-Quantum Considerations for Operational Technology,' CISA, Tech. Rep., 2024. Accessed: 15th Nov. 2025. [Online]. Available: https://www.cisa.gov/sites/default/files/2024-10/Post-Quantum%20Considerations%20for%20Operational%20Technology%20%28508%29.pdf.

[118] Embassy of the People's Republic of China in Norway. 'Embassy Spokesperson's Response to the threat reports of relevant intelligence agencies of Norway,' Embassy of the People's Republic of China in Norway, Accessed: 9th Dec. 2025. [Online]. Available: https://no.china-embassy.gov.cn/eng/zngx_0/sbjw/202502/t20250206_11549665.htm.

[119] Government of Norway. 'National Security Strategy.' Available: regjeringen.no (PDF), Government of Norway, Accessed: 8th Dec. 2025.

[120] K. Townsend. 'Russian Telco Hijacked Internet Traffic of Major Networks – Accident or Malicious Action?' SecurityWeek, Accessed: 19th Oct. 2025. [Online]. Available: https://www.securityweek.com/russian-telco-hijacked-internet-traffic-major-networks-accident-or-malicious-action/.

[121] Ministry of Local Government and Modernisation (Norway), 'Meld. St. 28 (2020–2021): «Vår felles digitale grunnmur – Mobil-, bredbånds- og internettjenester»,' Tech. Rep., 2021. Accessed: 20th Oct. 2025. [Online]. Available: https://www.regjeringen.no/no/dokumenter/meld.-st.-28-20202021/id2842784.

[122] Norwegian Communications Authority (Nkom), 'EkomROS 2024: Risk and Vulnerability Analysis for the Electronic Communications Sector — Public Version,' Nkom, Tech. Rep., 2024. Accessed: 20th Oct. 2025. [Online]. Available: https://nkom.no/rapporter-og-dokumenter/ekomros24/_/attachment/inline/84cae401-d246-42cf-b44e-82d5ab8925b0%3A5e694cce827ec208b2b37f9f9e455ee1e41e3004/EkomROS%202024%20-%20offentlig%20versjon.pdf.

[123] Czech Cyber and Information Security Agency (NÚKIB), 'Útoky „Harvest Now, Decrypt Later",' NÚKIB, Tech. Rep. Č. j. 1216/2025-NÚKIB-E/630, 2025. Accessed: 20th Dec. 2025. [Online]. Available: https://nukib.gov.cz/download/publikace/analyzy/HNDL-FINAL.pdf.

[124] P. Krugman, *Why most economists' predictions are wrong*, Archived copy via the Internet Archive Wayback Machine, Red Herring, 1998. Accessed: 20th Dec. 2025. [Online]. Available: https://web.archive.org/web/19980610100009/http://www.redherring.com:80/mag/issue55/economics.html.

Appendix A

Interview questions

This appendix lists the prepared interview questions used in this study. Additional follow-up questions were asked during interviews when needed and are not included here.

General preparedness and prioritisation

1. How prepared is Norway if a cryptographically relevant quantum computer becomes available earlier than expected?
2. Which Norwegian sectors or functions are most critical or exposed to quantum-enabled threats?
3. To what extent should foreign strategic objectives (for example China/Russia) influence what Norway prioritises in PQC migration?
4. How realistic is a 2030-style target for migrating critical services to PQC, and what are the biggest implementation challenges?
5. How mature are Norwegian organisations in understanding the quantum threat and the need for PQC?
6. Do organisations treat the quantum threat as a current risk or mainly a future problem?
7. Is the "Harvest Now, Decrypt Later" risk being taken seriously in Norway?

Threat development and uncertainty

1. How do you expect the quantum threat to manifest in practice over time?
2. What is your view on scepticism about large-scale quantum computers (feasibility and expected impact)?

Operational technology (OT) and critical infrastructure

1. How much visibility do you have into where public-key (asymmetric) cryptography is used across your OT environment, including legacy and embedded components?
2. Are there concrete plans or ongoing discussions to address PQC in OT systems, or is it currently deprioritised compared to other risks?
3. How feasible is it to update or replace cryptographic components in OT systems within the next three years, given operational, safety, and availability constraints?

NTNU | Fakultet for informasjons-teknologi og elektroteknikk

Declaration of AI aids and -tools

Have any AI-based aids or tools been used in the creation of this report?

[ ] No

[X] Yes

If *yes*: please specify the aid/tool and area of use below.

Text

[X] **Spell checking**. Are parts of the text checked by:
Grammarly, Ginger, Grammarbot, LanguageTool, ProWritingAid, Sapling, Trinka.ai or similar tools?

[X] **Text generation**. Are parts of the text generated by:
ChatGPT, GrammarlyGO, Copy.AI, WordAi, WriteSonic, Jasper, Simplified, Rytr or similar tools?

[ ] **Writing assistance**. Are one or more of the reports ideas or approach suggested by:
ChatGPT, Google Bard, Bing chat, YouChat or similar tools?

If *yes*, use of text aids/tools apply to this report - please specify usage here:

Grammarly and GPT-5.2 (OpenAI) tools were used for improving the grammar and clarity of sentences written by me. No new content was generated by any LLM tool. AI Assist (Overleaf) was used for LaTeX assistance.

Codes and algorithms

[ ] **Programming assistance**. Are parts of the codes/algorithms that i) appear directly in the report or ii) have been used to produce results such as figures, tables or numerical values been generated by: *GitHub Copilot, CodeGPT, Google Codey/Studio Bot, Replit Ghostwriter, Amazon CodeWhisperer, GPT Engineer, ChatGPT, Google Bard* or similar tools?

If *yes*, use of programming assistance aid/tools apply to this report - please specify usage here:

Images and figures

[ ] **Image generation**. Are one or more of the reports images/figures generated by:
Midjourney, Jasper, WriteSonic, Stability AI, Dall-E or similar tools?

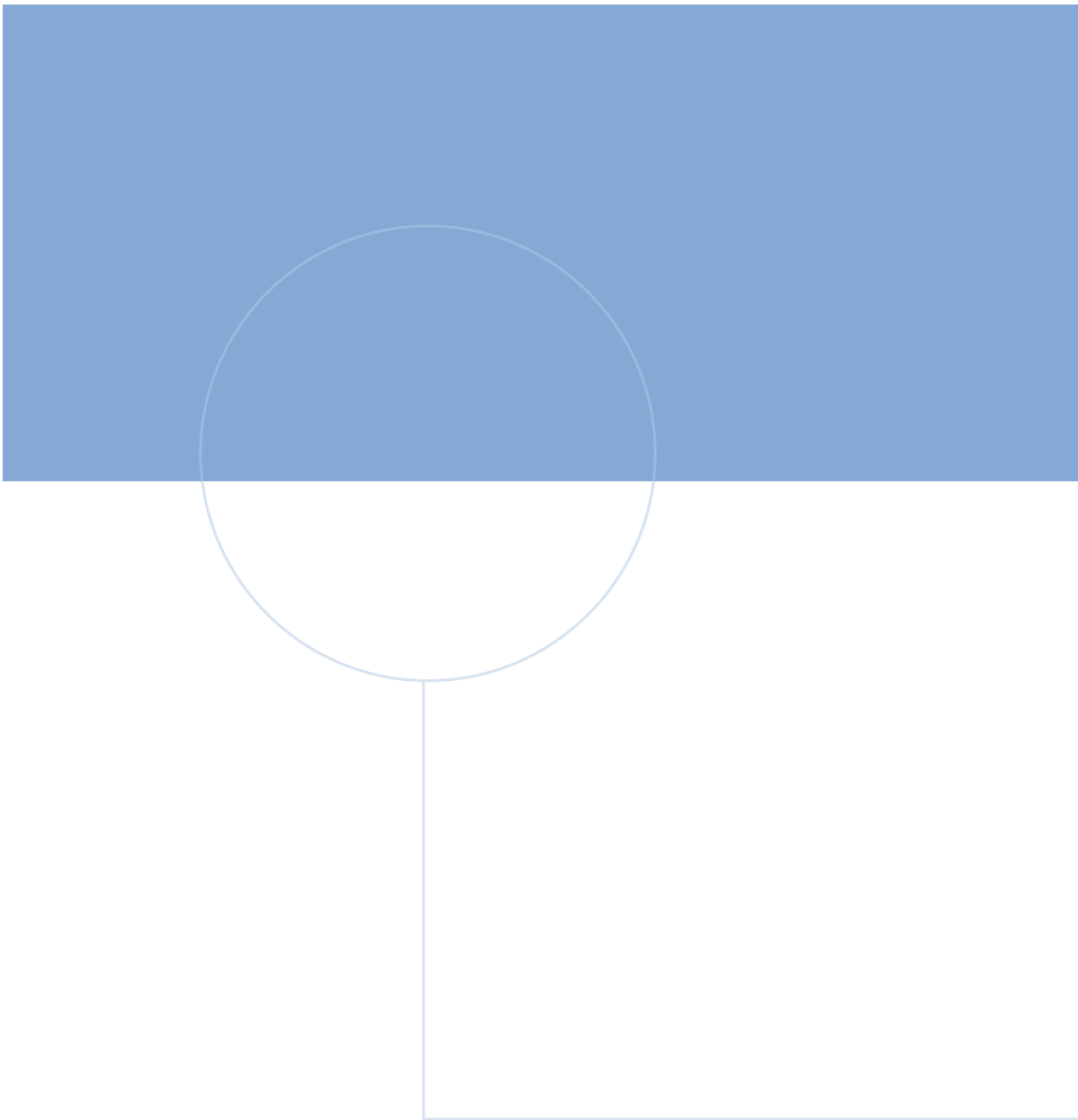
If *yes*, use of image generator aids/tools apply to this report – please specify usage here:

[ ] **Other AI aids or tools**. Have you used other types of AI aids or -tools in the creation of this report?
If yes, please specify usage here:

[X] I am familiar with NTNU's regulations: *Submitting a report generated with the assistance of AI tools and claiming the work to be partially or fully my own, is not permitted. I therefore declare that any use of AI aids or tools are explicitly stated i) directly in the report or ii) in this declaration form.*

Paulina Wesolowska, 22.12.25, Oslo

Signature/Date/Place



NTNU

Norwegian University of
Science and Technology