



**Focus on
quantum
technology
in central
government**

2026



**Netherlands
Court of Audit**

Contents

1. Executive summary | 3

2. About this investigation | 7

- 2.1 Why did we carry out this investigation? | 7
- 2.2 What is quantum technology? | 8
- 2.3 Structure of this report | 9

3. Opportunities for society | 10

- 3.1 Quantum applications | 10
- 3.2 Quantum technology development policy | 13
- 3.3 Investment results | 15
- 3.5 Final phase of the National Growth Fund | 18
- 3.6 Challenges for the future | 18

4. Opportunities for the State | 21

- 4.1 Experimenting with quantum in government | 21
- 4.2 Policy on the use of quantum technology | 24
- 4.3 Obstacles to the use of quantum technology | 24

5. The threat of quantum computers to the State | 27

- 5.1 Quantum computers can crack cryptography | 27
- 5.2 Organisations need to replace their cryptography | 30
- 5.3 How does central government promote quantum risk mitigation? | 32
- 5.4 The PQC migration of government organisations | 34
- 5.5 Obstacles to preparing for the quantum threat | 41

6. Response | 44

Appendices | 45

- Appendix 1 Methodology | 45
- Appendix 2 Selected organisations | 48
- Appendix 3 References | 50
- Appendix 4 Endnotes | 54

1.

Executive summary

Quantum technology. It sounds like something from the future, perhaps it is. But there is already a global race to master this new technology. A technology that, after AI, might revolutionise society. It offers many economic opportunities for the Netherlands, but also risks. How is the country preparing for quantum? What is the government doing to mitigate risks and seize opportunities? What public money is being invested and what policies are being implemented? These questions are at the heart of this investigation.

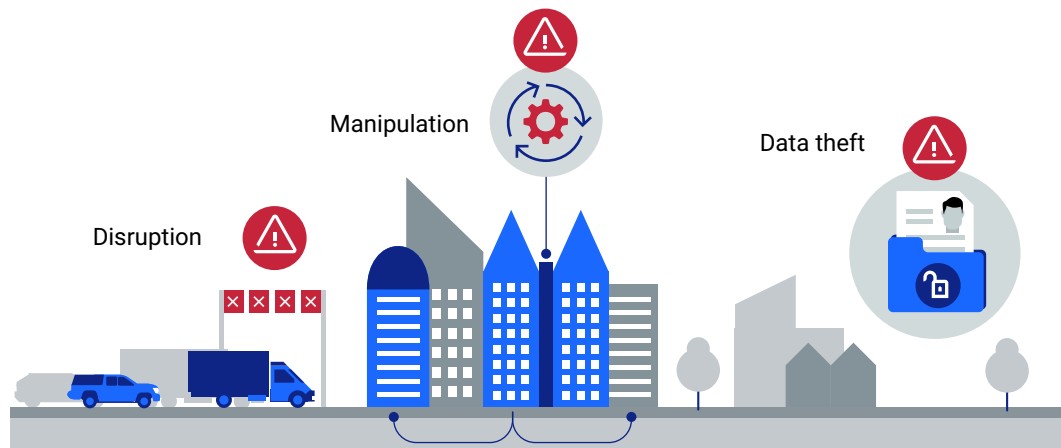
Quantum computers are a threat to the security of government information

- The risk of quantum technology is that powerful quantum computers could be used to crack cryptography. Cryptography is a technique to secure digital information and IT systems. The government uses it in all kinds of applications, for instance, to:
 - protect confidential personal and commercial information;
 - regulate access to vital infrastructure such as flood defences and bridges;
 - log in with DigiD, the government's official digital verification system;
 - verify the authenticity of passports.

If quantum computers can crack cryptography, they will put all these applications at risk, with the inevitable societal consequences. The moment they can crack cryptography is known as Q-day. It is uncertain when exactly Q-day will arrive, but the General Intelligence and Security Service (AIVD) warns that it could be as early as 2030 (AIVD et al., 2024).

Figure 1 Examples of quantum threats to the State

Quantum computers threaten confidential information and vital infrastructure of the State



The government must prepare for the threat of quantum computers

Worldwide, scientists are working hard to mitigate the quantum threat. New forms of cryptography are being developed that are resistant to quantum computers: post-quantum cryptography (PQC). To mitigate the risks, government organisations must transition their current cryptographic processes to this safer variant. The transition is known as PQC migration.

Government support to tackle quantum threats

The State Secretary for Digitalisation recognises that, when used by malicious actors, quantum computers can endanger national security. That is why he has launched QvC NL, a quantum-safe cryptography programme, to share information and develop guidelines and so help government organisations with their PQC migrations. Government organisations are themselves pushing to introduce quantum-safe cryptography.

Few government organisations have started addressing quantum threats

There are concerns that government organisations will not start their PQC migration in time. Although most of the government organisations we surveyed are strengthening their information security, few have taken measures that specifically address the threat posed by quantum computers.

Figure 2 Percentage of organisations that have started addressing quantum threats

71% of the organisations have not started addressing quantum threats



Most government organisations have not yet held talks with their suppliers about quantum-safe products or made plans to introduce quantum-safe cryptography. The main obstacles they name are lack of capacity and expertise, and other activities having higher priority because they are considered more urgent.

The government is investing in quantum technology

Quantum technology offers the government, society and the economy many opportunities. It may enable us to make more accurate measurements, communicate more securely and perform complex calculations. This offers opportunities for energy-efficient food production, new materials and enhanced cybersecurity. The government sees quantum technology as a key technology with huge economic potential for the Netherlands. The government will invest €615 million in its development through the National Growth Fund in 2021-2028.

The Netherlands is a quantum leader, but will it remain so?

Investment through the National Growth Fund has established a thriving quantum network and made the Netherlands an academic world leader in the technology. The network includes the Quantum Delta NL foundation, the Netherlands Organisation for Applied Scientific Research (TNO) and knowledge centres. The National Growth Fund's advisory committee is impressed with the results the investment has yielded so far. However, there is still work to be done. Many plans and projects are still being set up and it is difficult to predict whether the Netherlands will retain the top spot. The challenge for the future is to translate the potential into tangible applications and secure a position in the high-tech market. Some countries have invested substantially more public money than the Netherlands in quantum technology in recent years.

28% of government organisations have explored quantum opportunities

Quantum technology also offers opportunities to the government. Yet most of the government organisations we surveyed have not yet explored the technology's potential, partly because it is not clear what tasks quantum technology could perform better than current systems.

Figure 3 Percentage of organisations surveyed that have explored the potential of quantum technology

28% of the organisations have explored the opportunities offered by quantum technology



Most of the exploratory studies that have been carried out consider where and how quantum technologies can generate added value. Government organisations indicate that the technology still needs further development. They also say several obstacles will need to be overcome when the technology breaks through in the future, such as lack of knowhow and expertise and incompatibility with the current technical infrastructure.

The government is working on a government-wide Quantum Strategy

The Ministry of Economic Affairs is currently working with other ministries on a government-wide Quantum Strategy. The strategy will underline quantum technology's strategic importance and set targets and actions to address both the opportunities and the risks.

Why this investigation?

Risks need to be managed if central government is to perform and operate effectively. In our opinion, the current preparations should allow not only for the opportunities but also the threats. Only when it is known how the government is preparing for the opportunities and mitigating the risks can parliament oversee the responsible use of quantum technology. This investigation offers a first insight into the government's preparations for quantum's opportunities and risks. It also summarises the investment results achieved to date.

2.

About this investigation

2.1 Why did we carry out this investigation?

To celebrate the 100th anniversary of quantum mechanics, the United Nations has declared 2025 the International Year of Quantum Science and Technology. A meeting on quantum technology will take place somewhere in the world on every day of the year. The Netherlands is also taking part; the government sees quantum as a key technology to unlock multiple economic opportunities. The government defines a key technology as one that is vital to future economic growth and in which the Netherlands excels scientifically.

Through its National Technology Strategy (NTS), the government is promoting innovation and strengthening the Netherlands' technological leadership in 10 areas. Quantum technology is one of those areas (Ministry of Economic Affairs and Climate Policy, 2024). Through the National Growth Fund, the government will invest at least €615 million in the technology in 2021-2028. Quantum technology is projected to trigger governmental, business and societal innovations that are currently inconceivable.

The government is investing in quantum technology to guarantee the Netherlands' technological sovereignty. The thinking behind the investment is to create a strong, innovative and competitive economy that is more resilient to national security threats. This raises the question of what the investment has achieved so far. At present, however, there is no up-to-date public overview of the results. There is also a lack of insight into the opportunities that the government believes quantum technology holds for it.

Quantum technology, however, is not without risk. At some point, cracking current encryption methods will be child's play for a quantum computer. State or commercial secrets can then fall into the hands of malicious actors. There are also risks to vital infrastructure. The National Coordinator for Counterterrorism and Security (NCTV) argues that powerful quantum computers will pose a threat to national security.

The government's preparations for the technological risks are not known. However, due to rapid technological advances and geopolitical tensions, there is a growing need to know what they are. Developments in the Netherlands should be seen in the light of the European Commission's and the EU member states' response to the quantum threat.

2.2 What is quantum technology?

Quantum technology is a collective term for technologies that take advantage of the special properties of subatomic particles known as quanta (singular: quantum). Quantum technology uses the tiny particles' special behaviour to calculate, communicate and measure in a radically new way. This is different from current technology where computers work with bits (0 or 1). The building blocks of quantum computers are qubits. Thanks to the unique behaviour of quantum particles, qubits can simultaneously assume both the value 0 and 1. As a result, quantum computers can perform complex calculations much faster than classical computers.

2.2.1 Potential applications of quantum technology

Quantum technology offers a broad spectrum of applications to combat climate change, for the energy-efficient production of food, new materials and medicines, to solve optimisation problems, and for machine learning and cybersecurity. The 3 main quantum technologies are:

- **Quantum sensors** that use the characteristics of quantum mechanics to make ultra-precise measurements.
- **Quantum communication** that exchanges information between quantum computers and between quantum computers and quantum sensors.
- **Quantum computers** that perform complex calculations faster than classical computers (Rathenau Institute, 2023). The calculations can have major consequences for society. They can accelerate the development of new drugs, battery materials and superconductors (European Commission, 2025).

Despite all the opportunities, the enormous computing power of quantum computers is a risk to information security. Powerful quantum computers could crack important cryptography one day. Cryptography is a technique to digitally encrypt data when information is used and transferred within and between organisations, and also when information is stored on location or in the cloud. The solution to this threat is post-quantum cryptography (PQC). We will return to PQC in chapter 5.

2.3 Structure of this report

In chapter 3 we look at the opportunities of quantum technology and its current status in the Netherlands. In chapter 4 we describe how the government is seizing the quantum opportunities. Finally, in Chapter 5, we show how government organisations are currently preparing for the threats posed by quantum computers.

3.

Opportunities for society

The government sees quantum as a key technology with huge potential for the Netherlands' earning capacity. Quantum is not yet mainstream but there is a lot of excitement about its future applications. Quantum technology could trigger a new technological revolution. Through the National Growth Fund, the Netherlands will invest €615 million in this new technology between 2021 and 2028. A thriving quantum network has been established and the Netherlands has become an academic leader in the field. The results already achieved include the creation of several Houses of Quantum, testbeds for quantum sensors and a new quantum computer.

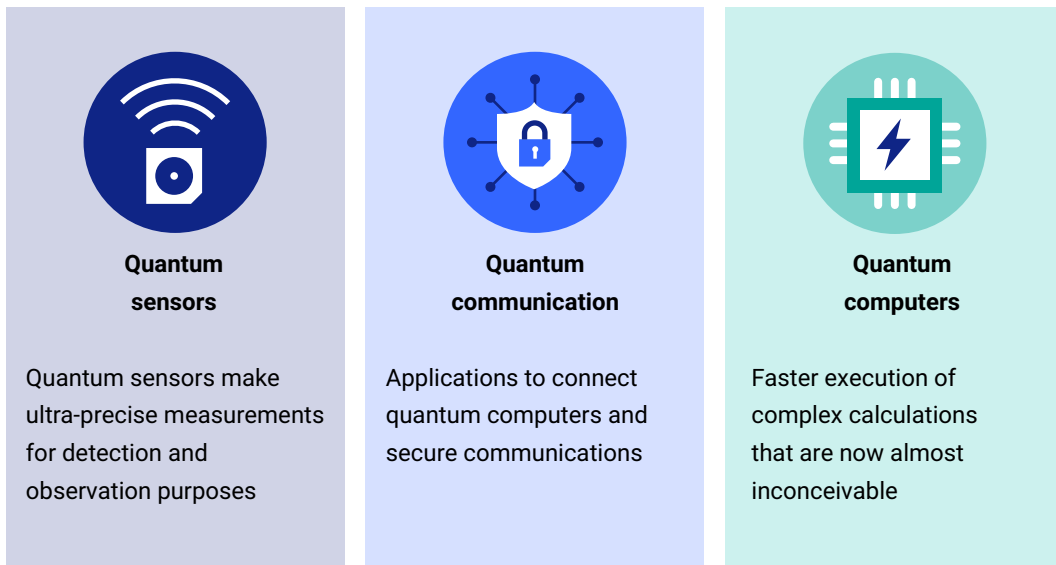
Many plans and projects are still under development and it is difficult to predict whether the Netherlands will retain its leadership. Other countries have invested substantially more public money in quantum technology in recent years. The government expects the quantum ecosystem to reach the next level of maturity after support from the National Growth Fund ends. Additional public funding will then be needed for further development.¹

3.1 Quantum applications

Quantum technology has great potential for society and government organisations. We can look forward to a raft of applications using the 3 forms of quantum technology.

Figure 4 *The 3 forms of quantum technology*

Quantum technology has 3 application areas



3.1.1 Quantum sensors

Quantum sensors can make ultra-precise measurements. They can detect magnetic fields, accelerations, rotations, time and pressure (Ministry of Infrastructure and Water Management, 2025). They can detect underground objects such as gas and water reservoirs, minerals, cables and pipelines and observe other phenomena, such as earthquakes (Europol, 2023). Quantum sensors also have the potential to measure electrical activity in the heart more accurately (World Economic Forum, 2024). Doctors will then be able to better detect medical conditions. Precision medicines will be just one of the benefits for the medical world (OECD, 2025).

Development of quantum sensors is relatively advanced. They will probably be the first widely applicable quantum technology. Although they are already on sale, it may take many years before they are truly useful in practice. Their high sensitivity also makes them susceptible to disturbances. Moreover, they are very expensive. As a result, quantum sensors that work well outside a laboratory environment are not yet available (Ministry of Infrastructure and Water Management, 2025).

3.1.2 Quantum communication

Quantum communication will enable very secure connections for quantum computers to exchange information with classical computers. Any attempt to intercept, read or retransmit qubits will be detectable. Quantum networks will also enable connections that are potentially very secure. This is relevant in the financial, logistics, internet and telecom sectors and to government (Quantum Delta NL, 2021).

A widely debated application is quantum key distribution (QKD) to securely exchange secret keys and enable secure communication between 2 parties. QKD has the potential to protect computers against highly advanced attacks. Several experts we spoke to saw secure quantum networks as one of quantum technology's first definite opportunities for government. They saw growing opportunities for secure quantum networks, particularly in view of current geopolitical tensions.

However, the technology still needs further development. Several limitations, such as operation over longer distances, costs and vulnerabilities, have yet to be resolved (AIVD et al., 2024). A small-scale quantum network has been built in the Port of Rotterdam (Port of Rotterdam, 2024) that is being used to experiment with secure connections. This network could be rolled out more widely in the future.

3.1.3 Quantum computers

Quantum computers can potentially solve problems that are practically unsolvable by classical computers. In particular, they can simulate the design of molecules and drugs. Simulating interactions between molecules requires far more computing power than today's supercomputers can provide. By performing these complex calculations faster and more accurately, quantum computers will accelerate the development of new drugs (OECD, 2025). Experts we spoke to said computing centres currently concentrate most of their capacity on such applications.

Quantum computers also offer opportunities in diverse optimisation fields such as complex logistics planning, especially if there are many variables in a product's supply chain. Quantum computers' potential to train AI systems is also being studied (OECD, 2025). The combination of quantum technology and AI could lead to new, faster and more economical AI models (Europol, 2023).

Quantum computing is the least advanced form of quantum technology.² At present, no quantum computer has made a calculation faster than a classical computer, which is the ultimate aim. By way of illustration, a quantum computer being built in Amsterdam will have a minimum of 'just' 16 qubits (Quantum Delta NL, 2024), whereas quantum computers have added value from about 1,000 qubits. Experts agree, however, that quantum computers are making steady progress.

3.2 Quantum technology development policy

The government sees quantum as a key technology. As early as 2012, it invested millions to support innovative quantum research (House of Representatives, 2012). In 2020, the government again claimed that quantum technology had huge potential for the future (House of Representatives, 2020). Leadership in quantum technology also enables the Netherlands to withstand national security threats (Ministry of Economic Affairs, 2025). Quantum technology offers opportunities not only to strengthen national security, but also for the earning capacity of the Netherlands. In 2021, the Quantum Delta NL programme was launched with a total investment of €615 million from the National Growth Fund. Its aim is to develop quantum technology for the benefit of the government, society, business and knowledge institutions.

3.2.1 The Netherlands' ambitions

Government policy is to create a world-class quantum ecosystem with the Netherlands as a world leader in quantum technology by 2035. The ecosystem is populated by scientific, educational, high-tech, startup and governmental organisations. The government wants Dutch businesses to be key players at European or global level, with a strategic market presence: the Netherlands as quantum technology's Silicon Valley, the home of new technologies and high-tech industry.

The Minister of Economic Affairs coordinates the promotion of quantum technology in the Netherlands. To put the policy into practice, Quantum Delta NL (QDNL) was established in 2020 to accelerate the Netherlands' development and commercialisation of quantum technology. It promotes quantum technology through the Quantum Delta NL programme. The various projects in the programme are carried out by QDNL itself or by established organisations and consortia such as QuTech, TNO, universities, the Dutch Research Council (NWO), the Netherlands Enterprise Agency (RVO) and NanoLabNL.

3.2.2 Investments

Together with Quantum Delta NL, the Minister of Economic Affairs submitted a grant application to the National Growth Fund for the Quantum Delta NL programme in 2021. Through the National Growth Fund, the government is investing in projects that will make the greatest possible contribution to sustainable and structural economic growth. Quantum Delta NL has received €615 million from the National Growth Fund (National Growth Fund, n.d.). The Quantum Delta NL programme will end in 2028,

after which there are no plans to provide more public money. The government has discontinued the final tranches of the National Growth Fund. Future plans therefore cannot be financed from the National Growth Fund.

Other organisations, such as TNO and NWO, are also contributing financially and scientifically to the development of quantum technology. Several other funding sources are available to promote quantum technology. The private sector is also investing in quantum technology. This investigation, however, focuses solely with the investment of public money through the National Growth Fund.

3.2.3 Monitoring and evaluation

Quantum Delta NL is accountable for the investments and programme results and the Ministry of Economic Affairs for their evaluation. Quantum Delta NL draws up a progress report every six months to account for the relationship between grant applicants and the Netherlands Enterprise Agency (RVO). In 2023 it also carried out a broader mid-term review of the programme.

Quantum Delta NL's internal evaluation concluded that the programme was on track. The findings were reported to the Minister of Economic Affairs, RVO and the National Growth Fund. The House of Representatives also receives progress information from the National Growth Fund's advisory committee regarding, for instance, the allocation of funds from the third evaluation round (House of Representatives, 2024). The House also received the National Growth Fund's 2024 annual report (Ministry of Economic Affairs, 2025). The National Growth Fund's advisory committee wrote that it was impressed with Quantum Delta NL's progress and performance.

3.2.4 European initiatives

The European Commission wants the European Union to benefit from quantum technology. Quantum technology can increase European industry's competitiveness and offer opportunities for Europe's technological sovereignty. The Commission has been investing in quantum technology for several years. In the past 5 years, it has allocated nearly €2 billion to various European quantum projects (Quantum Flagship, 2025). Notable initiatives include:

- the €1 billion Quantum Technologies Flagship, over 10 years (2018-2028) (European Commission, 2025b);
- the €7 billion European High Performance Computing Joint Undertaking (EuroHPC) to build quantum computers (European Commission, 2025c). The Netherlands is involved in the construction of a quantum computer in Amsterdam at a cost of €10 million;

- the €90 million EuroQCI initiative to develop an EU-wide quantum communication infrastructure (European Commission, 2025d). The Netherlands' contribution includes the €17.8 million SEEWQCI project.

European Quantum Strategy and Quantum Regulation

In July 2025, the European Commission published the European Quantum Strategy. It testifies to Europe's ambition to be a world leader in quantum technology by 2030. Key challenges facing the European Commission are the translation of academic breakthroughs into commercial successes and the fragmented approach and investments by EU member states.

The government welcomes the European Quantum Strategy as a desirable and opportune development. It is in line with the current Dutch policy to build a robust quantum ecosystem and capitalise on academic knowledge (Ministry of Economic Affairs, 2025b). The Ministry of Economic Affairs is seeking to link up with the European strategy in order to accelerate the Dutch ecosystem. The ambitions for quantum technology are very high worldwide and there is keen international competition. According to the Ministry of Economic Affairs, cooperation with other European countries is necessary to consolidate national initiatives, build additional strength and create a wider market.

The European Commission is also preparing a Quantum Regulation, with publication expected in 2026. Details are still missing but the policies and investment frameworks in the regulation will be more mandatory.

3.3 Investment results

Quantum Delta NL has been laying the foundations for a quantum ecosystem since its launch in early 2021. A substantial proportion of the funding (€181 million) from the National Growth Fund is spent on quantum research and development. Investments have been made in testbeds, quantum connections, training programmes and a quantum computer in the cloud with online user access. Another substantial part of the programme (€249 million) is devoted to the development of facilities and fixed infrastructure such as a national campus, technology platforms and cleanrooms to support quantum research and development. Cleanrooms are dust-free enclosed environments to develop quantum systems.

Quantum Delta NL has financed several projects from the National Growth Fund since 2021. The figure below shows budgeted amounts per action line.

Some interim results up to 2024 are presented in figure 5.

Figure 5 Results to date of the Quantum Delta Programme

The Quantum Delta NL programme

The amounts involved, results achieved and ambitions

Quantum Delta NL programme in millions of euros	Results (2024)	Ambition
Research and innovation ■ 42	75 ongoing PhDs in quantum technology and 23 top scientists	Promote foundational research for technology development
Quantum ecosystem ■ 83	House of Quantum in Delft, valorisation team operational and startup programme completed	National campus, quantum valorisation team, startup programme and field labs
Human Capital ■ 41	4 talent and learning centres established, 722 quantum graduates, national quantum course launched	Talent development and educational programmes
Societal Impact ■ 20	Centre for Quantum and Society established and governance for quantum technology	Growing societal acceptance of quantum technology
Quantum Computing & Simulation ■ 90	Quantum Inspire 2.0 with new quantum processors	Develop quantum computer with at least 100 qubits
National Quantum Network ■ 62	R&D Network with 3 quantum processors	Multiple quantum networks and fundamental national infrastructure
Quantum sensing applications ■ 29	3 quantum sensor testbeds operational	Further expansion of testbeds
Cleanroom facilities ■ 150	5 cleanrooms available to develop nano equipment	Renew equipment and adapt machines for future developments
Campus development ■ 99	Several House of Quantum locations opened	Multiple House of Quantum locations in the Netherlands, new cleanroom and more shared facilities

Source: Quantum Delta

3.4 Results to date

Several programme milestones have already been passed. A second House of Quantum has been opened in Delft, there is a first quantum network of 25 km between The Hague and Delft (Quantum Delta NL, 2024b), 3 testbeds for quantum sensors are operational and a fund has been established for quantum startups (Quantum Delta NL, 2025). Other results achieved by the programme include:

- the growth from 500 quantum jobs in 2021 to 800 in 2024;
- the retention of academic excellence;
- the establishment of a Centre for Quantum and Society to study the societal impact of quantum technology.

The programme is progressing in step with the goals it set for itself.

The organisations we spoke to that were benefiting from National Growth Fund projects were very satisfied with the opportunities: *'The National Growth Fund has made a very significant contribution to the quantum ecosystem in the Netherlands and to the country's international standing. It has also attracted a great deal of talent.'*

In recent years, the Netherlands has been a leader in quantum technology. According to the experts we spoke to, there is interest from abroad in the Dutch quantum ecosystem: *'The Netherlands is a global player, it's exemplary and is leading the way'*. They observe that many other countries do not have an umbrella organisation like Quantum Delta NL.

The people we interviewed confirmed that the Netherlands had a strong international reputation. Academic leadership was one of the reasons to establish Quantum Delta NL: to create economic opportunities through our academic pre-eminence. The Netherlands already ranked as one of the leading academic centres for research into quantum technology in 2020 (Birch, 2020). According to research by Quantum Delta NL (Birch, 2024), it still held a strong position in 2024. This study indicates that we are still among the top academic research centres for quantum technology.

3.5 Final phase of the National Growth Fund

The Quantum Delta NL programme's third and final phase began in 2025. This phase focuses on growing the ecosystem and generating economic added value for the Netherlands. Goals set for this phase include:

- 3,500 quantum-related jobs in the Netherlands;
- 100 startups;
- 25 end users of services developed with funding from Quantum Delta NL.

For the longer term (2040), Quantum Delta NL aims to boost gross domestic product by 0.02 to 0.04% (€230-460 million) every year. It also wants the programme to create between 8,000 and 18,000 jobs in the quantum industry. In total, the programme would then add €1.5 to 2.5 billion to the economy. This would recoup the €615 million investment more than threefold. The overarching goal for this phase is for quantum technology to have a resounding economic impact. Our interviewees at the Ministry of Economic Affairs believe that scaling up is needed now, startups need to become scaleups and there needs to be a real tie-in with the high-tech market.

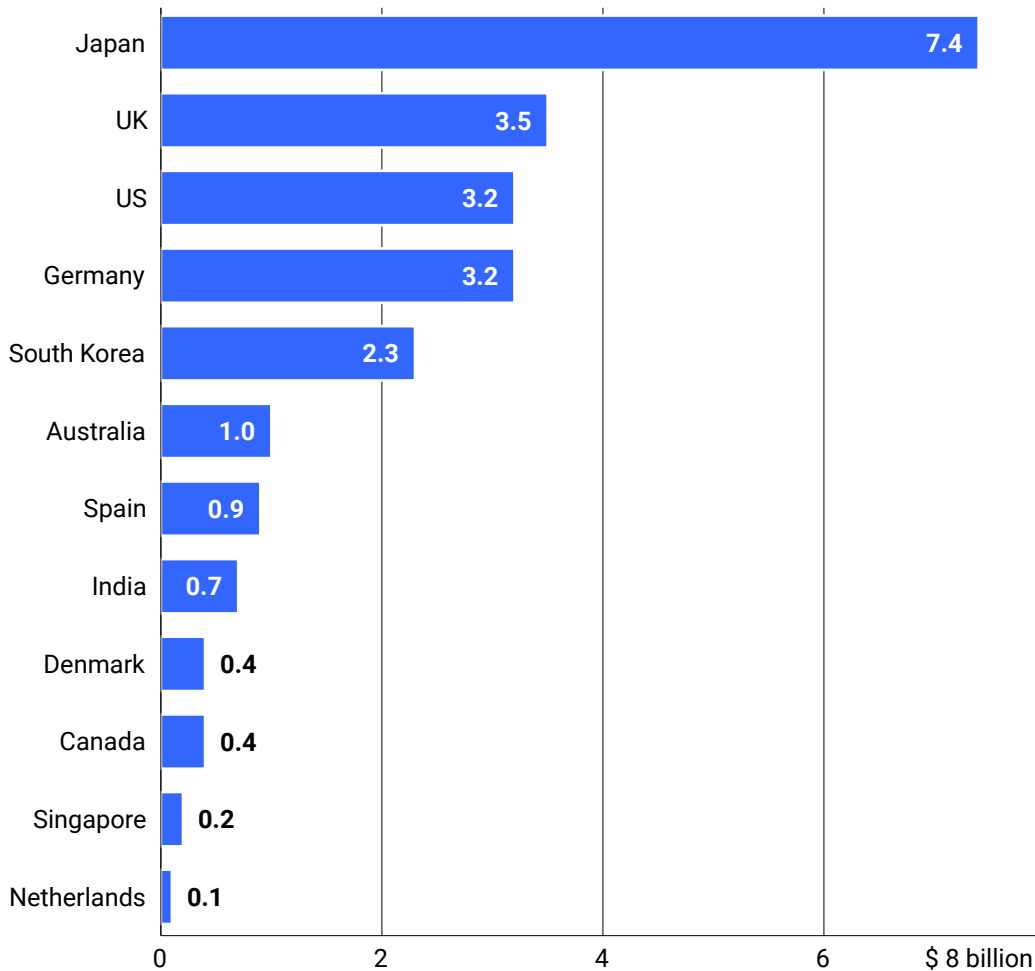
Although the programme is progressing well, the momentum has to be continued in the years ahead. Many of the programme's major milestones are yet to be achieved, such as the launch of Quantum Inspire 3.0, a quantum computer with 100+ qubits, scheduled for 2028. Other goals require a multiplication of the results achieved so far. For example, Quantum Delta NL's objective is to increase private sector investment in startups and scaleups from about €100 million in 2024 to about €750 million per annum by the time the programme ends. This is a substantial increase. Private sector investment in the Netherlands, however, is significantly lower than in other countries (Birch, 2024).

3.6 Challenges for the future

Recent years have seen an expansion in the Dutch quantum ecosystem. The main challenge now is to maintain the leadership the Netherlands has built up. Although the Dutch quantum ecosystem has grown and is internationally renowned, other countries are recording faster growth (Birch, 2024). The Netherlands stood out until 2022 for its substantial public investments, but other countries have been investing significantly more since 2023 (McKinsey, 2025). Japan, for instance, recently announced that it would invest 1 trillion yen (€6 billion) in quantum technology (Quantum Insider, 2025). It is feared that other countries are slowly overtaking the Netherlands and the country is losing its pre-eminence.

Figure 6 Announced public investments in quantum technology, 2023-2025

The Netherlands has invested relatively little public money in quantum technology



Private parties can also invest in quantum. Experts indicate that the ecosystem in the Netherlands should give higher priority to attracting private investors and end users of the quantum technology already developed. Quantum Delta NL says it is a challenge to find businesses that are willing to invest in the Netherlands and the programme will therefore work extra hard on attracting them during the final phase.

Some interviewees admitted that the end of Quantum Delta NL's funding would be a major challenge for the ecosystem in the Netherlands. The Dutch ecosystem is not yet mature and needs to attract capital. Experts we interviewed stressed the importance of a reliable long-term strategy. Without stability and confidence in the future of quantum technology, independent of a change of government, there is a risk that companies will look abroad.

The European Commission will continue to invest heavily in quantum technology in the coming years. However, our interviewees indicate that European funding cannot be a substitute for national investments. National cofinancing is a precondition for the receipt of EU funding. Money must also be available for national cofinancing. QCINed, for example, is an EU programme that would not be eligible for European funding without cofinancing from Quantum Delta NL.

The Minister of Economic Affairs is aware that support for quantum technology is still needed. We concluded from the discussions we held, however, that there is currently no prospect of further financing through a new growth fund. One interviewee put it as follows: *'By 2028, the programme's objectives should have been achieved and the ecosystem should have matured. The question of whether and how new funding will be needed will depend on a thorough analysis and recognition of what the ecosystem actually needs. A new growth fund may have a role to play but other forms of financing should also be considered'*. The Minister of Economic Affairs indicated that it would be logical for the Netherlands to continue its support in one way or another.

4.

Opportunities for the State

Quantum technology also offers opportunities for the State of the Netherlands. Exploratory studies of its potential for the State are in their infancy, but there is interest in the technology and its relevance to economic security. Yet most of the government organisations we interviewed said they had not explored the opportunities that quantum technology could offer. This was due partly to the lack of practical ideas about what quantum technology could do better than current systems.

Should quantum technology break through in the future, other obstacles might prevent the State from benefiting from the opportunities. Finding suitable quantum applications will be difficult. Its use might be restrained by high procurement and maintenance costs. New quantum technology must also be compatible with the current technical infrastructure in order to minimise the need for replacement investments.

4.1 Experimenting with quantum in government

In the future, there will be opportunities for the government to use quantum technology. Quantum sensors in particular offer opportunities to navigate without GPS and better detect submarines (European Parliamentary Research Service, 2024). This is particularly relevant to military applications. The Ministry of Defence has already tested a backpack with quantum sensors that can better detect and identify weapons remotely (Ministry of Defence, 2023). Sensors can also play a role in improving the measurement of water quality, air pollution and particulate matter, and in plastic recycling and traffic management.

We asked government organisations whether they saw applications for quantum technology. They showed interest in its potential in service delivery. Yet more than 60% (38) of the organisations said they had not explored the opportunities that quantum technology could offer (see figure 7). They gave various explanations for this. Some were more concerned about the threats of quantum technology. Others said *'there is no obvious use case'*. These organisations saw few avenues for the use of the new technology in their work.

Figure 7 Percentage of organisations surveyed that have explored quantum potential

28% of the organisations have explored the opportunities offered by quantum technology



A quarter of organisations (16) have explored or are currently exploring the opportunities of quantum technology. Some have published their findings in public reports. In *From Bits to Qubits* (May 2025), for instance, the Ministry of Infrastructure and Water Management sketches potential future applications that some of its organisations could use.

Quantum Delta NL has published a first survey of the Ministry of Finance's use of quantum technology (Quantum Delta NL, 2023b). The Central Government Audit Service has studied whether matching employees to projects could improve its annual staff planning. It has also piloted the use of quantum technology to detect discrepancies in annual reports. The ministry recognises there are opportunities but they must address specific problems: *'We have discovered that quantum technology can offer benefits but it does not improve everything.'* The ministry will nevertheless continue to follow the development of quantum technology.

Several organisations expressed an interest in quantum communication, especially for high-security connections. *Quantum Key Distribution* (QKD) has already been piloted in several projects in the Netherlands, including in a quantum network to test the use of quantum-protected communication at the Ministries of Foreign Affairs and Justice and Security (Central Government, 2025).

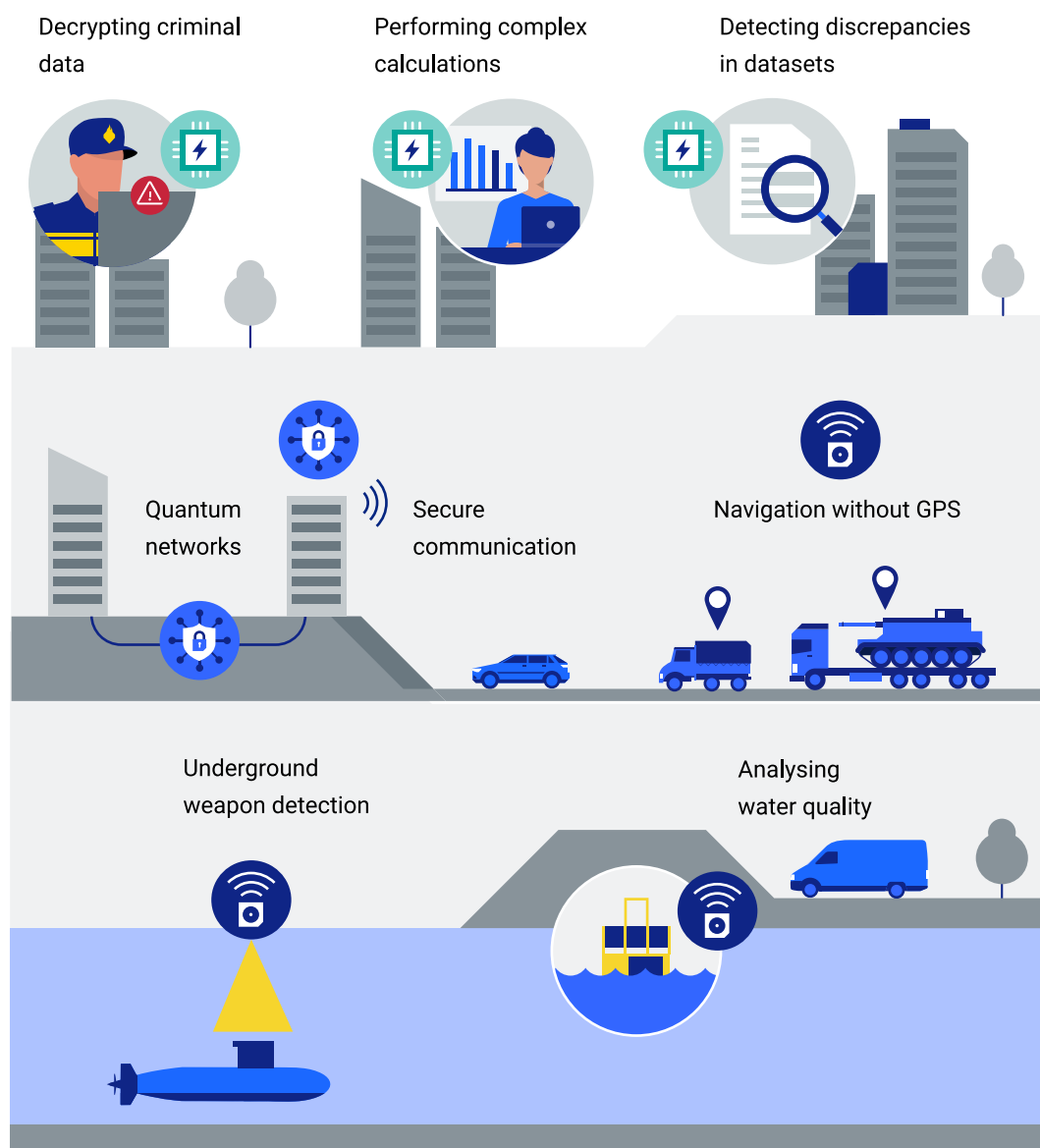
Some organisations also mentioned quantum computers' potential to overcome the limitations of current computing power. However, they indicated that most applications with quantum computers would be relevant to only a handful of highly

specific problems. Not every government agency has such problems. For the time being, they relate mainly to military applications or very complex calculations with many variables or the storage of data obtained from criminals for later decryption.

The exploratory studies have led to few concrete results or practical applications of the technology. Government organisations indicate that the technology still needs further development: *'So far, the conclusion is that it is rather too early to present concrete use cases for quantum technology'*. Another organisation said future advances could cast a different light on the studies. The exploratory studies may have to be revisited if there is a technological breakthrough.

Figure 8 Possible applications of quantum technology

Quantum technology offers central government many opportunities



4.2 Policy on the use of quantum technology

The State Secretary for Digitalisation indicated at the beginning of 2025 that quantum technology could fundamentally change the government (House of Representatives, 2025). In the long run, it could enable better, safer and faster digital services. We found that studies of possible opportunities for government organisations were carried out mainly on the initiative of the organisations themselves.

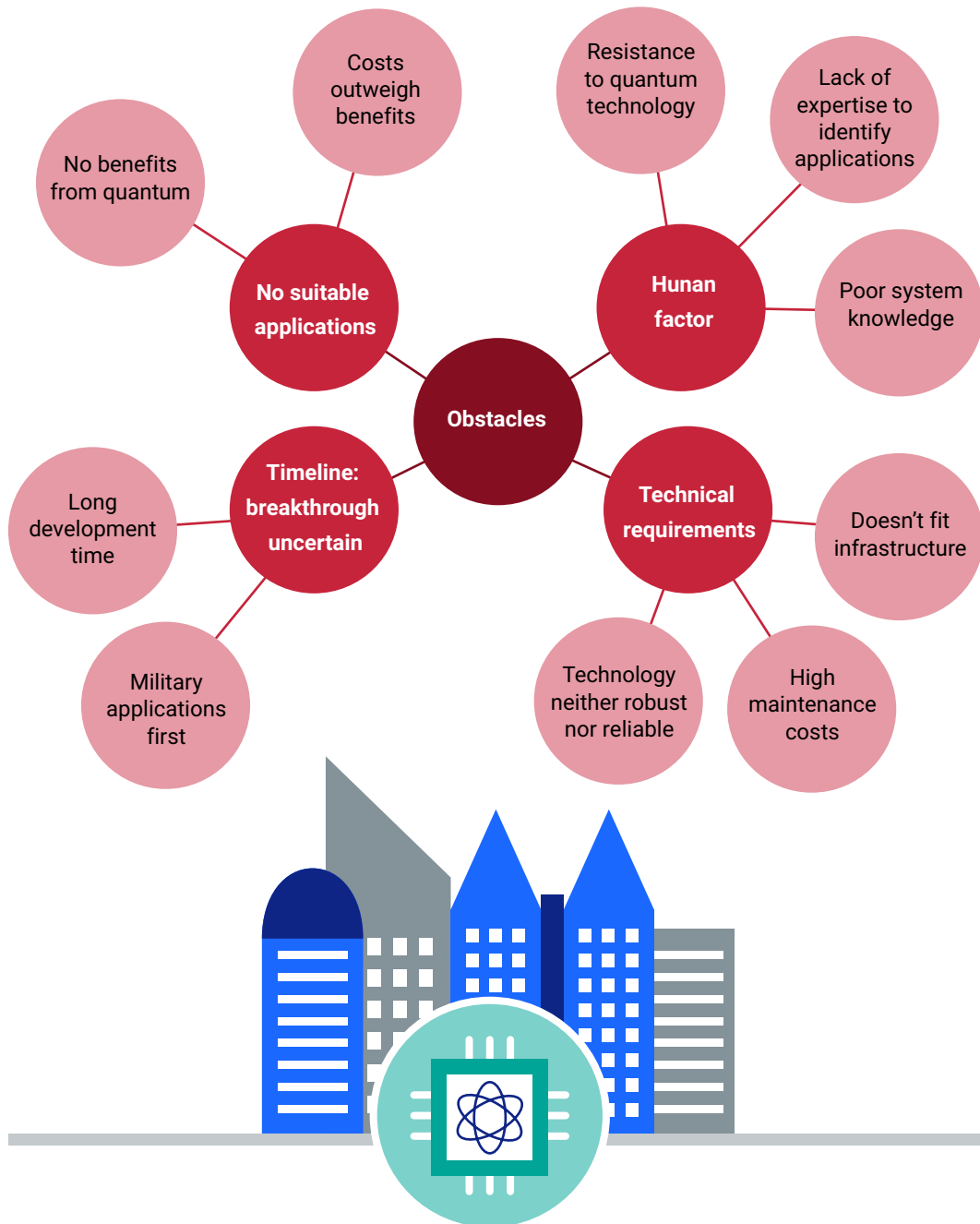
The Ministry of Economic Affairs is currently working with all the other ministries on a government-wide Quantum Strategy. It will stress the strategic importance of quantum technology and include goals and actions to address both the opportunities and risks. It is not known to what extent the strategy will include activities to encourage the use of quantum technology in government. A budget has not yet been earmarked for the strategy. However, implementation will not be possible without financial backing.

4.3 Obstacles to the use of quantum technology

Despite the interest, progress and potential, quantum technology in and of itself does not create opportunities. Several experts we spoke to warned against the hype and the idea of quantum technology as a silver bullet. The organisations we surveyed named several obstacles that prevented government organisations from realising the benefits of quantum technology, even if significant advances were made in the technology.

Figure 9 Obstacles to the adoption of quantum technology

Technology is not the only obstacle for quantum technology



First, there is the timeline. Despite the best of efforts, development could always be slower than expected or come to a complete standstill. A second, related, obstacle is finding suitable use cases for quantum technology, especially in government. Knowledge is also needed to find good applications. For example, one answer to our questionnaire was: *'Quantum computing is notoriously complex to understand. Few people with the theoretical background can seriously fathom where quantum could*

offer an opportunity'. Moreover, according to some interviewees, identifying opportunities requires a deep understanding of the systems and mathematical models that are currently in use.

Good applications must come at an acceptable cost that is offset by definite benefits. In addition, quantum technology must meet the government's own technical demands; it must be reliable, robust and proven in the field. Other conditions are: low maintenance costs and compatibility with the infrastructure already in place.

Finally, accountability for the future use of quantum technology may also be problematic. Quantum technology is particularly complex and quantum calculations will always give different results. How can the government justify its use?

5.

The threat of quantum computers to the State

The biggest threat of quantum technology to the State is that quantum computers will be able to crack common encryption techniques if government organisations do not upgrade their encryption in time. State actors or other malicious actors will be able to access sensitive data and attack vital infrastructures. Most of the government organisations we surveyed were working on their information security and many were taking stock of their processes, systems and suppliers. However, significantly fewer have taken measures that specifically address the threat of quantum computers. They have not yet discussed quantum-safe products with their suppliers or made plans to introduce quantum-safe cryptography. Neither have they considered the quantum threat in their risk management processes or assigned management responsibility for PQC migration. 71% of the organisations said they had not yet mapped out an approach to the quantum threat. The main obstacles were lack of capacity and expertise and other activities having higher priority.

5.1 Quantum computers can crack cryptography

Quantum computers pose the greatest threat to the State. Quantum computers do not work in the same way as classical computers. As a result, they will probably be able to crack current cryptographic methods, something that would take today's computers 300 trillion years (OECD, 2025). The government uses cryptography in all kinds of applications. For example, to:

- protect confidential personal and commercial information;
- control access to vital infrastructure such as flood defences and bridges;
- log in with DigiD, the government's official log-in and authentication application;
- verify the authenticity of passports.

If the cryptography can be cracked, all these applications will be at risk.

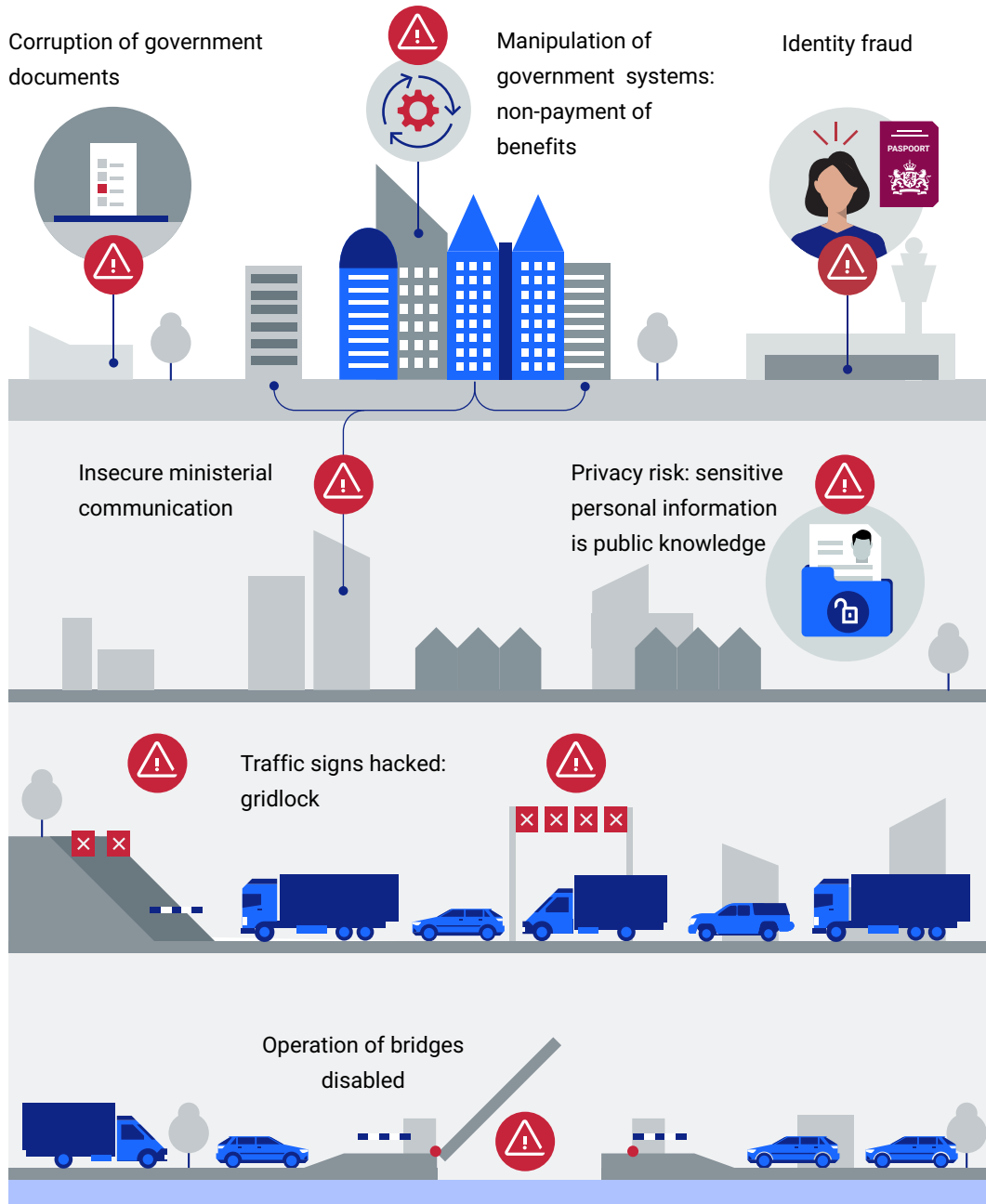
What is cryptography?

Cryptography is a method to encrypt information so that only the person with the corresponding key can read or edit it. Messages, personal data and other confidential information remain secure. Because it is known who holds the key, cryptography can also be used to confirm someone's identity. This is indispensable for applications such as DigiD and to manage access to vital infrastructure.

Cracking State cryptography would disrupt society. State actors would be able to open our locks and the information in our passports would no longer be trustworthy. Attacks by quantum computers could manipulate the data exchanged among government organisations. If the government can no longer adequately protect personal data, people will lose their trust in government. The threat of quantum computers will come mainly from state actors, because quantum computers are very expensive and only work in highly controlled environments.

Figure 10 *The main risks of quantum computers to government*

Quantum computers are a threat to confidential information and vital infrastructure of the State



Quantum computers are not yet powerful enough to crack cryptography. The strength of a quantum computer is measured in qubits, the building blocks of quantum computers. The more qubits, the more information a quantum computer can process and thus the more powerful it is. Scientists estimate that a quantum computer will need 1,024 to 3,072 qubits³ to crack the most common cryptographic technique. The largest quantum computers currently have fewer than 200 qubits (Gidney, 2025).

The moment that quantum computers are powerful enough to crack cryptography is known as Q-day. Expert opinions differ on whether and when Q-day will arrive.

Experts estimate that the first quantum computers will take about 7 days to crack a key. More powerful quantum computers with thousands of qubits could do it within 8 hours (Gidney, 2025). For the threat, it matters whether a quantum computer can crack a cryptography key in a minute or in 7 days. In the first case, quantum computers will be able to disclose confidential information; in the second, attacks will probably be targeted more specifically.

It is uncertain when there will be a powerful quantum computer and what it will be able to do. However, experts agree that government organisations must prepare for the threat quantum computers pose. Experts at the General Intelligence and Security Service (AIVD), the National Cyber Security Centre (NCSC), the European Commission and elsewhere give three reasons for this:

1. The ability to crack cryptography will have major consequences for national and international security.
2. Mitigating the quantum threat is a major challenge that will take several years to achieve.
3. Organisations are already at risk from store-now-decrypt-later attacks. Hostile actors are already stealing encrypted information, which they will crack in the future when a suitable quantum computer is available.

5.2 Organisations need to replace their cryptography

Overcoming the threat of quantum computers requires new security techniques that are resistant to quantum attacks. One response is post-quantum cryptography (PQC). This is a new form of cryptography that cannot be cracked by quantum computers. By replacing existing cryptography with PQC, organisations can protect themselves against the quantum threat.

Quantum key distribution (QKD) may also play a role in countering the threat. QKD is a technique to exchange cryptographic keys more securely (see Section 3.1.2). However, the AIVD and the European Commission argue that because of *'intrinsic constraints, QKD can only be used in a number of specific niche cases'* (AIVD et al., 2024). PQC should be prioritised in order to ensure that all information and processes are secure. The remainder of this chapter therefore focuses on PQC and government measures to replace existing cryptography techniques with quantum-safe alternatives.

5.2.1 PQC migration steps

In their PQC migration manual, the AIVD, TNO and Centrum Wiskunde & Informatica (CWI, the national research institute for mathematics and computer science in the Netherlands) point out that migration to PQC is time-consuming and complex (AIVD et al., 2024). Organisations must carefully analyse their cryptography, develop policies for its management and make agreements with suppliers about quantum-safe products. The following sections explain the main steps of PQC migration and the measures government organisations must take in each step. The steps are based on advisory reports issued by QvC NL (Digitale Overheid, 2025), the AIVD (AIVD et al., 2024), the NCSC (National Cyber Security Centre, 2023) and the European Commission (European Commission, 2025e). Some of the steps are important for information security in general, not just to prepare for the quantum threat.

Analyse quantum risks

The first step in PQC migration is risk assessment. Quantum computers are a very serious threat to information security, but organisations also face other urgent security challenges, such as cyberattacks and data breaches. It is not possible to tackle everything all at once. To protect critical information and processes, organisations must make firm decisions about where they focus their resources and attention. They cannot do this unless they understand how quantum computers threaten their systems and balance the risks against other priorities. The organisations must therefore incorporate the threat of quantum computers into their risk management processes.

Carry out a cryptography inventory

Organisations cannot replace their cryptography with PQC if they do not know what cryptography they have inhouse. Inventorising cryptography is complex, because a single ICT system can contain a dozen cryptographic components. Many organisations do not know exactly what ICT products they use because some of them are components of other ICT products. A cryptography inventory therefore requires an analysis of all an organisation's information systems and ICT products.

Make agreements with suppliers

Some cryptographic products are embedded in products provided by external suppliers. To migrate them to PQC, government organisations will have to make agreements with their suppliers about supplying quantum-safe cryptographic products. Suppliers will need to modify their products. If they do not, government organisations will have to look for new suppliers who do supply quantum-safe products.

Prepare a cryptography policy

Organisations need to have cryptography policies in place in order to keep a grip on their cryptography during and after PQC migration. Cryptography policy:

- defines cryptography roles and responsibilities;
- provides guidelines on the use of cryptography;
- details relevant laws and regulations (AIVD et al., 2024).

Under the Government Information Security Baseline (BIO), government organisations are already required to have a cryptography policy (Ministry of the Interior and Kingdom Relations, 2025b).

Manage the migration

To complete a complex PQC migration correctly and on time, organisations will need to manage the migration effectively. They must assign management responsibility for migration, set a timeline and mobilise sufficient capacity and resources.

Replace cryptography

The final step of PQC migration is actually replacing classical cryptography with quantum-safe cryptography. Organisations will upgrade their cryptography bit by bit, starting with the processes and cryptography that are most at risk. At present, very few quantum-safe products are available. This is because PQC techniques were only recently adopted. It takes time for developers and suppliers to incorporate the new techniques into their products.

5.2.2 Legal requirements for PQC migration

Government cryptography is subject to various laws and regulations. The government has committed itself, for example, to implementing the Government Information Security Baseline (BIO). It includes measures such as the formulation of policies on the use of cryptographic controls and key management (Ministry of the Interior and Kingdom Relations, 2019). The EU NIS2 Directive (National Cyber Security Centre, n.d.) contains more detailed cryptography requirements. The directive is already in force and will be transposed into Dutch law in 2026. NIS2 prescribes the application of '*state of the art encryption*' but does not specify that it must be PQC.

5.3 How does central government promote quantum risk mitigation?

PQC migration is a major challenge for all government organisations. The State Secretary for Digitalisation is coordinating the digitalisation of the Dutch

government. He stated at the beginning of 2025 that the use of quantum technology by malicious actors could endanger national security. The Ministry of the Interior and Kingdom Relations is supporting PQC migration through the Quantum Safe Cryptography NL (QvC NL) programme.⁴ On the launch of the Dutch Cybersecurity Strategy (2022), he provided funding to set up QvC NL and strengthen digital resilience. No money from the National Growth Fund is applied to control the risks of quantum technology.

5.3.1 Quantum Safe Cryptography NL

In 2023, the State Secretary for Digitalisation set up the QvC NL programme to help central government manage the risks of quantum computers to cryptography on a timely basis. The programme is intended to support government organisations in their migration to PQC. QvC NL does not provide a PQC migration framework for the government. Ministries and associated organisations themselves determine when and how they initiate PQC migration.

To date, QvC NL has focused on increasing awareness through workshops, presentations at conferences and the like. In addition, it has drawn up a government-wide policy framework for cryptography (Ministry of the Interior and Kingdom Relations, 2025b) and commissioned research into tools to carry out cryptography inventories (TNO, 2025). QvC NL is currently working on an expertise hub where experts and organisations can share their knowhow.

5.3.2 The Digitalisation Strategy

The government is also addressing the risk management of quantum technology through the National Digitalisation Strategy (NDS) it launched in July 2025. The Minister of the Interior and Kingdom Relations wants the strategy to promote PQC migration more strongly and anchor the need for it in policy. One of the NDS's strategic goals is a government-wide approach to quantum-safe cryptography. This has not been worked out in further detail. The ministry's 2026 budget states that a hub will be established for government-wide cooperation in the field of quantum-safe cryptography (House of Representatives, 2025b). The hub's relationship with QvC NL has not yet been revealed.

5.3.3 European actions: the roadmap

The European Commission also recognises the importance of migration to and preparations for PQC in all sectors. In mid-2025, EU member states and the European Commission published a roadmap (European Commission, 2025e) for coordinated migration to PQC. The roadmap is addressed to all EU member states

and includes recommendations for simultaneous migration. QvC NL is coordinating the Dutch response to the roadmap.

The European Commission acknowledges that migration will be difficult and protracted. Not all member states have made as much progress or recognised that the risks are urgent.

5.4 The PQC migration of government organisations

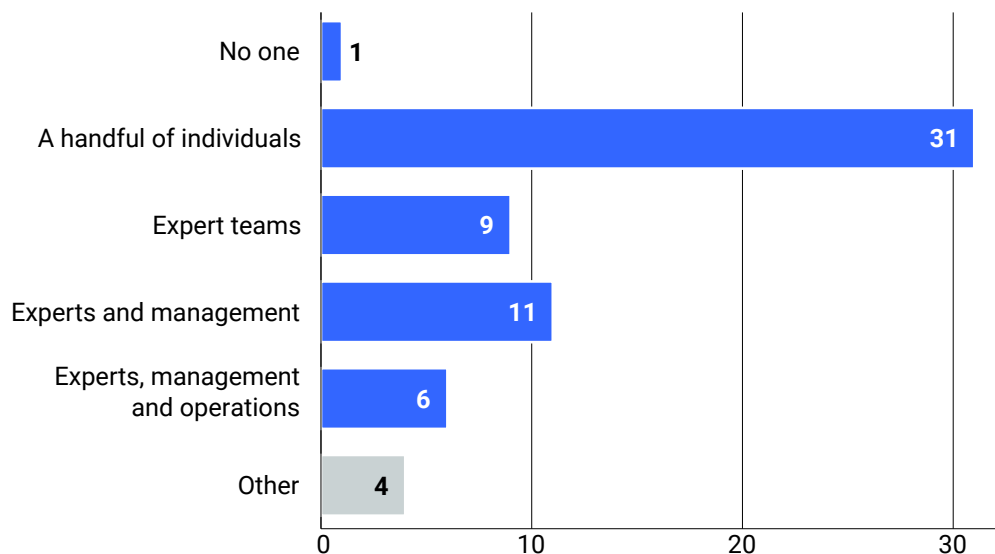
To gain an impression of the government's preparations to protect against the threat of quantum computers, we sent a questionnaire to the 63 organisations listed in appendix 2. We selected organisations that we believed processed personal or confidential information or provided vital infrastructure. The PQC Migration Handbook refers to these organisations as *urgent adopters*: ones that may be targeted by quantum computers and therefore need to take measures against the threat as soon as possible.⁵

5.4.1 Awareness of the quantum threat

QvC NL raises awareness about the threat posed by quantum computers. Almost all organisations in our survey were familiar with the threats. Only 1 indicated that no one within it was aware of the threat (see figure 11). At more than half of the organisations, however, awareness was limited to a few individuals or expert teams.

Figure 11 Awareness of the quantum threat at the organisations surveyed

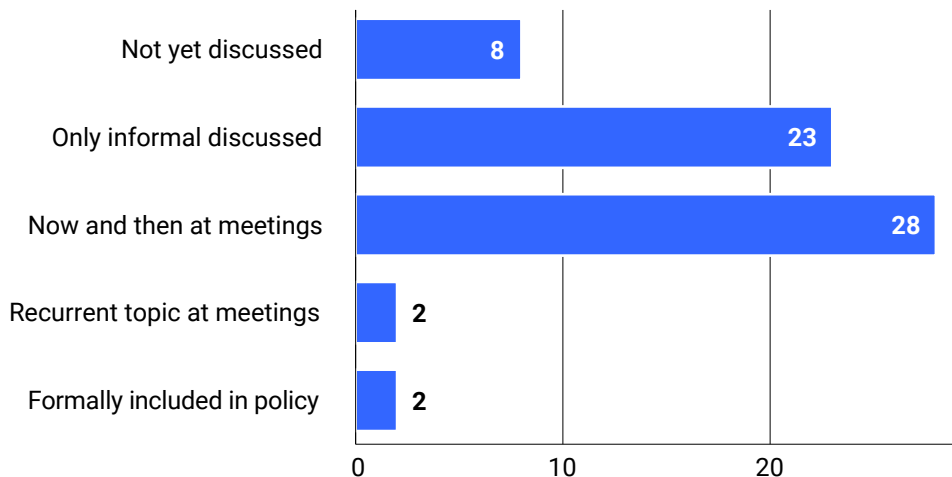
Awareness of quantum threats limited to individuals



The way in which organisations discuss the threat also reveals a lack of systematic awareness. Most organisations discuss the threat only informally or occasionally in specific meetings (see figure 12). Only 4 organisations systematically considered it or had formally incorporated the quantum threat into internal policies or strategies.

Figure 12 Awareness of the quantum threat at the organisations surveyed

Few organisations structurally aware of quantum threat



There is someone at almost all the organisations who is familiar with the quantum threat, but few organisations give it little if any management or organisation-wide consideration. QvC NL stresses that the threat must become more widely recognised because migration to quantum-safe cryptography will affect all parts of an organisation: from information management to procurement and from operational management to implementation. The challenge is not to reach more organisations but to spread awareness more widely within organisations.

5.4.2 Preparations by government organisations

We also asked the organisations whether they had started preparations to address the threat posed by quantum computers. Of the 63 organisations, 18 (29%) had (see figure 13). The other 45 (71%) had not yet started targeted preparations. Of these, 33 (52%) did not know if and when they would start.

Figure 13 Percentage of organisations surveyed that have started to address the quantum threat

71% of the organisations have not started addressing quantum threats



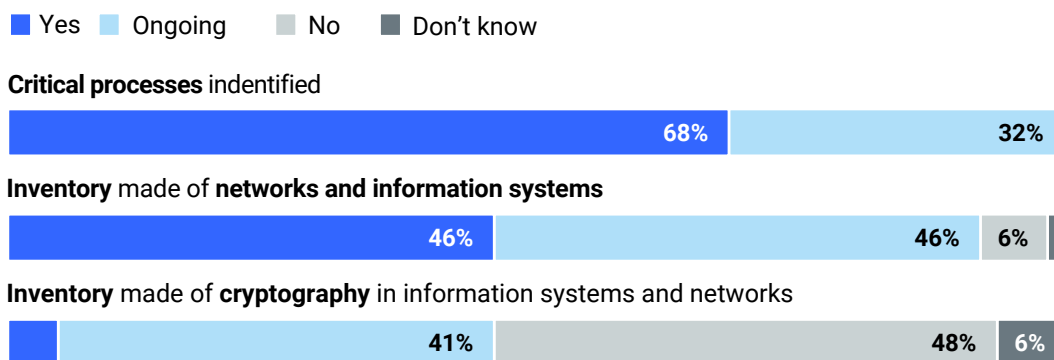
To determine what preparations the organisations had made, we asked them about the PQC migration steps considered in section 5.2.1. Migration steps such as making a cryptography inventory and drawing up a cryptography policy are relevant to more than just the quantum threat. Organisations may have already taken these general steps without having explicitly started preparations for the quantum threat.

Cryptography inventory

An important step organisations need to take is to identify their critical processes, ICT systems and cryptography. Organisations need to know what they have inhouse if they are to migrate to quantum-safe cryptography.

Figure 14 Percentage of organisations surveyed that have completed inventories

52% of the organisations have not yet completed inventories of their networks and information systems



Most of the organisations indicated that they were in the process of taking stock of their processes and IT systems (see figure 14). 43 of the 63 organisations (68%) said they had identified their business-critical processes. The remaining 20 (32%) were currently engaged in doing so. Business-critical processes are processes that are vital to an organisation's goals. They must be known for the migration to quantum-safe cryptography and probably need to be made quantum-safe first.

46% of the organisations indicated that they knew which networks and information systems they used in their business-critical processes. The reason that many organisations are identifying their business-critical processes and systems is that the knowledge is a basic condition for digital resilience and is already mandatory under the NIS2 Directive (National Cyber Security Centre, n.d.).

Significantly fewer organisations have started to take stock of cryptography in their processes and systems. 30 (48%) have made no start at all. This may be because cryptography inventories are very complex. Networks and information systems often

contain many different IT products that in turn contain other IT products. Each product often has multiple cryptographic components. A network or information system can contain hundreds of cryptographic components. Tools are being developed to automatically detect cryptography, but they are still expensive and have limited effectiveness, and the tools' creators cannot guarantee how complete their inventories are.

Nevertheless, it is essential that organisations know what cryptography they have inhouse. If they don't, they cannot migrate to quantum-safe cryptography. 29 organisations (46%) indicated that they had already started to make an inventory of their cryptography. One of them is the Tax and Customs Administration. In an interview, it emphasised the importance of starting, so that it could gradually learn where its cryptographic components were: *'If you don't have that knowledge when turnkey [inventory] solutions come onto the market, then you're too late'*.

Establishing a cryptography policy

A transparent cryptography policy is needed to organise cryptography inventories and keep them up to date. The policy should assign roles and responsibilities and describe how organisations carry out their inventories. 22 organisations (35%) are preparing such policies (see figure 15) and 9 (14%) have already introduced a policy.

Figure 15 Percentage of organisations surveyed that have developed cryptography policies

9 organisations have a comprehensive cryptography policy

■ Yes ■ Ongoing ■ No ■ Don't know

Cryptography policy developed based on government cryptography policy



The Government Information Security Baseline (BIO) requires government organisations to have a cryptography policy. The fact that so few have fully implemented such a policy is not surprising. It was not until March 2025 that the government-wide cryptography policy framework made clear exactly what should be included in cryptography policy (Ministry of the Interior and Kingdom Relations, 2025b). However, it is striking that 29 organisations (46%) have not yet started to develop policies in compliance with the framework.

Make agreements with suppliers

Organisations need to be aware of both their own cryptography and also their suppliers'. The cryptography in their suppliers' products must also migrate to PQC. Most of the information management tools some organisations have are provided by external suppliers. The products include analysis software, external data storage, digital workplaces of the government's shared service centre for ICT (SSC-ICT) and services provided by Logius such as DigiD.

Many organisations have identified not only their own business-critical processes and systems but also their business-critical suppliers (see figure 16). 30 (48%) have made an inventory of their suppliers. A further 26 (41%) are currently making preparations for an inventory.

Figure 16 Percentage of organisations that have discussed PQC with their suppliers

Few organisations have discussed PQC with their suppliers

■ Yes ■ Ongoing ■ No ■ Don't know

Business-critical suppliers have been identified



Talks started with suppliers about quantum-safe cryptography in their products



Few organisations are in talks with their suppliers about quantum-safe products. 15 (24%) have opened up talks, whereas 45 (71%) have not yet made any contact. Some organisations indicate that they are waiting for quantum-safe products to enter the market. Others feel that suppliers themselves are responsible for adapting their products.

QvC NL and the NCSC advise organisations to start talks immediately. Suppliers will then realise that there is a demand for quantum-safe products and tailor their development plans accordingly. Logius notes that organisations need to adapt their own processes and systems in response to suppliers adapting their cryptography. This is a time-consuming process that needs to know where cryptography is embedded in the organisation. It is why some organisations have already initiated talks with their suppliers. According to SSC-ICT: *'We are increasingly discussing quantum and developments in this area with our suppliers. To this end, SSC-ICT's service roadmap will be compared with the suppliers' roadmap.'*

These talks are important but the organisations feel that they alone should not be responsible for all the measures that need to be taken. Some products are used by multiple government organisations. The Repatriation and Departure Service (DT&V), for instance, points out that it is not the only user of eSignature. It believes that securing the software is a shared problem requiring coordination at a higher level.

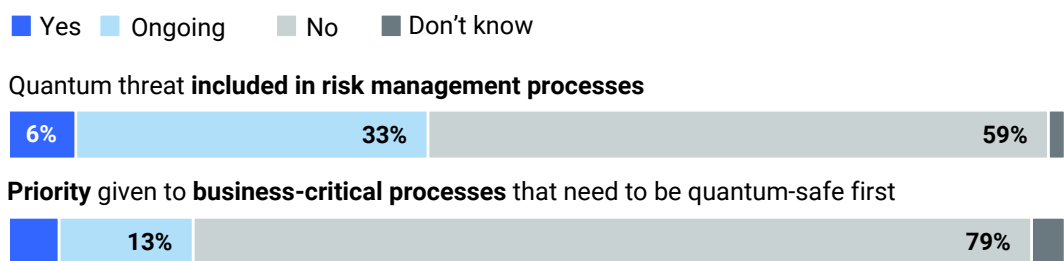
Analyse quantum risks

An inventory of processes, systems, cryptography and suppliers is an important first step. But the organisations need to translate it into concrete measures that address the quantum threat. They need to assess the scale of the threat and identify processes at highest risk. They also have to decide where to deploy their resources in the light of other information security threats. To justify these decisions, government organisations must continuously weigh the quantum risks against other risks.

However, only 4 of the 63 organisations we surveyed (6%) had considered the quantum threat in their risk management processes (see figure 17). 37 (59%) had not considered it at all, and only 3 (5%) had identified the business-critical processes they wanted to make quantum safe first.

Figure 17 Percentage of organisations surveyed that included the quantum threat in risk management processes

Few organisations have considered the quantum threat in their risk management



Many organisations have an insight into their processes and IT systems, but few have analysed how quantum computers can threaten them. This is consistent with a broader picture drawn from our survey: government organisations are working on general information security measures but hardly any concrete measures have been taken to address the quantum threat. One organisation put it this way: *'We are not dealing with threats from a quantum technology perspective, but we are actively implementing the BIO and NIS2. These are topics that are closer to the organisation.'*

Managing the migration

The lack of specific preparations is also evidenced by the fact that most organisations have not yet started managing and planning their PQC migration. 52 of the 63 organisations (83%) have not yet appointed a manager (see figure 18). 58 (92%) have not yet set a timeline and 59 (94%) are uncertain whether they have sufficient capacity for migration. Without an organisational basis, organisations can underestimate the challenge of a complex transition to quantum-safe cryptography.

Figure 18 Percentage of organisations surveyed that have prepared for PQC migration

Many organisations have not started to prepare for PQC migration

■ Yes ■ Ongoing ■ No ■ Don't know

Management responsibility appointed to mitigate the quantum threat



Timeline adopted for migration to quantum-safe cryptography



Known whether there is sufficient capacity for migration



Cryptographic migration

All preparations must ultimately enable organisations to migrate to quantum-safe cryptography. However, as mentioned in section 5.2.1 above, hardly any quantum-safe products are available at present. That is why we asked the government organisations only if they had already piloted PQC migration. 3 organisations (5%) had completed a pilot and 3 others (5%) were working on one.

Figure 19 Percentage of organisations surveyed that have piloted migration to PQC

3 organisations have piloted PQC migration

■ Yes ■ Ongoing ■ No ■ Don't know

A pilot project for the migration to quantum-safe cryptography has been carried out



5.5 Obstacles to preparing for the quantum threat

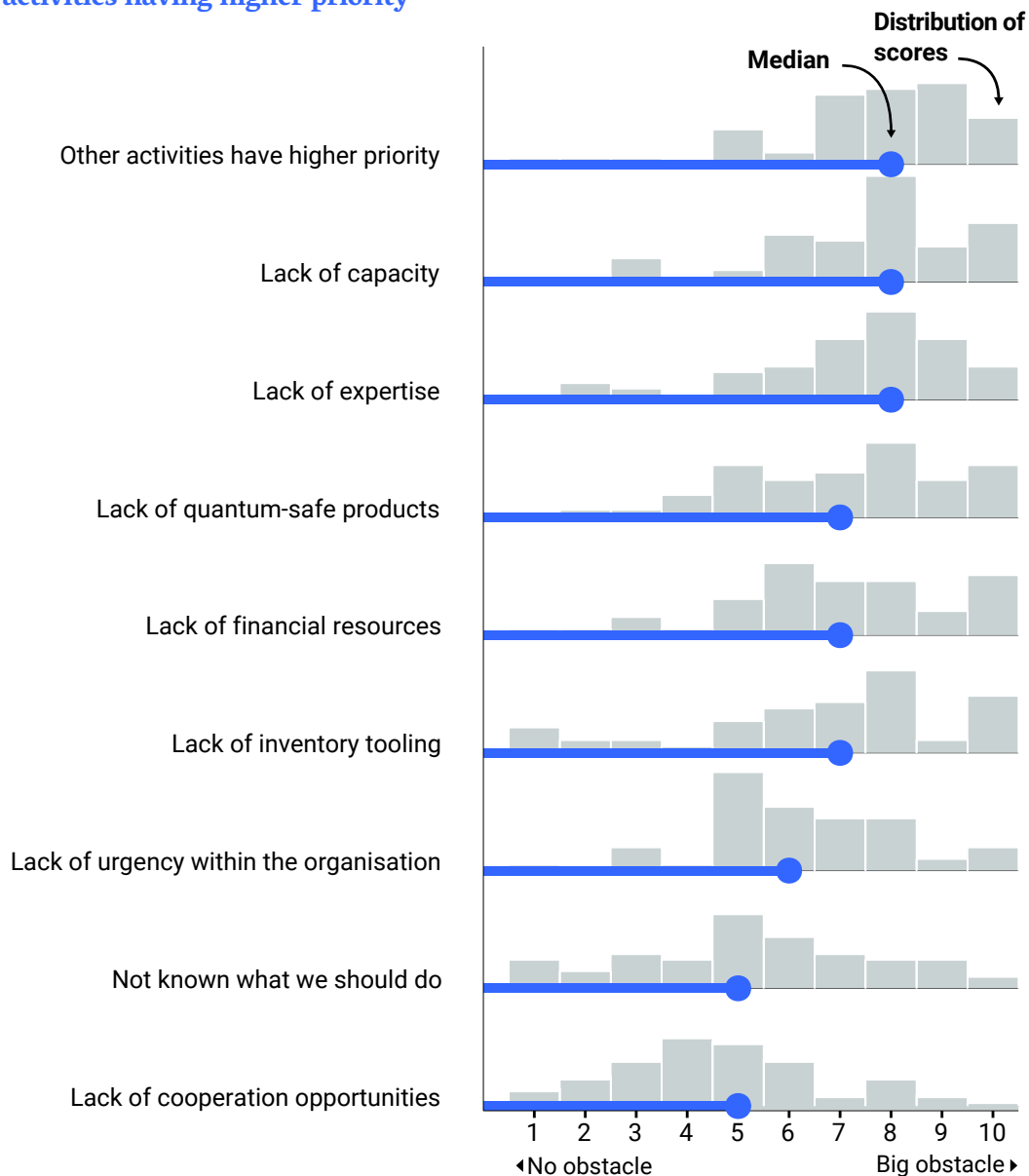
The previous section showed that many government organisations were still at the beginning of their PQC migration. The questionnaire revealed that the main obstacles they faced were: (1) other activities having higher priority, (2) lack of capacity and (3) lack of expertise (see figure 20). On average, organisations gave these 3 obstacles a rating of 8 on a scale of 1 to 10. The following sections consider them in more detail.

5.5.1 Many tasks and limited capacity

Besides the quantum threat, the organisations are facing many other threats. They must also be prepared for hacks of vulnerabilities, such as the Citrix vulnerability at the Public Prosecution Service, and DDoS attacks. In addition, there are broader challenges of information management. For example, there are modernisation challenges, delayed IT projects and overdependence on US technology companies. PQC migration is just one of the many activities that have to be carried out in the field of information management and information security.

Figure 20 Obstacles to PQC migration as scored by the organisations surveyed

De biggest obstacles are lack of capacity and expertise and other activities having higher priority



The organisations pointed out that their resources and capacity were limited. They feared that the savings announced in the 2025 Budget Memorandum (Central Government, 2024) would exert even more pressure on their limited capacity. PQC migration had to compete with other activities and obligations. The organisations had to give higher priority to threats perceived as being more urgent. PQC migration was often just one more task that had to be done.

The organisations thought PQC migration need not always be at the expense of other priorities. Some included PQC in their transition to a *zero-trust security* environment. Others thought PQC migration could piggyback on other initiatives and obligations such as the implementation of BIO and NIS2 legislation.

5.5.2 Lack of expertise

PQC migration requires a lot of expertise. Technical knowhow is needed to carry out cryptography inventories, assess PQC solutions and learn how to work with PQC products. Such expertise is difficult to find and retain. One of the organisations said it had difficulty holding on to specialists because they could not offer them suitable colleagues and challenges.

Government organisations therefore seek out external parties such as TNO and the AIVD to assess the safety of PQC products. To implement PQC, they hope to draw on the expertise of their suppliers. SSC-ICT has an advisory role in the procurement of services but recognises that organisations ultimately have to decide for themselves what cryptography they use and where.

The Ministry of Finance notes that many organisations will rely on the expertise of suppliers and specialists. To enable the suppliers and specialists to meet the demand, QvC NL is setting up an expertise centre (see section 5.3.1) that pools knowledge so that the government, businesses and knowledge institutions can work together on PQC migration. The centre could potentially help overcome the obstacles.

6. Response

In view of their responsibilities for the coordination of the Dutch government's digitalisation, we sent our draft report to the Minister of Economic Affairs (EZ) and the State Secretary for the Interior and Kingdom Relations (BZK). The Minister of EZ and the State Secretary for BZK responded to our draft report. Given the response, we see no reason for an afterword. We appreciate the serious way in which the Minister of Economic Affairs and State Secretary for BZK acknowledge our findings and undertake to continue working in this area. The letter (in Dutch) can be found on our website at www.rekenkamer.nl.

Appendices

Appendix 1 Methodology

The objective of this investigation was to outline the opportunities and risks of quantum technology. This methodology section explains what we investigated and how.

What we investigated?

Key question: How is the Dutch central government taking advantage of the opportunities of quantum technology and mitigating the risks?

To answer this key question, we asked the following sub-questions:

1. What opportunities does quantum technology offer to government and society?
2. How (financially and policy-wise) is central government taking advantage of the opportunities of quantum technology?
3. What are the results so far of the government's commitment to quantum technology?
4. What risks does quantum technology present to government?
5. How (financially and policy-wise) is the government managing the risks of quantum technology?
6. How are government organisations addressing the risks of quantum technology?

The findings presented in chapter 5 are based on self-reporting by the organisations we surveyed. Given the nature of this investigation, we did not carry out an independent analysis of the findings' correctness or completeness.

Approach

Focus investigation

This report presents the findings of a focus investigation carried out by the Netherlands Court of Audit. A focus investigation differs from an audit in that it is:

- carried out in a considerably shorter period of time,
- examines current events,
- answers specific, well-defined questions.

A focus investigation culminates in a clear, concise report without opinions or recommendations. For more information, see [Focus investigation](#).

Selection of organisations

For our investigation, we asked 63 government organisations to complete a questionnaire. All 63 organisations responded. The organisations are listed in appendix 2. We selected these organisations because they manage sensitive information and/or perform vital processes.

The following ministries completed the questionnaire jointly for their core departments:

- the Ministries of the Interior and Kingdom Relations (BZK) and Housing and Spatial Planning (VRO);
- the Ministries of Economic Affairs (EZ), Climate Policy and Green Growth (KGG) and Agriculture, Fisheries, Food Security and Nature (LVVN);
- the Ministries of Justice and Security (J&V) and Asylum and Migration (A&M).

Documentation

To answer questions 1 to 5, we studied public sources and internal documents issued by the Ministries of EZ and BZK and by Quantum Delta NL.

Interviews

We held interviews at the Ministries of EZ and BZK (the Quantum Safe Cryptography Programme (QvC NL)) to discuss their roles and responsibilities for the coordination of the development of quantum technology. We also held an interview at Quantum Delta NL about the programme's activities and the results achieved so far. In addition, we conducted interviews at TNO, the European Commission (Directorate-General for Communication Networks, Content and Technology), National Cyber

Security Centre (NCSC, part of the Ministry of J&V), Logius and Shared Service Centre ICT (SSC-ICT). All these organisations are central to addressing the opportunities and threats of quantum technology.

We conducted additional in-depth interviews at 10 organisations, selected on our assumption that they would be familiar with the opportunities and risks of quantum technology. Appendix 2 lists the organisations that completed the questionnaire and were selected for interview.

Scope

- We excluded the intelligence services and state-secret information from the investigation. They are very relevant to our investigation, but due to the short lead time of this focus investigation we were unable to use sources of a classified nature.
- Many organisations are investing in the development of quantum technology. For this investigation we focused exclusively on investments made through the National Growth Fund.

Appendix 2 Selected organisations

The table below lists the organisations selected for our investigation of quantum opportunities and risks.

We held additional in-depth interviews at the 10 organisations marked with an asterisk (*).

Ministry	Organisation	Status
General Affairs (AZ)	Core Department of General Affairs	Ministerial unit
Home Affairs and Kingdom Relations (BZK), and Housing and Spatial Planning (VRO)	Core department BZK and VRO	Departmental unit
	Logius	Agency
	National Office for Identity Data (RvIG)*	Agency
	Central Government Information Management Organisation	Ministerial unit
	P-Direkt	Agency
	Central Government Real Estate Agency (RVB)*	Agency
	Shared Service Centre ICT (SSC-ICT)	Agency
	Land registry	Arm's length body
	Electoral Council	Ministerial unit
Foreign Affairs (BZ)	Core Department of Foreign Affairs	Ministerial unit
Defence	Core Department of Defence*	Ministerial unit
	Defence Security Inspectorate	Inspection
Economic Affairs (EZ), Climate Policy and Green Growth (KGG) and Agriculture, Fisheries, Food Security and Nature (UNGA)	Core Department EZ, KGG and LVVN	Ministerial unit
	Netherlands Enterprise Agency (RVO)	Agency
	ICT Service (DICTU)	Agency
	Chamber of Commerce	Arm's length body
	Dutch Authority for Digital Infrastructure	Agency
	Statistics Netherlands (CBS)	Arm's length body
	Dutch Emissions Authority (NEa)	Agency
Finance	Core Department of Finance*	Ministerial unit
	Tax and Customs Administration*	Ministerial unit
	Customs	Ministerial unit
	Surcharges	Ministerial unit
	De Nederlandsche Bank (Dutch Central Bank)	Arm's length body
	Netherlands Authority for the Financial Markets (AFM)	Arm's length body
	Agency of the General Treasury	Ministerial unit
Infrastructure and Water Management (I&W)	Core Department of Infrastructure and Water Management*	Ministerial unit
	Authority for Nuclear Safety and Radiation Protection	Ministerial unit
	Human Environment and Transport Inspectorate (ILT)	Ministerial unit
	Air Traffic Control Netherlands	Arm's length body
	ProRail BV	Arm's length body
	Rijkswaterstaat (RWS)*	Agency
	Royal Netherlands Meteorological Institute (KNMI)	Agency

Ministry	Organisation	Status
Justice and Security (J&V) Asylum and Migration (A&M)	Core Department J&V* and A&M	Ministerial unit
	JUSTIS (Integrity and Screening Agency)	Agency
	Judicial Information Service (JustID)	Agency
	National Police*	Arm's length body
	Public Prosecution Service	Ministerial unit
	Central Judicial Collection Agency (CJIB)	Agency
	Custodial Institutions Agency (DJI)	Agency
	Netherlands Forensic Institute (NFI)	Agency
	Repatriation & Departure Service	Ministerial unit
	Immigration and Naturalisation Service (IND)	Agency
	Dutch Safety Board	Arm's length body
	Council for Child Protection	Ministerial unit
Education, Culture and Science (OCW)	Core Department of Education, Culture and Science	Ministerial unit
	National Archives (NA)	Agency
	Education Executive Agency (DUO)	Agency
Social Affairs and Employment (SZW)	Core Department of SZW	Ministerial unit
	Dutch Labour Inspectorate	Ministerial unit
	Benefits Intelligence Agency (IB)	Arm's length body
	Social Insurance Bank (SVB)	Arm's length body
	Employee Insurance Agency (UWV)*	Arm's length body
Health, Welfare and Sport (VWS)	Core Department of Health, Welfare and Sport	Ministerial unit
	CAK	Arm's length body
	BRIC	Agency
	CIZ	Arm's length body
	National Institute for Public Health and the Environment (RIVM)	Agency
	Medicines Evaluation Board (MEB)	Agency
	Implementing Agency for Grants to Institutions	Ministerial unit
	Health and Youth Care Inspectorate	Ministerial unit
Dutch Healthcare Authority (NZA)	Arm's length body	

Appendix 3 References

AIVD, CWI & TNO, (2024), The PQC Migration Handbook.

AIVD, French Cybersecurity Agency (ANSSI), Federal Office for Information Security (BSI), Netherlands National Communications Security Agency (NLNCSA), (2024), Position Paper on Quantum Key Distribution.

Birch, (2020), The Dutch Quantum Ecosystem.

Birch, (2024), Ecosystem update QDNL Midterm Review.

Central Government, (2024) Budget Memorandum.

Central Government, (2025), Quantum computers are coming and the Netherlands is prepared: <https://www.rijksoverheid.nl/actueel/nieuws/2025/07/10/quantumcomputers-komen-eraan>.

Digitale Overheid, (2025), Prepare for: <https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/quantumveilige-cryptografie/bereid-je-voor/>.

European Commission, (2025), Communication on the Quantum Europe Strategy.

European Commission, (2025b), Quantum Technologies Flagship: <https://digital-strategy.ec.europa.eu/nl/policies/quantum-technologies-flagship>.

European Commission, (2025c), European High Performance Computing Joint Undertaking - EuroHPC JU: <https://digital-strategy.ec.europa.eu/nl/policies/high-performance-computing-joint-undertaking>.

European Commission, (2025d), European Quantum Communication Infrastructure – EuroQCI: <https://digital-strategy.ec.europa.eu/nl/policies/european-quantum-communication-infrastructure-euroqci>.

European Commission, (2025th), Roadmap for the Transition to Post-Quantum Cryptography.

European Parliamentary Research Service, (2024), Quantum: What is it and where does the EU stand?

Europol (2023), The Second Quantum Revolution – The impact of quantum computing and quantum technologies on law enforcement, Europol Innovation Lab observatory report, Publications Office of the European Union, Luxembourg.

Gidney, C., (2025), How to factor 2048 bit RSA integers with less than a million noisy qubits: <https://arxiv.org/abs/2505.15917>.

House of Representatives, (2012), Press release of OCW and NWO 'Rijk invests 167 million in top Dutch research'.

House of Representatives, (2013), Letter from the Minister of Economic Affairs and State Secretary for Education, Culture and Science, Business Policy 32637 No 82.

House of Representatives, (2020), Cabinet Reaction National Quantum Technology Agenda, 29338 No. 216.

House of Representatives, (2024), Adoption of the budgetary statement of the National Growth Fund for the year 2024 36410 L No. 15.

House of Representatives, (2025), Report on a committee debate held on 30 January 2025, on emerging and future technologies. 26643-1311.

House of Representatives, (2025b), Adoption of the budget statements of the Ministry of the Interior and Kingdom Relations (VII) for the year 2026. Explanatory memorandum. 36 800 VII No 2.

McKinsey, (2025), The Year of Quantum: From concept to reality in 2025: <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-year-of-quantum-from-concept-to-reality-in-2025>.

Ministry of Defence, (2023), 'Quantum technology has an impact on the way it operates': <https://magazines.defensie.nl/materieelgezien/2023/08/defensie-verkent-quantumtechnologie>.

Ministry of Economic Affairs and Climate Policy, (2024), The National Technology Strategy.

Ministry of Economic Affairs and Climate Policy, (2025), Advisory Committee on National Growth Fund Annual Report 2024.

Ministry of Economic Affairs, (2025), Progress Cabinet approach to Economic Security.

Ministry of Economic Affairs, (2025b), Fiche 1: Communication on the EU Quantum Strategy.

Ministry of Finance & Quantum Delta NL, (2023), Report on broad ELSA Exploration of Quantum Computing Ministry of Finance: <https://assets.quantum-delta.prod.verveagency.com/assets/report-broad-elsa-exploration-quantum-computing-ministry-of-finance.pdf>.

Ministry of Infrastructure and Water Management, (2025), From Bits to Qubits.

Ministry of the Interior and Kingdom Relations, (2019), Government Information Security Baseline (BIO), page 41. 2019. Available via: <https://www.informatiebeveiligingsdienst.nl/producten/bio/>.

Ministry of the Interior and Kingdom Relations, (2025), Quantum Secure Cryptography Information Set, A Supplier Management Tool Version: 1.0.

Ministry of the Interior and Kingdom Relations, (2025b), Government-wide policy framework for cryptography - A framework for drafting cryptography policy.

National Cyber Security Centre, (2023), Make your organisation quantum safe.

National Cyber Security Centre, (n.d.), Basic Principle 1: Identify your risks: <https://www.ncsc.nl/wat-kun-je-zelf-doen/basisprincipes/breng-je-risicos-in-kaart>.

National Cyber Security Centre, (n.d.), Cyber Security Act <https://www.ncsc.nl/over-ncsc/wettelijke-taak/wat-gaat-de-nis2-richtlijn-betekenen-voor-uw-organisatie/hoe-kan-uw-organiseren-zich-voorbereiden-op-de-nis2-richtlijn>.

National Growth Fund (NGF), Quantum Delta NL: <https://www.nationaalgroeifonds.nl/overzicht-lopende-projecten/thema-sleuteltechnologieen-en-valorisatie/quantum-delta-nl>.

OECD, (2025), A quantum technologies policy primer, OECD Digital Economy Papers, No. 371, OECD Publishing, Paris, <https://doi.org/10.1787/fd1153c3-en>.

Port of Rotterdam, (2024), Consortium of parties is the first in the world to build a scalable quantum network in the Port of Rotterdam: <https://www.portofrotterdam.com/nl/nieuws-en-persberichten/consortium-van-partijen-legt-als-eerste-ter-wereld-een-schaalbaar-quantum>.

Quantum Delta NL (2021), Quantum Delta Netherlands project proposal, National Growth Fund.

Quantum Delta NL, (2024), New EuroHPC Quantum Computer to Be Hosted in the Netherlands <https://quantumdelta.nl/news/new-eurohpc-quantum-computer-to-be-hosted-in-the-netherlands>.

Quantum Delta NL, (2024b), A rudimentary quantum network link between Dutch cities: <https://quantumdelta.nl/news/a-rudimentary-quantum-network-link-between-dutch-cities>.

Quantum Delta NL, (2024c), Ministry of Finance exploration sessions results: detection of deviations in annual accounts and staff planning – ethics of quantum computing!: <https://quantumdelta.nl/news/ministry-of-finance-exploration-sessions-results-detection-of-deviations-in-annual-accounts-and-staff-planning-ethics-of-quantum-computing>.

Quantum Delta NL, (2025), QDNL Participations announces €60m global fund for early stage quantum startups, with €25m first close <https://quantumdelta.nl/news/qdnl-participations-announces-eur60m-global-fund-for-early-stage-quantum-startups-with-eur25m-first-close>.

Quantum Flagship, (2025), European funding opportunities for quantum technologies: <https://qt.eu/funding-opportunities>.

Quantum Insider, (2025), Japan Boosts Semiconductor, Quantum R&D with Trillion-Yen Budget: <https://thequantuminsider.com/2025/01/16/japan-boosts-semiconductor-quantum-rd-with-trillion-yen-budget>.

Rathenau Institute, (2023), Rathenau Scan: Quantum technology in society.

TNO, (2025), Cryptographic Asset Discovery and Inventory; market research and fit-gap analysis.

World Economic Forum, (2024), Quantum for Society.

Appendix 4 Endnotes

1. This passage was edited following the receipt of additional information during clearance at civil service level.
2. These are logical qubits.
3. Errors in quantum calculations, for example, must be corrected and the number and quality of the qubits that quantum computers use must be improved.
4. In response to a recommendation by the European Commission, the programme's scope was extended in 2024 to all parties covered by NIS2. The programme's name was accordingly changed from Quantum-safe cryptography in Central Government (QvC Rijk) to Quantum-safe cryptography Nederland (QvC NL).
5. For this reason, we do not present detailed results in this report.

This translation of the original Dutch text into English is provided by the Netherlands Court of Audit as a courtesy service. No rights can be derived from this translation. In the event of discrepancy between the Dutch original and the English translation, the Dutch original version shall prevail.

Netherlands Court of Audit

PO Box 20015
2500 EA The Hague
The Netherlands
+31 70 342 43 44
voorlichting@rekenkamer.nl
www.courtofaudit.nl

Photo: Rijksmediatheek
Economische Zaken

Original title

Focus op quantum bij de rijksoverheid

The Hague, February 2026