Quantum Exploration 2025
Security Delta (HSD)

Assessing the threats and opportunities of quantum technology for the Dutch digital ecosystem

Requested by: Province of South Holland
In collaboration with the Municipality of The Hague and InnovationQuarter

Written by: Saskia Noordewier, Carlijn Müller and Jonathan Verkuil, Security Delta (HSD)

HSD
securitydelta.nl

1. Introduction

Quantum technology might initiate a digital revolution. While it has existed for decades, recent breakthroughs have accelerated its applicability to a wide range of industries such as healthcare, defense, finance, and cybersecurity.[1] These breakthroughs are double-edged. On the one hand, quantum poses a serious threat to our cybersecurity, as it can break the cryptographic methods that currently protect our data. On the other hand, it also presents several opportunities, such as the creation of fast and secure communication. The Netherlands has expressed the ambition to become a leading center of knowledge and expertise on quantum, which is feasible due to a strong quantum ecosystem in South Holland. This brings new capital, talent, market, and innovation to South Holland. How this impacts the Dutch security, economy, and society, as well as who should act, often remains somewhat unclear. The Province of South Holland has therefore tasked Security Delta (HSD) with conducting a quantum exploration in 2025. We have executed this exploration in cooperation with the municipality of The Hague and InnovationQuarter.

2025 is the International Year of Quantum Science and Technology according to UNESCO, which shows that there is significant traction to engage with the quantum ecosystem in the Netherlands.[2] To protect our digital infrastructure and to leverage the opportunities presented by quantum, crucial steps should be taken to create urgency, raise awareness, facilitate more connections and develop practical guidelines. As HSD is a national cybersecurity cluster and a liaison between the triple helix, it could play a role in this. HSD has the expertise to bring people together and has experience with the challenges in doing so. To conduct the quantum exploration, discussions were held with many relevant stakeholders. A clear overview of these can be found in the Appendix 2.

First, background information regarding quantum technology and its dangers or opportunities is given. This leads to the formulation of two distinct research questions, focusing on the protections against the threats of quantum computers and the possibilities of cross-overs between the quantum and cybersecurity ecosystems. The results to these questions, based on interviews with relevant stakeholders, are indicated in the 'Results' section. One of the main questions during this exploration was the role of HSD as an instigator of digital innovation and cooperation in the cybersecurity ecosystem with regards to quantum technology. What are the tasks that HSD should take upon itself, if there are any? These questions are addressed in the last section of this exploration.

---

[1] Read more about the impact of quantum technology: https://assets.quantum-delta.prod.verveagency.com/assets/national-agenda-for-quantum-technology.pdf

[2] Read more about the international year of quantum: https://quantum2025.org/

2. Background information

The advancements in quantum technology can be categorised into three domains: computing, communications and sensing.[3] While sensing is relatively well-developed, the domains of computing and communicating are evolving rapidly and significantly impact our cybersecurity. They present a great opportunity for innovation in South-Holland. Apart from the three domains, quantum technology can also be divided into two perspectives: the threat-perspective and the opportunity-perspective. Below, these two perspectives will be further discussed.

Tabel 1

The three domains of quantum technology (Birch, 2021, p.10)

Technology	Description	Functionalities	Status
Sensing	Sensitive measurements	• Time measurement • Gravity measurement • Measurement of magnetism • Vibration measurement	Possible start of large-scale deployment in specialised applications. New generation of sensors is currently being developed
Communication	Secure and fast communication	• Cryptography • Quantum Key Distribution (QKD) • Quantum internet	Research phase and early applications, depending on the technological path
Computing	Ultra-fast calculations	• Simulation • Computing with specific quantum algorithms	Strongly dependent on application and qubit roadmap. Adoption of first-generation computers is beginning, but no applications yet that outperform classical computers

[3] Read more about the three domains: https://www.rathenau.nl/nl/digitalisering/rathenau-scan-quantumtechnologie-de-samenleving

The threats of quantum computing

The primary threat of quantum originates from the quantum computer, which uses qubits instead of normal bits. This allows it to perform complex mathematical calculations that classical computers cannot.[4] Companies such as Google and IBM are currently world leaders in developing practical quantum computers. In The Netherlands, several startups are also developing components of the quantum computer, such as QuantWare, QphoX, Delft Circuits, QBlox and Qu&Co. The quantum computer threatens our cybersecurity because it can break current cryptographic systems such as RSA and AES, allowing criminals to access sensitive data, cause breaches, steal state secrets and disrupt infrastructure and financial transactions. Additionally, the quantum computer enables automated cyberattacks by quickly identifying system vulnerabilities.[5]

Although current estimates tell us that quantum computers will only be strong enough to break classical cryptography in 2035, they already impact our current cybersecurity due to the 'Steal now, Decrypt later' principle. This means that data is being harvested so it can be encrypted retroactively in the future. Countries such as China and the United States engage in this practice, posing immediate threats to organisations with long-term sensitive data. Consider for instance governmental agencies or medical institutions. It is therefore crucial for these organisations to immediately adopt quantum-proof techniques such as Post-Quantum Cryptography (PQC). PQC includes cryptographic methods based on complex mathematical calculations that even the quantum computer cannot break.[6]

In 2024, the National Institute of Standards and Technology (NIST) released three PQC encryption standards after a long and intense developmental journey that can already be integrated into existing hardware and software.[7] Nonetheless, migration to PQC is estimated to take up to five years. It requires a well-structured plan, as some systems might be challenging to transition and not all systems can migrate simultaneously. Identifying what systems and cryptographic assets you should migrate to PQC, is a lengthy process. Companies with less long-term sensitive data therefore also need to start taking the first steps of their migration to PQC. The AIVD, CWI and TNO have developed a handbook to help them navigate this migration.[8] They note that while full migration to PQC may not be immediately necessary, implementing 'no-regret measures' can still enhance their

---

4 Read more about what the quantum computer can do: https://www.invest-nl.nl/media/attachment/id/2869

5 Read more about the quantum threat: https://prod.ucwe.capgemini.com/nl-nl/wp-content/uploads/sites/19/2023/10/Trends-in-Veiligheid-2023-Report.pdf

6 Read more about PQC: https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2023/november/8/factsheet-postquantumcryptografie/Factsheet_Post-quantum_cryptografie_okt23_NL_archief.pdf

7 Read more about the PQC-standards: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

8 Read the PQC-migration handbook: https://english.aivd.nl/binaries/aivd-en/documenten/publications/2024/12/3/the-pqc-migration-handbook/The+PQC+Migration+Handbook+.pdf

cybersecurity. Moreover, as PQC could cause latency and performance-loss of systems, the (local) government, vital infrastructure and product developers should start collaborating to test and enhance their products.

The opportunities of quantum technology

Beyond the threats, quantum technology also presents opportunities, particularly in the domain of quantum communication. By using quantum particles, a quantum network can be established. This network has two advantageous functions: it connects quantum computers so that their capabilities are increased, but it also connects classical computers with quantum computers through a quantum internet. With 'Blind Quantum Computing', users can utilise quantum computation from a remote server, without a third party in the middle. QuTech and KPN were the first in the Netherlands to establish a quantum internet connection and linked two independent quantum computers in Delft and The Hague with optical fiber. In the upcoming years, they aim to expand this network and try to solve the remaining scalability challenges. Another promising application within quantum communication is Quantum Key Distribution (QKD). QKD enables a secure distribution of encryption keys and signals any unwanted interference, which leads to unprecedented levels of security for the transmission of data. Currently, the Netherlands is a front-runner in the development of QKD, with parties such as Q-Bird developing usable QKD-hardware. In the Port of Rotterdam, Q-Bird and Eurofiber have established the first scalable quantum network with QKD. Although QKD still faces several issues, such as its vulnerability to DoS-attacks[9] and distance limitations, progress is being made to overcome these issues and to make a network that is designed to be secure; even with future advancements in quantum computing.

Additionally, quantum technology offers South Holland the chance to strengthen its position as a leading player in this rapidly developing field, particularly in areas such as Quantum Key Distribution (QKD). The region already benefits from a strong quantum ecosystem, where private tech companies, governments, and knowledge institutions actively collaborate.

The House of Quantum in Delft is a central hub within this ecosystem, but not a standalone initiative. It forms part of the broader Quantum Delta NL programme and functions as both a community and innovation hub. Similar facilities are being developed in Eindhoven, Amsterdam, and other cities. The House of Quantum provides office and lab space for start-ups to scale up beyond the university phase, while fostering connections across the ecosystem.

[9] Denial of service (DoS) attacks are attempts to overload a website or network, aiming to degrade its performance or even make it completely inaccessible (NCSC).

Alongside this, research consortia such as QuTech and QuSoft play a key role in advancing quantum knowledge and applications. Together, these initiatives stimulate investment, attract international talent, and drive the growth of high-tech manufacturing in South Holland. They also strengthen Europe's strategic position by building international ties with countries like France and Germany, while working toward a joint European quantum agenda.

At the same time, global competition is fierce. With massive investments in quantum technology from countries such as China and the United States, South Holland must commit to deeper collaboration and coordination to maintain and expand its leading role.

3. Exploration research questions

For the quantum exploration, it is essential to first critically assess if, and how, HSD could add value, especially considering that there are other major initiatives and organisations that already promote collaboration and raise awareness. One potential approach would be to have those initiatives and organisations to lead the development of a course of action and to raise awareness both within and outside of the quantum ecosystem. HSD could thereafter align itself with this strategy and leverage its own expertise to bring stakeholders together and encourage engagement with quantum security. Apart from raising awareness, HSD could also collectively work on developing the strategy and fostering innovations. This is under the condition that available resources will be allocated. Furthermore, it is important to acknowledge that only a limited section of the quantum field falls within HSD's scope: the intersection where quantum and security converge. Promoting the crossover between the quantum ecosystem and cybersecurity companies may fall within this scope but will only be effective if aligned with a broader course of action. Additionally, it is important to gain understanding of national-level initiatives and to assess if, and how, HSD could contribute to these efforts.

Based on the aforementioned information and the background on quantum technology, HSD's quantum exploration in 2025 focuses on two questions:

Question 1: Is there an opportunity for more alignment with existing and national initiatives that aim to mitigate the quantum-threat with practical tools and guidelines?	**Question 2: How could better collaboration between the quantum ecosystem and the cybersecurity ecosystem be established to increase innovation?**
Sub questions • Who is, and should be, taking the lead in developing and disseminating practical tools and	Sub questions • What challenges do parties focused on facilitating

guidelines for the various target groups? How would this network look like? • What are the first steps that should be taken to protect the ICT-infrastructure and business sector in South-Holland? • How could HSD support the dissemination and promotion of these initiatives (i.e. provide 'lessons learned, raise awareness among its network, in combination with existing initiatives such as the Cyber Resilience Centers and Regional collaboration).	collaboration within the quantum ecosystem face? • What additional opportunities does quantum bring to other security domains in South Holland? • Are parties within the HSD ecosystem interested in working cross sectoral on quantum? • How could HSD act as a liaison between the quantum ecosystem and its own network? Are the necessary resources available for this role and at what stage should it this happen?
Goal: Mobilising collaboration to deliver practical tools and guidelines to make local governments and the business sector in South-Holland quantum-proof, making use of national initiatives. A subgoal is the development of practical tools and guidelines for local governments to mobilize the business sector in their region.	Goal: Stimulating innovation and potentially facilitating the collaboration between the quantum ecosystem and the cybersecurity domain

To answer these questions, HSD expanded its network and held discussions with more relevant stakeholders. An overview of these stakeholders can be seen in Appendix 2. HSD also organised an HSD Café about quantum technology in June 2025 and gave attention to quantum from a communication perspective, to raise awareness and create a sense of urgency.

4. Results

The conversations that HSD held with the various stakeholders have revealed that there is significant momentum within the Dutch quantum ecosystem, and that South Holland's aspirations to become a central hub for quantum technology are, in fact, realistic. A sense of urgency is gradually emerging among larger parties such as the national government and municipalities, who should begin to engage with quantum technology to protect their critical infrastructure. However, mobilising policymakers remains a challenge due to the limited time and resources and because the quantum threat feels abstract and distant. Communicating this urgency and raising awareness appears a difficult task for parties that are technology focused. Moreover, it often remains unclear who is responsible for taking the first steps and what these steps should include. Although national initiatives are being developed, several parties have indicated that there is a need for someone to take the lead in developing practical tools and guidelines and to coordinate collaboration on multiple levels.

Question 1: alignment with initiatiatives to mitigate the quantum-threat

Overall, two target groups have been identified during the exploration. On the one hand, there are companies and organisations within the quantum ecosystem that focus on the opportunity side of the technology. They aim to leverage the advantages that quantum technology brings to the economy and security of South Holland. There are several strong initiatives (such as Quantum Delta) that foster collaboration within this ecosystem. Yet, some parties indicated that there is a need for better connections to combine forces and create further alignment. This applies to initiatives that operate on a similar level, but also across levels, for instance between companies and the national government. Some also indicated a need for more cross-sectoral connections, for instance between the quantum field and the cybersecurity field. In addition to focusing on critical infrastructure, quantum should also be brought to the attention of NIS2 parties who will need to address it in the future.

On the other hand, there is the threat side, with non-quantum companies that need to mitigate the quantum threat. Those companies fill up the biggest part of the ecosystem of Security Delta (HSD). Full migration will not be necessary for the upcoming years for these businesses, but it is crucial that companies and organisations start taking the first steps. Awareness should therefore be raised systematically from multiple angles. However, the required next steps vary across different stakeholders and this process should be phased. For instance, product developers should start testing new products in test environments provided by national and local governments, while SMEs should then be encouraged to start conversations with their IT-suppliers. And what is the role of the government (national, regional, local) in facilitating this process? Appendix 1 shows an overview with the different tasks of the different stakeholders.
Based on HSD's own expertise and the conversations held, the following steps have been observed in order to reach post-quantum security in a general sense, in light of the threats of quantum computing:

1) Enlarging basic cybersecurity levels
   Most interviewed partners of HSD indicated the importance of basic cybersecurity measures over starting with the post-quantum migration. Focus on data-minimalization: the less data you have, the less data you should protect against quantum computers. As long as the basic cybersecurity of a company is not in ready, starting with the post-quantum migration does not make sense. Basic cybersecurity is the low-hanging fruit.
2) Raising awareness
   Quantum technology is still generally perceived as an unknown and vague topic for senior managers. Besides that, it is perceived as a low-priority issue due to the futural

nature of the threat. Therefore, by providing timelines and explaining the dangers to the value propositions of businesses the awareness about the necessity of implementing post-quantum measures should be enlarged. There has to be a combination of perceived usefulness and perceived ease of use of those measures before the managers will start with implementing them. However, spreading awareness without action perspective is not helpful! Stand-alone awareness-events are not helpful, as these events do not foster effective change in the long run.

3) Implementing no-regret moves
There are certain 'no-regret' moves involved in the migration to a post-quantum safe company. One of them is for example mapping all the cryptographic assets of the company, through a scan or a 'nul-meting'. With such a scan, an advice and action plan on how to start the post-quantum migration of the company comes along. Several interviewed stakeholders envision a business case in offering this service. Effective cryptographic management facilitates the identification and resolution of risks and helps shorten response times during incidents—even when those incidents are unrelated to quantum computing.

4) Implementing the PQC-migration handbook
As mentioned above, the AIVD, CWI and TNO created a comprehensive guide steering companies towards the implementation of PQC. This handbook contains however much information, so several stakeholders indicated that practical guidance in implementing the handbook is needed for companies to make effective use of all the suggestions given in the document. The target audience of the handbook is the vital sector. SMEs should not right now be concerned with implementing PQC, but first with basic cybersecurity measures and mapping their cryptographic assets.

5) Reaching crypto agility
The final goal of most stakeholders involved in cryptographic asset management and post-quantum cryptography is 'crypto agility'. As cryptography and quantum computing continue to evolve, new vulnerabilities may arise. To address these emerging threats, companies must ensure forms of cryptographic agility when developing new products, applications, or hardware. This means that some forms of double cryptography should be used in companies, depending upon different methods of cryptography at the same time. Crypto agility will lead to higher levels of preparedness and resilience in the future.

6) Standardization & implementation of QKD
The final step in reaching full post-quantum security is the development of quantum-safe quantum networks, through innovations in Quantum Key Distribution. However, before QKD can be used widely there has to be a standardization process. Currently, the main value of QKD lies in the innovative and scientific fields as many business-related stakeholders indicated that QKD has no commercial value for them right now. It is seen therefore as an investment in the future. Once QKD is widely accepted as a security alternative, this will allow the Dutch digital ecosystem to reach full security by battling quantum through using quantum.

It seems best to raise awareness among different target groups during separate phases, as not all target groups have the same priority. Especially SME's, which are difficult to stimulate to work on their cybersecurity, should not be prioritised when there are no practical tools available yet. Isolated awareness sessions without practical follow-up will not stimulate SMEs. In contrast, the (local) government and IT-suppliers have a higher priority, as they need to develop and implement these tools. These target groups should therefore not be combined into one timeline.

One of the fields in which reaching crypto agility and post-quantum-security is of utmost importance is the field of Security by Design. When creating large infrastructural projects for example, it is needed that the software or hardware can be updated to a safe version once the quantum computer will be ready within 10 years. If the awareness of the quantum threat is spread to these engineers, post-quantum measures will be integrated from the start in the design of the products. That means that new developments and emerging threats can be countered in the future without major changes.

Question 2: collaboration between the quantum and cybersecurity ecosystem

South Holland is witnessing significant innovation in quantum technology, strengthening the Dutch position as a leader in this field. Progress in areas such as Quantum Key Distribution (QKD) demonstrates how the region is leveraging opportunities, while also highlighting the potential to deepen collaboration. One promising route is through stronger cross-sectoral connections—for example, linking the quantum and cybersecurity domains. Within HSD's network, several technology companies have already established teams dedicated to exploring the business potential of quantum, showing that interest is growing in both ecosystems.

Quantum technology is driving advances in sensing, communication, and computing (see Table 1). As HSD is a national cluster for security in a digitalized world, this exploration focuses primarily on its implications for cybersecurity. Nonetheless, other sectors—including defense, space, critical infrastructure, and data protection—are also preparing for quantum's impact, which is expected to become tangible within the next five years. For cybersecurity specifically, stakeholders noted that the immediate relevance remains limited to protecting digital data and adopting solutions such as PQC and QKD.

However, the lack of standards and certification remains a major obstacle. While the Netherlands has yet to establish leadership in this area, international efforts are advancing. Standardization bodies such as ETSI and ITU are active, with strong contributions from Asian companies. In South Korea, for example, QKD systems are already certified for use in governmental networks. Meanwhile, Europe is giving greater priority to quantum standardization, as reflected in the European Quantum Strategy, which includes a roadmap for European quantum standards to be published in 2026. The absence of such standards in the Netherlands hampers adoption: before companies are willing to invest, they need reliable proof of security. If a government or major industry player were to validate QKD, confidence and uptake would likely follow. Given Europe's broader focus on strategic autonomy, QKD standardization also carries geopolitical significance.

The main challenges in fostering collaboration between the quantum and cybersecurity fields are therefore twofold. First, the pace of quantum innovation makes it difficult for cybersecurity firms to keep up, especially when leadership teams are not yet convinced of its importance. With many organisations focused on meeting regulatory demands such as NIS2 and the Cyber Resilience Act (CRA), they lack the resources to actively engage with quantum developments. Second, the absence of clear standards and certified solutions prevents wider trust and implementation.

Despite these barriers, stakeholders recognize business opportunities already emerging—particularly in services that help organisations prepare for the post-quantum era. These include cryptographic asset mapping, consultancy on PQC implementation, and practical guidance for migration. While QKD is generally viewed as a long-term investment, PQC-related services already provide concrete commercial opportunities for partners within HSD's ecosystem.

5. Conclusion & Discussion: Security Delta's Role

To sum up this exploration, the threats and dangers of quantum technology for the digital ecosystem in South-Holland are unprecedented. Through the quantum computer, our digital stability comes under pressure as current encryption methods will no longer be suitable for the defense of our data. Because of the 'Store now, Decrypt later'-attack, companies best start with implementing security measures right away. The two main solutions are either the implementation of Post-Quantum Cryptography (focused on the threat of quantum technology) or the implementation of Quantum Key Distribution (focused on the opportunities of quantum technology). We state that the best approach is a synergy of both solutions, where PQC should be implemented as soon as possible and QKD provides security in the long term. There exists a high momentum within the Dutch quantum ecosystem. As 2025 has also been coined the international Year of Quantum Science and Technology by UNESCO, we believe that this is the time to act and prepare Dutch digital society for the quantum age.

Protections against the threat of quantum computer are available. However, if the basic cybersecurity measures are not taken, why bother with implementing post-quantum measures? Therefore, the first and most important step is enlarging basic cybersecurity levels throughout Dutch society. As a chain is as weak as the weakest link, this is an active task for all companies involved. One of the often-overlooked aspects in this is data-minimalization. The other results regarding the mitigation of the quantum-threat are: raising awareness, implementing no-regret moves and the PQC-migration handbook, reaching crypto-agility and standardise and implement QKD systems. It is important however to note that the digital ecosystem consists of different target groups with different plannings. These target groups should not be combined into one timeline.

There are opportunities to further strengthen the collaboration within the quantum ecosystem. One way to achieve this is by establishing cross-sectoral connections. Many companies within the network of HSD are interested in cooperating with quantum organisations, as well as the other way around. However, the practical implications of cooperating often stay vague. The main challenge in fostering collaboration between the quantum and cybersecurity fields is the lack of felt urgency, funding and human capital at the cybersecurity side. Another challenge is the lack of security proofs and certified standards of newly developed quantum systems. Stakeholders indicate nonetheless that opportunities exist for companies willing to invest in tools focused on the implementation of PQC measures and the mapping of cryptographic assets of a company.

Throughout this exploration, HSD has been looking for the places where we could add value. Enlarging basic cybersecurity levels throughout society falls into the scope of HSD, for example through the cyber resilience centers HSD supports in different sectors. Raising awareness about the importance of post-quantum measures is also a reachable goal. However, simply creating isolated awareness sessions will not achieve behavioural change; for that follow-up and practical support are required. This takes time and effort and requires structural financial support. One of the lessons HSD learned throughout the years is that general awareness sessions do not reach the wanted outcomes. Action-related activities, which give hands and feet to start the post-quantum journey, are effective in creating a momentum of change. Another lesson HSD learned is that when creating a movement, organizing a programme is more effective than stand-alone events. Funds are needed for this.

The partners of HSD are mainly tech-oriented and cybersecurity related. Enhancing and promoting innovations in quantum technology itself falls therefore not under the scope of activities of HSD. The main attention of HSD lies with the ‘threat-side’ of quantum, focusing on the importance of PQC for immediate mitigation of risks. Increased awareness of the quantum threat will likely also benefit the quantum industry. One of the main fields where innovations between cyber and quantum can emerge is in Security by Design/Smart Grids. Projects which are created now must last for decades. Quantum-security has to be integrated into the core of these projects.

The main power of HSD is to act as a bridge. HSD is aware of all the different companies and organisations in both the quantum and cyber ecosystems. HSD has the experience and the right contacts for setting up consortia and cooperations. When companies have questions regarding the post-quantum migration, for example when an SME is searching for a cryptographic asset-scan of the company, HSD knows who to connect. Setting up so-called ‘learning communities’ of companies involved in the post-quantum migration is however envisioned as a primary task for a knowledge institute or governmental organisation, such as QDNL. HSD can inform and refer companies interested in this to each other, but without a certain programme and accompanying fund HSD does not have the means and human capital to be the instigator of this.

HSD will communicate about quantum in its newsletters and talks. HSD can tell the message of becoming quantum-ready alongside with other messages of reaching wanted cybersecurity levels in the first places. The focus for SMEs will be on reaching basic cybersecurity first, as we cannot over-demand a company. The energy first has to be put in enlarging the overall level of cybersecurity. For bigger or more technical-advanced companies, the message will be to start with reaching post-quantum safety immediately. The migration to PQC and possibly later on QKD is however not solely cyber-focused, it is also very much affected by process management and the people involved. Therefore, reaching post-quantum maturity is a long-term project which has to start today. Let's innovate together!

6. Appendixes

Appendix 1: Different tasks of stakeholers

The table below shows the different stakeholders and their primary tasks related to preparing for the quantum threat or leveraging the opportunities created by quantum.

Stakeholder	Task/focus
Government	• Develop practical tools and guidelines for critical infrastructure and governments to implement • Incorporate quantum in already existing regulations
Local governments	• Stimulate the adoption of security measures across organisations and businesses within their own municipality. • Take measures to secure own infrastructure, for instance by making their ICT-infrastructure available as a test environment for product developers and IT-suppliers
IT-suppliers and product developers	• Develop and test new quantum products • Implement quantum-proof techniques into their products and services
Vital infrastructure	• Implement and allow for the testing of new quantum-proof products • Implement post-quantum-security in Security by Design
SME's	• Engage in conversations with their IT-suppliers • Start mapping their IT-infrastructure • Engage with no-regret moves

Apart from the difference in tasks, they also vary in the level of urgency and are sometimes subsequent activities. The first stated action of the national government, for instance, has a high priority because they need to develop tools and guidelines for local governments to use, which will be used by the local governments to stimulate the business within their municipality to innovate and implement security measures. Product developers and IT suppliers should simultaneously develop and test their products, after which they should start holding conversations with their clients, including SMEs.

Appendix 2: List of interviewees

Organisation	Person
Province of South-Holland	Jelmer Olsman Ilja van Ootegem
Municipality of The Hague	Saïda van Kalsbeek Ferry Tillekens Timo Koot
InnovationQuarter	Jacqueline Schardijn
Quantum Delta NL	Ahmed el-Kadars Dan Howell Richard van Harderwijk Ulrich Mans
Q-Bird	Ingrid Romijn
Luris	Tim Stegwee
Quantumveilige Cryptografie NL	Pieter Schneider
TNO	Thomas Attema
Quantum Gateway Foundation	Dimitri van Esch
CapGemini	Siebe Spee
Chunk Works	Dennis Schouten
Eurofiber	Marc Hulzebos
QuTech	Kees Eijkel
ON2IT	Jeroen Scheerder Karin Muller

Appendix 3: Referene List

AIVD, CWI, & TNO. (2025). Het PQC-migratie handboek: Richtlijnen voor het migreren naar Post-Quantumcryptografie (No. 26643, nr. 1273). AIVD. https://open.overheid.nl/documenten/oep-d0b3afabd21f66aef93ac89d3d387a808f334c7b/pdf

AIVD & NCSC. (2023). Maak je organisatie quantumveilig. NCSC. https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2023/september/18/ma ak-je-organisatie-quantumveilig/23405792_JenV_Maak_je_organisatie_quantumveilig_A4.pdf

Boutin, C. (2025, February 4). NIST releases first 3 Finalized Post-Quantum Encryption Standards. NIST. https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

Bruins Slot, H. G. J. (2024). Fiche: Aanbeveling Routekaart Post-Quantumcryptografie (No. 22112, nr. 3945). https://open.overheid.nl/documenten/oep-ad653d0e0aae850302bcbc4ae0e4618d03a2adfe/pdf

Deep Tech Fund. (2023). Venturing into Quantum Technology in the Netherlands. Invest-NL. https://www.invest-nl.nl/media/attachment/id/2869

European Commission. (2024). Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography. https://ec.europa.eu/newsroom/dae/redirection/document/104259

Karstens, B., Hijstek, B., & Kool, L. (2023). Quantumtechnologie in de samenleving. Rathenau Instituut. https://www.rathenau.nl/nl/digitalisering/rathenau-scan-quantumtechnologie-de-samenleving

Leonte, M.-B., & Schwabe, P. (2024, August 14). NIST standardizes quantum-safe cryptography methods. Centrum Wiskunde & Informatica. https://www.cwi.nl/en/news/nist-standardizes-quantum-safe-cryptography-methods/

Ministerie van Economische Zaken en Klimaat [EZK]. (2024). De Nationale Technologiestrategie (No. 33009, nr. 140). https://open.overheid.nl/documenten/oep-63dd4535fc4380c7bb24585ef5a3fe8a94d4e6a3/pdf

NCSC. (2023). Factsheet Post-Quantum Cryptografie. https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2023/november/8/factsheet-postquantumcryptografie/Factsheet_Post-quantum_cryptografie_okt23_NL_archief.pdf

Quantum Delta NL. (2019). Nationale Agenda Quantum Technologie. https://open.overheid.nl/repository/ronl-61f96d64-5471-48e7-aaeb-aad21a953d2c/1/pdf/Nationale%20Agenda%20Quantumtechnologie.pdf

Quantum Delta NL. (2020). Economic Impact of Quantum in The Netherlands. https://assets.quantum-delta.prod.verveagency.com/assets/economic-impact-of-quantum-in-the-netherlands.pdf

Stam, E., Van der Starre, B., & Cloosterman, E. (2020). Het Nederlandse Quantum Ecosysteem. QuTech. https://assets.quantum-delta.prod.verveagency.com/assets/het-nederlandse-quantum-ecosysteem-birch-:-university-of-utrecht.pdf

Van der Starre, B., Bos, C., Cloosterman, E., & Van den Toren, J. P. (2021). De impact van quantum. Scenario's voor de toekomst van quantumtechnologie in Zuid-Holland. Birch. https://www.zuid-holland.nl/publish/pages/28899/quantumtechnologiezuid-holland-scenariosvoordetoekomst-birch.pdf

Van Velzen, J., & Neelakantaiah, G. K. (2023). Quantumdreiging: Een nieuwe cyberdreiging voor organisaties in de publieke sector. In Trends in Veiligheid 2023-24: Innovatie in een Weerbare Digitale Samenleving. Capgemini. https://prod.ucwe.capgemini.com/nl-nl/wp-content/uploads/sites/19/2023/10/Trends-in-Veiligheid-2023-Report.pdf

Security Delta (HSD)
Wilhelmina van Pruisenweg 104
2595 AN The Hague
070 204 41 80

info@securitydelta.nl
www.securitydelta.nl
@HSD_NL