Docnr3

Algemene Rekenkamer

BEZORGEN
Voorzitter van de Eerste Kamer
der Staten-Generaal
Kazernestraat 52
2514 CV DEN HAAG

Postbus 20015
2500 EA Den Haag
070 342 43 44
voorlichting@rekenkamer.nl
www.rekenkamer.nl

datum 4 februari 2026
betreft publicatie *Focus op quantum bij de rijksoverheid*

Geachte mevrouw Vos,

Hierbij bieden wij u aan de publicatie *Focus op quantum bij de rijksoverheid*.
Deze publicatie verschijnt vandaag.

Algemene Rekenkamer

5.1.2.e
5.1.2.e

Pieter Duisenberg,
president

5.1.2.e
5.1.2.e

Mark Smolenaars,
wnd. secretaris

ons kenmerk 164478
bijlage(n) 1

Focus op quantum bij de rijksoverheid

2026

Algemene Rekenkamer

Inhoud

1. Samenvatting | 3

2. Over dit onderzoek | 7

2.1 Waarom dit onderzoek? | 7

2.2 Wat is quantumtechnologie? | 8

2.3 Leeswijzer | 9

3. Kansen voor de samenleving | 10

3.1 Toepassingen met quantumtechnologie | 10

3.2 Beleid voor de ontwikkeling van quantumtechnologie | 13

3.3 Resultaten van investeringen | 16

3.4 Tussenresultaten | 18

3.5 Laatste fase Nationaal Groeifonds | 19

3.6 Uitdagingen voor de toekomst | 19

4. Kansen voor de rijksoverheid | 22

4.1 Experimenteren met quantum bij de rijksoverheid | 22

4.2 Beleid voor het gebruik van quantumtechnologie | 25

4.3 Obstakels om quantumtechnologie in te zetten | 26

5. De dreiging van quantumcomputers voor het Rijk | 29

5.1 Quantumcomputers kunnen cryptografie kraken | 29

5.2 Organisaties moeten hun cryptografie vervangen | 32

5.3 Hoe bevordert het Rijk dat de risico's van quantum worden beheerst? | 35

5.4 De PQC-migratie van rijksoverheidsorganisaties | 36

5.5 Obstakels bij de voorbereidingen voor de quantumdreiging | 44

6. Reactie | 47

Bijlagen | 48

Bijlage 1 Methodologische verantwoording | 48

Bijlage 2 Geselecteerde organisaties | 51

Bijlage 3 Literatuur | 53

Bijlage 4 Eindnoten | 58

1. Samenvatting

Quantumtechnologie. Het klinkt alsof het uit de toekomst komt en voor een deel is dat ook zo. Toch is er nu al wereldwijd een wedloop gaande op de ontwikkeling van deze sleuteltechnologie. Een technologie die – na AI – de samenleving opnieuw op zijn kop kan zetten. Volop kansen voor het verdienvermogen van Nederland, maar ook risico's. Hoe bereidt Nederland zich daarop voor? Wat doet de rijksoverheid om de risico's te beperken en om de kansen te benutten? Welk publiek geld stelt het kabinet ter beschikking en welk beleid voert het uit? Daar gaat dit onderzoek over.

Quantumcomputers vormen een gevaar voor de informatiebeveiliging van het Rijk

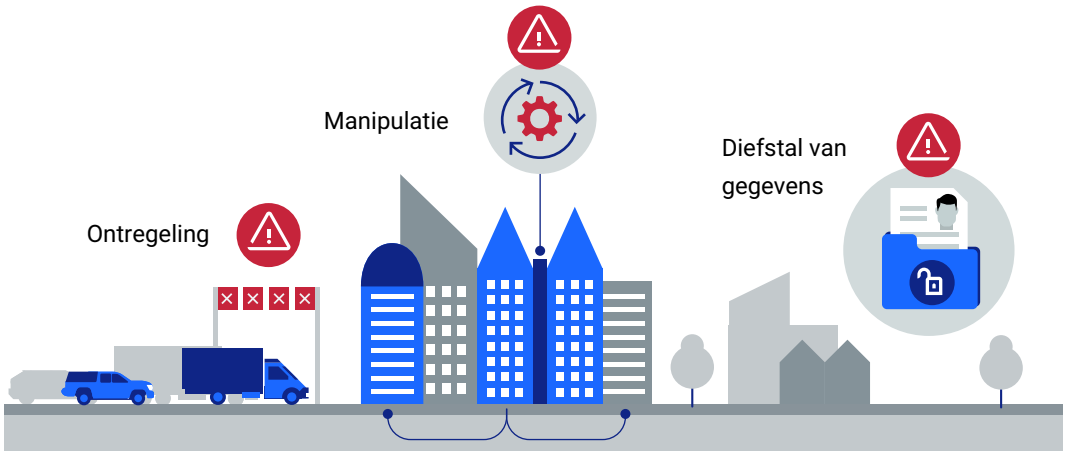
Het risico van quantumtechnologie is dat krachtige quantumcomputers in de toekomst gebruikt kunnen worden om *cryptografie* te kraken. Cryptografie is een technologie voor het beveiligen van digitale informatie en IT-systemen.
De rijksoverheid gebruikt het voor allerlei toepassingen, zoals:

- het beschermen van vertrouwelijke informatie van burgers en bedrijven;
- het regelen van toegang tot vitale infrastructuur zoals waterkeringen en bruggen;
- het inloggen met DigiD;
- het waarborgen van de authenticiteit van paspoorten.

Als cryptografie wordt gekraakt, lopen al deze toepassingen gevaar. Dat kan grote maatschappelijke gevolgen hebben. Het moment waarop quantumcomputers dat kunnen, heet *Q-day*. Het is nog onduidelijk wanneer Q-day precies komt, maar de AIVD waarschuwt dat het al in 2030 kan zijn (AIVD et al., 2024).

Figuur 1 *Voorbeelden van de risico's van quantumcomputers voor het Rijk*

Quantumcomputers bedreigen de vertrouwelijke informatie en vitale infrastructuur van het Rijk



De rijksoverheid moet zich voorbereiden op de dreiging van quantumcomputers

Wereldwijd wordt hard gewerkt aan het beperken van de quantumdreiging. Daarvoor zijn nieuwe vormen van cryptografie ontwikkeld die bestand zijn tegen quantum-computers: *post-quantum cryptografie* (PQC). Om de risico's te beperken, moeten rijksoverheidsorganisaties hun huidige cryptografie tijdig omzetten naar deze veiligere variant. Deze overgang heet de PQC-migratie.

Het kabinet stimuleert de rijksoverheid om quantumdreiging aan te pakken

De staatssecretaris Digitalisering erkent dat quantumcomputers de nationale veiligheid in gevaar kunnen brengen, als ze door kwaadwillenden worden ingezet. Daarom heeft de staatssecretaris het programma Quantumveilige cryptografie NL (QvC NL) ingericht om rijksoverheidsorganisaties te helpen met hun PQC-migraties. QvC NL doet dit door informatie te delen en handreikingen te ontwikkelen. Rijksoverheidsorganisaties zijn zelf aan zet om quantumveilige cryptografie in te voeren.

Weinig rijksoverheidsorganisaties zijn gestart met aanpak quantumdreiging

Er zijn zorgen dat organisaties niet op tijd met de PQC-migratie beginnen. Alhoewel de meeste ondervraagde rijksoverheidsorganisaties werken aan hun informatie-beveiliging, zijn er weinig die maatregelen hebben getroffen die specifiek gericht zijn op de dreiging van quantumcomputers.

Figuur 2 *Percentage ondervraagde organisaties dat is gestart met hun aanpak van quantumdreiging*

Rijksoverheidsorganisaties hebben bijvoorbeeld nog geen gesprekken gevoerd met leveranciers over quantumveilige producten en nog geen plannen gemaakt voor het invoeren van quantumveilige cryptografie. De belangrijkste obstakels die zij zien zijn een gebrek aan capaciteit en expertise, en andere activiteiten die meer prioriteit hebben omdat ze als acuter worden ervaren.

Het kabinet investeert in de ontwikkeling van quantumtechnologie

Quantumtechnologie biedt ook allerlei kansen voor de overheid, maatschappij en economie. Mogelijk kunnen we door quantumtechnologie preciezer meten, veiliger communiceren en complexe berekeningen doen. Dit biedt kansen voor onder andere energiezuinige voedselproductie, het ontwikkelen van nieuwe materialen en cybersecurity. Het kabinet ziet quantumtechnologie als een sleuteltechnologie met een groot potentieel voor het verdienvermogen van Nederland. Het kabinet investeert daarom via het Nationaal Groeifonds, in de periode 2021-2028, € 615 miljoen in het ontwikkelen van deze technologie.

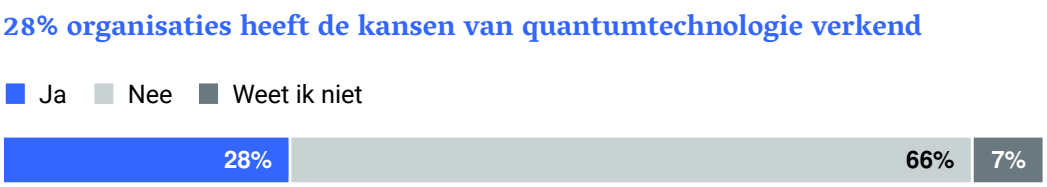
Nederland heeft een toppositie op quantum, dat dit zo blijft is niet vanzelfsprekend

Met de investeringen uit het Nationaal Groeifonds is een bloeiend quantumnetwerk opgezet en heeft Nederland een academische toppositie verkregen. Dit netwerk bestaat onder andere uit de stichting Quantum Delta NL, TNO en kennisinstellingen. De adviescommissie van het Nationaal Groeifonds is onder de indruk van de tussenresultaten die de investeringen tot nu toe hebben opgeleverd. Het werk is echter nog niet af. Veel plannen en projecten staan nog in de steigers en het is lastig te voorspellen of Nederland de toppositie ook in de toekomst gaat behouden. De grote uitdaging voor de toekomst is om deze beloften te vertalen naar concrete marktoepassingen en een plek te veroveren op de hightechmarkt. Daarbij speelt dat sommige andere landen de afgelopen jaren aanzienlijk meer publiek geld in quantumtechnologie investeerden.

28% van rijksoverheidsorganisaties heeft de kansen van quantum verkend

Ook bij de rijksoverheid zijn er in de toekomst mogelijkheden om quantum-technologie in te zetten. Toch hebben de meeste ondervraagde rijkoverheids-organisaties de kansen van deze technologie niet verkend. Dit komt onder andere doordat het nog niet duidelijk is welke taken beter uitgevoerd zouden kunnen worden met quantumtechnologie, in plaats van met huidige systemen.

Figuur 3 *Percentage ondervraagde organisaties dat de kansen van quantum-technologie heeft verkend*



De verkenningen die wel zijn uitgevoerd onderzoeken vooral waar en hoe quantum-technologieën mogelijk in de toekomst meerwaarde kunnen bieden. Rijksoverheidsorganisaties geven aan dat de technologie zich nog verder moet ontwikkelen. Daarbij geven ze aan dat wanneer de technologie in de toekomst doorbreekt, verschillende obstakels moeten worden overbrugd. Denk hierbij aan gebrek aan kennis en expertise of het passend maken van quantumtechnologie in de huidige technische infrastructuur.

Het kabinet werkt aan een rijksbrede Quantum Strategie

Momenteel werkt het ministerie van EZ samen met andere ministeries aan het opstellen van een rijksbrede Quantum Strategie. Deze aankomende strategie onderstreept het strategische belang van quantumtechnologie en zal doelen en acties bevatten om zowel de kansen als risico's van quantumtechnologie te adresseren.

Waarom dit onderzoek?

Voor een goed functionerende en presterende rijksoverheid moeten risico's goed worden beheerst. Volgens de Algemene Rekenkamer is het belangrijk om, naast het hebben van zicht op kansen, zicht te hebben op de voorbereidingen die worden gedaan om dreigingen aan te pakken. Alleen als bekend is hoe de rijksoverheid zich voorbereidt op de kansen en het afdekken van de risico's, kan het parlement sturen op een verantwoorde inzet. Met dit onderzoek bieden we een eerste inzicht in de voorbereidingen op de kansen en dreigingen van quantumtechnologie. Daarnaast geeft dit onderzoek ook op hoofdlijnen inzicht in tussenresultaten van de investeringen.

2. Over dit onderzoek

2.1 Waarom dit onderzoek?

De Verenigde Naties hebben 2025 uitgeroepen tot het International Year of Quantum Science and Technology. Dit is om het 100-jarig jubileum van de quantummechanica te vieren. Dit jaar vindt elke dag wel ergens op de wereld een bijeenkomst plaats over quantumtechnologie. In Nederland is die aandacht er ook: het kabinet ziet quantum-technologie als sleuteltechnologie die veel economische kansen biedt. Een sleutel-technologie is een specifieke technologie die cruciaal is voor toekomstige economische groei en waar Nederland wetenschappelijk in uitblinkt.

Met de Nationale Technologiestrategie (NTS) richt de rijksoverheid zich op het stimuleren van innovatie en het versterken van Nederland als technologisch leider op 10 technologiegebieden. Quantumtechnologie is een van die gebieden (Ministerie van Economische Zaken en Klimaat, 2024). De rijksoverheid investeert in de periode 2021-2028 via het Nationaal Groeifonds tenminste € 615 miljoen in de ontwikkeling van deze technologie. De verwachting is dat quantumtechnologie innovaties in beweging zal zetten voor overheid, particuliere sector en maatschappij, die met de huidige technologieën onmogelijk zijn.

Door te investeren in quantumtechnologie wil de rijksoverheid de technologische soevereiniteit van Nederland waarborgen. Het idee daarbij is dat een sterke, innoverende en concurrerende economie beter bestand is tegen dreigingen voor de nationale veiligheid. Hierbij rijst de vraag wat de resultaten tot nu toe zijn van deze investeringen. Een actueel openbaar overzicht hiervan ontbreekt. Ook ontbreekt

inzicht in de kansen die de rijksoverheid voor zichzelf ziet door de inzet van quantumtechnologie.

Tegelijkertijd brengt de komst van quantumtechnologie risico's met zich mee. Naar verwachting zal de quantumcomputer op een gegeven moment de versleuteling van huidige computers makkelijk kunnen kraken. Hierdoor kunnen staats- of bedrijfsgeheimen in handen komen van partijen met kwade bedoelingen. Ook zijn er risico's voor de vitale infrastructuur. De Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) stelt dan ook dat toekomstige krachtige quantumcomputers een dreiging vormen voor de nationale veiligheid.

Hoe de rijksoverheid zich voorbereidt op de risico's van deze technologie is onbekend. Vanwege de snelle technologische ontwikkelingen en geopolitieke spanningen neemt de noodzaak voor het inzicht in die voorbereidingen echter toe. De ontwikkelingen in Nederland staan dan ook niet los van de aanpak van de dreiging van quantumcomputers door de Europese Commissie en de Europese lidstaten.

2.2 Wat is quantumtechnologie?

Quantumtechnologie is een verzamelnaam voor technologieën die gebruikmaken van de bijzondere eigenschappen van deeltjes die kleiner zijn dan atomen. Zo'n deeltje wordt ook wel 'quantum' genoemd. Quantumtechnologie benut het bijzondere gedrag van deze allerkleinste deeltjes om op een radicaal nieuwe manier te rekenen, communiceren en meten. Dat is anders dan bij de huidige technologie. Zo werken computers nu nog met klassieke bits (0 of 1). Quantumcomputers werken daarentegen met qubits, de bouwstenen van de quantumcomputer. Dankzij het unieke gedrag van quantumdeeltjes, kunnen deze qubits tegelijkertijd zowel de waarde 0 als 1 aannemen. Daardoor kan quantumtechnologie complexe berekeningen veel sneller uitvoeren dan klassieke computers.

2.2.1 Mogelijke toepassingen van quantumtechnologie

Quantumtechnologie biedt een breed spectrum aan toepassingen voor onder andere het klimaat, energiezuinige voedselproductie, nieuwe materialen, medicijnen, optimalisatievraagstukken, machine learning en cybersecurity. We onderscheiden 3 belangrijke quantumtechnologieën:

- **Quantumsensoren**: deze gebruiken de kenmerken van quantummechanica om zaken zeer nauwkeurig te meten.
- **Quantumcommunicatie**: dit maakt communicatie tussen quantumcomputers onderling en tussen quantumcomputers en quantumsensoren mogelijk.
- **Quantumcomputers**: quantumcomputers kunnen in de toekomst bepaalde berekeningen sneller doen dan gewone computers (Rathenau Instituut, 2023). Deze berekeningen kunnen grote gevolgen hebben voor onze samenleving. Ze kunnen helpen bij het sneller ontwikkelen van nieuwe medicijnen, batterij-materialen of supergeleiding (Europese Commissie, 2025).

Naast alle kansen die quantumcomputers kunnen bieden, is die enorme rekenkracht ook een risico voor onze informatieveiligheid. Krachtige quantumcomputers zouden in de toekomst belangrijke cryptografie kunnen kraken. Cryptografie is de techniek die wordt gebruikt om gegevens digitaal te versleutelen. Dit versleutelen gebeurt bij het gebruik en de overdracht van informatie binnen en tussen organisaties. Maar ook bij de opslag van informatie, op locatie of in de cloud. Voor het gevaar dat quantum-computers de cryptografie kunnen kraken, bestaat een remedie: het migreren naar *post-quantum cryptografie* (PQC). Daarover vertellen we meer in hoofdstuk 5.

2.3 Leeswijzer

In hoofdstuk 3 beschrijven we de kansen van quantumtechnologie voor de Nederlandse samenleving en hoe het er op dit moment voor staat. In hoofdstuk 4 beschrijven we hoe de rijksoverheid de kansen van quantumtechnologie benut. In hoofdstuk 5 laten we tot slot zien hoe rijksoverheidsorganisaties zich op dit moment voorbereiden op de dreigingen van quantumcomputers.

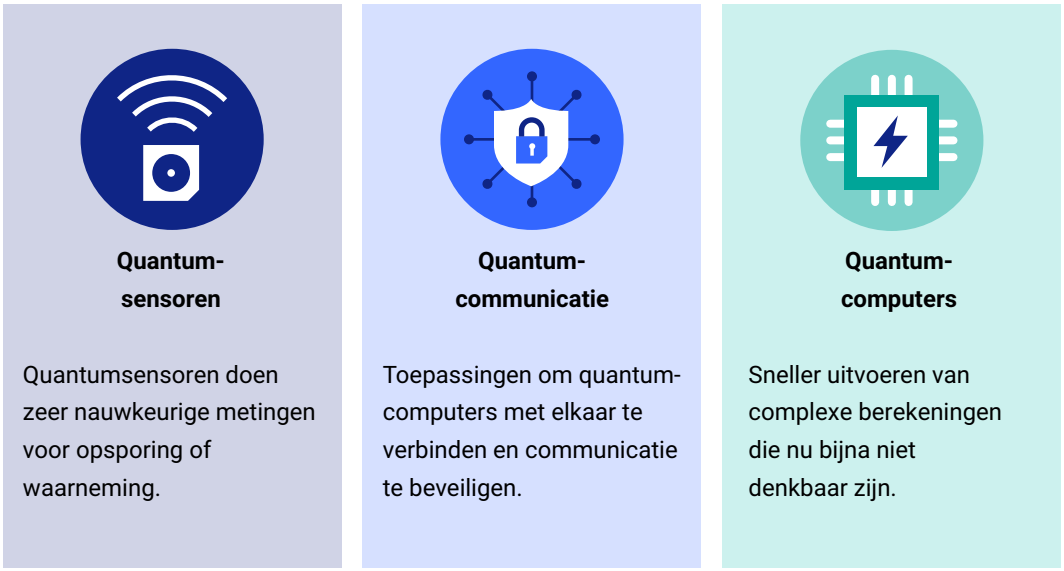
3. Kansen voor de samenleving

Het kabinet ziet quantumtechnologie als een sleuteltechnologie met een groot potentieel voor het verdienvermogen van Nederland. Hoewel dé doorbraak van quantumtechnologie nog niet heeft plaatsgevonden, is er veel interesse voor de toekomstige toepassingen van quantumtechnologie. De mogelijkheid bestaat dat quantumtechnologie een nieuwe technologische revolutie teweeg zal brengen in de samenleving. Nederland investeert daarom via het Nationaal Groeifonds tussen 2021 en 2028 € 615 miljoen in deze technologie. Hiermee is een bloeiend netwerk opgezet en heeft Nederland een academische toppositie verkregen. Enkele resultaten zijn al behaald, zoals het realiseren van meerdere House of Quantum locaties, testlocaties voor quantumsensoren en een nieuwe quantumcomputer. Veel plannen en projecten staan nog in de steigers. Het is lastig te voorspellen of Nederland de toppositie ook in de toekomst zal behouden. De afgelopen jaren investeerden andere landen aanzienlijk meer publiek geld in quantumtechnologie. Het kabinet verwacht dat het quantumecosysteem na afloop van de groeifonds-financiering een volgende fase van volwassenheid heeft bereikt, maar verwacht ook dat aanvullende publieke financiering nodig zal zijn om de ontwikkeling verder te ondersteunen.[1]

3.1 Toepassingen met quantumtechnologie

Quantumtechnologie biedt verschillende mogelijkheden voor de samenleving en overheidsorganisaties. We kunnen uitkijken naar verschillende toepassingen met de 3 vormen van quantumtechnologie in de toekomst.

Figuur 4 *De 3 vormen van quantumtechnologie*



3.1.1 Quantumsensoren

Quantumsensoren kunnen heel precieze metingen doen. Deze sensoren kunnen bijvoorbeeld magnetische velden, versnellingen, rotaties, tijd of druk opsporen (Ministerie van Infrastructuur en Waterstaat, 2025). Hierdoor kunnen ondergrondse objecten worden gedetecteerd, zoals gas- en waterreservoirs, mineralen, of kabels en leidingen detecteren. Ook andere verschijnselen, zoals aardbevingen kunnen beter worden waargenomen (Europol, 2023). Quantumsensoren hebben ook de potentie om de elektrische activiteit van het hart nauwkeuriger te meten (World Economic Forum, 2024). Hierdoor kunnen artsen medische aandoeningen wellicht beter opsporen. Dit biedt kansen voor de medische wereld, zoals precisiemedicatie (OECD, 2025).

De ontwikkeling van quantumsensoren is relatief vergevorderd. Daardoor is deze quantumtechnologie waarschijnlijk als eerste breed toepasbaar. Quantumsensoren zijn nu al te koop. Maar het kan nog jaren duren voordat deze in de praktijk echt van nut zijn. De grote gevoeligheid van de sensoren maakt deze ook vatbaar voor verstoringen. Bovendien zijn ze erg duur. Daardoor zijn er nog geen quantumsensoren beschikbaar die goed werken buiten een laboratoriumomgeving (Ministerie van Infrastructuur en Waterstaat, 2025).

3.1.2 Quantumcommunicatie

Quantumcommunicatie maakt het mogelijk om quantumapparaten en normale computers aan elkaar te koppelen. Dat is nodig om informatie uit te wisselen tussen

apparaten die wel gebruikmaken van quantumtechnologie en apparaten die dat niet doen. Daarnaast bieden quantumnetwerken ook verbindingen die in potentie zeer veilig zijn. Iedere poging om qubits te onderscheppen, te lezen en weer door te sturen, kan worden gedetecteerd. Deze ontwikkeling is onder andere relevant voor de financiële, logistieke, internet- en telecomsector en de overheid (Stichting Quantum Delta, 2021).

Een veel besproken voorbeeld is de inzet van *quantum key distribution* (QKD). Het doel van QKD is het veilig uitwisselen van geheime sleutels tussen 2 partijen, waardoor een veilige communicatie mogelijk is. QKD heeft de potentie om te beschermen tegen zeer geavanceerde aanvallen. Verschillende experts die wij spraken zien dit als een van de eerste concrete kansen van quantumtechnologie voor de overheid. Zij zien toenemende kansen voor beveiligde quantumnetwerken, mede gelet op geopolitieke ontwikkelingen.

Wel moet de technologie nog verder ontwikkeld worden. Meerdere beperkingen, zoals werking bij langere afstand, kosten en kwetsbaarheden moeten nog worden opgelost (AIVD et al., 2024). In de Rotterdamse haven ligt inmiddels een kleinschalig quantumnetwerk (Port of Rotterdam, 2024). Werknemers van de haven gebruiken dit netwerk om te experimenteren met de beveiligde verbinding. In de toekomst kan dit worden uitgebreid.

3.1.3 Quantumcomputers

Quantumcomputers kunnen in potentie problemen oplossen die voor klassieke computers praktisch onoplosbaar zijn. Ze bieden door middel van simulaties met name kansen voor molecuul- en medicijnontwerp. Het nabootsen van (interacties tussen) moleculen vereist heel veel rekenkracht, de huidige supercomputers kunnen die niet bieden. Quantumcomputers kunnen deze ingewikkelde berekeningen sneller en nauwkeuriger uitvoeren, waardoor nieuwe medicijnen kunnen worden ontwikkeld (OECD, 2025). Experts die wij spraken, geven aan dat momenteel de meeste capaciteit van rekencentra naar dit soort toepassingen gaat.

Ook bieden quantumcomputers kansen in verschillende optimalisatievraagstukken. Denk aan ingewikkelde logistieke processen optimaal plannen. Zeker als de toe-leveringsketen van een product veel variabelen kent. Daarnaast wordt onderzocht hoe quantumcomputers een bijdrage kunnen leveren in het trainen van AI-systemen (OECD, 2025). De combinatie van quantumtechnologie en AI kan mogelijk leiden tot nieuwe, snellere en zuinigere AI-modellen (Europol, 2023).

In vergelijking met de andere soorten quantumtechnologie is de ontwikkeling van quantumcomputers het minst ver.[2] Momenteel is er nog geen quantumcomputer die een berekening heeft gemaakt die daadwerkelijk sneller is dan met huidige computers. Dat is uiteindelijk wel het doel van de ontwikkelingen. Ter illustratie: in Amsterdam wordt nu een quantumcomputer gebouwd. Deze zal over 'slechts' minimaal 16 qubits beschikken (Quantum Delta NL, 2024). Quantumcomputers bieden echter pas een meerwaarde vanaf ongeveer 1.000 qubits. Experts zien de afgelopen periode wel een stabiele groei in de ontwikkeling van quantumcomputers.

3.2 Beleid voor de ontwikkeling van quantumtechnologie

Het kabinet ziet quantumtechnologie als een cruciale technologie voor Nederland. Al in 2012 investeerde het kabinet miljoenen in toponderzoek naar quantum-technologie (Tweede Kamer, 2012). In 2020 gaf het kabinet opnieuw aan dat quantumtechnologie een groot potentieel heeft voor de toekomst (Tweede Kamer, 2020). Door een leiderschapspositie op het gebied van quantumtechnologie in te nemen, is Nederland ook bestand tegen dreigingen voor de nationale veiligheid (Ministerie van Economische Zaken, 2025). De Nederlandse overheid ziet dat quantumtechnologie niet alleen kansen biedt voor de veiligheid, maar ook voor het verdienvermogen van Nederland. In 2021 is het Quantum Delta NL-programma gestart met een totale investering uit het Nationaal Groeifonds van € 615 miljoen om quantumtechnologie in Nederland verder te ontwikkelen, zowel voor de overheid, maatschappij als het bedrijfsleven en kennisinstellingen.

3.2.1 Doelen van Nederland

Het doel van het kabinetsbeleid is dat Nederland in 2035 een quantumecosysteem van wereldklasse heeft en een koploperspositie heeft in quantumtechnologie. Het ecosysteem is een netwerk dat bestaat uit onder meer de wetenschap, het onderwijs, het (tech)bedrijfsleven, start-ups en de overheid. Nederlandse bedrijven moeten volgens het kabinet Europees of mondiaal een sleutelpositie gaan innemen, met een strategische marktpositie in de wereld: Nederland als een Silicon Valley van quantumtechnologie. Volgens het kabinet wordt Nederland dan de plek waar nieuwe technologie vandaan komt en een hightechindustrie wordt gecreëerd.

De minister van EZ coördineert de stimulering van quantumtechnologie in Nederland. Om dit beleid in de praktijk te realiseren is in 2020 de stichting Quantum Delta NL (QDNL) opgericht. Deze stichting richt zich op het versnellen van de ontwikkeling en commercialisering van quantumtechnologie in Nederland.

De stichting stimuleert quantumtechnologie in Nederland met het programma Quantum Delta NL. De verschillende onderdelen van het programma worden uitgevoerd door de stichting of bestaande organisaties en consortia zoals QuTech, TNO, universiteiten, Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO), Rijksdienst voor Ondernemend Nederland (RVO) en NanoLabNL.

3.2.2 Investeringen

Samen met de stichting Quantum Delta NL heeft de minister van EZ in 2021 een aanvraag gedaan bij het Nationaal Groeifonds voor het programma Quantum Delta NL. Met het Nationaal Groeifonds investeert het kabinet in projecten die een zo groot mogelijke bijdrage leveren aan duurzame en structurele economische groei. Quantum Delta NL heeft € 615 miljoen uit het Nationaal Groeifonds toegekend gekregen (Nationaal Groeifonds, z.d.). In 2028 loopt het programma Quantum Delta NL af. Er komt volgens de huidige plannen geen nieuw geld beschikbaar. De laatste tranches van het Nationaal Groeifonds zijn inmiddels stopgezet door het kabinet. Vervolgplannen kunnen niet uit het Nationaal Groeifonds gefinancierd worden.

Ook andere organisaties, zoals TNO en NWO, dragen financieel en wetenschappelijk bij aan de ontwikkeling van quantumtechnologie. Daarnaast zijn er meerdere andere subsidies beschikbaar voor het stimuleren van quantumtechnologie. Ook de private sector investeert in quantumtechnologie. In dit onderzoek richten we ons echter uitsluitend op de publieke investeringen via het Nationaal Groeifonds.

3.2.3 Monitoring en evaluatie

Quantum Delta NL verantwoordt de investeringen en resultaten van het programma. Het ministerie van EZ evalueert deze. Quantum Delta NL stelt elk halfjaar een voortgangsrapportage op vanwege de verantwoording vanuit de subsidierelatie tussen aanvragers en Rijksdienst voor Ondernemend Nederland (RVO). Quantum Delta NL heeft daarnaast in 2023 een bredere tussentijdse evaluatie gedaan van de voortgang van het programma.

Uit deze interne evaluatie van Quantum Delta NL blijkt dat het programma op schema loopt. De stichting rapporteert hierover aan de minister van EZ, RVO en het Nationaal Groeifonds. Ook de Tweede Kamer ontvangt informatie over de voortgang van het programma. Bijvoorbeeld in het advies dat de adviescommissie van het Nationaal Groeifonds opstelde over de verdeling van het geld uit de derde beoordelingsronde (Tweede Kamer, 2024). De Tweede Kamer ontving ook het jaarverslag van het Nationaal Groeifonds over 2024 (Ministerie van Economische

Zaken, 2025). De adviescommissie van het Nationaal Groeifonds schrijft dat zij onder de indruk is van de voortgang en prestaties van Quantum Delta NL.

3.2.4 Europese initiatieven

Ook de Europese Commissie wil de kansen van quantumtechnologie benutten in de Europese Unie. Quantumtechnologie kan de Europese industrie competitiever maken en biedt mogelijkheden voor Europese technologische soevereiniteit. Hiervoor investeert de Europese Commissie al meerdere jaren in quantumtechnologie. In de afgelopen 5 jaar is bijna € 2 miljard aan verschillende Europese quantumprojecten toegewezen (Quantum Flagship, 2025). Noemenswaardige initiatieven zijn onder andere:

- het Quantum Technologies Flagship met € 1 miljard gedurende 10 jaar (2018-2028) (Europese Commissie, 2025b);
- het Europese High Performance Computing Joint Undertaking project (EuroHPC) met € 7 miljard waarmee onder andere quantumcomputers worden gebouwd (Europese Commissie, 2025c). Nederland is aangesloten met bijvoorbeeld de bouw van een quantumcomputer in Amsterdam met € 10 miljoen;
- het EuroQCI-initiatief voor de ontwikkeling van quantumcommunicatie-infrastructuur voor de hele EU met € 90 miljoen (Europese Commissie, 2025d). Nederland bouwt mee via onder andere het SEEWQCI-project van € 17,8 miljoen.

Europese Quantumstrategie en Quantumverordening

In juli 2025 heeft de Europese Commissie de Europese Quantumstrategie gepubliceerd. Met deze strategie maakt Europa duidelijk in 2030 een wereldleider op het gebied van quantumtechnologie te willen zijn. Belangrijke uitdagingen voor de Europese Commissie zijn het vertalen van academische successen naar de markt en de gefragmenteerde aanpak en investeringen door de Europese lidstaten.

Het kabinet vindt de Europese Quantumstrategie wenselijk en opportuun. Deze sluit aan bij het huidige Nederlandse beleid om een goed quantumecosysteem op te bouwen en wetenschappelijke kennis te verzilveren (Ministerie van Economische Zaken, 2025b). Het ministerie van EZ zoekt dan ook aansluiting bij de Europese context om het Nederlandse ecosysteem te stimuleren. De ambities met quantum-technologie zijn wereldwijd heel hoog en er is veel internationale concurrentie. Volgens EZ is samenwerking met andere Europese landen is dan ook noodzakelijk om nationale initiatieven te bundelen, extra slagkracht te verkrijgen en een bredere afzetmarkt te creëren.

De Europese Commissie werkt ook aan de Quantumverordening. Deze wordt naar verwachting in 2026 gepubliceerd. Hoewel details nog ontbreken, zal de verordening meer bindend beleid en investeringskaders bevatten.

3.3 Resultaten van investeringen

Het Quantum Delta NL-programma richt zich vanaf het begin in 2021 op het opzetten van de fundamenten voor de ontwikkeling van het quantumecosysteem. Een groot deel van het budget (€ 181 miljoen) uit het Nationaal Groeifonds gaat naar onderzoek en ontwikkeling van quantumtechnologie, zoals het bouwen van testfaciliteiten, het aanleggen van de quantumverbindingen, opleidingstrajecten en een quantum-computer in de cloud, online toegankelijk voor gebruikers. Een ander groot deel van het programma (€ 249 miljoen) gaat naar de ontwikkelingen van faciliteiten en niet-verplaatsbare infrastructuur. Die zijn nodig om het onderzoek en de ontwikkeling van quantumtechnologie te ondersteunen. Dit zijn onder andere het ontwikkelen van de nationale campus, technologieplatforms en cleanrooms. Cleanrooms zijn stofvrije afgesloten ruimten die het mogelijk maken om quantumsystemen te ontwikkelen.

Quantum Delta NL heeft sinds 2021 verschillende projecten gefinancierd met geld uit het Nationaal Groeifonds. Onderstaande figuur toont een overzicht van de begrote bedragen per actielijn en de voortgang van de ambities. Enkele tussentijdse resultaten tot en met 2024 zijn benoemd.

Figuur 5 *Tussenresultaten Programma Quantum Delta*

Programma Quantum delta NL

Wat zijn de bedragen, wat is er al gerealiseerd en wat was de ambitie?

Programma in Quantum Delta NL Budget in mln €	**Resultaten (2024)**	**Doelen**
Research and innovation **42**	75 lopende PhDs in quantumtechnologie en 23 topwetenschappers	Funderend onderzoek stimuleren voor technologieontwikkeling
Quantum ecosystem **83**	House of Quantum in Delft, valorisatieteam operationeel en startupprogramma gerealiseerd	Nationale campus, quantum-valorisatieteam, startup-programma en field labs
Human Capital **41**	4 Talent en learning centers opgericht, 722 studenten afgestudeerd in quantum, Nationale Quantum Cursus gelanceerd	Talentontwikkeling en onderwijsprogramma's ontwikkelen
Societal Impact **20**	Centre for Quantum and Society is opgericht en governance voor quantumtechnologie	Sociale bereidheid om quantum te gebruiken groeien
Quantum Computing & Simulation **90**	Quantum Inspire 2.0 met nieuwe quantumprocessoren	Quantumcomputer ontwikkelen met ten minste 100 qubits
National Quantum Network **62**	R&D Netwerk met 3 quantumprocessoren	Meerdere quantumnetwerken en fundament nationale infrastructuur
Quantum sensing applications **29**	Drie quantum sensor-testbeds zijn operationeel	Testbedden verder uitbreiden
Cleanroom facilities **150**	5 cleanrooms beschikbaar voor ontwikkelen van nanoapparatuur	Vernieuwen van apparatuur en machines geschikt maken voor toekomstige ontwikkelingen
Campusontwikkeling **99**	Aantal locaties House of Quantum geopend	Meerdere House of Quantum locaties in Nederland, nieuwe cleanroom en meer gedeelde faciliteiten

Bron: Quantum Delta

3.4 Tussenresultaten

Een aantal mijlpalen van het programma is al gerealiseerd. Het tweede House of Quantum is in Delft geopend, er ligt een eerste quantumnetwerk van 25 km tussen Den Haag en Delft (Quantum Delta NL, 2024b), 3 testfaciliteiten voor quantum-sensoren zijn operationeel en een fonds voor quantumstartups opgericht (Quantum Delta NL, 2025). Andere resultaten die het programma Quantum Delta NL heeft bereikt, zijn:

- de groei van 500 quantumbanen in 2021 naar 800 in 2024;
- het behouden van de wetenschappelijke toppositie;
- het Centre for Quantum and Society is opgericht om de maatschappelijk impact van quantumtechnologie te onderzoeken.

De voortgang van het programma komt overeen met de doelen die het programma zichzelf had gesteld.

Organisaties die wij spraken en die gebruikmaakten van de mogelijkheden van de projecten uit het Nationaal Groeifonds waren hier zeer tevreden mee: "*Het Nationaal Groeifonds heeft een hele belangrijke bijdrage geleverd aan het quantumecosysteem in Nederland en de internationale positionering daarvan. Verder heeft het ervoor gezorgd dat er veel talent is aangetrokken*."

De afgelopen jaren heeft Nederland een vooraanstaande positie in quantum-technologie gekregen. Er is volgens de experts die wij spraken interesse vanuit het buitenland in het Nederlandse quantumecosysteem: "*Nederland speelt mee op het wereldtoneel, heeft een voorbeeldfunctie en een koppositie*". Zij noemen bijvoorbeeld dat Quantum Delta NL als een koepelorganisatie iets is wat veel andere landen niet hebben.

Onze gesprekspartners geven aan dat Nederland internationaal gezien een sterke basis heeft. Deze hoogwaardige academische positie was één van de redenen om met Quantum Delta NL te starten: economische kansen creëren met onze academische toppositie. In 2020 behoorde Nederland al tot de leidende academische onderzoekscentra in quantumtechnologie (Birch, 2020). Deze positie is ook in 2024 nog sterk, blijkt uit onderzoek door Quantum Delta NL (Birch, 2024). We behoren volgens dit onderzoek op wetenschappelijk gebied (nog steeds) tot de academische top voor onderzoek naar quantumtechnologie.

3.5 Laatste fase Nationaal Groeifonds

Momenteel bevindt het programma Quantum Delta NL zich in de derde en laatste fase, gestart in 2025. Deze fase richt zich op het stimuleren van bedrijvigheid in het ecosysteem en het zorgen voor economische meerwaarde voor Nederland. Doelen die voor deze fase zijn gesteld zijn bijvoorbeeld:

- 3.500 quantumgerelateerde banen in Nederland;
- 100 start-ups;
- 25 eindgebruikers die diensten gebruiken die met geld via Quantum Delta NL zijn ontwikkeld.

Voor de lange termijn (2040) beoogt Quantum Delta NL dat door het programma er jaarlijks 0,02 tot 0,04% van het bruto binnenlands product (€ 230 tot 460 miljoen) wordt toegevoegd. Ook wil Quantum Delta NL dat er door het programma dan tussen de 8.000 en 18.000 banen in de quantumindustrie bij zijn gekomen. In totaal zou het programma dan € 1,5 tot 2,5 miljard aan de economie toevoegen. Daarmee zou de investering van € 615 miljoen meer dan 3 keer worden terugverdiend. Het overkoepelende doel voor deze fase is om met quantumtechnologie naar echte economische impact te gaan. Onze gesprekspartners bij het ministerie van EZ geven aan: er moet nu worden opgeschaald, start-ups moeten scale-ups worden en er moet echte verbinding komen met de hightechmarkt.

Hoewel het programma goed verloopt, is het belangrijk dat de ontwikkeling de komende jaren doorzet. Veel van de grote mijlpalen van het programma moeten nog worden behaald, zoals de lancering van Quantum Inspire 3.0, een quantumcomputer met 100+ qubits, gepland voor 2028. Andere doelen vereisen een verveelvoudiging van de tot nu toe behaalde resultaten. Bijvoorbeeld, het doel van Quantum Delta NL is dat private investeringen in start-ups en scale-ups zo'n € 750 miljoen per jaar bedragen als het programma Quantum Delta NL is afgelopen. In 2024 was dit ongeveer € 100 miljoen. Dat betekent dat deze investeringen flink moeten toenemen. Vergeleken met andere landen blijven de private investeringsbedragen echter aanzienlijk achter (Birch, 2024).

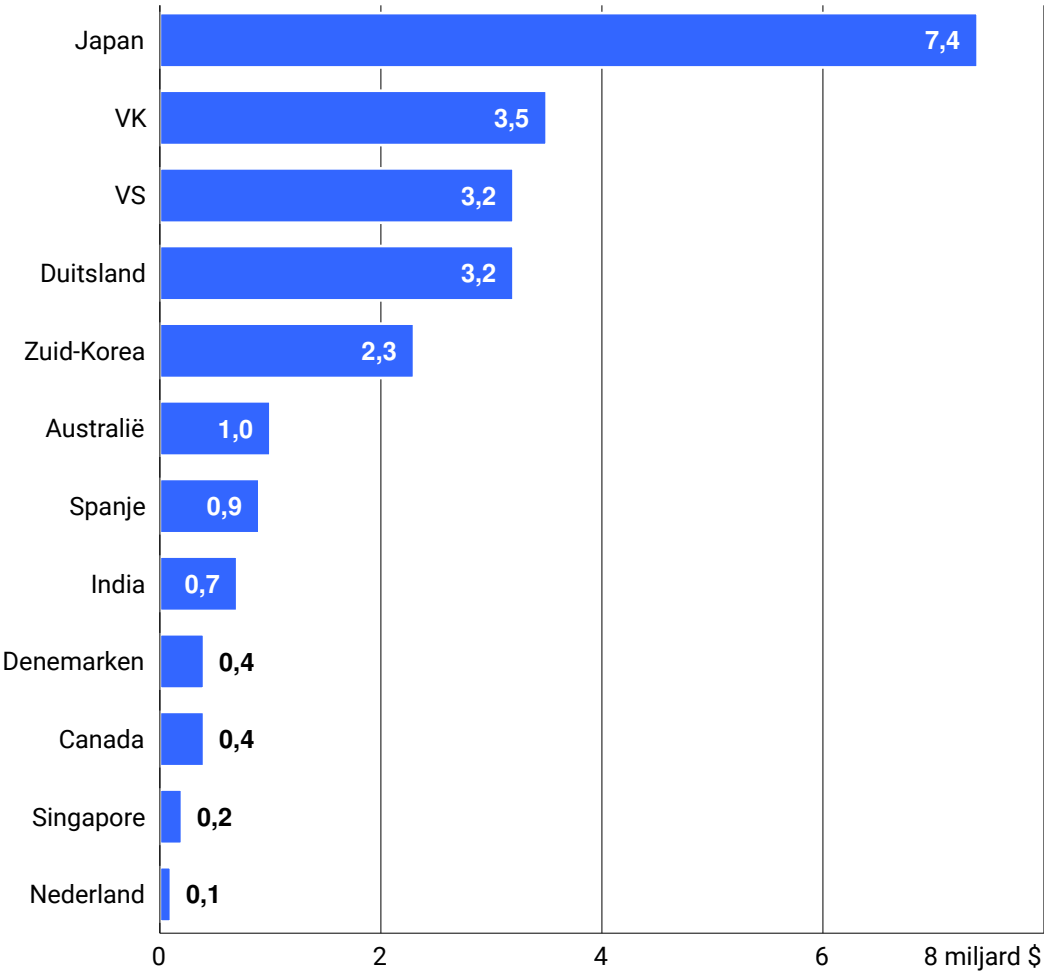
3.6 Uitdagingen voor de toekomst

Het quantumecosysteem van Nederland is de afgelopen jaren gegroeid. De belangrijkste uitdaging is om de koploperpositie die Nederland in de afgelopen jaren heeft opgebouwd te behouden. Hoewel het Nederlandse quantumecosysteem is gegroeid en internationaal bekend is, groeit het in andere landen harder (Birch, 2024).

Daar waar Nederland tot 2022 opviel vanwege de aanzienlijke publieke investeringen, investeren andere landen vanaf 2023 aanzienlijk meer (McKinsey, 2025). Zo kondigde Japan recent aan 1 biljoen yen (€ 6 miljard) in quantumtechnologie te investeren (Quantum Insider, 2025). De zorg bestaat dat Nederland langzaam wordt ingehaald door andere landen en we onze leidende positie kwijtraken.

Figuur 6 *Overzicht aangekondigde publieke investeringen in quantumtechnologie tussen 2023 en 2025*

Nederland investeert relatief weinig publiek geld in quantumtechnologie



Bron: McKinsey (2025)

Ook private partijen kunnen investeren. Experts geven aan dat het ecosysteem in Nederland meer prioriteit moet geven aan het vinden van private investeringen en eindgebruikers van de ontwikkelde quantumtechnologie. Quantum Delta NL geeft aan dat het een uitdaging is om bedrijven te vinden die bereid zijn om gezamenlijk te investeren in Nederland. Daarom gaat het programma in de laatste fase van het project hier extra aan werken.

Enkele gesprekspartners gaven aan dat het aflopen van de financiering voor Quantum Delta NL een grote uitdaging zal zijn voor het ecosysteem in Nederland. Het Nederlandse ecosysteem is nog niet volwassen en moet kapitaal aantrekken. Experts die wij spraken benadrukken het belang van een betrouwbare langetermijnvisie. Dit vereist stabiliteit en vertrouwen dat quantumtechnologie in de toekomst blijft ontwikkelen, onafhankelijk van een wisseling van de samenstelling van het kabinet. Het risico bestaat dat bedrijven anders naar het buitenland vertrekken.

De Europese Commissie gaat ook de komende jaren veel investeren in quantumtechnologie. Onze gesprekspartners geven echter aan dat Europese budgetten geen vervanging kunnen zijn voor nationale investeringen. Europese samenwerking vereist namelijk nationale cofinanciering. Daar moeten ook middelen voor beschikbaar zijn in de toekomst. Bijvoorbeeld, QCINed is een EU programma wat cofinanciering vanuit Quantum Delta NL gebruikt om de Europese financiering te ontvangen.

De minister van EZ ziet dat de stimulering van quantumtechnologie nog niet af is. Er zijn momenteel echter geen mogelijkheden voor vervolgfinanciering via een nieuw groeifonds, blijkt uit de gesprekken die wij voerden. Een geïnterviewde verwoordde het als volgt: "*In 2028 zouden de doelen van het programma behaald moeten zijn en het ecosysteem meer volwassen zijn geworden. De vraag of en op welke wijze er daarna nieuwe financiering nodig is, hangt af van een goede analyse en onderbouwing van wat het ecosysteem dan nodig heeft. Dan kan een nieuw groeifonds allicht een rol spelen, maar er moet ook gekeken worden naar andere vormen van financiering*". De minister van EZ geeft wel aan dat het logisch zou zijn als Nederland de stimulering op een of andere manier zou voortzetten.

4. Kansen voor de rijksoverheid

Quantumtechnologie biedt ook kansen voor de rijksoverheid. De verkenningen naar de mogelijkheden van quantum bij de rijksoverheid staan in de kinderschoenen. Er is interesse voor de techniek en het belang voor de economische veiligheid. Toch geven de meeste onderzochte rijksoverheidsorganisaties aan dat zij niet hebben verkend welke kansen quantumtechnologie kan bieden. Dat komt bijvoorbeeld door gebrek aan concrete ideeën voor taken die quantumtechnologie beter kan uitvoeren dan de huidige systemen.
Mocht quantumtechnologie in de toekomst doorbreken, dan zijn er ook andere obstakels die het realiseren van de kansen beperken. Zo blijft het ingewikkeld om geschikte toepassingen van quantumtechnologie binnen de rijksoverheid te vinden. De hoge aanschaf- en onderhoudskosten van nieuwe quantumtechnologie kunnen het gebruik ervan belemmeren. Nieuwe quantumtechnologie moet bovendien passen binnen de huidige technische infrastructuur, zodat niet alles vervangen hoeft te worden.

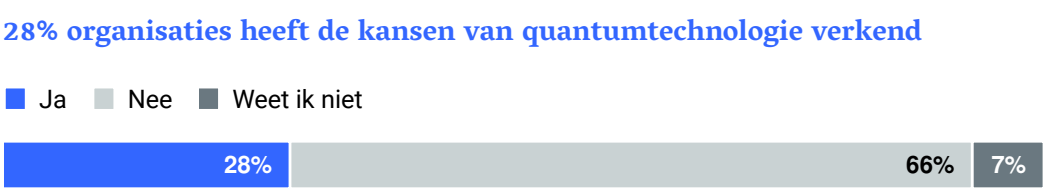
4.1 Experimenteren met quantum bij de rijksoverheid

Ook bij de rijksoverheid zijn er in de toekomst mogelijkheden om quantumtechnologie in te zetten. Deze liggen vooral bij de quantumsensoren. Die bieden bijvoorbeeld mogelijkheden om zonder gps te navigeren en onderzeeboten beter op te sporen (European Parliamentary Research Service, 2024). Dit is met name relevant voor militaire toepassingen. Het ministerie van Defensie heeft al getest met een rugzak met quantumsensoren die wapens op afstand beter kunnen detecteren en kwalificeren (Ministerie van Defensie, 2023). Sensoren kunnen ook een rol spelen bij

het verbeteren van het meten van de waterkwaliteit, vervuiling en fijnstof in de lucht, recycling van plastic en het verkeer.

We hebben de rijksoverheidsorganisaties in dit onderzoek gevraagd of ze kansen zien om quantumtechnologie in te zetten. Zij tonen interesse in de mogelijkheden van quantumtechnologie voor de dienstverlening. Toch geeft meer dan 60% (38) van de onderzochte organisaties aan dat zij niet hebben verkend welke kansen quantum-technologie kan bieden (zie figuur 7). Hiervoor geven zij verschillende verklaringen. Sommigen hebben een dergelijke verkenning nog niet gedaan, omdat zij prioriteit geven aan de dreigingskant van quantumtechnologie. Anderen hebben de kansen nog niet verkend omdat "*er geen voor de hand liggende use case is voor de werkzaamheden*". Deze organisaties zien dus nog weinig aanknopingspunten voor gebruik van de nieuwe technologie voor hun werkzaamheden.

Figuur 7 *Percentage ondervraagde organisaties dat de kansen van quantum-technologie heeft verkend*



Een kwart van de organisaties (16) heeft de kansen van quantumtechnologie wel verkend of is hiermee bezig. Een deel van wat is verkend, is in openbare rapporten gepubliceerd. Bijvoorbeeld de verkenning van het ministerie van Infrastructuur en Waterstaat *Van Bits naar Qubits* (mei 2025). In dit rapport staan potentiële toekomstige toepassingen bij een aantal organisaties binnen het ministerie.

Ook een eerste verkenning van quantumtechnologie bij het ministerie van Financiën door Quantum Delta (Quantum Delta NL, 2023b) is gepubliceerd. De Auditdienst Rijk heeft verkend of de interne jaarlijkse personeelsplanning verbeterd kan worden: het matchen van medewerkers en projecten. Daarnaast is getest of met behulp van quantumtechnologie afwijkingen in jaarverslagen kunnen worden opgespoord. Het ministerie ziet dat het kansen biedt, alhoewel het moet aansluiten op een specifiek probleem: "*Ontdekt is dat quantumtechnologie voordelen kan bieden, maar dat lang niet alles ermee verbeterd wordt*". Dit is reden voor het ministerie om de ontwikkelingen van quantumtechnologie te blijven volgen.

Meerdere organisaties gaven aan interesse te hebben voor de toepassing van quantumcommunicatie, zeker voor verbindingen die een hoog niveau van beveiliging

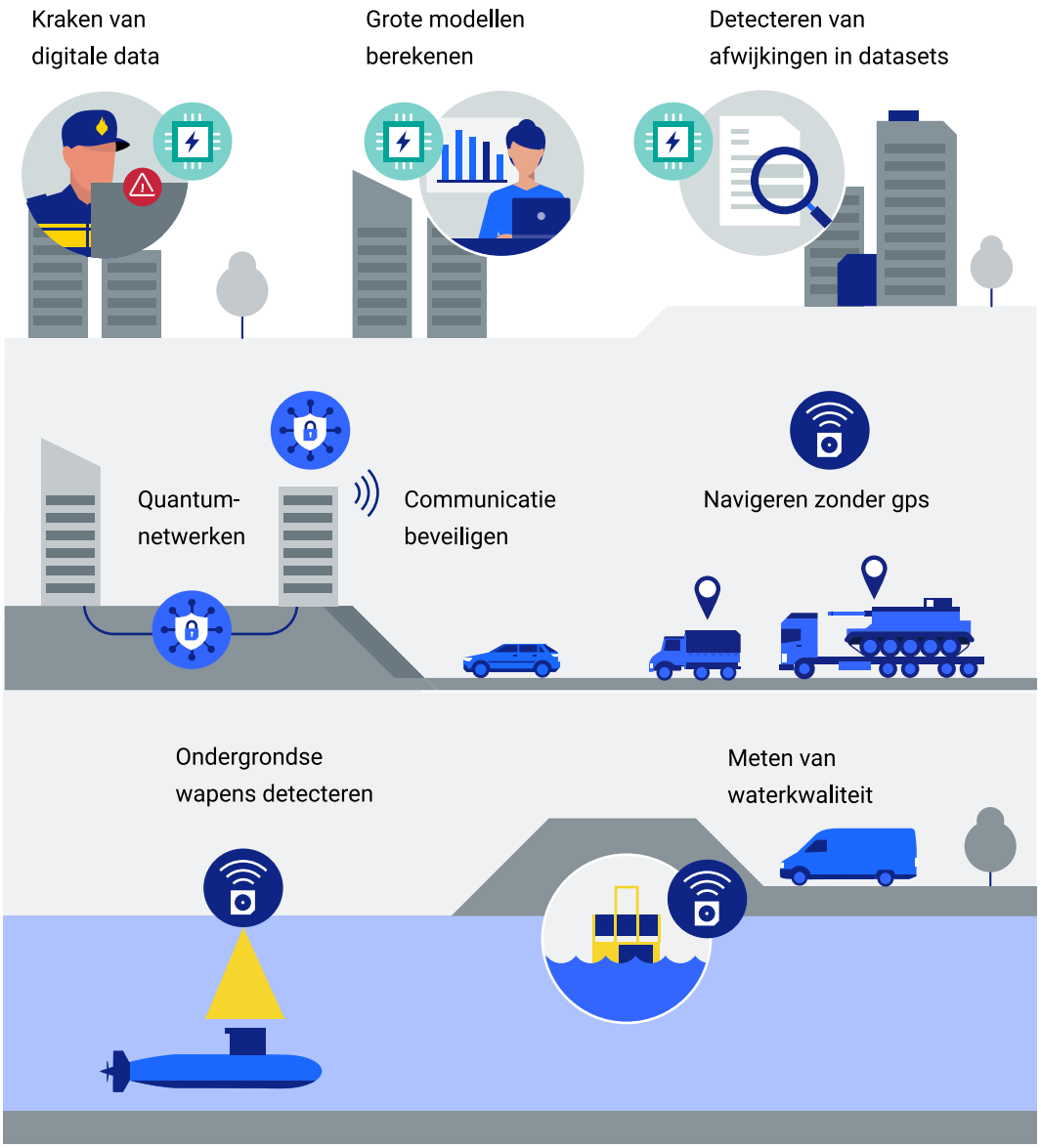
vereisen. In Nederland is al getest met *Quantum Key Distribution* (QKD) in verschillende pilotprojecten, zoals in een quantumnetwerk van de ministeries van Buitenlandse Zaken en Justitie en Veiligheid (Rijksoverheid, 2025). Dit is een proefopstelling waarin het gebruik van deze quantumbeveiligde communicatie-methode is getest.

Enkele organisaties noemden ook de mogelijkheid van quantumcomputers om huidige beperkingen met computerrekenkracht in de toekomst te overbruggen. Zij geven echter aan dat de meeste toepassingen met quantumcomputers alleen relevant zijn voor heel specifieke problemen. Niet elke overheidsorganisatie heeft daarmee te maken. Vooralsnog gaat het met name om militaire toepassingen of zeer complexe berekeningen, zoals grote modellen met heel veel variabelen of het veiligstellen van data van criminelen om deze later te kunnen ontsleutelen.

De verkenningen hebben nu nog nauwelijks geresulteerd in iets concreets of implementatie van de technologie. Rijksoverheidsorganisaties geven aan dat de technologie nog verder moet ontwikkelen: "*Tot nu toe is de conclusie dat het wat vroeg is om use cases voor de kansen van quantumtechnologie concreet vorm te geven*". Een andere organisatie geeft aan dat toekomstige ontwikkelingen eerder gedane verkenningen in een ander licht kunnen zetten. Wanneer ontwikkelingen doorbreken, zal de verkenning opnieuw geëvalueerd moeten worden.

Figuur 8 *Overzicht van verschillende mogelijke toepassingen van quantumtechnologie*

Quantumtechnologie biedt veel kansen voor de rijksoverheid



4.2 Beleid voor het gebruik van quantumtechnologie

De staatssecretaris Digitalisering gaf begin 2025 aan dat quantumtechnologie de overheid fundamenteel kan veranderen (Tweede Kamer, 2025). Op termijn zou het kansen bieden voor een betere, veiligere en snellere digitale dienstverlening. Uit ons onderzoek blijkt dat de verkenningen naar mogelijke kansen voor overheids-organisaties met name uit eigen initiatief van de organisaties zelf komt.

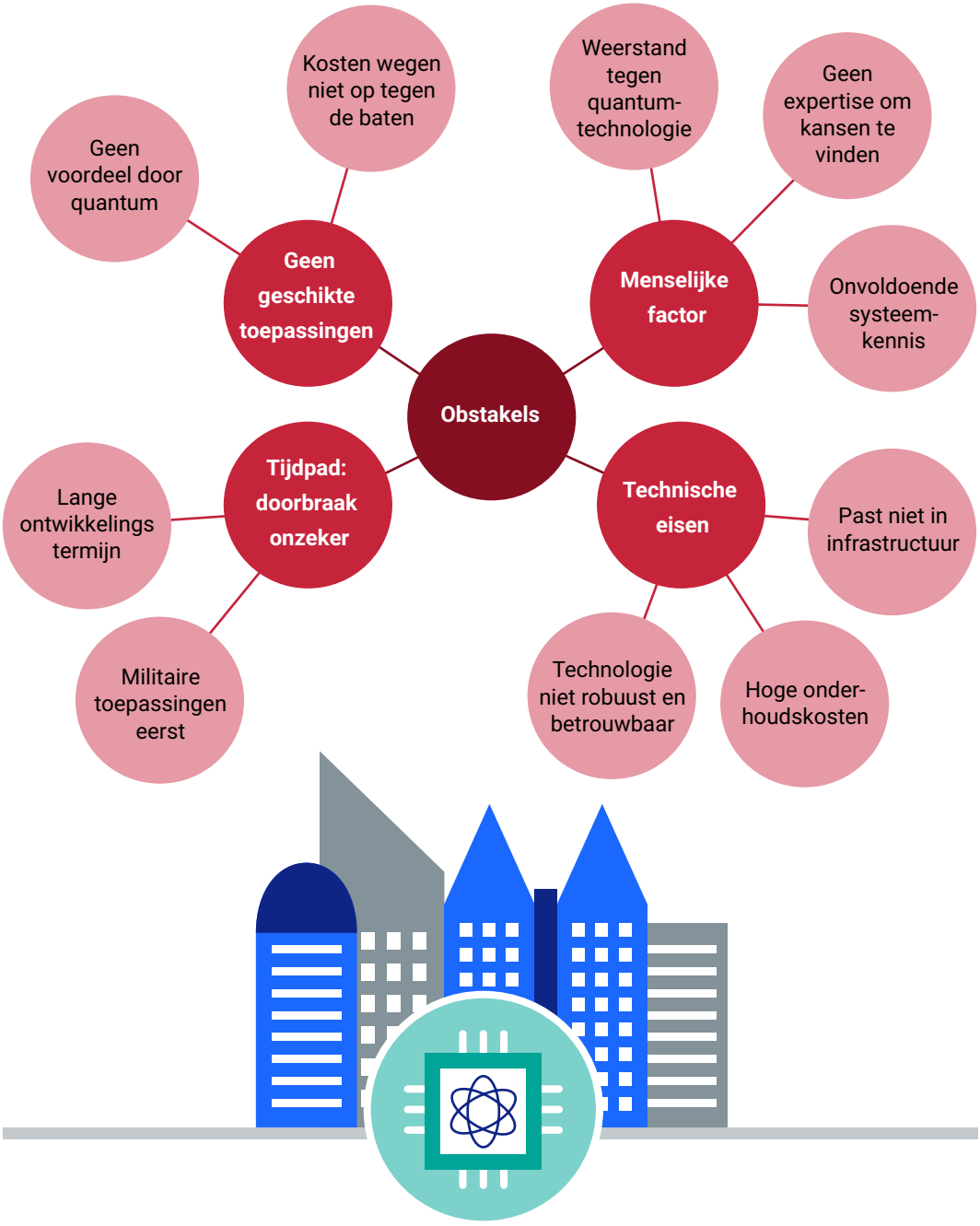
Momenteel werkt het ministerie van EZ samen met alle andere ministeries aan het opstellen van een rijksbrede Quantum Strategie voor de rijksoverheid. Deze aankomende strategie onderstreept het strategische belang van quantumtechnologie en zal doelen en acties bevatten om zowel de kansen als risico's van quantumtechnologie te adresseren. Het is onbekend in hoeverre de strategie activiteiten bevat om quantumtechnologie binnen de rijksoverheid te stimuleren. Wij constateren dat er momenteel nog geen budget is gereserveerd om de strategie uit te voeren. Wel is bekend dat er financiële bijdrages nodig zullen zijn om de strategie uit te voeren.

4.3 Obstakels om quantumtechnologie in te zetten

Ondanks de interesse, vooruitgang en mogelijkheden, gaat quantumtechnologie niet vanzelfsprekend kansen bieden. Meerdere experts die wij spraken waarschuwden dan ook voor de hype en de gedachtegang dat quantumtechnologie alle problemen gaat oplossen. In ons onderzoek hebben we ook gevraagd welke obstakels het realiseren van de kansen van quantumtechnologie voor de rijksoverheidsorganisaties belemmeren, ook wanneer de technologie verder ontwikkeld is. De onderzochte organisaties geven in de gesprekken verschillende factoren aan die een rol spelen.

Figuur 9 *Belemmeringen in het toepassen van quantumtechnologie*

Niet alleen techniek vormt een obstakel voor quantumtechnologie



Allereerst is er het tijdpad. Het blijft namelijk altijd mogelijk dat, ondanks de inspanningen, de techniek zich niet of wellicht langzamer dan verwacht verder ontwikkelt. Een tweede, gerelateerd obstakel is het vinden van passende *use cases* voor quantumtechnologie, met name binnen de rijksoverheid. Ook is kennis nodig om goede toepassingen te vinden. Zo bleek uit een antwoord op onze vragenlijst: "*Quantumcomputing is berucht complex om te begrijpen. Er zijn maar weinig mensen*

met de theoretische achtergrond om serieus te kunnen doorgronden waar quantum een kans zou kunnen bieden". Bovendien vereist het vinden van kansen volgens sommige gesprekspartners veel kennis van huidige systemen en gebruikte (wiskundige) technieken.

Als er een goede toepassing wordt gevonden, dan moeten de kosten voor de inzet van de quantumtechnologie passend zijn en opwegen tegen de baten. Daarnaast moet de quantumtechnologie ook voldoen aan de technische eisen van de overheid: betrouwbaar, robuust, getest in het veld. Andere voorwaarden zijn: weinig onderhoudskosten en passend bij de huidige infrastructuur.

Tot slot kunnen bij toekomstig gebruik van quantumtechnologie ook uitdagingen ontstaan bij de verantwoording. Quantumtechnologie is bijzonder complex en berekeningen met een quantumcomputer zullen steeds andere uitkomsten geven. Hoe kan de overheid dat in de toekomst goed verantwoorden?

5. De dreiging van quantumcomputers voor het Rijk

De grootste dreiging van quantumtechnologie voor het Rijk is dat quantum-computers in de toekomst een zeer veel voorkomende versleutelingstechniek kunnen kraken, als overheidsorganisaties hun versleuteling niet op tijd vervangen. Statelijke actoren of andere kwaadwillenden kunnen daarmee toegang krijgen tot gevoelige gegevens en vitale infrastructuren aanvallen. Uit ons onderzoek blijkt dat de meeste ondervraagde overheidsorganisaties werken aan hun informatie-beveiliging. Zo zijn veel organisaties bezig met het inventariseren van hun processen, systemen en leveranciers. Aanzienlijk minder organisaties hebben echter maat-regelen getroffen die specifiek gericht zijn op de dreiging van quantumcomputers. Ze hebben nog geen gesprekken gevoerd met leveranciers over quantumveilige producten en nog geen plannen gemaakt voor het invoeren van quantumveilige cryptografie. Ook hebben ze de quantumdreiging niet opgenomen in hun risico-managementprocessen en hebben ze geen bestuurlijk verantwoordelijken aangewezen voor de migratie. 71% van de organisaties geeft aan nog niet begonnen te zijn met hun aanpak van de quantumdreiging. De belangrijkste obstakels voor organisaties bij de aanpak zijn een gebrek aan capaciteit en expertise, en andere activiteiten die meer prioriteit hebben.

5.1 Quantumcomputers kunnen cryptografie kraken

Quantumcomputers vormen de grootste dreiging voor het Rijk. Quantumcomputers werken op een andere manier dan normale computers. Daardoor kunnen ze in de toekomst waarschijnlijk onze huidige cryptografie kraken. Iets waar huidige computers 300 biljoen jaar over zouden doen (OECD, 2025). De rijksoverheid gebruikt cryptografie voor allerlei toepassingen. Bijvoorbeeld voor:

- het beschermen van vertrouwelijke informatie van burgers en bedrijven;
- het regelen van toegang tot vitale infrastructuur zoals waterkeringen en bruggen;
- het inloggen met DigiD;
- het waarborgen van de authenticiteit van paspoorten.

Als de cryptografie gekraakt kan worden, lopen al deze toepassingen gevaar.

Wat is cryptografie?

Cryptografie is een techniek om informatie te beveiligen door die te versleutelen. Alleen iemand met de bijbehorende sleutel kan de informatie weer lezen of bewerken. Zo blijven berichten, persoonsgegevens en andere vertrouwelijke informatie beschermd. Omdat je weet wie de sleutel bezit, kun je cryptografie ook gebruiken om iemands identiteit te bevestigen. Dit is onmisbaar voor toepassingen zoals DigiD en het veilig beheren van toegang tot vitale infrastructuur.

Het kraken van de cryptografie van het Rijk kan de maatschappij ontwrichten. Statelijke actoren kunnen onze sluizen openzetten of gegevens op onze paspoorten zijn niet meer te vertrouwen. Aanvallen van quantumcomputers kunnen gegevens-uitwisselingen tussen overheidsorganisaties manipuleren. Als de overheid de gegevens van burgers niet meer voldoende kan beschermen, raken burgers hun vertrouwen in de overheid kwijt. De dreiging van quantumcomputers zal vooral vanuit statelijke actoren komen, omdat quantumcomputers erg duur zijn en alleen in zeer gecontroleerde omgevingen werken.

Figuur 10 D*e belangrijkste risico's van quantumcomputers voor de rijksoverheid*

Quantumcomputers bedreigen de vertrouwelijke informatie en vitale infrastructuur van het Rijk

Op dit moment zijn quantumcomputers nog niet krachtig genoeg om cryptografie te kraken. Hoe sterk een quantumcomputer is, wordt gemeten in zogenaamde *qubits*. Qubits zijn de bouwstenen van quantumcomputers. Hoe meer qubits, hoe meer informatie een quantumcomputer kan verwerken en dus hoe krachtiger die computer is. Wetenschappers schatten in dat een quantumcomputer 1.024 tot 3.072 qubits[3] moet hebben om de meest voorkomende cryptografietechniek te kunnen kraken.

De grootste quantumcomputers hebben op dit moment minder dan 200 qubits (Gidney, 2025). Het moment waarop quantumcomputers sterk genoeg zijn om cryptografie te kraken wordt *Q-day* genoemd. Expertmeningen lopen uiteen over of en wanneer Q-day komt.

Experts schatten in dat de eerste quantumcomputers ongeveer 7 dagen nodig zullen hebben om een sleutel te kraken. Krachtigere quantumcomputers met duizenden qubits zouden het ook binnen 8 uur kunnen (Gidney, 2025). Voor de dreiging maakt het uit of een quantumcomputer een cryptografiesleutel kan kraken in 1 minuut of in 7 dagen. In het eerste geval kunnen quantumcomputers op grote schaal vertrouwelijke informatie openbaren, terwijl aanvallen in het tweede geval waarschijnlijk gerichter zullen zijn.

Het is dus onzeker wanneer er een krachtige quantumcomputer is en wat die kan. Experts zijn het er echter over eens dat (overheids)organisaties zich nu al moeten voorbereiden op de dreiging van quantumcomputers. Experts van onder andere de Algemene Inlichtingen- en Veiligheidsdienst (AIVD), het Nationaal Cyber Security Centrum (NCSC) en de Europese Commissie geven daar 3 redenen voor:

1. Het kunnen kraken van cryptografie heeft grote gevolgen voor de (nationale) veiligheid.
2. Het beperken van de quantumdreiging is een grote opgave voor organisaties, die meerdere jaren zal duren.
3. Organisaties lopen nu al gevaar via *store-now-decrypt-later*-aanvallen. Dit houdt in dat vijandige actoren nu al versleutelde informatie stelen, die ze in de toekomst kunnen kraken, wanneer er een geschikte quantumcomputer is.

5.2 Organisaties moeten hun cryptografie vervangen

De dreiging van quantumcomputers betekent dat overheidsorganisaties nieuwe beveiligingstechnieken moeten gebruiken die bestand zijn tegen zulke aanvallen. Een belangrijke oplossing hiervoor is *post-quantum cryptografie* (PQC). Dit is een nieuwe vorm van cryptografie die niet gekraakt kan worden door quantumcomputers. Door bestaande cryptografie te vervangen door PQC, kunnen organisaties zich dus beschermen tegen de quantumdreiging.

In de toekomst kan *quantum key distribution* (QKD) mogelijk ook een rol spelen bij het tegengaan van de dreigingen. QKD is een techniek om cryptografische sleutels op een veiligere manier uit te wisselen (zie paragraaf 3.1.2). De AIVD en de Europese Commissie stellen echter dat QKD vanwege *"intrinsieke beperkingen [...] alleen in een*

aantal specifieke niche gevallen gebruikt [kan] worden" (AIVD et al. ,2024). Om te garanderen dat alle informatie en processen veilig zijn, moet PQC volgens hen prioriteit krijgen. De rest van dit hoofdstuk richt zich daarom op PQC en het werk van de rijksoverheid om bestaande cryptografie te vervangen door quantumveilige alternatieven.

5.2.1 PQC-migratiestappen

In hun PQC-migratiehandboek wijzen de AIVD, TNO en het Centrum Wiskunde & Informatica (CWI) erop dat een migratie naar PQC tijdrovend en complex is (AIVD et al., 2024). Organisaties moeten hun cryptografie zorgvuldig in kaart brengen, beleid ontwikkelen voor het beheer ervan en afspraken maken met leveranciers over quantumveilige producten. In de volgende paragrafen lichten we de belangrijkste stappen van de PQC-migratie toe. We beschrijven per stap hoe rijksoverheids-organisaties dit invullen. Deze stappen zijn gebaseerd op adviezen van QvC NL (Digitale Overheid, 2025), de AIVD (AIVD et al., 2024), het NCSC (Nationaal Cyber Security Centrum, 2023) en de Europese Commissie (Europese Commissie, 2025e). Een deel van deze stappen is sowieso belangrijk voor informatiebeveiliging, niet alleen als voorbereiding op de quantumdreiging.

Quantumrisico's analyseren

Organisaties moeten hun migratie beginnen met een risicoafweging. Quantum-computers zijn een zeer serieuze informatiebeveiligingsdreiging, maar organisaties staan ook voor andere urgente beveiligingsuitdagingen, zoals cyberaanvallen of datalekken. Alles tegelijk aanpakken is onmogelijk. Om hun belangrijkste informatie en processen te beschermen, moeten organisaties dus scherpe keuzes maken over waar zij hun middelen en aandacht op richten. Dat kan alleen als ze begrijpen hoe quantumcomputers hun systemen bedreigen en als ze deze risico's afwegen tegen andere prioriteiten. Daarom is het essentieel dat organisaties de dreiging van quantumcomputers meenemen in hun risicomanagement.

Cryptografie inventariseren

Organisaties kunnen hun cryptografie pas vervangen door PQC als ze weten welke cryptografie ze in huis hebben. Het inventariseren van cryptografie is complex, omdat een enkel ICT-systeem al snel tientallen cryptografische onderdelen bevat. Bovendien weten organisaties vaak niet precies welke ICT-producten ze gebruiken, omdat een deel van die producten bijvoorbeeld onderdeel uitmaakt van andere ICT-producten. Een inventarisatie van cryptografie vereist dus ook een inventarisatie van informatiesystemen en ICT-producten.

Afspraken maken met leveranciers

Een deel van de cryptografie van organisaties zit in producten van externe leveranciers. Om dat deel te migreren naar PQC zullen rijksoverheidsorganisaties afspraken moeten maken met leveranciers over het leveren van producten met quantumveilige cryptografie. Leveranciers moeten hun bestaande producten aanpassen. Gebeurt dat niet, dan moeten overheidsorganisaties op zoek naar nieuwe leveranciers die wel quantumveilige producten leveren.

Cryptografiebeleid opstellen

Organisaties moeten cryptografiebeleid hebben, zodat ze tijdens en na de PQC-migratie grip blijven houden op hun cryptografie. Cryptografiebeleid:

- legt onder andere de rollen en verantwoordelijkheden voor cryptografie vast;
- biedt richtlijnen voor het gebruik van cryptografie;
- beschrijft relevante wet- en regelgeving (AIVD et al., 2024).

Rijksoverheidsorganisaties zijn volgens de Baseline Informatiebeveiliging Overheid (BIO) al verplicht om een cryptografiebeleid te hebben (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2025b).

Migratie aansturen

Om de complexe PQC-migratie in goede banen te leiden en op tijd af te krijgen, zullen organisaties de aansturing van de migratie goed moeten inrichten. Dat houdt bijvoorbeeld in dat organisaties een bestuurlijk verantwoordelijke moeten aanwijzen voor de migratie, een tijdslijn moeten opstellen en voldoende capaciteit en middelen moeten vrijmaken.

Cryptografie vervangen

De laatste stap van de PQC-migratie is het daadwerkelijk vervangen van cryptografie door quantumveilige PQC. Organisaties zullen hun cryptografie beetje bij beetje vervangen, beginnend bij de processen en cryptografie die het meest risico lopen. Nu zijn er nog nauwelijks quantumveilige producten beschikbaar. Dat komt doordat er pas net geaccepteerde PQC-technieken zijn. Het kost tijd voordat ontwikkelaars en leveranciers die technieken hebben verwerkt in producten.

5.2.2 Wettelijke verplichtingen voor de PQC-migratie

Verschillende wetten en regels stellen eisen aan cryptografie voor overheids-organisaties. Zo heeft de overheid zich verplicht de Baseline Informatiebeveiliging Overheid (BIO) te implementeren. Daarin staan beheersmaatregelen zoals het opstellen van beleid over het gebruik van cryptografische beheersmaatregelen en sleutelbeheer (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2019).

Ook in de NIS2-richtlijn (Nationaal Cyber Security Centrum, (z.d.b) staan uitgebreidere eisen aan cryptografie. Deze richtlijn geldt al en wordt in Nederland in 2026 omgezet in nationale wetgeving. De NIS2 schrijft voor om '*state of the art encryption*" toe te passen. Er staat niet expliciet dat dit PQC moet zijn.

5.3 Hoe bevordert het Rijk dat de risico's van quantum worden beheerst?

De PQC-migratie is een grote opgave voor alle rijksoverheidsorganisaties.
De staatssecretaris Digitalisering heeft een coördinerende rol op het gebied van digitalisering van de Nederlandse overheid. Hij heeft begin 2025 gesteld dat als quantumtechnologie door kwaadwillenden wordt gebruikt, dit de nationale veiligheid in gevaar kan brengen. Daarom stimuleert het ministerie van BZK de migratie naar PQC door middel van het programma Quantumveilige cryptografie NL (QvC NL).[4]
Bij de lancering van de Nederlandse Cybersecurity Strategie (2022) heeft de minister van BZK geld beschikbaar gesteld voor digitale weerbaarheid, daar wordt ook QVC NL uit gefinancierd. Er gaat geen geld uit het Nationaal Groeifonds naar de beheersing van de risico's van quantumtechnologie.

5.3.1 Quantumveilige Cryptografie NL

In 2023 heeft de staatssecretaris Digitalisering het programma QvC NL ingericht om de rijksoverheid te helpen om de risico's van quantumcomputers voor cryptografie op tijd te beheersen. Het programma is bedoeld om (overheids)organisaties te steunen bij hun migratie naar PQC. QvC NL heeft geen kaderstellende rol als het gaat om de migratie naar PQC binnen de rijksoverheid. Ministeries en daarmee verbonden organisaties zijn zelf aan zet om te bepalen wanneer en hoe ze de PQC-migratie in gang zetten.

Tot nu toe richtte QvC NL zich vooral op bewustwording, onder meer via workshops en presentaties op conferenties. Daarnaast stelde QvC NL een rijksbreed beleidskader cryptografie op (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2025b) en liet het onderzoek doen naar tools voor het inventariseren van cryptografie (TNO, 2025). Op dit moment werkt QvC NL aan een expertisehub waar experts en organisaties kennis kunnen uitwisselen.

5.3.2 De Nederlandse Digitaliseringsstrategie

Het kabinet stimuleert de risicobeheersing van quantumtechnologie daarnaast ook via de in juli 2025 gepresenteerde Nederlandse Digitaliseringsstrategie (NDS).

Hiermee wil de minister van BZK de PQC-migratie sterker bevorderen en de noodzaak ervan verankeren in beleid. Een van de strategische doelen van de NDS is een overheidsbrede aanpak van quantumveilige cryptografie. Dit is nog niet verder uitgewerkt. In de begroting 2026 van het ministerie van BZK staat dat een hub wordt gerealiseerd voor overheidsbrede samenwerking op het gebied van quantumveilige cryptografie (Tweede Kamer, 2025b). Hoe de hub zich verhoudt tot QvC NL is nog niet bekendgemaakt.

5.3.3 Acties van Europa: de routekaart

Ook de Europese Commissie ziet het belang in van migratie naar en voorbereidingen op PQC binnen alle sectoren. Medio 2025 hebben de EU-lidstaten samen met de Europese Commissie een routekaart gepubliceerd (Europese Commissie, 2025e). Deze routekaart beschrijft een gecoördineerde migratie naar PQC. De routekaart is gericht aan alle EU-lidstaten en bevat aanbevelingen voor een gelijktijdige migratie naar PQC. QvC NL coördineert de Nederlandse reactie op de routekaart.

De Europese Commissie stelt ook dat migraties lastig zullen zijn om uit te voeren en lang zullen duren. Niet alle lidstaten zijn al even ver gevorderd of herkennen de risico's als dringend.

5.4 De PQC-migratie van rijksoverheidsorganisaties

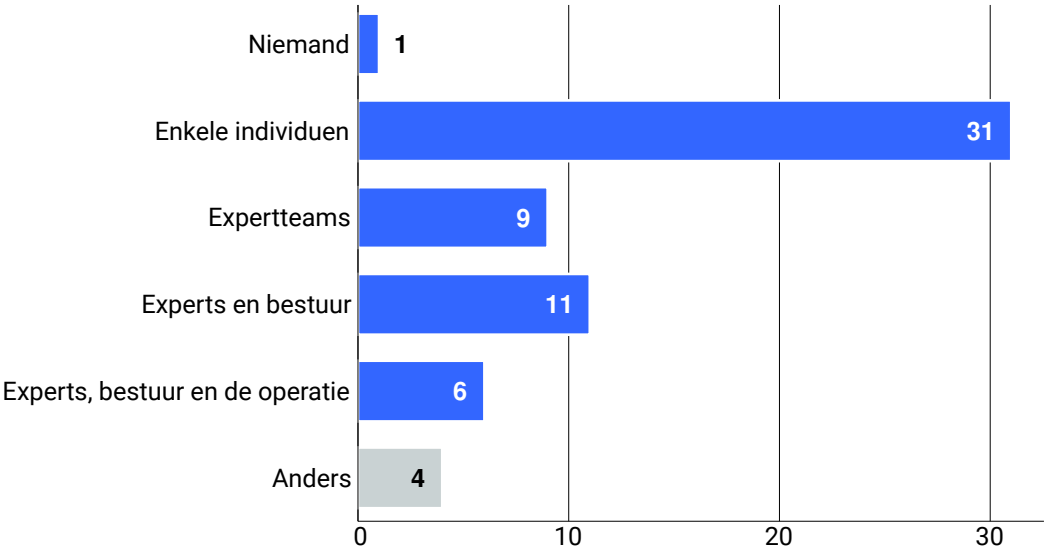
Om een beeld te krijgen van hoe ver de rijksoverheid is in de voorbereidingen voor bescherming tegen de dreiging van quantumcomputers, hebben we een vragenlijst uitgestuurd naar 63 organisaties. Deze organisaties zijn opgenomen in bijlage 2. Wij hebben organisaties geselecteerd die volgens ons persoonlijke of vertrouwelijke informatie verwerken of vitale infrastructuur leveren. Het PQC-migratiehandboek bestempelt dit soort organisaties namelijk als *urgent adopters*: organisaties die mogelijk een doelwit zijn voor aanvallen met quantumcomputers en dus zo snel mogelijk maatregelen moeten nemen tegen deze dreiging.[5]

5.4.1 Aandacht voor quantumdreiging

QvC NL richt zich op het vergroten van het bewustzijn bij organisaties over de dreiging van quantumcomputers. Vrijwel alle organisaties in ons onderzoek zijn hiermee bekend. Slechts 1 overheidsorganisatie geeft aan dat niemand binnen de organisatie bekend is met de dreiging (zie figuur 11). Bij meer dan de helft van de organisaties blijft het bewustzijn echter beperkt tot enkele individuen of expertteams.

Figuur 11 *Bekendheid met de quantumdreiging bij de ondervraagde organisaties*

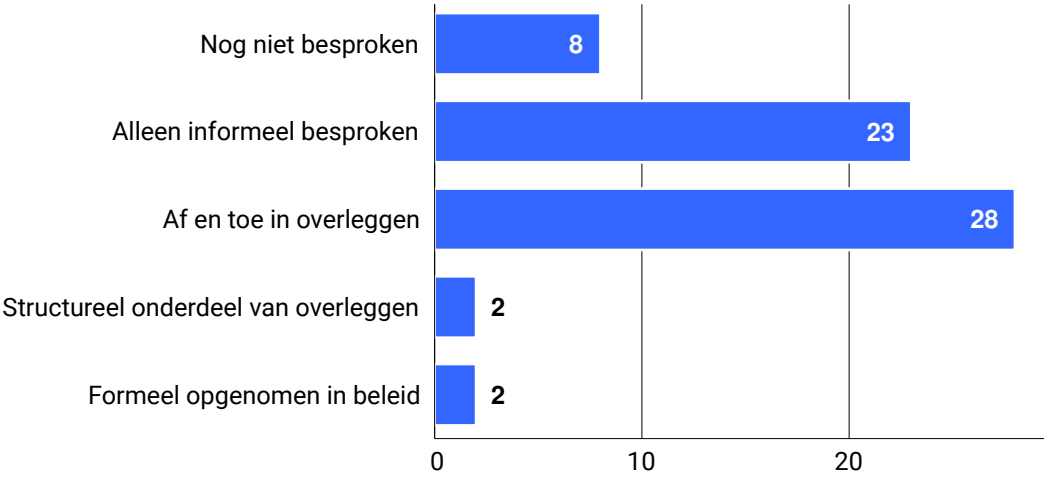
Bekendheid met quantumdreiging beperkt zich tot individuen



Ook de manier waarop organisaties de dreiging bespreken, laat zien dat structurele aandacht ontbreekt. Bij de meeste organisaties wordt de dreiging van quantum-computers uitsluitend informeel besproken of komt de dreiging alleen af en toe terug in relevante overleggen (zie figuur 12). Slechts 4 van de ondervraagde organisaties besteden structureel aandacht aan de dreiging van quantumcomputers of hebben dit formeel opgenomen in intern beleid of strategieën.

Figuur 12 *Aandacht voor de quantumdreiging binnen de ondervraagde organisaties*

Weinig organisaties besteden structureel aandacht aan de quantumdreiging



Bij bijna alle organisaties is dus wel iemand bekend met de quantumdreiging. Maar bij veel organisaties ontbreekt bestuurlijke of organisatiebrede aandacht voor het onderwerp. QvC NL benadrukt dat de dreiging breder moet gaan leven binnen organisaties, omdat de overstap naar quantumveilige cryptografie alle onderdelen van een organisatie raakt: van informatievoorziening tot inkoop en van bestuur tot uitvoering. De uitdaging is daarom niet om meer organisaties te bereiken, maar om de kennis binnen organisaties breder te verspreiden.

5.4.2 Voorbereidingen van rijksoverheidsorganisaties

We hebben in het onderzoek ook gekeken of organisaties al begonnen zijn met hun voorbereidingen op de dreiging van quantumcomputers. Van de 63 organisaties zijn 18 (29%) gestart met hun aanpak van de quantumdreiging (zie figuur 13). De andere 45 organisaties (71%) zijn nog niet begonnen met gerichte voorbereidingen. Daarvan weten 33 (52%) überhaupt nog niet of en wanneer ze zullen beginnen.

Figuur 13 *Percentage ondervraagde organisaties dat is gestart met hun aanpak van quantumdreiging*

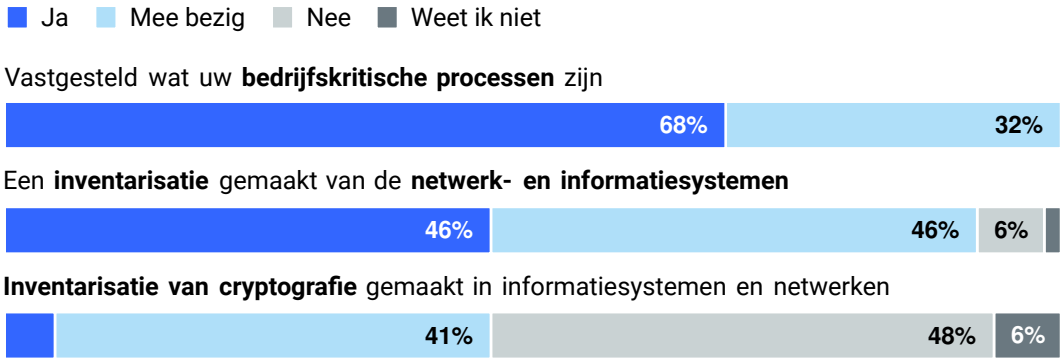
Om te weten hoe ver organisaties zijn met hun voorbereidingen, hebben we ook gevraagd naar de PQC-migratiestappen uit paragraaf 5.2.1. Migratiestappen zoals het inventariseren van cryptografie en het opstellen van cryptografiebeleid zijn niet alleen relevant voor de quantumdreiging. Organisaties kunnen deze algemene stappen dus al hebben gezet, zonder expliciet te zijn begonnen met voorbereidingen op de quantumdreiging.

Cryptografie inventariseren

Een van de belangrijke dingen waar organisaties mee moeten beginnen, is het inventariseren van hun kritieke processen, ICT-systemen en cryptografie. Organisaties moeten weten wat ze in huis hebben om uiteindelijk hun cryptografie om te kunnen zetten naar quantumveilige cryptografie.

Figuur 14 *Percentage ondervraagde organisaties dat inventarisaties heeft afgerond*

52% organisaties is niet klaar met het inventariseren van hun netwerk- en informatiesystemen



Het merendeel van de organisaties geeft aan bezig te zijn met het inventariseren van hun processen en IT-systemen (zie figuur 14). Zo geven 43 van de 63 organisaties (68%) aan hun bedrijfskritische processen te hebben vastgesteld. De overgebleven 20 organisaties (32%) zijn daarmee bezig. Met bedrijfskritische processen bedoelen we processen die kritiek zijn voor het behalen van de doelen van de organisaties. Voor de migratie naar quantumveilige cryptografie is het belangrijk om deze processen in beeld te hebben, omdat dit de processen zijn die waarschijnlijk als eerste quantumveilig gemaakt moeten worden.

Verder geeft 46% van de organisaties aan te weten welke netwerk- en informatie-systemen ze gebruiken binnen hun bedrijfskritische processen. Dat veel organisaties bezig zijn met het inventariseren van bedrijfskritische processen en systemen valt te verklaren. Dit inzicht is een basisvoorwaarde voor digitale weerbaarheid en is al verplicht vanuit de NIS2-richtlijn (Nationaal Cyber Security Centrum, z.d.b).

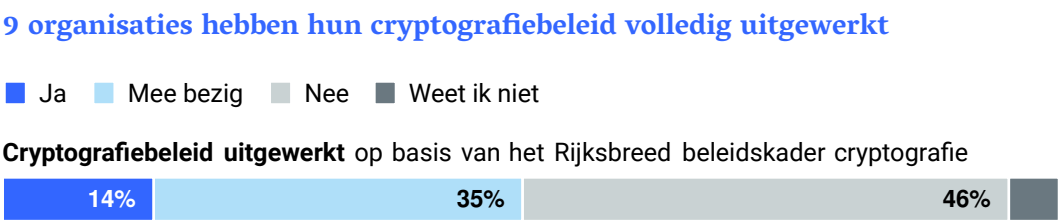
Aanzienlijk minder organisaties zijn begonnen met het inventariseren van de cryptografie binnen hun processen en systemen. 30 organisaties (48%) zijn er helemaal nog niet mee begonnen. Dit kan komen doordat het inventariseren van cryptografie erg complex is. Netwerk- en informatiesytemen bestaan vaak uit veel verschillende IT-producten, en die bestaan op zichzelf ook weer uit andere IT-producten. Vervolgens heeft elk product vaak meerdere cryptografische onderdelen. Zo kan een netwerk- of informatiesysteem al snel honderden cryptografische onderdelen bevatten. Er wordt gewerkt aan tools om automatisch cryptografie te ontdekken, maar deze tools zijn nog duur en beperkt effectief. Zo kunnen de makers van de tools geen garanties geven over hoe volledig hun inventarisatie is.

Desondanks is het essentieel dat organisaties een beeld krijgen van de cryptografie die ze in huis hebben. Als je niet weet welke cryptografie je hebt, kun je de cryptografie niet vervangen met quantumveilige cryptografie. 29 organisaties (46%) geven aan wel al gestart te zijn met het inventariseren van cryptografie. Een daarvan is de Belastingdienst. In een interview benadrukken zij het belang van beginnen, zodat je gaandeweg leert waar cryptografie in zit: *"Als je dat overzicht pas gaat creëren als totaaloplossingen [voor inventarisatie] vanuit de markt er zijn, dan ben je te laat"*.

Cryptografiebeleid opstellen

Om inventarisaties van cryptografie gestructureerd en actueel te houden, is een duidelijk cryptografiebeleid nodig. Zo'n beleid legt rollen en verantwoordelijkheden vast en beschrijft hoe organisaties inventarisaties uitvoeren. 22 organisaties (35%) zijn bezig met het opstellen van beleid (zie figuur 15). 9 organisaties (14%) hebben het beleid al ingevoerd.

Figuur 15 *Percentage ondervraagde organisaties dat cryptografiebeleid heeft uitgewerkt*



De Baseline Informatiebeveiliging Overheid (BIO) verplicht rijksoverheidsorganisaties om cryptografiebeleid te hebben. Dat nog maar weinig organisaties dit volledig hebben ingevoerd, is niet verrassend. Pas in maart 2025 heeft het rijksbreed beleidskader cryptografie duidelijk gemaakt wat er precies in cryptografiebeleid moet staan (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2025b). Wel valt op dat 29 organisaties (46%) nog helemaal niet zijn gestart met de uitwerking van beleid volgens dit kader.

Afspraken maken met leveranciers

Organisaties moeten niet alleen zicht hebben op hun eigen cryptografie, maar ook op die van hun leveranciers. Ook de cryptografie in die geleverde producten moet omgezet worden naar PQC. Voor sommige organisaties komt het grootste deel van de informatievoorziening van leveranciers. Denk hierbij aan analysesoftware, externe dataopslag, digitale werkplekken van SSC-ICT en Logius-diensten zoals DigiD.

Net als bij hun eigen processen en systemen hebben veel organisaties al een beeld van hun leveranciers (zie figuur 16). 30 organisaties (48%) hebben hun leveranciers geïnventariseerd. Nog eens 26 organisaties (41%) zijn daar nu mee bezig.

Figuur 16 *Percentage ondervraagde organisaties dat gesprekken heeft gevoerd met leveranciers over PQC*

Toch zijn nog weinig organisaties in gesprek met leveranciers over quantumveilige producten.15 organisaties (24%) zijn hiermee gestart, terwijl 45 organisaties (71%) nog geen enkel contact hebben gelegd. Sommige organisaties geven aan te wachten met gesprekken tot quantumveilige producten op de markt komen. Andere vinden dat leveranciers zelf verantwoordelijk zijn om hun producten aan te passen.
QvC NL en het NCSC adviseren organisaties wel juist nu gesprekken te voeren. Leveranciers zien zo dat er vraag is naar quantumveilige producten en kunnen hun ontwikkelplannen daarop afstemmen. Logius benadrukt dat organisaties ook tijdig hun eigen processen en systemen moeten aanpassen, wanneer leveranciers hun cryptografie veranderen. Dit is een tijdrovend proces en vereist inzage in waar deze zijn ingebed in de organisatie. Daarom zijn sommige organisaties al begonnen met gesprekken. Zo meldt SSC-ICT: "*Quantum wordt steeds vaker besproken met onze leveranciers en welke ontwikkelingen zij daarin maken. Daartoe wordt de service roadmap van SSC-ICT vergeleken met de roadmap van de leveranciers*."

Hoewel deze gesprekken belangrijk zijn, vinden organisaties ook dat het werk niet alleen bij hen kan liggen. Producten van leveranciers worden vaak door meerdere overheidsorganisaties gebruikt. De Dienst Terugkeer en Vertrek (DTenV) wijst er bijvoorbeeld op dat zij niet de enige gebruiker zijn van eHandtekening. Het quantum-veilig maken daarvan is volgens hen dus een gezamenlijk probleem, dat vraagt om coördinatie op hoger niveau.

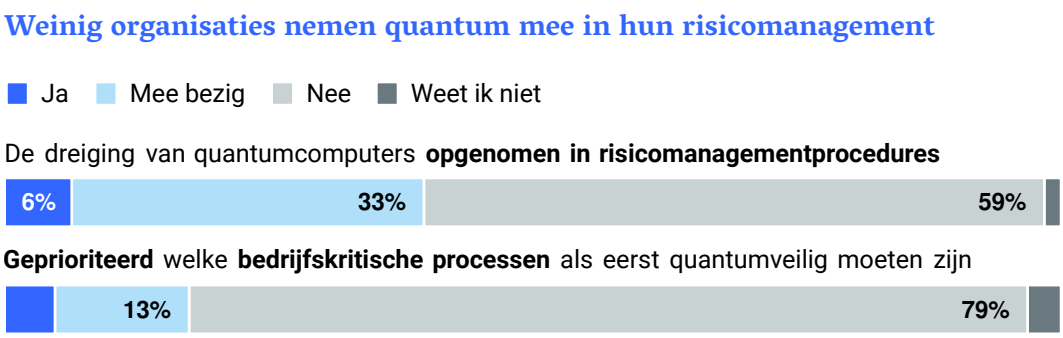
Quantumrisico's analyseren

Kennis van processen, systemen, cryptografie en leveranciers is een belangrijke eerste stap. Maar organisaties moeten dit ook vertalen naar concrete

voorbereidingen op de dreiging van quantumcomputers. Daarvoor moeten zij nagaan hoe groot die dreiging voor hen is en welke processen het meeste risico lopen. Ook zullen organisaties scherpe keuzes moeten maken over waar zij hun middelen inzetten, omdat ze tegelijkertijd voor andere dreigingen staan op het gebied van informatiebeveiliging. Om die keuzes verantwoord te maken, moeten rijksoverheids-organisaties de risico's van quantum continu afwegen tegen andere risico's.

Toch hebben slechts 4 van de 63 ondervraagde organisaties (6%) de dreiging van quantumcomputers opgenomen in hun risicomanagement (zie figuur 17). 37 organisaties (59%) zijn hier helemaal nog niet mee begonnen. Ook hebben slechts 3 organisaties (5%) bepaald welke bedrijfskritische processen ze als eerste quantum-veilig willen maken.

Figuur 17 *Percentage ondervraagde organisaties dat de dreiging van quantumcomputers heeft opgenomen in risicomanagementprocessen*



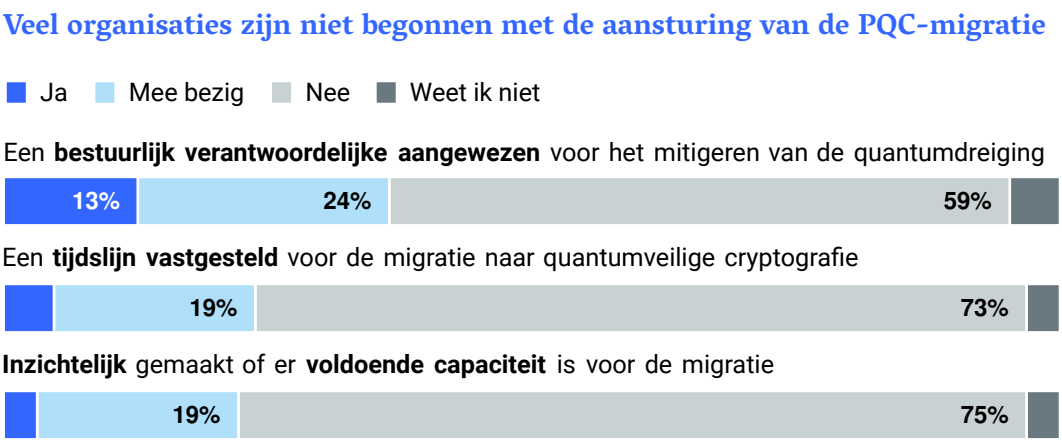
Hoewel veel organisaties zicht hebben op hun processen en IT-systemen, hebben maar weinig geanalyseerd hoe quantumcomputers die kunnen bedreigen. Dit past in een breder beeld uit de vragenlijst: rijksoverheidsorganisaties werken wel aan algemene maatregelen voor informatiebeveiliging, maar nog nauwelijks aan concrete voorbereidingen op de quantumdreiging. Een organisatie verwoordde het zo: "*Wij zijn niet vanuit het oogpunt van quantumtechnologie bezig met dreigingen, maar wel actief bezig met de implementatie van de BIO en NIS2. Dit zijn onderwerpen die dichter bij de organisatie staan.*"

Migratie aansturen

Het gebrek aan specifieke voorbereidingen blijkt ook uit het feit dat de meeste organisaties nog niet begonnen zijn met de aansturing en planning van de PQC-migratie. 52 van de 63 organisaties (83%) hebben nog geen bestuurlijk verantwoordelijke aangewezen (zie figuur 18). 58 organisaties (92%) hebben nog geen tijdslijn vastgesteld en 59 organisaties (94%) hebben niet inzichtelijk gemaakt of ze voldoende capaciteit hebben voor de migratie. Zonder deze organisatorische

basis wordt de complexe transitie naar quantumveilige cryptografie lastig en kan het onderwerp onderbelicht blijven binnen organisaties.

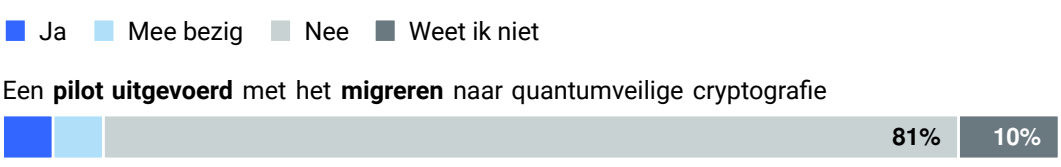
Figuur 18 *Percentage ondervraagde organisaties dat de aansturing van hun PQC-migratie heeft geregeld*



Cryptografie vervangen

Alle voorbereidingen moeten er uiteindelijk toe leiden dat organisaties hun cryptografie kunnen vervangen met quantumveilige cryptografie. Maar zoals eerder genoemd in paragraaf 5.2.1, zijn er nu nog nauwelijks quantumveilige producten beschikbaar. Daarom hebben we rijksoverheidsorganisaties alleen gevraagd of ze al pilots hebben uitgevoerd met het vervangen van cryptografie naar PQC. 3 organisaties (5%) hebben een pilot afgerond en 3 organisaties (5%) zijn ermee bezig.

Figuur 19 *Percentage ondervraagde organisaties dat een pilot heeft uitgevoerd met het vervangen van cryptografie naar PQC*



5.5 Obstakels bij de voorbereidingen voor de quantumdreiging

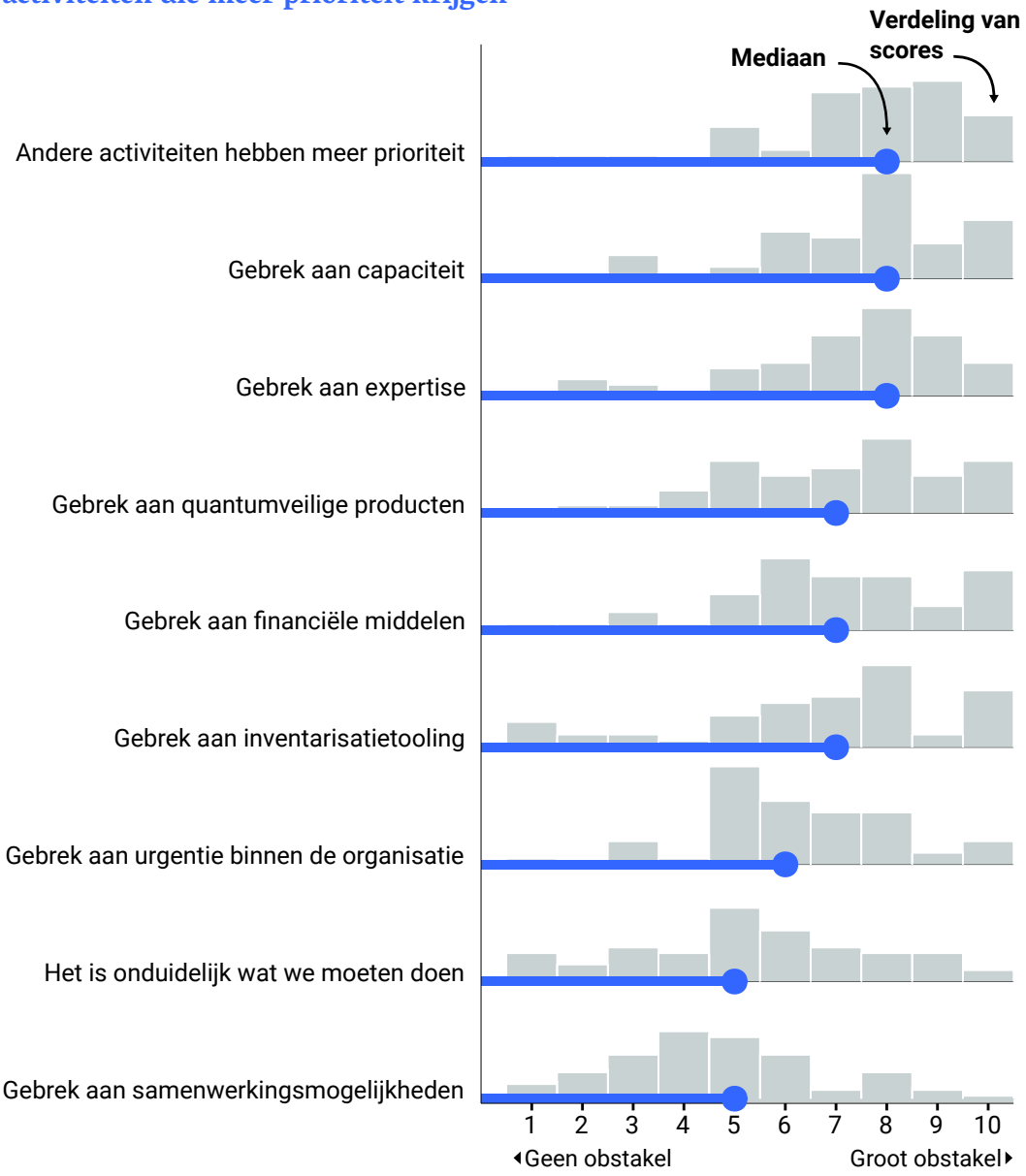
Uit de vorige paragraaf blijkt dat veel rijksoverheidsorganisaties nog aan het begin staan van hun PQC-migratie. In de vragenlijst vroegen we hen welke obstakels daarbij het meest in de weg zitten. Voor de ondervraagde organisaties zijn de grootste obstakels: (1) andere activiteiten die voorrang krijgen, (2) een gebrek aan capaciteit en (3) een gebrek aan expertise (zie figuur 20). Gemiddeld beoordelen organisaties deze 3 obstakels met een 8 op een schaal van 1 tot 10. De volgende paragrafen gaan hier dieper op in.

5.5.1 Veel taken en beperkte capaciteit

Voor organisaties is de quantumdreiging één van vele risico´s. Ze moeten ook rekening houden met hacks met kwetsbaarheden, zoals de Citrix-kwetsbaarheid bij het Openbaar Ministerie, en met DDoS-aanvallen. Daarbovenop spelen bredere uitdagingen in de informatievoorziening. Zo staan organisaties voor moderniserings-opgaven, zijn ze druk met vertraagde IT-projecten of willen ze minder afhankelijk worden van Amerikaanse technologiebedrijven. De PQC-migratie is voor organisaties dus één van de vele taken op het gebied van informatievoorziening en -beveiliging.

Figuur 20 *Obstakels bij de PQC-migratie zoals gescoord door de ondervraagde organisaties*

De grootste obstakels zijn een gebrek aan capaciteit en expertise, en andere activiteiten die meer prioriteit krijgen



Organisaties geven aan dat hun middelen en capaciteit beperkt zijn. Door de taakstelling in de Miljoenennota 2025 (Rijksoverheid, 2024) vrezen zij dat die beperkte capaciteit verder onder druk komt te staan. De PQC-migratie moet daardoor concurreren met andere taken en verplichtingen. Organisaties geven dan prioriteit aan dreigingen die zij als acuter ervaren. Voor de PQC-migratie betekent dit vaak dat medewerkers het erbij moeten doen.

De PQC-migratie hoeft volgens organisaties niet altijd ten koste te gaan van andere prioriteiten. Sommigen nemen PQC mee in hun overgang naar een *zero-trust*

security-omgeving. Andere organisaties koppelen het verbeteren van hun cryptografie aan de implementatie van de BIO en de NIS2-wetgeving. Zo kan de PQC-migratie meeliften op lopende initiatieven en verplichtingen.

5.5.2 Een gebrek aan expertise

Migreren naar PQC vereist veel expertise. Technische kennis is nodig om cryptografie in kaart te brengen, om PQC-oplossingen te beoordelen en om te weten hoe PQC-producten toegepast moeten worden. Voor organisaties is deze expertise lastig te vinden en moeilijk vast te houden. Een van de geïnterviewde organisaties legt uit dat ze specialisten moeilijk vast kunnen houden, omdat ze hen niet genoeg vakgenoten en uitdagingen kunnen bieden.

Daarom zoeken overheidsorganisaties kennis bij externe partijen. Zo kijken organisaties voor de beoordeling van de veiligheid van PQC-producten naar TNO en de AIVD. Voor het implementeren van PQC hopen ze te leunen op de expertise van leveranciers. SSC-ICT ziet ook een adviesrol voor zichzelf bij het aanschaffen van diensten, maar benadrukt dat organisaties uiteindelijk zelf moeten beslissen welke cryptografie ze waar inzetten.

Het ministerie van Financiën merkt op dat veel organisaties een beroep zullen doen op de expertise van leveranciers en specialisten. Zij moeten die vraag wel aankunnen. Om hierbij te helpen, werkt QvC NL aan een expertisecentrum (zie paragraaf 5.3.1). Dit centrum moet een plek worden waar kennis samenkomt en waar overheid, bedrijven en kennisinstellingen samenwerken aan de PQC-migratie. Dit centrum kan in potentie bijdragen aan een oplossing voor deze belemmering.

6. Reactie

Vanwege hun coördinerende rollen betreffende de digitalisering van de Nederlandse overheid hebben wij ons conceptrapport toegezonden aan de minister van Economische Zaken (EZ) en de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties (BZK). De minister van EZ heeft, mede namens de staatssecretaris van BZK, gereageerd op ons conceptrapport. Gezien zijn reactie zien we geen aanleiding tot een nawoord. Wij waarderen de serieuze reactie waarin de minister van EZ en staatssecretaris van BZK onze bevindingen erkennen en toezeggen om verder aan de slag te gaan. De brief van de minister staat op onze website (www.rekenkamer.nl).

Bijlagen

Bijlage 1 Methodologische verantwoording

Het doel van dit onderzoek is om de kansen en risico's die zijn verbonden aan de ontwikkeling van quantumtechnologie op hoofdlijnen in kaart te brengen. In deze methodologische verantwoording beschrijven we wat we hebben onderzocht en hoe we dat hebben aangepakt.

Wat hebben we onderzocht?

Hoofdvraag: Op welke manier bevordert de rijksoverheid dat kansen van quantumtechnologie worden benut en de risico's worden gemitigeerd?

Om deze hoofdvraag te beantwoorden, hebben we onderstaande deelvragen beantwoord:

1. Welke kansen biedt quantumtechnologie voor de rijksoverheid en de Nederlandse samenleving?
2. Op welke manier (financieel en beleidsmatig) bevordert de rijksoverheid dat de kansen van quantumtechnologie worden benut?
3. Wat zijn dusver de resultaten van de inzet van de rijksoverheid in quantumtechnologie?
4. Welke risico's zijn er voor de rijksoverheid met de opkomst van quantumtechnologie?
5. Op welke manier (financieel en beleidsmatig) bevordert de rijksoverheid dat de risico's van quantumtechnologie worden beheerst?
6. Wat doen rijksoverheidsorganisaties om zich voor te bereiden op de risico's van quantumtechnologie?

Onze bevindingen voor hoofdstuk 5 zijn gebaseerd op zelfrapportage van de ondervraagde organisaties. Wij hebben – gegeven het karakter van dit onderzoek – geen zelfstandige analyse gedaan van de mate van correctheid of volledigheid.

Aanpak

Focusonderzoek

We hebben dit onderzoek uitgevoerd in de vorm van een focusonderzoek. Een focusonderzoek is een type onderzoek van de Algemene Rekenkamer dat zich onderscheidt door:

- een aanzienlijk kortere doorlooptijd dan ander onderzoek van de Algemene Rekenkamer;
- aansluiting bij de actualiteit;
- een scherpe en afgebakende vraagstelling.

Een focusonderzoek leidt tot een heldere, bondige publicatie zonder oordelen en aanbevelingen. Zie https://www.rekenkamer.nl/over-de-algemene-rekenkamer/werkwijze/innovatie/focusonderzoeken.

Selectie van organisaties

In dit onderzoek hebben we 63 rijksoverheidsorganisaties gevraagd om een vragenlijst in te vullen. Alle 63 organisaties hebben gereageerd. Deze organisaties zijn opgenomen in bijlage 2. Wij hebben deze organisaties geselecteerd vanwege het beheer van gevoelige informatie en/of het uitvoeren van vitale processen.
Enkele ministeries hebben de vragenlijst voor hun kerndepartementen gezamenlijk ingevuld. Het gaat hier om:

- de ministeries van Binnenlandse Zaken en Koninkrijksrelaties (BZK) en Volkshuisvesting en Ruimtelijke Ordening (VRO);
- de ministeries van Economische Zaken (EZ), Klimaat en Groene Groei (KGG) en Landbouw, Visserij, Voedselzekerheid en Natuur (LVVN);

de ministeries van Justitie en Veiligheid (JenV) en Asiel en Migratie (AenM).

Documentatie

Voor het schrijven van dit rapport hebben we openbare bronnen en interne documenten van de ministeries van EZ, BZK en Quantum Delta NL bestudeerd om de onderzoeksvragen 1 tot en met 5 te kunnen beantwoorden.

Interviews

Bij de ministeries van EZ en BZK (het programma Quantumveilige cryptografie (QvC NL) hebben we interviews gehouden over hun coördinerende rollen en taken in relatie tot quantumtechnologie. Ook hebben we een interview gehouden bij Quantum Delta NL over de werkzaamheden van het programma en de resultaten die het programma tot nu toe heeft opgeleverd. Daarnaast hebben we interviews gehouden bij TNO, de Europese Commissie (onderdeel Directorate-General for Communications Networks, Content and Technology), Nationaal Cyber Security Centrum (NCSC, onderdeel JenV), Logius en Shared Service Center ICT (SSC-ICT). Dit zijn allemaal organisaties die centraal staan bij de aanpak van kansen en dreigingen van quantumtechnologie.
Daarnaast hebben we bij 10 organisaties een aanvullend diepte-interview gehouden. Wij hebben deze geselecteerd op basis van onze aanname dat zij bekend zijn met de kansen en risico's van quantumtechnologie. In bijlage 2 is aangegeven welke organisaties, die ook de vragenlijst hebben ingevuld, hiervoor zijn geselecteerd.

Afbakening

- We hebben de inlichtingendiensten en staatsgeheime informatie buiten de scope van dit onderzoek gehouden. Deze zijn weliswaar zeer relevant, maar vanwege de korte doorlooptijd van dit focusonderzoek konden we geen gebruikmaken van bronnen met een gerubriceerd karakter.
- Veel organisaties investeren in de ontwikkeling van quantumtechnologie. In dit onderzoek richten we ons uitsluitend op de investeringen via het Nationaal Groeifonds.

Bijlage 2 Geselecteerde organisaties

De tabel hieronder laat zien welke organisaties we hebben geselecteerd voor het onderzoek naar de kansen en risico's van quantumtechnologie.

Bij 10 organisaties hebben we een asterisk (*) geplaatst. Daar hebben we een aanvullend diepte-interview gehouden.

Ministerie	Organisatie	Status
Algemene Zaken (AZ)	Kerndepartement Algemene Zaken	Onderdeel ministerie
Binnenlandse Zaken en Koninkrijksrelaties (BZK) en Volkshuisvesting en Ruimtelijke Ordening (VRO)	Kerndepartement BZK en VRO	Onderdeel ministerie
	Logius	Agentschap
	Rijksdienst voor Identiteitsgegevens (RvIG)*	Agentschap
	Rijksorganisatie voor Informatiehuishouding	Onderdeel ministerie
	P-Direkt	Agentschap
	Rijksvastgoedbedrijf (RVB)*	Agentschap
	Shared Service Center ICT (SSC-ICT)	Agentschap
	Kadaster	zbo/rwt
	Kiesraad	Onderdeel ministerie
Buitenlandse Zaken (BZ)	Kerndepartement Buitenlandse Zaken	Onderdeel ministerie
Defensie	Kerndepartement Defensie*	Onderdeel ministerie
	Inspectie Veiligheid Defensie	Inspectie
Economische Zaken (EZ), Klimaat en Groene Groei (KGG) en Landbouw, Visserij, Voedselzekerheid en Natuur (LVVN)	Kerndepartement EZ, KGG en LVVN	Onderdeel ministerie
	Rijksdienst voor Ondernemend Nederland (RVO)	Agentschap
	Dienst ICT Uitvoering (DICTU)	Agentschap
	Kamer van Koophandel (KvK)	zbo/rwt
	Rijksinspectie Digitale infrastructuur	Agentschap
	Centraal Bureau voor de Statistiek (CBS)	zbo/rwt
	Nederlandse Emissieautoriteit (NEa)	Agentschap
Financiën	Kerndepartement Financiën*	Onderdeel ministerie
	Belastingdienst*	Onderdeel ministerie
	Douane	Onderdeel ministerie
	Toeslagen	Onderdeel ministerie
	De Nederlandsche Bank	zbo/rwt
	Autoriteit Financiële Markten (AFM)	zbo/rwt
	Agentschap van de Generale Thesaurie	Onderdeel ministerie
Infrastructuur en Waterstaat (IenW)	Kerndepartement Infrastructuur en Waterstaat*	Onderdeel ministerie
	Autoriteit Nucleaire Veiligheid en Stralingsbescherming	Onderdeel ministerie
	Inspectie Leefomgeving en Transport (ILT)	Onderdeel ministerie
	Luchtverkeersleiding Nederland	zbo/rwt
	Prorail BV	rwt
	Rijkswaterstaat (RWS)*	Agentschap
	Koninklijk Nederlands Meteorologisch Instituut (KNMI)	Agentschap

Ministerie	Organisatie	Status
Justitie en Veiligheid (JenV) Asiel en Migratie (AenM)	Kerndepartement JenV* en AenM	Onderdeel ministerie
	Dienst JUSTIS (Justitiële Uitvoeringsdienst Toetsing, Integriteit, Screening)	Agentschap
	Justitiële Informatiedienst (JustID)	Agentschap
	Nationale Politie*	rwt
	Openbaar Ministerie	Onderdeel ministerie
	Centraal Justitieel Incassobureau (CJIB)	Agentschap
	Dienst Justitiële Inrichtingen (DJI)	Agentschap
	Nederlands Forensisch Instituut (NFI)	Agentschap
	Dienst Terugkeer & Vertrek	Onderdeel ministerie
	Immigratie- en Naturalisatiedienst (IND)	Agentschap
	Onderzoeksraad voor Veiligheid	zbo/rwt
	Raad voor de Kinderbescherming	Onderdeel ministerie
Onderwijs Cultuur en Wetenschap (OCW)	Kerndepartement OCW	Onderdeel ministerie
	Nationaal Archief (NA)	Agentschap
	Dienst Uitvoering Onderwijs (DUO)	Agentschap
Sociale Zaken en Werkgelegenheid (SZW)	Kerndepartement SZW	Onderdeel ministerie
	Nederlandse arbeidsinspectie	Onderdeel ministerie
	Inlichtingenbureau (IB)	rwt
	Sociale Verzekeringsbank (SVB)	zbo/rwt
	Uitvoeringsinstituut Werknemersverzekeringen (UWV)*	zbo/rwt
Volksgezondheid, Welzijn en Sport (VWS)	Kerndepartement VWS	Onderdeel ministerie
	CAK	zbo/rwt
	CIBG	Agentschap
	CIZ	zbo/rwt
	Rijksinstituut voor Volksgezondheid en Milieu (RIVM)	Agentschap
	College ter Beoordeling van Geneesmiddelen (CBG)	Agentschap
	Dienst Uitvoering Subsidies aan Instellingen	Onderdeel ministerie
	Inspectie Gezondheidszorg en Jeugd	Onderdeel ministerie
	Nederlandse Zorgautoriteit (Nza)	zbo/rwt

Bijlage 3 Literatuur

AIVD, CWI & TNO, (2024), Het PQC- migratie handboek

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

Birch, (2020), Het Nederlandse Quantum Ecosysteem

Birch, (2024), Ecosystem update QDNL Midterm Review

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

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

Europese Commissie, (2025), Communication on the Quantum Europe Strategy

Europese Commissie, (2025b), Vlaggenschip voor kwantumtechnologieën: https://digital-strategy.ec.europa.eu/nl/policies/quantum-technologies-flagship

Europese Commissie, (2025c), Gemeenschappelijke Onderneming Europese high-performance computing - EuroHPC JU: https://digital-strategy.ec.europa.eu/nl/policies/high-performance-computing-joint-undertaking

Europese Commissie, (2025d), Europese kwantumcommunicatie-infrastructuur – EuroQCI: https://digital-strategy.ec.europa.eu/nl/policies/european-quantum-communication-infrastructure-euroqci

Europese Commissie, (2025e), Roadmap for the Transition to Post-Quantum Cryptography

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

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

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, (2019), Baseline Informatiebeveiliging Overheid (BIO), pagina 41. 2019. Beschikbaar via: https://www.informatiebeveiligingsdienst.nl/producten/bio/

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, (2025), Informatieset Quantumveilige Cryptografie, Een hulpmiddel voor leveranciersmanagement Versie: 1.0

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, (2025b), Rijksbreed beleidskader cryptografie - Een raamwerk voor het opstellen van cryptografiebeleid

Ministerie van Defensie, (2023), 'Quantumtechnologie heeft impact op manier van opereren': https://magazines.defensie.nl/materieelgezien/2023/08/defensie-verkent-quantumtechnologie

Ministerie van Economische Zaken en Klimaat, (2024), De Nationale Technologie Strategie

Ministerie van Economische Zaken en Klimaat, (2025), Adviescommissie Nationaal Groeifonds Jaarverslag 2024

Ministerie van Economische Zaken, (2025), Voortgang Kabinetsaanpak Economische Veiligheid

Ministerie van Economische Zaken, (2025b), Fiche 1: Mededeling EU-kwantumstrategie

Ministerie van Financiën & 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

Ministerie van Infrastructuur en Waterstaat, (2025), Van Bits naar Qubits

Nationaal Cyber Security Centrum, (2023), Maak je organisatie quantumveilig

Nationaal Cyber Security Centrum, (z.d.), Basisprincipe 1: Breng je risico's in kaart: https://www.ncsc.nl/wat-kun-je-zelf-doen/basisprincipes/breng-je-risicos-in-kaart

Nationaal Cyber Security Centrum, (z.d.b), Cyberbeveiligingswet Bereid je voor: 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

Nationaal Groeifonds, (z.d.), 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 van partijen legt als eerste ter wereld een schaalbaar quantum netwerk aan in Rotterdamse haven: https://www.portofrotterdam.com/nl/nieuws-en-persberichten/consortium-van-partijen-legt-als-eerste-ter-wereld-een-schaalbaar-quantum

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 Instituut, (2023), Rathenau Scan: Quantumtechnologie in de samenleving

Rijksoverheid, (2024) Miljoenennota

Rijksoverheid, (2025), Quantumcomputers komen eraan en Nederland is voorbereid: https://www.rijksoverheid.nl/actueel/nieuws/2025/07/10/quantumcomputers-komen-eraan

Stichting Quantum Delta NL (2021), Quantum Delta Nederland Projectvoorstel Nationaal Groeifonds

TNO, (2025), Cryptographic Asset Discovery and Inventory; een marktverkenning en fit-gap-analyse.

Tweede Kamer, (2012), Persbericht van OCW en het NWO “Rijk investeert 167 miljoen in Nederlands top-onderzoek”

Tweede Kamer, (2013), BRIEF VAN DE MINISTER VAN ECONOMISCHE ZAKEN EN STAATSSECRETARIS VAN ONDERWIJS, CULTUUR EN WETENSCHAP, Bedrijfslevenbeleid 32637 nr. 82

Tweede Kamer, (2020), Kabinetsreactie Nationale Agenda Quantum Technologie, 29338 Nr. 216

Tweede Kamer, (2024), Vaststelling van de begrotingsstaat van het Nationaal Groeifonds voor het jaar 2024 36410 L Nr. 15

Tweede Kamer, (2025), Verslag van een commissiedebat, gehouden op 30 januari 2025, over opkomende en toekomstige technologieën. 26643-1311

Tweede Kamer, (2025b), Vaststelling van de begrotingsstaten van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (VII) voor het jaar 2026. Memorie van Toelichting. 36 800 VII nr. 2.

World Economic Forum, (2024), Quantum for Society

Bijlage 4 Eindnoten

1. Deze passage is geactualiseerd op basis van aanvullende informatie die werd ontvangen bij het bestuurlijk wederhoor.
2. Zo moeten er verbeteringen komen in de foutcorrectie bij berekeningen van quantumcomputers en de aantallen en de kwaliteit van de qubits die quantumcomputers gebruiken.
3. Het gaat hier om logische qubits.
4. In 2024 is de scope van het programma uitgebreid naar alle partijen die onder de NIS2 vallen. Dit naar aanleiding van een aanbeveling van de Europese Commissie. Daarom is de naam van het programma aangepast van Quantumveilige cryptografie Rijk (QvC Rijk) naar Quantumveilige cryptografie Nederland (QvC NL).
5. Om diezelfde reden vermelden we in dit rapport geen gedetailleerde resultaten.

Algemene Rekenkamer
Postbus 20015
2500 EA Den Haag
(070) 342 44 00
voorlichting@rekenkamer.nl
www.rekenkamer.nl

Foto: Rijksmediatheek
Economische Zaken

De tekst in dit document is
vastgesteld op 2 februari 2026.
Dit document is op 4 februari 2026
aangeboden aan de Tweede Kamer.

Den Haag, februari 2026