TNO Vector

Sleutelspeler of toeschouwer?

Toekomstscenario's voor Nederland met en zonder toegang tot een quantumcomputer en de impact op onze digitale veiligheid

TNO Publiek ⟩ TNO 2026 P10063

27 januari 2026

Centre for Societal Innovation and Strategy

ICT, Strategy & Policy
tno.vector.nl
+31 88 866 00 00
info@tno.nl

TNO 2026 P10063 – 27 januari 2026

Sleutelspeler of toeschouwer?

Toekomstscenario's voor Nederland met en zonder toegang tot een quantumcomputer en de impact op onze digitale veiligheid

Auteurs	Iris Kaliën, Julian Rabbie
Rubricering rapport	TNO Publiek
Aantal pagina's	35 (excl. voor- en achterblad)
Aantal bijlagen	2
Opdrachtgever	Ministerie van Defensie
Programmanaam	Purple Nectar
Projectnaam	QSHOR
Projectnummer	060.65598

Disclaimer
Dit onderzoek is (gedeeltelijk) gesponsord door het Ministerie van Defensie onder toekenning nr. QCPN2504. De in dit document opgenomen opvattingen, conclusies en aanbevelingen zijn die van de auteurs en worden niet noodzakelijkerwijs onderschreven, noch mogen zij worden geïnterpreteerd als een weergave van het officiële beleid, expliciet of impliciet, van het Ministerie van Defensie van Nederland. Het Ministerie van Defensie is gemachtigd om reproducties en herdrukken voor overheidsdoeleinden te vervaardigen en te verspreiden, ongeacht enige copyrightvermelding hierin.

Samenvatting

Quantumcomputing is een opkomende sleuteltechnologie die zowel disruptieve toepassingen als grote risico's met zich mee brengt. In het bijzonder vormt Shor's algoritme een directe bedreiging voor asymmetrische encryptie, de basis van onze digitale infrastructuur. Zodra quantumcomputers krachtig genoeg zijn om dit algoritme uit te voeren, kunnen gangbare cryptografische systemen worden gekraakt, met mogelijk grote implicaties voor onze nationale veiligheid, economie en maatschappelijke stabiliteit.

Dit rapport verkent vier toekomstscenario's voor 2035, waarin Nederland en andere landen al dan niet toegang hebben tot een quantumcomputer die Shor's algoritme kan uitvoeren. De scenario's zijn ontwikkeld aan de hand van de scenario planning methode en geanalyseerd met een ELSA-raamwerk (ethische, juridische en sociale dimensies, aangevuld met technologische en geopolitieke dimensies). De inhoud is gebaseerd op expertinterviews in combinatie met literatuuronderzoek.

De vier scenario's zijn gebaseerd op twee assen die vooraf zijn bepaald en kunnen worden beschreven zoals te zien is in Figuur 1.1.

Figuur 1.1: Overzicht van de vier toekomstscenario's die ontstaan op basis van de twee gekozen assen.

Per scenario zijn de geopolitieke, technologische, juridische, ethische en sociaal-maatschappelijke aspecten uitgewerkt. Dit biedt perspectief op hoe de toekomst er mogelijk uit zou kunnen komen te zien met de komst van quantumcomputers, wat vervolgens teruggeleid kan worden tot concrete strategische acties die nu in gang kunnen worden gezet om ons hierop voor te bereiden. Een overzicht van de belangrijkste elementen en een passende analogie per scenario wordt weergeven in Figuur 1.2.

Aspect	Scenario 1: Uniek strategisch middel voor NL	Scenario 2: Mutually Assured Decryption	Scenario 3: In de schaduw van grootmachten	Scenario 4: Quantum Winter
Geopolitiek 	• Tijdelijke informatievoorsprong, internationale druk en spionagerisico neemt toe. • Dilemma: geheimhouden of (openbaar) inzetten?	• Instabiele situatie met heimelijke afschrikking en risico op escalatie • Internationale afspraken nodig voor inzet	• Verslechterde onderhandelingspositie en afhankelijkheid van partnerlanden • Strategische autonomie staat onder druk	• Relatieve stabiliteit en ruimte voor samenwerking en kennisopbouw • Blijvende onzekerheid over (geheime) doorbraken houdt geopolitieke alertheid in stand
Technologisch 	• Nederland heeft een control point in handen • Opschaling en kennisbehoud cruciaal • Regels over toegang en gebruik	• Technologische wapenwedloop met behoefte aan nationale technologiesoevereiniteit • Versnelling van migratie naar quantum-safe encryptie	• Inzetten op control points op het gebied van componenten / subsystemen • Urgentie voor migratie naar quantum-safe encryptie in NL	• Open innovatie en technologische spin-offs • Vertraagde quantum-safe migratie • Ademruimte voor fundamenteel onderzoek
Juridisch 	• Juridische kaders nodig voor inzet en eigenaarschap • Evaluatie en aanscherping van wetgeving rondom nationale en economische veiligheid	• *Dual use* maakt wetgeving en handhaving complex • Behoefte aan non-proliferatie-achtige verdragen	• Focus op defensief beleid • Beperkte invloed op totstandkoming internationale kaders	• Meer tijd voor juridische voorbereiding • Wetgeving kan proactief worden ontwikkeld
Ethisch 	• Norm engineering mogelijk • Afweging tussen strategisch voordeel en publieke waarden	• Normalisering van surveillance dreigt • SEA-principes nodig voor verantwoord innoveren	• Dreiging kan leiden tot gedragsverandering • Dilemma's over transparantie en bescherming van burgerrechten	• Kans op structurele integratie van publieke waarden • Minder hype, meer reflectie • Ethisch ontwerp vanaf de basis beter mogelijk
Sociaal-maatschappelijk 	• Dreiging van surveillance en impact op digitale diensten • Maatschappelijke discussie over geheimhouding complex	• Vergroten van *digital divide* • Behoefte aan "quantumgeletterdheid" • Mogelijke parallellen met Snowden-onthullingen	• Wantrouwen en onrust; terugval op analoge communicatie • Economische achterstand dreigt	• Afnemende hype en mogelijke teleurstelling • Kans op bewustwording en inclusieve ontwikkeling
Analogie	**De Enigma-machine**	**Mutually Assured Destruction (MAD)**	**Afhankelijkheid van het Amerikaanse GPS**	**De ontwikkeling van kernfusie**
	Zoals de geallieerden tijdens WOII de Enigma-code kraakten en dit geheim hielden, staat Nederland voor de keuze: inzetten of onthullen? Geheimhouding kan strategisch zijn, maar ethisch complex.	Net als bij kernwapens leidt wederzijdse dreiging tot afschrikking, maar waar MAD zichtbaar was, kan quantumdecryptie heimelijk worden ingezet, wat de dynamiek fundamenteel verandert.	Nederland is lange tijd afhankelijk geweest het Amerikaanse GPS-systeem, met beperkte controle over kritieke infrastructuur. Een soortgelijke situatie kan ontstaan rondom quantumcomputing.	Net als kernfusie blijft quantumcomputing een belofte die nog niet is waargemaakt. De technologische ontwikkeling kan tientallen jaren nodig hebben, maar de potentie blijft.

Figuur 1.2 Overzicht van de belangrijkste elementen per ELSA-aspect voor de verschillende scenario's en bijbehorende analogie.

De belangrijkste overeenkomsten die in elk scenario terugkomen zijn:

- Quantum-safe encryptie is een noodzakelijke investering;
- De ontwikkeling van control points bieden invloed, ook zonder eigen quantumcomputer;
- Juridische kaders en internationale samenwerking zijn cruciaal om onze nationale veiligheid en strategische autonomie te waarborgen;
- Verschillende ethische dillema's spelen in elk scenario een rol en de koplopers zullen waarschijnlijk de norm bepalen;
- Sociaal-maatschappelijke impact (met name vertrouwen en bewustwording van burgers) vraagt om actieve betrokkenheid en transparante communicatie.

Inhoudsopgave

1 Introductie: quantumtechnologie als strategische sleuteltechnologie

Quantumtechnologie zal op de lange termijn cruciaal zijn voor ons verdienvermogen en nationale veiligheid.[1] Door gebruik te maken van de exotische eigenschappen van de allerkleinste deeltjes in de natuur, worden toepassingen mogelijk voor het uitvoeren van berekeningen (quantumcomputing), het verzenden van informatie (quantumcommunicatie) en het doen van nauwkeurige metingen (quantumsensing). Wereldwijd hebben meer dan dertig landen een nationale quantumtechnologie strategie gepubliceerd met een totale publieke investering van meer dan €50 miljard,[2] in combinatie met een soortgelijk bedrag aan private investeringen.[3] Die investeringsverdeling heeft direct te maken met de opkomende status van quantumtechnologie, waarbij publieke middelen worden ingezet om het ecosysteem te stimuleren en onderzoek te versnellen.[4]

De meeste middelen en aandacht binnen dit domein worden besteed aan quantumcomputers, die een bepalende factor kunnen gaan worden in de wereldwijde machtsbalans. De combinatie van civiele en militaire toepassingen die hiermee binnen handbereik komen, maken het mogelijk om quantumcomputers in te zetten om zowel de economische als nationale veiligheid van een land te waarborgen.[5] Dit vormt ook een spanningsveld tussen open innovatie en nationale belangen: open innovatie en internationale samenwerking versnellen de ontwikkeling, verlagen kosten en maken bredere adoptie van quantumtoepassingen mogelijk. Tegelijkertijd zet toenemende militaire interesse druk op strategische autonomie en kennisbescherming. Zo wordt quantumcomputing expliciet genoemd in de nationale veiligheidsstrategie van zowel de Verenigde Staten als China.[6][7] Alhoewel dit de adoptie van verder ontwikkelde toepassingen kan versnellen, kunnen deze meer gesloten innovatieprocessen de bredere technologische vooruitgang (en *time-to-market* voor civiele toepassingen) vertragen.

Hoewel de huidige generatie quantumcomputers nog beperkt zijn in rekenkracht, zijn er aan de lopende band doorbraken op het gebied van technologische innovatie en hebben een groot aantal bedrijven de ambitie om de komende vijf á tien jaar quantumcomputers te ontwikkelen die huidige simulaties overtreffen en op grotere en nuttige schaal kunnen worden ingezet.[8]

1.1 Leeswijzer

De rest van deze sectie bevat achtergrondinformatie over quantumcomputing en Shor's algoritme. Deze context is nodig om te begrijpen wat een quantumcomputer is, wat de belangrijkste toepassingen zijn, en welke maatregelen kunnen worden genomen om mogelijke dreigingen te mitigeren. Vervolgens worden in Sectie 2 de vier toekomstscenario's

uitgewerkt, waarin Nederland en andere landen al dan niet toegang hebben tot een quantumcomputer. Elk scenario wordt uitgewerkt langs vijf dimensies (geopolitiek, technologisch, juridisch, ethisch en sociaal-maatschappelijk) en geïllustreerd met een analogie. Daarnaast lichten we per scenario toe welke (subjectieve) indicatoren er mogelijk op wijzen dat we in de richting van een bepaald scenario aan het toe bewegen zijn. Tot slot volgt in Sectie 3 een overkoepelende analyse, waar de belangrijkste overeenkomsten en verschillen tussen de scenario's samen worden benoemt en de rode draden die in alle scenario's relevant zijn.

1.2 De toepassingen van quantumcomputers

Quantumcomputers bieden een breed scala aan mogelijke toepassingen: van materiaalkunde en medicijnontwikkeling tot optimalisatieproblemen, kunstmatige intelligentie en het ontsleutelen van cryptografie.[9] Deze worden mogelijk gemaakt door de inherente eigenschappen van de onderliggende bouwstenen van quantumcomputers (zogeheten quantum bits, of "qubits"), die een quantumcomputer in staat stellen om hele specifieke problemen op een fundamenteel andere manier op te lossen. De verwachting is dat quantumcomputers een nieuwe tool zullen worden in een breder scala van rekenkracht die gebruikt kan worden om complexe problemen op te lossen. Dit is vergelijkbaar met hoe grafische processors (GPU's) tegenwoordig naast gewone processors (CPU's) worden gebruikt. CPU's zijn goed in het uitvoeren van algemene taken, terwijl GPU's zijn gespecialiseerd in het snel verwerken van grote hoeveelheden data, bijvoorbeeld bij beeldbewerking of kunstmatige intelligentie. In moderne computersystemen werken deze twee soorten processors samen, waarbij ze elk hun eigen sterke kanten benutten. Quantumcomputers zullen naar verwachting een vergelijkbare rol gaan spelen: ze zullen de "klassieke" computers waarschijnlijk niet vervangen, maar juist aanvullen door specifieke problemen op een fundamenteel andere manier op te lossen.[10]

Quantumcomputers kunnen in uiteenlopende sectoren worden ingezet om complexe logistieke vraagstukken sneller of beter op te lossen en om ingewikkelde scenario's te simuleren.[11] Dit draagt bij aan snellere en betere besluitvorming en optimalisatie van middelen. Daarnaast maken quantumcomputers het mogelijk om simulaties van complexe moleculaire structuren en interacties uit te voeren, wat de ontwikkeling van geavanceerde materialen kan versnellen. Denk hierbij aan lichtere en sterkere materialen voor voertuigen, innovatieve coatings, maar ook toepassingen in de farmaceutische industrie en de energietransitie, zoals het ontwikkelen van nieuwe geneesmiddelen en efficiëntere batterijen.[12,13]

Daarnaast kan, eventueel in combinatie met AI, quantum computing worden ingezet voor het analyseren van grote en complexe datasets, bijvoorbeeld voor inlichtingendoeleinden zoals patroonherkenning in satellietbeelden of het detecteren van cyberdreiging.[14] Geavanceerde Quantum Machine Learning (QML) algoritmen hebben hiernaast ook belangrijke toepassingen binnen het civiele domein. Zo heeft de financiële sector baat bij snellere en nauwkeurigere voorspellingen voor risicoanalyse en fraudedetectie, en kan het de gezondheidszorg vooruitbrengen op gebied van medicijnontwikkeling, diagnose en behandelplanning.[15]

Toepassingen van quantum computing hebben dus een duaal karakter: ze kunnen bijdragen aan nationale veiligheid, maar tegelijkertijd ook aan economische groei, technologische innovatie en maatschappelijke vooruitgang. Hierdoor is quantumcomputing een zogeheten *dual-use* technologie.[16] In dit rapport ligt de focus echter op de impact van quantumcomputing op de nationale veiligheid en strategische autonomie, waarbij we ingaan

op een van de meest disruptieve toepassingen: het breken van asymmetrische encryptie met behulp van Shor's algoritme.

1.2.1 Shor's algoritme en de decryptiemogelijkheden van quantumcomputers

Al meer dan dertig jaar geleden voorzag de wiskundige Peter Shor (1994) dat quantumcomputers gebruikt kunnen worden voor de specifieke wiskundige problemen die de basis vormen voor de encryptie van onze digitale informatie. Hij ontdekte een algoritme, dat later naar hem vernoemd werd, dat het mogelijk maakt om op een efficiënte manier priemfactoren te bepalen en discrete logaritmen te berekenen;[17] twee wiskundige problemen die voor klassieke computers praktisch onhaalbaar zijn voor grote getallen. Deze onhaalbaarheid maken de twee problemen bij uitstek geschikt als middelen voor encryptie - totdat dit fundament door de ontdekking van Shor onderuit werd gehaald door aan te tonen dat quantumcomputers dit exponentieel sneller kunnen oplossen dan klassieke computers.

Om het belang hiervan te begrijpen, is het noodzakelijk om te kijken naar de rol van asymmetrische encryptie in onze digitale samenleving. Asymmetrische encryptie, ook wel *public key cryptografie* genoemd, berust op het gebruik van twee sleutels: een publieke sleutel (die vrij gedeeld mag worden) en een privésleutel (die geheim wordt gehouden). De veiligheid van dit systeem leunt op het feit dat het met klassieke computers praktisch onmogelijk is de privésleutel af te leiden uit de publieke sleutel, omdat dit het oplossen van bovengenoemde wiskundige problemen vergt. Deze wiskundige bewerkingen zijn namelijk eenvoudig toe te passen voor het versleutelen, maar extreem moeilijk om omgekeerd uit te voeren voor het ontsleutelen.

Op het moment van schrijven vormt asymmetrische cryptografie de basis van onze digitale beveiliging. Zo wordt het factoriseren van grote priemgetallen gebruikt in RSA-encryptie, en vormen discrete logaritme-problemen de kern van prominente systemen zoals DSA, Diffie-Hellman en Elliptic Curve Cryptography (ECC).[18] Deze asymmetrische algoritmen worden gebruikt in vrijwel alle protocollen die onze digitale communicatie beveiligen, waaronder:

- Veilig online betalen en andere beveiligde websites;
- Digitale handtekeningen voor software-updates, blockchaintransacties en elektronische documenten;
- Veilig inloggen op servers;
- Versleutelde netwerkverbindingen;
- Beveiligde e-mail;
- Bescherming van kritieke civiele en militaire infrastructuren.

De impact van het ontsleutelen van de encryptie van al deze systemen kan dus enorm zijn. In alle gevallen geldt, hoe groter de sleutel, hoe moeilijker het wordt om het systeem te kraken, maar ook hoe meer datatransmissie ervoor nodig is. De sleutellengtes worden daarom zodanig vastgesteld dat de toepassing ervan zo efficiënt mogelijk is en het tegelijkertijd onmogelijk is om binnen praktisch haalbare tijd de sleutel te kraken. Zo adviseert het Amerikaanse NIST (tot 2030) het gebruik van 256-bits ECC-sleutels, en 2048-bits sleutels voor RSA.[19] Echter, zodra een zogeheten "cryptografisch-relevante" quantumcomputer beschikbaar komt die Shor's algoritme op grote schaal kan uitvoeren, kunnen deze sleutels worden gekraakt. Dit zou betekenen dat de vertrouwelijkheid, integriteit en authenticiteit van digitale communicatie niet langer gegarandeerd kunnen worden.

Naast asymmetrische encryptie wordt voor de versleuteling van grote hoeveelheden data (zoals bij het verzenden van bestanden of het beveiligen van een VPN-verbinding) ook vaak symmetrische encryptie gebruikt. Hierbij delen beide communicatiepartijen dezelfde geheime sleutel, die voor zowel het versleutelen als ontsleutelen wordt gebruikt. Symmetrische encryptie is sneller en efficiënter dan asymmetrische, maar vereist dat beide partijen vooraf een gedeelde sleutel kunnen afspreken. Dit gebeurt juist vaak met behulp van asymmetrische cryptografie, waardoor de dreiging voor asymmetrische algoritmen een indirecte dreiging voor het hele beveiligingssysteem vormt.

1.2.1.1 De impact van Shor's algoritme

Het ontsleutelen van onze digitale informatie kan leiden tot verlies van vertrouwelijkheid en authenticiteit, alsook het destabiliseren van onze vitale infrastructuren. Gevoelige gegevens die vandaag versleuteld worden verzonden – denk aan medische dossiers, financiële transacties of staatsgeheimen – zouden in de toekomst openbaar kunnen worden door de inzet van quantumcomputers. Daarnaast kunnen digitale handtekeningen die nu worden gebruikt om software, websites of documenten te verifiëren, worden vervalst.[16] Kwaadwillende kunnen zich hierdoor voordoen als legitieme partijen. Ook communicatie binnen het veiligheidsdomein, zoals informatie over militaire operaties, inlichtingenwerk en gerubriceerde communicatie tussen bondgenoten of eenheden kan worden onderschept of bekendgemaakt. Daarnaast bestaat het risico dat private of statelijke actoren via Shor's algoritme digitaal toegang kunnen verkrijgen tot onze vitale infrastructuur, waarmee grote maatschappelijke schade kan worden aangericht.

Een belangrijk tijdsgebonden aspect waar hierbij rekening mee gehouden moet worden is de zogeheten 'store now, decrypt later' (SNDL) strategie.[20] Bij de SNDL-strategie worden potentieel gevoelige gegevens nu al onderschept en opgeslagen, om deze vervolgens later te ontsleutelen zodra een quantumcomputer met geschikte capaciteit beschikbaar is. Meer dan 50% van cybersecurity experts maken zich zorgen over dit scenario,[21] met name omdat dit een bijzonder risico vormt voor informatie die langdurig vertrouwelijk moet blijven, zoals staatsgeheimen, medische dossiers en juridische documenten. Dit is een reële mogelijkheid: de SNDL-strategie is tijdens de Tweede Wereldoorlog al toegepast door de Amerikanen, waarbij berichten van de Sovjets werden onderschept die vervolgens pas later jaren werden ontsleuteld toen hiaten in het Sovjetencryptiesysteem werden ontdekt.[22]

Daarnaast vormt Shor's algoritme een reële dreiging voor blockchaintechnologie, omdat de bijbehorende transactiedata per definitie openbaar is en opgeslagen wordt. Dit brengt bijvoorbeeld risico's met zich mee voor *privacy-blockchains* zoals Monero, aangezien transacties uit het verleden kunnen worden ontsleuteld.[23] Inzicht in deze data kan vervolgens gebruikt worden om transacties die hiermee hebben plaatsgevonden te de-anonimiseren. De impact kan echter nog veel groter zijn op Bitcoin, dat gebruikt maakt van asymmetrische cryptografie om eigenaarschap van digitale munten te beveiligen. Met name verouderede *legacy* Bitcoin wallets maken gebruik van sleutels die door toekomstige quantumcomputers gekraakt kunnen worden, en volgens recente schattingen lopen hiermee in totaal meer dan 6 miljoen Bitcoins met een gezamenlijke waarde van meer dan €500 miljard een risico.[24] Door de toenemende regulering en acceptatie van Bitcoin,[25] vormen quantumcomputers hiermee een dreiging voor het wereldwijde financiële systeem. Dit risico is echter breed bekend binnen de Bitcoin community en er wordt actief gewerkt aan maatregelen om de (mogelijke) negatieve impact van Shor's algoritme te mitigeren.[26]

1.2.1.2 Beperkingen van Shor's algoritme

De praktische inzetbaarheid van Shor's algoritme hangt af van de beschikbaarheid van quantumcomputers met voldoende qubits en robuuste foutencorrectie. Daarnaast spelen beperkingen op het gebied van energieverbruik en ondersteunende infrastructuur ook een belangrijke rol. Algemene schattingen voor het ontsleutelen van een 2048-bits RSA sleutel gaan uit van ongeveer 20 miljoen fysieke, niet-fout-gecorrigeerde qubits. Dankzij recente vooruitgang op zowel hardware als software gebied, is dit aantal echter aanzienlijk verlaagd: de nieuwste schattingen suggereren dat er minder dan een miljoen fysieke qubits voldoende zouden zijn om een 2048-bits RSA-getal binnen een week te ontsleutelen[27].

Toch blijven er aanzienlijke technologische en infrastructurele uitdagingen. De beste quantumcomputers beschikken momenteel nog over een beperkt aantal qubits (rond de 1.000) en de kwaliteit ervan is vaak onvoldoende. Hierdoor zijn in de praktijk slechts een klein deel van de qubits op een betrouwbare manier bruikbaar. De kwaliteit kan echter onder andere worden verhoogd via foutcorrectie, waarbij meerdere fysieke qubits samenwerken om één stabiele, fout-gecorrigeerde qubit te vormen. Dit worden ook wel "logische qubits" genoemd. Deze logische qubits zijn essentieel om complexe processen zoals Shor's algoritme uit te voeren. Het uitvoeren van de foutcorrectie vereist echter enorm veel rekenkracht van klassieke computers. Hierdoor ontstaat de noodzaak om quantumcomputers nauw te laten samenwerken met krachtige supercomputerclusters. Deze hybride infrastructuur is nodig om de enorme hoeveelheid berekeningen die foutcorrectie met zich meebrengt efficiënt te kunnen verwerken.[28]

Een andere factor is het energieverbruik dat gepaard gaat met het uitvoeren van Shor's algoritme. Dit wordt vooral bepaald door hardware omvang, de benodigde foutcorrectie en ondersteunende systemen zoals cryogene koeling. Hoewel het algoritme zelf theoretisch energiezuinig kan zijn, leidt praktische uitvoering op grote schaal tot hoog energieverbruik. Zo wordt geschat dat het uitvoeren van Shor's algoritme 125 megawatt continu vermogen vergt voor het breken van een 2048-bit RSA-sleutel, wat overeenkomt met het vermogen van een kleine elektriciteitscentrale.[29] Daarnaast kan de energie die nodig is voor het klassiek optimaliseren van de operaties die nodig zijn voor de uitvoering van Shor's algoritme oplopen tot wel 1 GWh voor optimalisaties van ongeveer 8.000 qubits.[30] Dit staat gelijk aan het jaarlijkse energieverbruik van ongeveer 300 huishoudens in Nederland.[31] Grootschalige cryptografische toepassingen vergen door schaal en koeling hoge energie-inspanningen, waardoor operationele kosten oplopen en voor problemen kunnen zorgen binnen Nederland vanwege de bestaande netcongestie in het elektriciteitsnetwerk. Toekomstige hardware- en softwareverbeteringen zullen deze energiekosten naar verwachting echter wel verlagen.

1.2.2 De risico's van Shor's algoritme mitigeren met quantum-safe encryptie

Het groeiende besef over de kwetsbaarheid van bestaande cryptografische systemen en de mogelijke komst van krachtige quantumcomputers heeft ertoe geleid dat de migratie naar quantum-safe cryptografie wereldwijd in gang is gezet. Alhoewel de urgentie breed wordt erkend, vooral door organisaties die gevoelige data langdurig moeten beschermen of kritieke infrastructuur beheren, bevindt dit proces zich echter nog in een vroege fase. Voor de migratie naar encryptie die bestand is tegen de dreiging van quantumcomputers staan twee methodes centraal: post-quantum cryptografie (PQC) en quantum key distribution (QKD).

1.2.2.1 Post-quantum cryptografie

PQC omvat nieuwe cryptografische algoritmen die ontworpen zijn om bestand te zijn tegen aanvallen door quantumcomputers.[16] In tegenstelling tot bestaande asymmetrische algoritmen zoals RSA en ECC, die kwetsbaar zijn voor Shor's algoritme, zijn PQC-algoritmen gebaseerd op wiskundige problemen waarvan tot nu toe geen efficiënte "quantum-aanvallen" bekend zijn. Hieronder vallen extreem complexe wiskundige problemen (zoals zogeheten "lattice-based" of "hash-based" problemen en multivariate vergelijkingen) die quantumcomputers moeilijk kunnen oplossen. Het grote voordeel van PQC is dat deze algoritmen op bestaande digitale infrastructuren kunnen worden geïmplementeerd, vaak zonder dat er nieuwe hardware nodig is. Wel kunnen PQC-algoritmen de communicatie vertragen of zwaarder maken doordat de bewerkingen voor versleutelen en ontsleutelen vaak intensiever zijn, wat vooral merkbaar is bij systemen met strikte eisen aan snelheid en bandbreedte. Desalniettemin is PQC is vaak de meest bruikbare oplossing voor het beschermen van digitale communicatie en data tegen toekomstige quantumdreigingen. In augustus 2024 zijn de eerste internationale PQC-standaarden door het Amerikaanse NIST gepubliceerd, waarmee wereldwijd de migratie naar deze nieuwe cryptografiegeneratie op gang is gekomen.[32] Grote organisaties zijn gestart met de overstap, en overheden en toezichthouders ontwikkelen regelgeving om deze transitie te versnellen. In juni 2025 heeft de Europese Commissie bijvoorbeeld een gecoördineerde roadmap gepubliceerd voor de migratie naar PQC, waarin staat dat de belangrijkste systemen in 2030 moeten zijn gemigreerd, en zo veel mogelijk andere digitale systemen in 2035.[33] De migratie is echter een complex en tijdrovend proces, dat door de diepgewortelde toepassing van cryptografie in alle lagen van beveiligingssystemen en het ontbreken van cryptografische wendbaarheid ("crypto agility") vaak meer dan vijf jaar kan duren. Daarnaast loopt, door verschillen in wet- en regelgeving per sector, het gevoel van urgentie en bewustwording, de adoptie in de praktijk vaak achter op de richtlijnen.[19]

1.2.2.2 Quantum key distribution

QKD is een alternatieve benadering die gebruikmaakt van de principes van de quantummechanica om het uitwisselen van encryptiesleutels veilig te maken. Hierbij worden sleutels via een quantumkanaal verstuurd, waarbij elke poging tot afluisteren direct detecteerbaar is. De beveiliging vindt hierdoor plaats op basis van natuurkundige verschijnselen in plaats van wiskundige structuren. QKD biedt in theorie fundamentele veiligheid voor sleuteluitwisseling, maar kent in de praktijk belangrijke beperkingen: het vereist speciale hardware en infrastructuur en is momenteel alleen bruikbaar op beperkte afstand. Daarnaast vereist QKD een geauthentiseerd klassiek kanaal om sleutels te verifiëren, waarbij vaak PQC wordt toegepast voor digitale handtekeningen of authenticatie van communicatie. Daarom adviseren veel veiligheidsdiensten wereldwijd momenteel vooral PQC als primaire route voor de bescherming van asymmetrische encryptie,[34] een wordt QKD vooral gezien als een aanvullende optie voor zeer specifieke toepassingen en kritieke infrastructuren. Op de lange termijn kunnen QKD-netwerken echter wel fungeren als basis voor een geavanceerd *quantum internet* waarmee quantumcomputers op afstand met elkaar verbonden kunnen worden, waardoor er los van de veiligheidsoverwegingen een andere prikkel is om deze netwerken op te bouwen.[35] Dit wordt momenteel in Nederland gedaan als onderdeel van het Europese EuroQCI programma.[36]

1.3 Conclusies

We bevinden ons momenteel in een turbulente fase waarin er wereldwijd enorm wordt geïnvesteerd in zowel de ontwikkeling van quantumcomputers als de verdediging hiertegen. Hoewel het onmogelijk is om exact te voorspellen of en wanneer we op het punt komen dat

quantumcomputers op grote schaal bruikbaar ingezet kunnen worden – en daarmee ook Shor’s algoritme kan worden uitgevoerd – is het duidelijk dat hun komst verstrekkende gevolgen kan hebben. In het bijzonder kan de toepassing van Shor’s algoritme een directe bedreiging vormen voor de vertrouwelijkheid, integriteit en authenticiteit van digitale communicatie. Deze dreiging raakt niet alleen militaire en civiele infrastructuren, maar ook bredere maatschappelijke en economische domeinen. Het is daarom van essentieel belang om ons nu al voor te bereiden op de toekomst, door tijdig te anticiperen op deze technologische ontwikkeling en bijbehorende risico’s in kaart te brengen en te mitigeren.

2 Vier toekomstscenario's voor quantumcomputers

Om meer inzicht te krijgen in hoe de toekomst eruit zou kunnen zien, hebben we vier scenario's ontwikkeld, welke in dit hoofdstuk zullen worden toegelicht. Deze scenario's zijn bedoeld om inzicht te geven in mogelijke ontwikkelingen en relevante indicatoren te identificeren, zodat organisaties en beleidsmakers zo goed mogelijk voorbereid zijn op de komst van quantumcomputers.

Strategic foresight en scenarioanalyse zijn cruciale instrumenten om (beleid)keuzes vorm te geven in situaties van grote onzekerheid. Ze maken het mogelijk om op gestructureerde wijze trends, risico's en kansen te identificeren, en om robuuste strategieën te ontwikkelen die bestand zijn tegen verschillende toekomstmogelijkheden.[37] Zowel de Europese Commissie als de OECD benadrukken het belang van deze methoden voor het anticiperen op disruptieve technologische ontwikkelingen en het versterken van strategische veerkracht.[38,39] Voor het ontwikkelen van de scenario's passen we de klassieke scenario planning methode toe.[40] Hierbij worden een set aan belangrijke externe trends verzameld, waarna de twee trends met de grootste onzekerheid en impact tegen elkaar worden uitgezet op twee assen, waaruit vervolgens vier scenario's ontstaan. Er is in dit geval vooraf een keuze gemaakt over de twee assen die het meest relevant zijn om te analyseren, namelijk:

1. **Nederland heeft wel/geen toegang tot een quantumcomputer**
2. **Andere landen hebben wel/geen toegang tot een quantumcomputer**

Hieruit volgen vier specifieke scenario's – zie Figuur 2.1. Ondanks dat de twee assen met elkaar verbonden zijn doordat internationaal kennis wordt uitgewisseld, nemen we aan dat deze twee assen zich onafhankelijk van elkaar ontwikkelen.

Figuur 2.1 Overzicht van de vier scenario's die we hebben gevormd op basis van de twee assen.

Met “een quantumcomputer” bedoelen wij specifiek een quantumcomputer die in staat is om op praktische schaal Shor’s algoritme uit te voeren en gangbare encryptie te omzeilen. Om technische discussies te vermijden, specificeren we dit niet verder aan de hand van aantal qubits of andere indicatoren. Met “andere landen” zijn wij in dit geval agnostisch of dit partner- of risicolanden zijn. Dit onderscheid zullen we per scenario waar nodig verder uitweiden. Het begrip “toegang tot” hebben we hier verder bewust abstract gehouden, omdat nog niet duidelijk is op welke wijze quantumcomputers op grote schaal zullen worden ontwikkeld in de toekomst. Er zijn namelijk verschillende mogelijkheden, zoals:

- Een privaat bedrijf ontwikkelt de quantumcomputer in-house en de toegang hiertoe wordt vervolgens aangeboden via een clouddienst. Dit bieden bedrijven zoals IBM, PsiQuantum, D-Wave en Pasqal momenteel aan;
- Een publiek-privaat consortium bouwt een quantumcomputer, waarna het eigenaarschap en de toegang via specifieke juridische voorwaarden verloopt. Dit gebeurt momenteel bij de quantumcomputers die onder het EuroHPC programma worden ontwikkeld;
- Een ministerie of ander overheidsorgaan kan een quantumcomputer aankopen als *launching customer*. Dergelijke initiatieven worden momenteel uitgetest in bijvoorbeeld de Verenigde Staten en het Verenigd Koninkrijk, en in landen als China zal de overheid in de praktijk in grote mate zeggenschap hebben over de quantumcomputers die binnenlands worden ontwikkeld.

Hiernaast kunnen door middel van wetgeving of internationale afspraken bepaalde landen wel of niet in staat zijn toegang te verkrijgen tot quantumcomputers die buiten hun eigen landsgrenzen staan. Om agnostisch te blijven over welke van deze mogelijkheden in de toekomst realiteit wordt, nemen we aan dat Nederland of andere landen op een dusdanige manier toegang hebben tot een quantumcomputer dat zij autonoom algoritmes kunnen uitvoeren en de bijbehorende resultaten betrouwbaar kunnen ontvangen en verwerken.

De twee gekozen assen vormen samen vier onderscheidende en plausibele scenario’s die wij in dit rapport verder zullen uitwerken. Kort samengevat zijn de vier scenario’s:

1. **Scenario 1**: Nederland heeft *wel* toegang tot een quantumcomputer, maar andere landen *niet*. In dit scenario hebben wij een unieke machtspositie in het wereldwijde speelveld met de toegang tot een strategisch middel die wij als enige kunnen inzetten.
2. **Scenario 2**: Nederland heeft *wel* toegang tot een quantumcomputer, maar andere landen *ook*. In dit scenario is er sprake van een gelijk(er) speelveld, waarin Nederland slechts een van de landen is die een quantumcomputer als strategische asset heeft.
3. **Scenario 3**: Nederland heeft *geen* toegang tot een quantumcomputer, maar andere landen *wel*. In deze situatie hebben andere landen ons ingehaald en kunnen zij een quantumcomputer inzetten tegen Nederland, maar wij niet andersom. Dit creëert een risico en mogelijk een afhankelijkheid van anderen.
4. **Scenario 4**: Nederland heeft *geen* toegang tot een quantumcomputer, maar andere landen *ook niet*. Dit scenario omschrijft min of meer de status quo. Ondanks de grote ambities wereldwijd, is de ontwikkeling van een quantumcomputer erg complex gebleken en is er sprake van technologische stagnatie.

Deze vier scenario's moeten beschouwd worden als toekomstbeelden van hoe de externe wereld eruit kan komen te zien. Als tijdshorizon gebruiken we het jaar 2035 voor deze scenario's, aangezien de meeste huidige bedrijven verwachten dat ze in dit jaartal een werkende en effectieve quantumcomputer op grote schaal zullen hebben ontwikkeld,[6] rekening houdend met een aantal jaar onvoorziene vertraging. Hierbij zullen we niet ingaan op de wijze waarop we in elk van deze scenario's kunnen belanden en hoe realistisch of wenselijk elk scenario is. Daarnaast is het ook niet waarschijnlijk dat we heel duidelijk in één van deze scenario's terecht zullen komen; de realiteit zal waarschijnlijk ergens tussen de verschillende toekomstbeelden in liggen en achteraf zal pas met zekerheid kunnen worden gezegd in welke situatie we terecht zijn gekomen. De scenario's dienen vooral het doel om strategische en robuust handelingsperspectief te bieden en voorbereid te zijn op de verschillende manieren waarop de externe wereld zich kan ontwikkelen.

Methode voor de uitwerking van de scenario's

Deze scenario's zijn ontwikkeld op basis van tien kwalitatieve interviews met experts op zowel technologisch als niet-technologisch gebied. Deze experts zijn afkomstig vanuit verschillende kennisinstellingen en andere organisaties. Een pseudo-anoniem overzicht van de interviews kan worden teruggevonden in Bijlage A. De uitkomsten van deze interviews zijn aangevuld met een uitgebreide literatuurstudie. Generatieve AI tools (Elicit, Perplexity en Google NotebookLM) zijn gebruikt om het zoekproces naar relevante literatuur te versnellen, en een lokale versie van Microsoft Copilot is gebruikt voor het samenvatten van de interviewverslagen. De inhoudelijke verwerking en het schrijven van de tekst van dit rapport is volledig gedaan door de auteurs.

In de rest van deze sectie zullen we de vier scenario's verhalend omschrijven aan de hand van een ELSA-raamwerk. In Bijlage B wordt dit raamwerk verder toegelicht, en wordt per ELSA-dimensie uitgelegd wat de belangrijkste aandachtspunten zijn. Ondanks dat de komst van een grootschalige quantumcomputer een breed aantal (civiele) toepassingen met zich meebrengt, zullen we ons inhoudelijk hoofdzakelijk beperken tot de impact van Shor's algoritme. Daarnaast zullen we per scenario een aantal subjectieve indicatoren toevoegen die gebruikt kunnen worden als mogelijke signalen dat we in de richting van een bepaald scenario aan het toe bewegen zijn. Deze indicatoren zijn grotendeels gebaseerd op twee workshops die zijn uitgevoerd in het kader van de Purple Nectar quantum challenges, waaraan ongeveer tien experts hebben deelgenomen. De bevindingen zijn verder aangevuld met inzichten uit publieke en niet-publieke scenariostudies die in het verleden zijn uitgevoerd

door TNO en anderen waarin een soortgelijke setting werd geanalyseerd. [41] Tot slot voegen we ook aan elk scenario een passende analogie toe die helpt bij het tastbaar en herkenbaar maken van het scenario.

2.1 Scenario 1: een uniek strategisch middel voor Nederland

In dit scenario heeft Nederland een unieke positie op militair, economisch en geopolitiek vlak. Door een combinatie van technologische doorbraken is het ons gelukt om als eerste en vooralsnog enige toegang te verkrijgen tot een quantumcomputer die in staat is om op praktische schaal Shor's algoritme uit te voeren. De potentiële impact van Shor's algoritme zal voor landen die wel al over zijn gegaan op quantum-safe encryptie beperkt blijven,[42] ondanks dat zij geen toegang hebben tot een quantumcomputer. De vraag blijft wel tot in hoeverre de migratie naar quantum-safe encryptie volledig voltooid zal zijn voor alle belangrijke digitale systemen in de praktijk, en in welke mate informatie die via de SNDL-strategie is vergaard bruikbaar en nuttig is.

Door deze unieke strategische asset heeft Nederland een competitief voordeel ten opzichte van de rest van de wereld; een uniek *control point*. Met een control point bedoelen we hier een strategische positie binnen een technologische infrastructuur waarbij een actor (Nederland) exclusieve toegang heeft tot een cruciale technologie of capaciteit.[43] In dit geval betekent het dat Nederland in staat is om versleutelde communicatie te lezen, maar ook om zelf berichten te genereren die als authentiek worden beschouwd en afkomstig lijken te zijn van een legitieme partij. Dit biedt een strategisch voordeel, met name in het kader van desinformatie en digitale oorlogsvoering,[44] onder de aanname dat relevante (buitenlandse) communicatie nog niet volledig versleuteld is met quantum-safe encryptie.

Drie belangrijke vragen die in Scenario 1 beantwoord moeten worden zijn: (1) *kunnen* we de quantumcomputer inzetten? Zo ja, (2) *willen* we de quantumcomputer inzetten? En zo ja, (3) willen we de inzet vervolgens *kenbaar* maken? Hier gaan we op in bij de sub-secties over de juridische en ethische dimensie, maar we beginnen eerst bij de geopolitieke en technologische dimensie.

2.1.1 Geopolitieke dimensie

In algemene zin ontstaat er een tijdelijke asymmetrie waarin Nederland een (digitale) informatievoorsprong heeft op anderen, ook al zal de inzet van een quantumcomputer kostbaar en kennis- en tijdsintensief zijn. Hierdoor zullen belangrijke keuzes gemaakt moeten worden wat betreft waar deze quantumcomputer voor wordt ingezet.[45] De dreiging van spionage van andere landen zal toenemen, met name voor sleutelpersonen en bedrijven die de kennis bezitten om de quantumcomputer te ontwikkelen of de toegang hiertoe beheren. Dit omvat zowel de fysieke als digitale beveiliging van deze kritieke assets.[46] De sleutelpersonen kunnen riante salarissen voorgehouden worden door buitenlandse bedrijven, wat momenteel bijvoorbeeld ook zichtbaar is voor toonaangevende experts op het gebied van generatieve AI.[47] Dit kan leiden tot een (nog grotere) wereldwijde technologische wapenwedloop op het gebied van quantumcomputing, waarbij Nederland een enorme opgave zal hebben om de voorsprong te behouden. Inzetten op kennisveiligheid is hierbij een belangrijk aandachtspunt.

Aan de andere kant zullen buitenlandse bedrijven en overheden graag met Nederlandse spelers willen samenwerken om toegang te krijgen tot cruciale kennis. Dit maakt Nederland

een centrale speler in het internationale krachtenveld. In ruil hiervoor zouden we interessante kennis en intelligence van anderen kunnen ontvangen: zo kan een buitenlandse statelijke actor gevoelige data hebben vergaard, die vervolgens in of door Nederland kan worden ontsleuteld. Vooral als veel landen op de achtergrond de SNDL-strategie hebben toegepast, zal er veel interessante data klaarliggen die landen graag willen ontcijferen om hun kennispositie te versterken.

De quantumcomputer kan tenslotte worden ingezet om economische spionage te plegen. Dit zou Nederland potentiële toegang geven tot handelsgeheimen, financiële gegevens en intellectueel eigendom van andere landen en hun bedrijven.[42] Het resultaat is een potentieel aanzienlijk economisch voordeel, maar tegelijkertijd ook een geopolitiek risico voor Nederland als andere landen dit ontdekken. Tegelijkertijd zou de bestaande cybersecuritymarkt ingrijpend kunnen worden verstoord wanneer de vraag naar PQC (en QKD) oplossingen explodeert, wat een marktkans kan bieden aan andere Nederlandse bedrijven die opereren in dit domein.

2.1.2 Technologische dimensie

De mogelijkheid om digitale communicatie van andere landen te onderscheppen, kan verregaande gevolgen hebben op verschillende niveaus. Aangezien militaire netwerken over het algemeen goed beveiligd zullen zijn, bijvoorbeeld door middel van symmetrische encryptie, zullen met name civiele netwerken van andere landen risico lopen. Denk hierbij aan Internet of Things (IoT) -devices zoals drones, kritieke infrastructuur of (sociale) medianetwerken waarvan de communicatie onderschept en eventueel zelfs gemanipuleerd kan worden, wat tot grote maatschappelijke schade en onrust kan leiden.[42] Hierdoor is de verwachting dat de focus op quantum-safe encryptie bij andere landen zal toenemen.

Landen die niet beschikken over een quantumcomputer zullen waarschijnlijk aanzienlijke middelen inzetten om hun eigen quantumtechnologie programma's te ontwikkelen of uit te breiden, of alternatieve vormen van verdediging en afschrikking aan te schaffen. Daarnaast zullen buitenlandse bedrijven en overheden in de rij staan om met Nederlandse partijen samen te werken om toegang te krijgen tot cruciale (technische) kennis, wat economische kansen kan bieden. Tegelijkertijd zal er binnen onze eigen landsgrenzen aanzienlijke middelen moeten worden gemobiliseerd om deze technologische voorsprong te behouden en uit te breiden. Eén enkele quantumcomputer zal naar verwachting namelijk niet voldoende zijn om aan alle vraag te voldoen.

De unieke toegang tot een quantumcomputer brengt ook organisatorische afwegingen met zich mee, met name rondom wie recht heeft en prioriteit krijgt om deze in te zetten. Indien een organisatie zelf volledig beheer heeft over de quantumcomputer, kan zij bepalen wanneer en voor welke doeleinden deze wordt ingezet. Wanneer de quantumcomputer echter in beheer is door een andere partij, zoals een bedrijf of publiek-private samenwerking, zullen afspraken moeten worden gemaakt over het gebruik hiervan.

Een relevant voorbeeld voor een publiek-private governance is het gedeelde gebruiksmodel van EuroHPC (de European High-Performance Computing Joint Undertaking). Hierbij zijn de systemen eigendom van EuroHPC, maar worden ze gehost in nationale datacenters. Capaciteit wordt verdeeld via publieke tenders, primair gericht op wetenschappelijk onderzoek, innovatie en industriële toepassingen. Projecten worden geselecteerd via *peer review* met duidelijke onafhankelijkheidsregels en gelijke vertegenwoordiging.[48] Toegang voor organisaties zou in dit geval mogelijk kunnen zijn via samenwerking met civiele onderzoeksinstellingen of via *Strategic* of *Emergency Access*, onder toezicht van de

EuroHPC Governing Board.[49] Hostingovereenkomsten bepalen dat maximaal 50% van de capaciteit van een quantumcomputer wordt toegewezen aan Europese onderzoeksprojecten (open competitie) en industriële gebruikers (kostenmodel), en de rest aan het gastland (meestal 15–20% gegarandeerd) of -consortium. Alle gebruikers moeten een gebruiksovereenkomst ondertekenen en voldoen aan EU-wetgeving en ethische richtlijnen. Toepassingen die strijdig zijn met Europese regelgeving of internationale verdragen zijn niet toegestaan. Eventuele toeegang is dus afhankelijk van politieke besluitvorming, naleving van EU-regels en aansluiting bij civiele onderzoeksagenda's.

2.1.3 Juridische dimensie

Het antwoord op de vraag of we een quantumcomputer *kunnen* inzetten zal hoofdzakelijk afhangen van of de juridische kaders op dat moment voldoende draagvlak bieden om Shor's algoritme in te zetten. Al in 2020 werd opgeroepen dat nieuwe juridische kaders nodig zouden zijn voor quantumcomputers, waarbij een balans moet worden gevonden tussen nationale veiligheid enerzijds en het recht op privacy en de vrijheid van meningsuiting anderzijds. [43] Het juridische kader voor de Nederlandse veiligheidsdiensten, de Wiv2017, is in principe technologie-agnostisch wat betreft de manier waarop onderschepte data ontsleuteld wordt, [50] maar verder onderzoek is nodig of deze wet ook specifiek toereikend is voor de inzet van quantumcomputers voor het verkrijgen van intelligence, inclusief via de SNDL-strategie. Wanneer de Wiv de komende tien jaar vernieuwd wordt, is het belangrijk om de komst van quantumcomputers hierbij expliciet mee te nemen om voorbereid te zijn op drie van onze vier scenario's.

Hiernaast zal de druk op het economische veiligheidsbeleid van Nederland (en wellicht in het verlengde van de EU) enorm toenemen. Specifiek zullen de Wet Vifo, Exportcontrole en Kennisveiligheid worden ingezet als middel om onze unieke positie te beschermen.[5] Zo zullen buitenlandse investeringen in, of overnames van, de Nederlandse bedrijven die betrokken zijn bij de ontwikkeling of beheer van de quantumcomputer waarschijnlijk worden geblokkeerd, zal de export van cruciale componenten en de bijbehorende kennis strengt worden gecontroleerd, en zullen zichtbare en onzichtbare maatregelen worden genomen om te voorkomen dat cruciale kennis weglekt naar het buitenland.

2.1.4 Ethische dimensie

Het antwoord op de tweede vraag (*willen* we de quantumcomputer inzetten) zal naast geopolitiek ook van ethische kwesties afhangen. Nederland kan ervoor kiezen een ethische norm te stellen door de technologie niet in te zetten omwille van bijvoorbeeld privacybescherming en internationale verantwoordelijkheid – ook wel bekend als *norm engineering*. Het voeren van een maatschappelijke discussie hierover zal echter complex zijn, met name in het begin wanneer onze toegang tot een quantumcomputer niet breed bekend is. Daarnaast kan een gebrek aan transparantie rondom de inzet van Shor's algoritme en de bijbehorende verantwoordelijkheid en risico op misbruik ethische punten van zorg met zich meebrengen. Uiteindelijk zullen de waarden en uitgangspunten van de betrokken organisaties en eventuele andere (mede-)eigenaren van de quantumcomputer centraal staan bij het maken van dergelijke afwegingen.

Het antwoord op de derde vraag (willen we de inzet *kenbaar* maken) zal afhangen van hoe we verschillende geopolitieke, ethische, juridische en sociale belangen afwegen in het kader van transparantie. Al hoewel het op grote schaal verkrijgen van data waarschijnlijk sporen zal achterlaten, is het in principe niet traceerbaar of en wanneer reeds onderschepte versleutelde informatie ontcijferd wordt met een quantumcomputer,[51] waardoor het gebruik

hiervan in eerste instantie ongemerkt zal blijven. Pas in de loop van de tijd zal dit (indirect) worden opgemerkt wanneer eerder ontoegankelijke informatie plotseling toegankelijk is voor anderen.

2.1.5 Sociaal-maatschappelijke dimensie

De unieke toegang tot een quantumcomputer kan zich uiten in een verlies van of verschuiving in vertrouwen tussen burgers, bedrijven, overheden en internationale partners, met name wanneer het onduidelijk is of en wanneer deze technologie wordt ingezet. Zowel overheden als burgers zonder toegang tot een quantumcomputer worden geconfronteerd met het vooruitzicht dat hun persoonlijke gegevens, financiële informatie en digitale privécommunicatie door Nederland blootgesteld kunnen worden. Dit leidt mogelijk tot wantrouwen, angst een afname van het gebruik van digitale diensten. Internationale rechtbanken hebben in verschillende rechtszaken zelfs bepaald dat alleen al de dreiging van surveillance kan resulteren in een schending van het recht tot privacy.[43] Het vermogen om geheimen bloot te leggen kan bovendien worden gebruikt om de publieke opinie te manipuleren of politieke rivalen te ondermijnen. Wanneer breed bekend wordt dat Nederland een quantumcomputer in handen heeft, kan al met al dus leiden tot significante maatschappelijke spanning en discussie.

2.1.6 Mogelijke indicatoren

In Scenario 1 is er sprake van een toegenomen internationale belangstelling voor toegang tot Nederlandse kennis en bedrijven, waarbij zowel bedrijven als statelijke actoren openlijk en achter de schermen interesse tonen. Tegelijkertijd worden er vanuit Nederland nieuwe of strengere exportcontrolemaatregelen rondom quantumtechnologie ingevoerd, die mogelijk onder internationale druk verder worden aangescherpt. Daarnaast worden mogelijk bestaande of nieuwe beleidsinstrumenten ingezet om strategische kennis en expertise zoveel mogelijk binnen Nederland te behouden.[52]

Analogie voor Scenario 1: de Enigma machine

De parallellen met de Enigma-machine tijdens de Tweede Wereldoorlog zijn treffend, ondanks dat de ontwikkeling van deze technologie in oorlogstijd plaatsvond. De Enigma-machine kon gebruikt worden om beveiligde communicatie van het Nazi regime in Duitsland te ontsleutelen. Deze technologische informatievoorsprong werd geheim gehouden, wat allerlei morele, ethische, technologische en maatschappelijke dilemma's met zich meebracht. Zo werd ervoor gekozen om niet op alle ontsleutelde berichten te acteren door de noodzaak om de decryptie mogelijkheden geheim te houden.[53] Dit betekende dat men soms bewust aanvallen liet doorgaan, met alle gevolgen van dien. Tegelijkertijd werd er op grote schaal data vergaard via spionage of diefstal, wat werd gelegitimeerd door het verkorten van de oorlog en het redden van levens. De mensen die betrokken waren bij de decryptie worstelde met hun plichtsbesef tegenover de gevolgen van hun handelen, waarbij het bewaren van geheimhouding soms zwaarder woog dan het direct redden van mensenlevens. Technologisch gezien leidde de Enigma-machine tot een voortdurende wapenwedloop, waarbij elke doorbraak snel werd ingehaald door maatregelen van de tegenpartij. Dit vereiste een combinatie van hoogtechnologische en schaarse kennis van onder andere wiskundigen, ingenieurs en informatici, waarbij operationele uitdagingen ontstonden rondom geheimhouding. Zelfs na de oorlog bleef de vraag wanneer en hoe deze successen openbaar gemaakt moesten worden een punt van discussie, met implicaties voor het maatschappelijk vertrouwen in instituties.[54]

2.2 Scenario 2: Mutually Assured Decryption

In dit scenario beschikken zowel Nederland als andere landen over een quantumcomputer die in staat is om op praktische schaal Shor's algoritme uit te voeren. De wereld is hiermee een nieuwe fase van geopolitieke en technologische rivaliteit binnengetreden, waarin decryptie van de huidige gangbare cryptografische protocollen een strategisch machtsmiddel is geworden. Anders dan bij kernwapens, waarvan het bezit en gebruik zichtbaar en verifieerbaar is, is het gebruik van Shor's algoritme niet (direct) traceerbaar of zichtbaar. Dit creëert een fundamenteel andere dynamiek: een wereld waarin niemand zeker weet of gangbare digitale communicatie nog veilig is, zolang deze nog niet is gemigreerd naar quantum-safe encryptie.

2.2.1 Geopolitieke dimensie

De geopolitieke verhoudingen worden in deze situatie over het algemeen instabieler. De inzet van de quantumcomputer wordt een strategisch machtsmiddel, waarbij landen (een deel van) elkaars digitale communicatie kunnen inzien. Als landen niet tijdig zijn overgegaan op quantum-safe encryptie creëert dit een fragiel evenwicht: landen moeten overwegen of ze terughoudend zijn bij het inzetten van hun quantumcomputer (voor zover dit kenbaar is of wordt gemaakt) uit angst voor vergelding en het risico op misverstanden, escalatie en wantrouwen neemt toe.[55,56]

Er is enigszins een analogie met de "mutually assured destruction" (MAD) situatie uit de Koude Oorlog (zie kader aan het eind van deze sectie), maar in plaats van nucleaire vernietiging gaat het hier om het blootleggen van informatie: "mutually assured *decryption*". Door grootschalige toepassing van de SNDL-strategie zal er gevoelige informatie uit het verleden openbaar kunnen worden gemaakt, wat kan leiden tot politieke schandalen en diplomatieke druk.

Bij de klassieke MAD-situatie met kernwapens werkt afschrikking doordat landen openlijk laten zien dat ze over vernietigende capaciteit beschikken. Die zichtbaarheid zorgt voor een balans: niemand durft aan te vallen, omdat iedereen weet dat er vergelding volgt. Bij quantumdecryptie is dat anders. De inzet van een quantumcomputer is moeilijk te detecteren, waardoor landen niet weten of en wanneer hun communicatie wordt afgeluisterd of gemanipuleerd. Dit vergroot de onzekerheid en kan leiden tot instabiliteit.[57]

In dit scenario kan het heimelijk houden van het bezit of gebruik van een quantumcomputer voor landen een strategisch voordeel bieden. Zo voorkomt het dat andere landen versneld overstappen op quantum-safe encryptie en vergroot het de kans op succesvolle interceptie. Daarnaast is politieke druk door het openbaar maken van gevoelige informatie alleen effectief zolang die informatie nog niet publiek is. In tegenstelling tot klassieke MAD is er hier sprake van een heimelijke, asymmetrische vorm van afschrikking.

Net als bij kernwapens zal er waarschijnlijk een vorm van "treaty governance" ontstaan zodra publiek bekend is dat meerdere landen een quantumcomputer hebben: internationale verdragen kunnen worden opgesteld waarin landen onderling afspraken maken over het gebruik, de inzet en de controle van quantumcomputers.[58] De haalbaarheid van zulke verdragen hangt sterk af van of het gebruik in de praktijk effectief gecontroleerd kan worden, wie de betrokken partijen zijn en welke internationale gremia het meeste draagvlak hebben wanneer de verdragen worden opgesteld. Als het gaat om landen met gedeelde waarden, zoals (momenteel) de NAVO- of EU-lidstaten, is samenwerking waarschijnlijker dan wanneer vanuit ons perspectief risicolanden betrokken zijn. In dat laatste geval zal de dynamiek meer

worden bepaald door *realpolitik* dan door gedeelde waarden, waarbij een coalitie van leidende landen (vergelijkbaar met de VN-Veiligheidsraad) de spelregels kunnen bepalen.

Nederland bevindt zich in dit scenario in een complex krachtenveld. Het heeft als een van de koplopers toegang tot een strategische technologie, maar tegelijkertijd is het als klein land afhankelijk van anderen voor internationale samenwerking en afspraken. De technologische voorsprong geeft ons invloed, maar alleen als Nederland ook actief samenwerkt met partners door te investeren in *soft power*, diplomatieke en politieke netwerken en standaardisatie-initiatieven binnen internationale fora.

2.2.2 Technologische dimensie

De technologische wapenwedloop zal in dit scenario in volle gang zijn. Landen investeren massaal in het opschalen van hun quantumcomputers, het verder verbeteren van foutencorrectie en het optimaliseren van algoritmen. Daarnaast zal er forse concurrentie plaatsvinden tussen bedrijven wereldwijd voor het verkrijgen van control points binnen internationale waardeketens. Tegelijkertijd zal de PQC (en QKD) markt wereldwijd een enorme versnelling doorgaan, nu de dreiging van de inzet van Shor's algoritme reëel en op grote schaal aanwezig is. Nieuwe encryptiestandaarden zullen (halsoverkop) door grote bedrijven en overheidsorganisaties worden geïmplementeerd, maar de adoptie zal in de praktijk niet overal even snel gaan. Vooral digitale handtekeningen en verouderde systemen zullen lastig te migreren zijn.[19]

De kans is groot dat de huidige koplopers zowel op het gebied van quantum computing als quantum-safe cryptografie in de toekomst in handen zullen hebben, zoals de VS, het VK, een aantal EU-landen, China, Japan, Canada en Australië. Zij kunnen door deze voorsprong hun economische positie versterken door gebruik te maken van (disruptieve) quantumcomputing applicaties naast Shor's algoritme en betere beveiliging van hun digitale netwerken, terwijl minder ontwikkelde landen afhankelijk zullen blijven van buitenlandse technologie. Dit vergoot het risico op een mondiale *digital divide*; een digitale kloof tussen landen met en zonder toegang tot deze technologie.[59]

Nederland zal, in navolging van Europese en nationale richtlijnen, zijn kritieke digitale infrastructuur grotendeels gemigreerd hebben naar quantum-safe encryptie, maar blijft kwetsbaar voor SNDL-aanvallen op data die eerder vergaard is. De inzet van quantumcomputers beperkt zich bovendien niet tot decryptie: ook civiele toepassingen binnen de optimalisatie, AI en materiaalontwikkeling worden belangrijker, zowel voor civiel en militair gebruik. Dit vraagt, naast internationale verdragen over het gebruik van quantumdecryptie, ook om technische maatregelen om misbruik van bepaalde applicaties door kwaadwillende te voorkomen.[60] Zo kunnen er technische maatregelen worden genomen en verplichtingen worden gesteld om quantumalgoritmes te screenen om ongewenste toepassingen te blokkeren en kan de toegang tot quantumcomputers via de cloud worden beperkt tot selecte gebruikers. Daarnaast zullen in internationaal verband afspraken moeten worden gemaakt over wie toegang krijgt tot de rekenkracht van quantumcomputers en onder welke voorwaarden, bijvoorbeeld binnen de NAVO Communication and Information Agency.

2.2.3 Juridische dimensie

Nationale en internationale juridische kaders staan in dit scenario onder druk. Bestaande wetgeving die raakt aan zowel economische- als nationale veiligheid zullen deels ontoereikend zijn en moeten worden aangepast door het dual-use karakter van quantumcomputing. In dit scenario zal wetgeving rondom exportcontrole een belangrijke rol

spelen. Regels zoals het Amerikaanse International Traffic in Arms Regulations (ITAR) hebben een extraterritoriale werking en zouden de uitwisseling van quantumtechnologie en gerelateerde componenten sterk kunnen beperken.[61] In combinatie met andere wetgeving rondom economische- en nationale veiligheid zal internationale samenwerking juridisch complexer worden, zeker wanneer quantumtechnologie in grotere mate wordt aangemerkt als strategisch of veiligheidsgevoelig.

In het algemeen zullen er nationaal en internationaal verdragen en wetgeving moeten worden opgesteld voor onder andere de toegang tot quantumcomputers (bv. via clouddiensten) en de inzet van quantumcomputers voor zowel civiel en militair gebruik. Wetgeving zal in de praktijk echter complex zijn om te handhaven, omdat quantumcomputers inherent stochastisch zijn en deels fungeren als *black box*. De toepassing van zogeheten “blind quantumcomputing” protocollen stellen gebruikers bovendien in staat om algoritmes uit te voeren zonder dat de server kan achterhalen welke berekening wordt uitgevoerd.[62]

Nederland zal vanwege haar positie als relatief klein land binnen internationale fora waarschijnlijk pleiten voor nieuwe verdragen, vergelijkbaar met het non-proliferatieverdrag, en tegelijk nationale wetgeving ontwikkelen die inzet reguleert op basis van proportionaliteit en noodzakelijkheid.[63] Een vergelijkbare situatie is van toepassing voor het gebruik van uranium: een grondstof die zowel civiel kan worden ingezet voor energieopwekking in kernreactoren, als militair voor de productie van kernwapens.[64] Dit vereist specifieke verdragen waarin het gebruik, de verspreiding en de toegang worden gereguleerd.[65] De snelheid van technologische ontwikkeling gaat over het algemeen in de praktijk vaak sneller dan wetgeving kan bijbenen. Bij snelle technologische doorbraken rondom quantumcomputers, zal de druk toenemen op overheden om quantum-safe encryptie (vervroegd) verplicht te stellen en hun zorgplicht richting burgers en bedrijven waar te maken.

2.2.4 Ethische dimensie

De ethische dilemma’s in dit scenario zijn complex en gelaagd. Net als in Scenario 1 raakt de inzet van quantumdecryptie fundamentele waarden zoals privacy, autonomie en gelijkheid. Als meerdere landen toegang hebben tot deze technologie, dreigt een normalisering van grootschalige surveillance en informatie-extractie. De drempel voor misbruik daalt, zeker wanneer ethische normen ontbreken of niet worden gehandhaafd.

Nederland staat voor de keuze: volgt het de internationale trend, of probeert het een ethische standaard te zetten? Dit vraagt om een expliciete strategie voor verantwoord innoveren, gebaseerd op de SEA-principes (Safeguarding, Engaging, Advancing).[66] Daarbij is het van belang om ethiek niet pas achteraf toe te voegen, maar al vanaf het beginstadium te integreren in het ontwerp, gebruik en toezicht op quantumcomputers. Juist in deze vroege fase worden fundamentele keuzes gemaakt over functionaliteit, toegankelijkheid en controlemechanismen. Als ethiek pas later wordt ingebracht, is het vaak moeilijker om ongewenste effecten te corrigeren of ingebouwde risico’s te mitigeren.[67]

Door de technologische voorsprong van enkele koplopers dreigt de wereld zich op te splitsen in machtsblokken met ongelijke toegang tot quantumtechnologie. Landen buiten deze blokken, met name in de *global south*, worden mogelijk uitgesloten van besluitvorming, samenwerking en veilige communicatie. Dit vergroot de *digital divide* en ondermijnt fundamentele waarden zoals solidariteit, gelijkheid en inclusiviteit. Ethisch gezien is dit zorgwekkend: het creëert een asymmetrisch speelveld waarin kwetsbare landen afhankelijk blijven en het risico op misbruik en mondiale instabiliteit toeneemt.[68]

2.2.5 Sociaal-maatschappelijke dimensie

Evenals in Scenario 1, leidt het besef dat meerdere landen in staat zijn om huidige en historische versleutelde communicatie te ontsleutelen tot het afnemen van vertrouwen in digitale systemen. Burgers, bedrijven en overheden worden ook hier geconfronteerd met de mogelijkheid dat hun data, van medische dossiers tot politiek-gevoelige communicatie, niet langer veilig zijn. Dit leidt tot onzekerheid, angst en mogelijk zelfs een terugval in digitale adoptie, vergelijkbaar met de maatschappelijke reactie op de Snowden-onthullingen.[69] Tegelijkertijd groeit de behoefte aan transparantie, educatie en publieke betrokkenheid. “Quantumgeletterdheid” wordt een strategische noodzaak: niet alleen voor beleidsmakers, maar ook voor burgers. Nederland zal moeten inzetten op bewustwording en samenwerking met maatschappelijke partners om het vertrouwen in digitale veiligheid te behouden. Overheden wordt aanbevolen te investeren in bewustwordingscampagnes om duidelijk te maken wat de kansen en risico’s van quantumcomputers zijn en dat quantum-safe encryptie adequate verdediging biedt tegen Shor’s algoritme.[70]

2.2.6 Mogelijke indicatoren

In Scenario 2 zien we een aanhoudende en exponentieel groeiende stroom van wetenschappelijke publicaties, waarbij de factoringschalen steeds verder oplopen. Dit patroon kan worden onderbroken door plotselinge stiltes bij koplopers, wat duidt op strategische terughoudendheid of geheimhouding. Tegelijkertijd versnellen internationale PQC-standaarden en migratieprogramma’s, waardoor organisaties wereldwijd hun digitale infrastructuur aanpassen aan de nieuwe eisen van quantumveiligheid. Op marktniveau vindt er consolidatie plaats, waarbij vooral de spelers met een technologische voorsprong hun positie versterken door middel van strategische acquisities en fusies. Internationale barrières worden aangescherpt om nationale en economische veiligheid te waarborgen, bijvoorbeeld door strengere exportcontrolemaatregelen. Daarnaast neemt het aantal landen toe dat doorbraken op het gebied van quantumtechnologie claimt te hebben gerealiseerd, hoewel deze claims niet altijd verifieerbaar zijn.

Analogie voor Scenario 2: mutually assured destruction

De proliferatie van quantumcomputers vertoont parallellen met het Koude Oorlog-concept van mutually assured destruction (MAD).[44] Waar MAD stabiliteit bracht via wederzijdse nucleaire dreiging, ontstaat bij quantumcomputing een soort digitale variant hierop. Staten ontwikkelen quantumcapaciteiten uit angst dat anderen hen voor zijn, wat leidt tot een strategische wapenwedloop. Quantumcomputing kan hierbij zowel als wapen als afschrikmiddel dienen: het vermogen om encryptie te breken creëert een dreiging van wederzijdse blootstelling van gevoelige informatie. Dit kan de machtsbalans en diplomatieke invloed verschuiven in het voordeel van de landen die toegang hebben tot een quantumcomputer. Daarnaast kan de technologische wapenwedloop vooruitgang versnellen, vergelijkbaar met de innovatiedruk tijdens de nucleaire competitie. Dit zal verder worden versterkt door de economische potentie van quantumcomputing, vergelijkbaar met hoe nucleaire technologie ook kan worden ingezet voor energieopwekking. De inzet van quantumcomputers is echter niet fysiek destructief of detecteerbaar, wat attributie en vergelding moeilijker maakt. Het strategisch verzwijgen van het bezit of gebruik van quantumdecryptie capaciteit om het voordeel van onopgemerkte toegang tot informatie te behouden en de reactie van andere landen (zoals versnelde PQC-migratie) te voorkomen wordt denkbaar. Ondanks dat quantumcomputers bij lange na niet dezelfde apocalyptische dreiging vormen als kernwapens, spelen vergelijkbare strategische keuzes een rol bij de inzet hiervan.

2.3 Scenario 3: in de schaduw van grootmachten

Scenario 3 schetst een situatie waarin Nederland geen toegang heeft tot een quantumcomputer die Shor's algoritme kan uitvoeren, terwijl andere landen dit wel hebben. In deze toekomst is er sprake van een mogelijke externe dreiging, en zijn we als Nederland afhankelijk van anderen voor de toegang tot een quantumcomputer. Het mitigeren van risico's, waarbij migratie naar quantum-safe cryptografie en samenwerking met andere landen centraal staat, zal in dit scenario van groot belang zijn.

2.3.1 Geopolitieke dimensie

In deze toekomst worden we geconfronteerd met een geopolitieke afhankelijkheid en een noodzaak tot strategisch manoeuvreren. Als de migratie naar quantum-safe encryptie achterloopt, zal het gebrek aan toegang tot een quantumcomputer de diplomatieke positie van Nederland ten opzichte van de landen die dit wel hebben relatief verzwakken. Met name als belangrijke onderdelen van onze diplomatieke communicatie en bijbehorende documenten en staatsgeheimen niet adequaat beveiligd zijn tegen de dreiging van Shor's algoritme komt onze internationale machts- en onderhandelingspositie onder druk te staan. In geopolitieke zin zijn we in deze situatie eerder "speelbal" dan "spelverdeler".[71]
Dit zal met name gelden in de situatie waarin niet-partnerlanden toegang hebben tot een quantumcomputer, zoals China. Bij partnerlanden zoals Duitsland is deze dreiging minder groot, en zal vooral de samenwerking opgezocht moeten worden, bijvoorbeeld binnen EU- of NAVO-verband. In het begin is de kans echter groot dat nationale belangen voorop zullen staan voor de landen die een quantumcomputer in bezit hebben, waardoor kennisdeling en toegang tot buitenlandse quantumcomputer(s) naar verwachting zal worden beperkt.

2.3.2 Technologische dimensie

Doordat we zelf geen toegang hebben tot een volledig werkend quantumcomputing systeem, zullen we als Nederland met name opzoek moeten gaan naar control points op het gebied van applicaties, algoritmes en/of (technologische) componenten. Hiermee kunnen we indirect technologische en economische invloed uitoefenen op de landen die wel toegang hebben tot een quantumcomputer. Zo is ASML als systeemintegrator van lithografiesystemen nog steeds afhankelijk van het Duitse Zeiss en Trumpf voor de productie van respectievelijk spiegels en lasers.[72] De druk op onze kennisinstellingen en bedrijven zal naar verwachting toenemen wanneer duidelijk wordt dat andere landen op ons voorlopen. Tegelijkertijd kan het besef dat we achterlopen leiden tot een verlies van vertrouwen in deze organisaties.

De migratie naar quantum-safe encryptie is extra urgent in dit scenario, maar zal in de praktijk complex zijn, vooral voor (niche)apparaten van externe leveranciers zoals IoT-devices. Daarnaast is een extra complicerende factor dat de effectieve werking en doorontwikkeling van post-quantum cryptografie algoritmes niet gevalideerd kan worden doordat wij de toegang missen tot de quantumcomputing kracht die hiervoor nodig is. Veel van de macht voor de uitrol van quantum-safe encryptie zal liggen bij BigTech bedrijven die een groot deel van onze digitale (communicatie) infrastructuur voorzien, en die buiten het machtsbereik van Nederland vallen. We zullen gebaat zijn bij het versnellen van standaardisatie om markttoegang te vergroten, en zullen waar nodig (op grote schaal) moeten overstappen op dienstverleners die expliciet en verifieerbaar quantum-safe encryptie waarborgen. In uiterste gevallen kan zelfs worden overwogen terug te keren naar vormen van niet-digitale communicatie om de dreiging van de quantumcomputer de omzeilen.

2.3.3 Juridische dimensie

Juridisch gezien zal in Scenario 3 de druk toenemen om de ontwikkeling van wet- en regelgeving te versnellen, met name ter verdediging van onze belangen. Binnen Nederland zal dit hoofdzakelijk gaan om de migratie naar quantum-safe cryptografie ter bescherming van onze privacy en vertrouwelijke communicatie, terwijl Nederland internationaal druk kan uitoefenen om wetgeving te vormen voor het gebruik van quantumcomputers (en wellicht Shor's algoritme in het specifiek). Onze invloed op dit laatste kan echter beperkt zijn doordat wij zelf geen toegang tot een quantumcomputer hebben. Het voortouw hiervoor zal waarschijnlijk worden genomen door de groep landen die wel toegang hebben tot deze asset, voor zover deze dit openlijk bekend maken. Hierbij kunnen ze mogelijk barrières opwerpen voor anderen landen om de technologie verder te ontwikkelen voor militaire doeleinden, zoals nu ook wordt voorgeschreven in het non-proliferatieverdrag voor nucleaire technologie.[73] Dit kan een significante impact hebben op de positie van Nederlandse bedrijven en kennisinstellingen.

2.3.4 Ethische dimensie

De mogelijkheid dat verouderde en/of huidige digitale communicatie kan worden ontsleuteld door andere landen kan leiden tot een vertrouwensbreuk in de samenleving. Burgers en organisaties kunnen zich genoodzaakt voelen hun communicatiegedrag aan te passen, wat leidt tot veranderende waarden en mogelijke polarisatie. De druk op de overheid om privacy van burgers te waarborgen zal toenemen, waardoor er ethische afwegingen moeten worden gemaakt over de mate waarin de Nederlandse overheid openlijk communiceert over de (mogelijke) dreiging en de impact van Shor's algoritme. Dit zal wederom mede afhangen van of de landen die toegang hebben tot een quantumcomputer bevriende staten zijn of risicolanden.

2.3.5 Sociaal-maatschappelijke dimensie

Sociaal-maatschappelijk heeft Scenario 3 verstrekkende gevolgen. De dreiging dat verouderde en/of huidige digitale communicatie openbaar wordt gemaakt door statelijke actoren kan tot maatschappelijke onrust leiden en in het algemeen tot wantrouwen in de overheid en digitale systemen. Burgers en organisaties zullen zich aanpassen door ofwel de nieuwe realiteit te accepteren, ofwel terug te vallen op oudere niet-digitale vormen van communicatie.

Daarnaast zal Nederland ook een mogelijke economische achterstand oplopen door het gebrek aan een quantumcomputer. Dit zal niet alleen een gevolg zijn van economische spionage van anderen waardoor onze eigen technologische kennis en concurrentiepositie kan worden ondermijnd,[74] maar ook doordat andere landen eerder de (civiele) toepassingen van quantumcomputers in de praktijk kunnen brengen, waarmee de bijbehorende bedrijven een *first-mover advantage* zullen hebben.[75] De urgente dreiging om over te gaan op quantum-safe encryptie zal daarnaast om een significante overheidsinvestering vragen, waardoor de druk op andere overheidsdossiers zal toenemen.

2.3.6 Mogelijke indicatoren

In Scenario 3 worden afwijkende patronen zichtbaar die kunnen wijzen op het (retrospectief) ontsleutelen van digitale communicatie. Tegelijkertijd ontstaan er steeds grotere barrières rondom kennisdeling en de toegang tot buitenlandse leveranciers en klanten, wat de internationale samenwerking bemoeilijkt. Daarnaast is er sprake van een afnemende economische en kennispositie van Nederlandse bedrijven en kennisinstellingen, doordat zij minder toegang hebben tot cruciale technologieën en markten.

Analogie voor Scenario 3: onze afhankelijkheid van het Amerikaanse GPS

Nederland en andere Europese lidstaten zijn lang afhankelijk geweest van het Amerikaanse global positioning system (GPS) voor navigatie.[76] Deze technologie is sinds de jaren 80 het fundament gaan vormen van een significant deel van onze civiele- en militaire infrastructuur, waardoor het van groot belang is voor zowel onze economische als nationale veiligheid om hiertoe toegang te hebben. De uiteindelijke zeggenschap van de navigatiesystemen ligt echter buiten ons bereik, waardoor we onderaan de streep afhankelijk zijn van anderen en onze toegang door geopolitieke spanningen kan worden ontzegd. Pas in 2001 heeft de Europese Unie het Galileo programma gelanceerd met als doel om een eigen satellietsysteem voor navigatie te ontwikkelen, welke vervolgens vijftien jaar later operationeel werd.[77] Dit heeft meer dan €10 miljard gekost. Een soortgelijke situatie kan zich in de toekomst voordoen in de context van quantumcomputers wanneer Nederland en de EU de technologische race verliezen van andere landen en er een afhankelijkheid ontstaat voor kritieke (digitale) infrastructuur.

2.4 Scenario 4: Quantum Winter

In het vierde en laatste scenario is de grote doorbraak van quantumcomputers die Shor's algoritme op relevante schaal kunnen uitvoeren uitgebleven. De technologische race is niet gestopt, maar de wereld verkeert in een soort "quantum winter": de hype is voorbij, investeringen nemen af, en niemand weet of en wanneer een echte doorbraak zal komen. Desondanks blijft de onzekerheid over de toekomst van quantumcomputing een belangrijke

factor in beleid, strategie en innovatie. Landen blijven zich voorbereiden op een mogelijke doorbraak, maar de meeste zullen de prioriteit verleggen naar andere technologiegebieden.

2.4.1 Geopolitieke dimensie

De internationale verhoudingen in de context van quantumcomputers zijn in dit scenario relatief stabiel, maar niet zonder spanning. Omdat niemand een doorslaggevende doorbraak heeft bereikt, blijft de machtsbalans grotendeels onveranderd. Tegelijkertijd blijft de onzekerheid bestaan of dominante spelers zoals China op de achtergrond blijven door ontwikkelen en op een gegeven moment alsnog een doorbraak realiseren. De SNDL-strategie zal hierdoor nog steeds een dreiging vormen.

Voor Nederland biedt dit scenario echter ook kansen. De afgenomen hype, investeringsdruk en acute risico's bieden ruimte om internationaal samen te werken om technische componenten, kennis en infrastructuur verder te ontwikkelen en optimaal te benutten. Hierbij kan de kennispositie van Nederland en de EU behouden blijven of zelfs uitgebreid worden. Met name ten opzichte van regio's waarin de ontwikkeling van quantumcomputers wordt gedreven door de private sector kan dit een voordeel bieden, aangezien commerciële investeerders zich massaal zullen hebben teruggetrokken. In dit scenario is er ook meer ademruimte voor de internationale standaardisatie, doorontwikkeling en implementatie van quantum-safe encryptie, met name voor niet-essentiële digitale communicatiesystemen.

2.4.2 Technologische dimensie

Ondanks de grote hype rondom quantumcomputing, zijn sommige wetenschappers al jaren sceptisch over de fundamentele en praktische haalbaarheid van quantumcomputers.[78] Deze sceptici zullen in dit scenario gelijk hebben gekregen. De afwezigheid van een grote doorbraak betekent echter niet dat de technologische ontwikkeling stilstaat. De grote hoeveelheden middelen die geïnvesteerd zijn in quantumcomputing zullen waarschijnlijk leiden tot (meerdere) spin-off technologieën op het gebied van bijvoorbeeld fotonica of halfgeleiders die eventueel marktpotentie bieden buiten quantumcomputers. In dit scenario ontstaat er ruimte voor open innovatie en fundamenteel onderzoek, waarvan (opkomende) quantumtechnologie met civiele toepassingen profiteren. Daarnaast zal de potentie van grootschalige quantumcomputing applicaties nog steeds overeind kunnen staan, wat kan leiden tot een kleinere maar doorgezette stroom van investeringen. De ontwikkeling van nieuwe technologieën gaat in het algemeen regelmatig in cycli die in totaal tientallen jaren in beslag kunnen nemen, waardoor de hoop nooit helemaal verloren zal gaan (zie ook de analogie met kernfusie in het kader onderaan deze sectie). Het heeft meer dan vijftig jaar geduurd voordat (generatieve) AI modellen op grote schaal werkend zijn in de praktijk,[79] en ook quantumcomputing kan een technologiegebied van de lange adem worden.

2.4.3 Juridische dimensie

In dit scenario is er meer tijd om passende juridische kaders te ontwikkelen en evalueren voor het gebruik van en de verdediging tegen quantumcomputers. De druk om bestaande kaders zoals de Wiv en wetgeving rondom economische veiligheid aan te passen zal afnemen, en er is meer ruimte om internationale afspraken en verdragen over de inzet van quantumcomputing en quantum-safe encryptie te vormen. Toch blijft onzeker of de bestaande wet- en regelgeving toereikend is als quantumcomputers alsnog doorbreken wanneer een gevoel van urgentie mist, en zullen beperkingen op het gebied van bijvoorbeeld exportcontrole waarschijnlijk niet snel teruggedraaid worden. Het is daarom verstandig om

juridische scenario's en aanpassingen klaar te hebben liggen, zodat snel kan worden geschakeld als de situatie verandert.

2.4.4 Ethische dimensie

Ethische vraagstukken rondom het gebruik van quantumcomputers blijven relevant, ook als de doorbraak uitblijft. Transparantie over de (on)mogelijkheden van quantumcomputing is belangrijk om onrealistische verwachtingen en angst te voorkomen, en uit te leggen waarom deze potentie nog niet is waargemaakt. Dergelijke narratieven zullen meer ruimte krijgen wanneer de hype vanuit de private sector is afgenomen. Door de tijd te nemen om ethiek te integreren in ontwerp, gebruik en toezicht op quantumcomputing, kunnen publieke waarden beter worden beschermd.

2.4.5 Sociaal-maatschappelijke dimensie

De uitblijvende doorbraak leidt in dit scenario waarschijnlijk tot afnemende aandacht, investeringen en urgentie bij bedrijven en overheden. Organisaties stellen migratie naar quantum-safe encryptie mogelijk uit, aangezien de dreiging van quantumcomputers is afgenomen en andere zaken prioriteit krijgen. De bedrijven die de migratie desondanks doorzetten, kunnen de tijd nemen om hun digitale hygiëne en bewustwording op peil te brengen. De *digital divide* zal in dit scenario niet verder zijn toegenomen door de komst van quantumcomputers, waardoor er een kans ontstaat voor landen die momenteel minder ver zijn in hun ontwikkeling om bij te benen.

2.4.6 Mogelijke indicatoren

In Scenario 4 zien we dat publicaties en investeringen in de quantumsector vertragen of stagneren, wat ertoe leidt dat bedrijven failliet gaan of worden overgenomen. De aandacht in beleidsdocumenten verschuift naar andere strategische technologieën, waardoor quantum minder prioriteit krijgt. Regionale quantum-ecosystemen, en samenwerkingsverbanden en laboratoria hierbinnen, verliezen hun kritische massa en innovatiekracht, waardoor ze krimpen of zelfs worden opgeheven. Onderzoekers en academici verlaten de quantumsector en stappen over naar aanverwante vakgebieden zoals kunstmatige intelligentie, fotonica of de halfgeleiderindustrie, waardoor organisaties nog meer moeite hebben om talent aan te trekken of te behouden. Tegelijkertijd neemt het aantal studenten dat kiest voor quantum-gerelateerde opleidingen en het aantal openstaande vacatures in de sector structureel af, wat wijst op een verminderde instroom van nieuw talent.

Analogie voor Scenario 4: de ontwikkeling van kernfusietechnologie

Dit scenario heeft parallellen met de ontwikkeling van kernfusietechnologie, waar al sinds de jaren 40 aan wordt gewerkt. Beide zijn zeer complexe technologieën die tot op heden alleen op kleine (test)schaal werkend zijn gekregen. Optimistische toekomstvoorspellingen over het gebruik van kernfusie voor energieopwekking, en de grote impact die dit kan hebben op de wereldwijde economie en machtsverhoudingen, hebben sinds die tijd plaatsgevonden zonder veelbelovend resultaat. De tijdshorizon werd hierbij steeds verder vooruit verlegd.[80] Recent is er een nieuwe cyclus van hoopvolle investeringen gestart en zijn een aantal nieuwe bedrijven opgericht die beloven dat de technologie nu echt op het punt van doorbreken staat, maar het blijft onduidelijk of dit in de praktijk ook zo zal zijn.[81] Uiteindelijk zullen we ook rekening moeten houden met de situatie waarin quantumcomputers over 10 jaar (of meer) hun belofte nog steeds niet hebben waargemaakt.

3 Belangrijkste overeenkomsten en verschillen tussen de scenario's

De vier scenario's die in dit rapport zijn uitgewerkt, bieden uiteenlopende toekomstbeelden voor de inzet en impact van quantumcomputers die Shor's algoritme kunnen uitvoeren. Ondanks hun verschillen zijn er ook duidelijke overeenkomsten zichtbaar. In deze sectie analyseren we beknopt de rode draden en contrasten tussen de scenario's, op basis van de vijf ELSA-dimensies.

Als eerst hebben we in Figuur 3.1 een overzicht gecreëerd van de belangrijkste aspecten per dimensie voor elk scenario. Dit overzicht biedt de mogelijkheid om in één oogopslag de belangrijkste uitkomsten te analyseren en de overeenkomsten en verschillen tussen de scenario's te zien.

Kort samengevat zijn de belangrijkste overeenkomsten:

- Quantum-safe encryptie is in alle scenario's een noodzakelijke investering. Ongeacht of quantumcomputers daadwerkelijk beschikbaar zijn, vormt de migratie naar quantum-safe encryptie een structurele vereiste voor digitale veiligheid.
- Technologische afhankelijkheid en het belang van control points in waardeketens keren in elk scenario terug, maar wel op een ander niveau. Zowel directe toegang tot quantumcomputers als indirecte invloed via componenten, kennisposities en standaarden zijn strategisch relevant.
- Governance en normstelling zijn essentieel om de inzet van quantumcomputing te legitimeren. In elk scenario is er behoefte aan duidelijke kaders voor eigenaarschap, toegang en gebruik.
- Internationale samenwerking speelt een sleutelrol, vooral in scenario's waarin asymmetrische toegang tot quantumcomputers bestaat. Coalitievorming en diplomatieke netwerken zijn cruciaal om strategische autonomie collectief te versterken.
- Sociaal-maatschappelijke impact is in alle scenario's significant. Vertrouwensverlies, gedragsverandering en maatschappelijke onrust zijn terugkerende thema's, die vragen om transparante communicatie en publieke betrokkenheid.

De belangrijkste verschillen zijn:

- Strategische autonomie varieert sterk per scenario. In Scenario 1 heeft Nederland een unieke machtspositie, terwijl in Scenario 3 sprake is van afhankelijkheid en kwetsbaarheid.
- Technologische druk is het hoogst in Scenario 2, waarin een mondiale wapenwedloop ontstaat. Scenario 4 biedt ademruimte voor open innovatie en fundamenteel onderzoek.

- Urgentie van juridische aanpassing is het hoogst in Scenario 1 en 2, waar quantumcomputers operationeel zijn. In Scenario 4 is er juist ruimte voor proactieve en zorgvuldigere voorbereiding.
- Ethiek en transparantie zijn in Scenario 1 en 2 complexer door de mogelijkheid tot heimelijke inzet. Scenario 4 biedt juist ruimte om publieke waarden structureel te integreren.
- De belangrijkste aspecten binnen het maatschappelijk debat varieert van angst en wantrouwen (Scenario 1–3) tot bewustwording en educatie (Scenario 4).

De scenario's verschillen in urgentie, strategische autonomie en maatschappelijke impact, maar tonen allen aan dat quantum-safe encryptie, technologisch leiderschap, adequate governance, internationale samenwerking en maatschappelijke betrokkenheid cruciaal zijn om voorbereid te zijn op elk scenario.

Aspect	Scenario 1: Uniek strategisch middel voor NL	Scenario 2: Mutually Assured Decryption	Scenario 3: In de schaduw van grootmachten	Scenario 4: Quantum Winter
Geopolitiek 	• Tijdelijke informatievoorsprong, internationale druk en spionagerisico neemt toe. • Dilemma: geheimhouden of (openbaar) inzetten?	• Instabiele situatie met heimelijke afschrikking en risico op escalatie • Internationale afspraken nodig voor inzet	• Verslechterde onderhandelingspositie en afhankelijkheid van partnerlanden • Strategische autonomie staat onder druk	• Relatieve stabiliteit en ruimte voor samenwerking en kennisopbouw • Blijvende onzekerheid over (geheime) doorbraken houdt geopolitieke alertheid in stand
Technologisch 	• Nederland heeft een control point in handen • Opschaling en kennisbehoud cruciaal • Regels over toegang en gebruik	• Technologische wapenwedloop met behoefte aan nationale technologiesoevereiniteit • Versnelling van migratie naar quantum-safe encryptie	• Inzetten op control points op het gebied van componenten / subsystemen • Urgentie voor migratie naar quantum-safe encryptie in NL	• Open innovatie en technologische spin-offs • Vertraagde quantum-safe migratie • Ademruimte voor fundamenteel onderzoek
Juridisch 	• Juridische kaders nodig voor inzet en eigenaarschap • Evaluatie en aanscherping van wetgeving rondom nationale en economische veiligheid	• *Dual use* maakt wetgeving en handhaving complex • Behoefte aan non-proliferatie-achtige verdragen	• Focus op defensief beleid • Beperkte invloed op totstandkoming internationale kaders	• Meer tijd voor juridische voorbereiding • Wetgeving kan proactief worden ontwikkeld
Ethisch 	• Norm engineering mogelijk • Afweging tussen strategisch voordeel en publieke waarden	• Normalisering van surveillance dreigt • SEA-principes nodig voor verantwoord innoveren	• Dreiging kan leiden tot gedragsverandering • Dilemma's over transparantie en bescherming van burgerrechten	• Kans op structurele integratie van publieke waarden • Minder hype, meer reflectie • Ethisch ontwerp vanaf de basis beter mogelijk
Sociaal-maatschappelijk 	• Dreiging van surveillance en impact op digitale diensten • Maatschappelijke discussie over geheimhouding complex	• Vergroten van *digital divide* • Behoefte aan "quantumgeletterdheid" • Mogelijke parallellen met Snowden-onthullingen	• Wantrouwen en onrust; terugval op analoge communicatie • Economische achterstand dreigt	• Afnemende hype en mogelijke teleurstelling • Kans op bewustwording en inclusieve ontwikkeling
Analogie	**De Enigma-machine**	**Mutually Assured Destruction (MAD)**	**Afhankelijkheid van het Amerikaanse GPS**	**De ontwikkeling van kernfusie**
	Zoals de geallieerden tijdens WOII de Enigma-code kraakten en dit geheim hielden, staat Nederland voor de keuze: inzetten of onthullen? Geheimhouding kan strategisch zijn, maar ethisch complex.	Net als bij kernwapens leidt wederzijdse dreiging tot afschrikking, maar waar MAD zichtbaar was, kan quantumdecryptie heimelijk worden ingezet, wat de dynamiek fundamenteel verandert.	Nederland is lange tijd afhankelijk geweest het Amerikaanse GPS-systeem, met beperkte controle over kritieke infrastructuur. Een soortgelijke situatie kan ontstaan rondom quantumcomputing.	Net als kernfusie blijft quantumcomputing een belofte die nog niet is waargemaakt. De technologische ontwikkeling kan tientallen jaren nodig hebben, maar de potentie blijft.

Figuur 3.1 Overzicht van de belangrijkste elementen per ELSA aspect voor de verschillende scenario's en bijbehorende analogie.

4 Aanbevelingen voor vervolgonderzoek

De vier scenario's die in dit rapport zijn uitgewerkt, laten zien dat de impact van quantumcomputers sterk afhankelijk is van wie toegang heeft tot deze technologie en in welke mate quantum-safe encryptie tijdig is geïmplementeerd. De scenario-analyse toont aan dat strategische voorbereiding noodzakelijk is, ongeacht het tempo van technologische doorbraken. Zowel juridische, technologische, ethische als sociaal-maatschappelijke dimensies vragen om anticiperende beleidsvorming en handelingsperspectieven.

Hoewel dit rapport zich primair richt op de impact van Shor's algoritme en de strategische implicaties voor Nederland, zijn er meerdere relevante thema's die buiten scope zijn gebleven en vervolgonderzoek verdienen:

- **Internationale waardeketens en control points**
  De ontwikkeling van quantumcomputers is sterk afhankelijk van een complexe internationale waardeketen, waarin hardware, software en infrastructuur samenkomen. Met namen in Scenario 3 is het cruciaal dat Nederland, ook zonder eigen cryptografisch-relevante quantumcomputer, strategische invloed behoudt via control points: componenten en kennisgebieden die moeilijk te omzeilen zijn en leverage bieden in samenwerking en onderhandelingen. Vervolgonderzoek zou zich kunnen richten op vragen als: welke hardware- en softwarecomponenten in de quantumtechnologie waardeketen zijn het meest strategisch voor Nederland om in te investeren? En hoe kan Nederland internationaal invloed uitoefenen om haar positie te versterken?

- **Verdiepende analyse van juridische en ethische kaders**
  Quantumtechnologie stelt bestaande wet- en regelgeving op scherp. Hoe moeten juridische kaders zoals de Wiv 2017, de Wet Vifo en exportcontrole worden aangepast om zowel nationale veiligheid als fundamentele rechten te waarborgen richting de toekomst? Vervolgonderzoek kan zich richten op de toepassing van bestaande juridische en ethische kaders op digitale oorlogsvoering en quantumdecryptie, inclusief de rol van militaire ethiek en internationale oorlogswetgeving. Ook is het belangrijk om te verkennen hoe ethische normstelling kan worden afgestemd met internationale partners en hoe maatschappelijke waarden kunnen worden geborgd in een context van geopolitieke druk.

- **Missiegedreven innovatie**
  Kan Nederland een missiegedreven innovatieaanpak ontwikkelen die niet alleen economische groei stimuleert, maar ook gericht is op het oplossen van grote maatschappelijke uitdagingen zoals digitale veiligheid en strategische autonomie? Dit vraagt om het koppelen van R&D aan concrete missies met duidelijke doelen en tijdslijnen, en om governance- en innovatiemodellen die versnippering voorkomen en samenwerking tussen civiele en militaire domeinen versterken. Hierbij kunnen modellen van het Amerikaanse DARPA en de verdere uitwerking van de Nationale Technologiestrategie worden verkend. Hierbij is het belangrijk om raamwerken te ontwikkelen voor sociaal-maatschappelijke innovatie die publieke dialoog, ethische

normen en participatie structureel integreren, zodat draagvlak en vertrouwen gewaarborgd blijven.

Bijlage A
Overzicht interviews

De onderstaande tabel bevat een pseudo-anoniem overzicht van de personen die wij hebben geïnterviewd voor onze scenario's. In totaal zijn tien interviews van ongeveer een uur uitgevoerd en hiernaast hebben enkele andere experts hun input per email met ons gedeeld.

Organisatie	**Rol**
Ministerie van Defensie	Lead quantumtechnologie
QuiX Quantum	Wetenschappelijk lead, partnership manager
TNO (x4)	Expert quantum computing applicaties Expert post-quantum cryptografie Expert kernwapenstrategie Expert cybersecurity en geopolitiek
Quantum Delta NL	Partnership manager
TU Delft	Professor ethiek
Universiteit van Amsterdam	Professor informatierecht
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties	Quantumtechnologie expert

Als basis voor de interviews hebben we het ESLA-raamwerk van Bijlage B gebruikt. Deze hebben we vervolgens toegespitst op basis van de specifieke expertise van de geïnterviewde. We zijn alle geïnterviewden dankbaar voor hun waardevolle bijdrage.

Bijlage B
ELSA-raamwerk

Het ELSA-raamwerk is ontwikkeld om de impact van Shor's algoritme systematisch te analyseren vanuit verschillende perspectieven, en biedt een gestructureerde basis voor het uitwerken van toekomstscenario's. De afkorting ELSA staat hierbij voor "ethical, legal and societal aspects", welke specifiek zijn aangevuld met technologische en (geo)politieke aspecten. Dit raamwerk is opgebouwd op basis van inzichten uit de literatuur die inzoomen op de verschillende aspecten die de impact van quantumtechnologie beïnvloeden.[82,83,84,85,86]

Doel en opzet

Het ELSA-raamwerk is bedoeld om inzicht te geven in hoe de machts- en informatiepositie van Nederland ten opzichte van andere landen beïnvloed kan worden door de ontwikkeling van quantumcomputers die in staat zijn om Shor's algoritme uit te voeren. Het raamwerk is opgebouwd uit vijf factoren:

(Geo)politieke factoren: De ontwikkeling en inzet van quantumcomputers beïnvloedt internationale machtsverhoudingen en de strategische posities van landen. Hierbij spelen afhankelijkheden, samenwerking en controlemechanismen een belangrijke rol bij het waarborgen van transparantie en het beheersen van technologische export.

Technologische factoren: Vragen rondom de toegang tot quantumcomputers, verantwoord beheer, technische eisen en standaardisatie staan hier centraal. Hierbij wordt aandacht besteed aan de technologische randvoorwaarden, beveiliging van systemen en vitale infrastructuren, evenals dual-use toepassingen en mogelijke indirecte gevolgen van quantumtechnologie.

Sociaal-maatschappelijke factoren: Quantumtechnologie beïnvloedt het vertrouwen van burgers, bedrijven en overheden. Dit aspect analyseert welke stakeholders op welke manier geraakt worden, en wat er op het gebied van communicatie, bewustwording en betrokkenheid nodig is om het vertrouwen tussen burgers, maar ook het vertrouwen van burgers richting de overheid te waarborgen.

Juridische factoren: Hier wordt ingegaan op welke bestaande kaders en regelgeving relevant zijn voor de toepassing van Shor's algoritme. Hierbij wordt gekeken naar (huidige) internationale verdragen, nationale wetgeving en sectorspecifieke regels, en de eventuele behoefte aan nieuwe of aangepaste kaders rondom eigendom, aansprakelijkheid, inzet en toezicht.

Ethische factoren: Quantumtechnologie kan publieke waarden zoals privacy, autonomie, transparantie en gelijkheid onder druk zetten. Dit aspect behandelt op welke manier deze waarden een rol kunnen spelen bij de inzet van Shor's algoritme en welke ethische dilemma's kunnen ontstaan bij asymmetrische toegang tot gevoelige informatie.

Referenties

[1] De Nationale Technologiestrategie | Titel uitgave
[2] Quantum Initiatives Worldwide 2025 - Qureca
[3] Quantum Technology Monitor 2025 | McKinsey
[4] ECI_25_PolicyBrief_06-2025_LY03.pdf
[5] TNO 2025 P11381 - Touwtrekken om technologie
[6] 2025-National-Security-Strategy.pdf
[7] China's National Security in the New Era_Information Office of the State Council of the People's Republic of China
[8] Quantum Computing Roadmaps: A Look at The Maps And Predictions of Major Quantum Players
[9] Quantum computing applications for your organisation
[10] Towards a Dutch Hybrid Quantum/HPC Infrastructure
[11] Supply chain logistics with quantum and classical annealing algorithms | Scientific Reports
[12] Commercial applications of quantum computing - PMC
[13] Industry quantum computing applications | EPJ Quantum Technology | Full Text
[14] Quantum technology for military applications | EPJ Quantum Technology | Full Text
[15] Use Cases – Quantum for Good
[16] Dual-use technologies - European Commission
[17] Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantumcomputer | SIAM Review
[18] Het PQC-migratie handboek | Publicatie | AIVD
[19] Recommendation for Key Management: Part 1 - General
[20] Soms wordt dit ook wel “harvest now, decrypt later” genoemd
[21] Future-Proofing Data: Assessing the Feasibility of Post-Quantum Cryptographic Algorithms to Mitigate ‘Harvest Now, Decrypt Later’ Attacks
[22] Venona project - Wikipedia
[23] Discussion: Post-quantum security and ethical considerations over elliptic curve cryptography · Issue #131 · monero-project/research-lab
[24] Project 11 - Vulnerable Bitcoin Tracker
[25] Establishment of the Strategic Bitcoin Reserve and United States Digital Asset Stockpile – The White House
[26] bit20250418_posam.htm
[27] [2505.15917] How to factor 2048 bit RSA integers with less than a million noisy qubits
[28] Evaluation of the classical hardware requirements for lage-scale quantum computations
[29] Estimating the Energy Requirements to Operate a Cryptanalytically Relevant Quantumcomputer
[30] Energy Cost of Quantum Circuit Optimisation: Predicting That Optimising Shor's Algorithm Circuit Uses 1 GWh
[31] Gemiddeld energieverbruik in Nederland | Milieu Centraal
[32] NIST Releases First 3 Finalized Post-Quantum Encryption Standards | NIST
[33] A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography | Shaping Europe’s digital future
[34] Position paper: Quantum Key Distribution kent beperkingen | Nieuwsbericht | AIVD
[35] Quantum internet: A vision for the road ahead | Science
[36] QCINed | Quantum Delta NL
[37] Foresight for Science, Technology and Innovation | SpringerLink
[38] Strategic foresight
[39] Strategic Foresight Toolkit for Resilient Public Policy | OECD
[40] Scenario Planning: A Tool for Strategic Thinking
[41] De impact van quantumtechnologie - Birch
[42] Quantum technologies, U.S.-China strategic competition, and future dynamics of cyber stability | IEEE Conference Publication | IEEE Xplore
[43] Grip op control points om gerichter te kunnen innoveren - TNO Vector
[44] Analysis of the likelihood of quantum computing proliferation - ScienceDirect
[45] Developing a human rights compatible governance framework for quantum computing | Research Directions: Quantum Technologies | Cambridge Core

[46] Hoe breng ik mijn te beschermen belangen in kaart? | Wat kun je zelf doen? | Nationaal Cyber Security Centrum
[47] Hinge, Meta, Nvidia Offering 6-Figure Salaries to Attract AI Talent - Business Insider
[48] 30614065-6dd6-4206-8065-fc97948e5e2c_en
[49] Regulation - 2021/1173 - EN - EUR-Lex
[50] wetten.nl - Regeling - Wet op de inlichtingen- en veiligheidsdiensten 2017 - BWBR0039896
[51] Making and breaking with science and conscience - Thesis Ot van Daalen
[52] Nederland grijpt hard in bij chipfabrikant Nexperia uit angst voor lekken chipkennis naar China - NRC
[53] 027588_EnigmaBorchure_inside.qxp, page 1-60 @ Normalize (027588_EnigmaBorchure_inside.qxp)
[54] Enigma machine - Wikipedia
[55] Quantum technology for military applications | EPJ Quantum Technology | Full Text,
[56] Analysis of the likelihood of quantum computing proliferation - ScienceDirect
[57] Developing a human rights compatible governance framework for quantum computing
[58] Developing a human rights compatible governance framework for quantum computing
[59] Quantum Shifts: The Societal Implications of Quantum Computing on Security, Privacy, and the Economy
[60] Quantum for Good and the Societal Impact of Quantum Computing.pdf
[61] TCSP-Info-Sheet-ITAR-092024.pdf
[62] Private quantum computation: an introduction to blind quantum computing and related protocols | npj Quantum Information
[63] Grondwet en digitale technologie
[64] Mitigating the Nuclear 'Dual-Use Dilemma': Suggestions for the Enhancement of the Culture of Responsibility | SpringerLink
[65] Export control and nuclear safeguards
[66] Towards Responsible Quantum Technology | Berkman Klein Center
[67] Ethical, Legal and Social Implications of Emerging Technology (ELSIET) Symposium | Journal of Bioethical Inquiry
[68] The Digital Divide Meets the Quantum Divide
[69] How Americans have viewed surveillance and privacy since Snowden leaks
[70] Developing a human rights compatible governance framework for quantum computing
[71] Speelbal of spelverdeler? Concurrentiekracht en nationale veiligheid in een open economie
[72] Het succesverhaal van ASML, ZEISS en TRUMPF
[73] wetten.nl - Regeling - Verdrag inzake de niet-verspreiding van kernwapens - BWBV0004367
[74] Economische veiligheid en klassieke spionage | Economische veiligheid | AIVD
[75] Preparing Businesses to Implement Quantum Computing | BCG
[76] EUR-Lex - 52011SC1447 - EN - EUR-Lex
[77] Galileo (satellite navigation) - Wikipedia
[78] PHYS771 Lecture 14: Skepticism of Quantum Computing
[79] History of artificial intelligence - Wikipedia
[80] Will Quantum Computing Turn Out Just Like Nuclear Fusion? Always 50 Years Away?
[81] Fusion power - Wikipedia
[82] Quantum-ELSPI: A Novel Field of Research | Digital Society
[83] [2303.16671] Towards responsible quantum technology, safeguarding, engaging and advancing Quantum R&D
[84] ecp.nl/wp-content/uploads/2023/02/Exploratory-Quantum-Technology-Assessment-Nederlands.pdf
[85] [1.3] Responsible Quantum Report - reviewed version
[86] Quantum computing: Practical guide to navigating the future - VTT's Research Information Portal