Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2024–2025

22 112 Nieuwe Commissievoorstellen en initiatieven van de lidstaten van de Europese Unie

Nr. 3964

VERSLAG VAN EEN SCHRIFTELIJK OVERLEG

Vastgesteld 25 september 2024

De vaste commissie voor Digitale Zaken heeft een aantal vragen en opmerkingen voorgelegd aan de Minister van Binnenlandse Zaken en Koninkrijksrelaties over de brief van 17 mei 2024 over het Fiche: Aanbeveling Routekaart Post-Quantumcryptografie (Kamerstuk 22 112, nr. 3945).

De vragen en opmerkingen zijn op 20 juni 2024 aan de Minister van Binnenlandse Zaken en Koninkrijksrelaties voorgelegd. Bij brief van 24 september 2024 zijn de vragen beantwoord.

De fungerend voorzitter van de commissie,
Kathmann

Adjunct-griffier van de commissie,
Muller

kst-22112-3964
ISSN 0921 - 7371
's-Gravenhage 2024

Inhoudsopgave

I Vragen en opmerkingen vanuit de fracties

Vragen en opmerkingen van de leden van de GroenLinks-PvdA-fractie

De leden van de GroenLinks-PvdA-fractie hebben kennisgenomen van het Fiche Aanbeveling Routekaart Post-Quantumcryptografie. Deze leden erkennen het belang van cryptografisch veilige communicatie binnen het digitale domein voor de samenleving als geheel en de uitdagingen die quantum computing met zich meebrengt voor traditionele manieren van asymmetrische cryptografie. Deze leden juichen het dan ook toe dat zowel de Europese Commissie als de Minister zich inzet voor technologieën die ook in een post-quantum wereld nog bestand zijn tegen kraken. Wel hebben de leden van de GroenLinks-PvdA-fractie enkele vragen en opmerkingen over het fiche.

2. Essentie voorstel

De leden van de GroenLinks-PvdA-fractie juichen het toe dat de Europese Commissie lidstaten aanraadt om reeds na te denken over een post-quantum wereld. Deze leden zijn benieuwd naar de juridische en praktische gevolgen van een Routekaart Post-Quantum Cryptografie waar de Europese Commissie op aanstuurt. Kan de Minister aangeven wat een dergelijke routekaart in de praktijk zal betekenen? Kan Nederland eigenstandig andere mogelijke technologieën onderzoeken die in een post-quantum wereld cryptografisch van nut zouden kunnen zijn indien die niet in de routekaart zijn opgenomen? Kan de Minister aangeven hoe zij een dergelijke routekaart waardeert?

Daarnaast zijn de leden van de GroenLinks-PvdA-fractie van mening dat Europese samenwerking op het gebied van post-quantum cryptografie zeer nuttig kan zijn. Deze leden zijn dan ook verheugd dat de Europese Commissie oproept om de acties te coördineren via een op te richting toegewijd lidstatenforum. Tegelijk is Nederland lid van de Appropriately Qualified Authorities (AQUA) Reference Group. Kan de Minister aangeven hoe zij dit op te richten toegewijd lidstatenforum waardeert ten opzichte van de AQUA Reference Group? Is Nederland voorstander van een op te richten lidstatenforum? Is zij van plan om toe te treden tot het lidstaten-forum en blijft Nederland in dat geval óók lid van de AQUA Reference Group? Welke rol ziet zij daarin voor Nederland weggelegd? Hoe beoordeelt zij de overeenkomsten en verschillen tussen beiden gremia?

3. Nederlandse positie ten aanzien van het voorstel

a) Essentie Nederlands beleid op dit terrein

De leden van de GroenLinks-PvdA-fractie vinden het prettig dat reeds in 2021 is begonnen met het Rijksbrede programma Quantumveilige Cryptografie Rijk en dat er sinds 2014 aandacht is voor de dreiging van de quantumcomputer. In dat kader zijn deze leden benieuwd naar hoe de

Minister kijkt naar de store now decrypt later problematiek, waarin datasets die eerder verzameld zijn op een later moment nog door een krachtige computer worden ontsleuteld. Welke risico's brengt deze problematiek met zich mee, hoe kunnen deze worden gemitigeerd?

b) Beoordeling + inzet ten aanzien van dit voorstel

De leden van de GroenLinks-PvdA-fractie delen de positieve houding van het kabinet ten aanzien van de voorgestelde acties uit de aanbeveling van de Commissie om de transitie EU-breed aan te pakken. Deze leden zijn echter wel verrast over de kritiekpunten van het kabinet op het voorstel van de Commissie. Zij snappen de keuze van de Commissie om zowel post-quantum cryptografie (PQC) als quantum key distribution (QKD) onder hybride constructies te verstaan. Kan de Minister aangeven waarom zij dit anders ziet? Wat is het risico als QKD ook wordt opgenomen in de Europese routekaart? Wat zijn de voor- en nadelen van het investeren in QKD *naast* PQC?

De leden van de GroenLinks-PvdA-fractie snappen dat QKD zich nog in een ontwikkelfase bevindt en dat PQC al verder ontwikkeld is, waarbij QKD tevens praktische bezwaren kent als dure en weinig beschikbare benodigde hardware. Deze leden zijn echter vooral benieuwd naar de redenen om QKD als technologie op voorhand af te wijzen, waarbij op dit moment nog niet duidelijk is of de use-case van QKD naast PQC wél van nut kan zijn in de toekomst. Deelt het kabinet de visie dat praktische bezwaren van QKD die er op korte termijn zijn, op langere termijn wellicht wél weggenomen kunnen worden? Waarom zou QKD niet genoemd kunnen worden in de aanbeveling als de EU hier samen met lidstaten wel in investeert, onder andere in het kader van de European Quantum Communication Infrastructure? Welke lidstaten delen de visie van de inlichtingendiensten van Nederland, Frankrijk, Duitsland en Zweden t.a.v. het niet opnemen van QKD in de aanbeveling en in de gezamenlijke Europese Routekaart en welke niet? Welke redenen geven de lidstaten die wél voorstander zijn van het opnemen van QKD in de aanbeveling? Ondersteunt het kabinet op dit moment onderzoeksprojecten op het gebied van de praktische toepassing van QKD? Zo ja, welke projecten zijn dat? Zo nee, welke praktische, inhoudelijke en principiële redenen liggen daaraan ten grondslag? Wat is een mogelijk nadeel als de EU – in navolging van de wens van Nederland – in dit stadium nog niet inzet op QKD en andere grootmachten wel? Kan de Minister in de breedste zin van het woord op reflecteren op bovenstaande vragen?

Daarnaast snappen de leden van de GroenLinks-PvdA-fractie de wens van het kabinet tot het volgen van standaardisatieorganisaties zoals de ISO, NIST, en IETF. Deze leden hebben hier echter nog wel enkele vragen over. Ten eerste vragen zij hoe het kabinet de invloed van andere geopolitieke grootmachten binnen dergelijke standaardisatieorganisaties beoordeeld. Hoe ziet het kabinet de relatieve invloed van grootmachten als de Verenigde Staten, de Europese Unie, China en anderen binnen dergelijke standaardisatieorganisaties op het gebied van Post Quantum Cryptografie en Quantum Key Distribution? Wat zijn de mogelijke gevolgen wanneer andere grootmachten binnen dergelijke standaardisatieorganisaties hun invloed laten gelden en – bijvoorbeeld – QKD als primaire technologie naar voren schuiven? Wat zijn de mogelijke gevolgen voor het Nederlandse beleid? Kan de Minister hier in de breedste zin op reflecteren?

Daarnaast vragen de leden van de GroenLinks-PvdA-fractie of er ook Europese standaardisatie-organisaties zijn die kaders ontwikkelen voor de transitie naar PQC en/of QKD? Kunnen deze op achterstand raken als alleen de kaders van de ISO, NIST en IETF genoemd worden in de

aanbeveling? Hoe beoordeelt de Minister het idee om de genoemde organisaties als een niet-uitputtende lijst op te nemen in de aanbeveling? Wat zou het nadeel zijn als uitsluitend de door het kabinet voorgestelde standaardisatie-organisaties worden genoemd in de aanbeveling?

Ook lezen de leden van de GroenLinks-PvdA-fractie dat het kabinet van mening is dat de Routekaart naar post-quantum cryptografie aanpasbaar is, onder andere omdat de technologie nog volop in beweging is en er dus ook nog geen definitieve EU-breed gedeelde post-quantumcryptografie standaarden zijn. Deze leden prijzen de wil tot flexibiliteit van het kabinet. Tegelijk zijn zij verbaasd dat deze wil van flexibiliteit niet lijkt te gelden bij de keuze voor een specifieke technologie, gezien de voorkeur van het kabinet voor PQC ten opzichte van QKD. De leden van de GroenLinks-PvdA-fractie willen nogmaals benadrukken dat zij geen specifieke voorkeur hebben voor een van beide technologieën, maar dat zij ook graag met een open blik wensen te kijken naar beide opties. Hoe beoordeelt het kabinet de eigen wil tot flexibiliteit ten aanzien van PQC met de keuze om bij de Commissie expliciet niet in te zetten op QKD? Kan de Minister hier in de breedste zin van het woord op reflecteren?

De leden van de GroenLinks-PvdA-fractie lezen ook dat het kabinet vindt dat de Europese routekaart uit moet gaan van een risico-gehanteerde aanpak. Wat bedoelt het kabinet hiermee? Hoe ziet het kabinet het concreet voor zich om dit voor elkaar te krijgen?

Vragen en opmerkingen van de leden van de VVD-fractie

De leden van de VVD-fractie zien de quantumcomputer als een veelbelovende technologie en tegelijkertijd als een groot risico voor onze (informatie)veiligheid vanwege «store now, decrypt later». Deze leden hebben kennisgenomen van het Fiche aanbeveling Routekaart Post-Quantumcryptografie en hebben hierover nog enkele vragen.

Uit antwoord op schriftelijke vragen «Het bericht «NIST kiest wapens tegen quantumcomputer als cryptokraker» (Kamerstuk 4064) van het lid Rajkowski (VVD) blijkt dat er wordt gewerkt aan een veelzijdig programma ter bescherming van staatsgeheimen en andere informatie. Hoe verhoudt dat programma zich tot de kabinetsinzet op dit fiche, zo vragen de leden van de VVD-fractie? Ziet het kabinet Quantum Key Distribution (QKD) als een technologie waarbij het van belang om in te investeren? Zo nee, waarom niet? Zo ja op welke manier wenst zij dit vorm te gaan geven?

Gezien de snelle ontwikkelingen rondom QKD en de leidende rol van onder andere China, vragen de leden van de VVD-fractie waarom QKD niet genoemd zou kunnen worden in de aanbeveling als de EU hier samen met lidstaten wel in investeert, onder andere in het kader van de European Quantum Communication Infrastructure?

De leden van de VVD-fractie vragen welke lidstaten de visie delen van de inlichtingendiensten van Nederland, Frankrijk, Duitsland en Zweden t.a.v. het niet opnemen van QKD in de aanbeveling en in de gezamenlijke Europese routekaart. Welke doen dit niet? Wordt er samen met deze landen opgetrokken? Zo ja, hoe uit dit zich?

De leden van de VVD-fractie zijn van mening dat het belangrijk is om zich te kunnen beschermen tegen de ontwikkelingen op het gebied van QKD in grootmachten als China en de VS en hierin niet achter te lopen. Is het kabinet het hiermee eens? Wat is een mogelijk nadeel als de EU in dit stadium nog niet inzet op QKD en grootmachten als China en de VS al wel? Hoe gaat het kabinet hiermee om?

Hoe verhouden ontwikkelingen en innovaties die in Nederland plaatsvinden zich tot de Europese ambities en doelstellingen met betrekking tot post-quantumcryptografie (PQC)? De leden van de VVD-fractie vragen in hoeverre we Nederlandse ontwikkelingen kunnen versterken en beschermen met Europese doelstellingen.

Vragen en opmerkingen van de leden van de NSC-fractie

De leden van de NSC-fractie hebben kennisgenomen van het fiche over de aanbeveling Routekaart Post-Quantumcryptografie. Daarbij hebben deze leden nog enkele vragen en opmerkingen.

De leden van de NSC-fractie constateren dat het kabinet van inzicht verschilt van de Europese Commissie in enerzijds de betekenis van de term «hybride cryptografische constructies» en anderzijds de beoogde rol van Quantum Key Distribution (QKD) binnen die constructies. Deze leden steunen het kabinetsstandpunt in dat het onwenselijk is om in dit stadium in te zetten op het gebruik van QKD voor beveiliging tegen de quantumdreiging en het in plaats daarvan verstandiger is om ons te richten op de migratie naar post-quantumcryptografie (PQC). Zij vragen daarbij wat het kabinet verwacht dat de potentiële toekomstige use cases zullen zijn voor vormen van quantumcommunicatie, waaronder QKD. Dit aangezien quantumcommunicatie als onderdeel van quantumtechnologieën in de Nationale Technologiestrategie wel wordt beschouwd als strategisch aandachtspunt. Zo heeft Nederland een trekkers- en coördinerende rol in internationale initiatieven als de Quantum Internet Alliance. Is de verwachting dat quantumcommunicatie in de toekomst wel toegevoegde waarde zal hebben voor informatiebeveiliging, of zal PQC in alle voorziene gevallen volstaan? Welke use cases buiten het domein van informatiebeveiliging voorziet het kabinet voor quantumcommunicatie en quantumnetwerken?

Het kabinet benoemt terecht het belang van inzetten op wendbaarheid van cryptografie, ook wel crypto-agility genoemd. De leden van de NSC-fractie vragen of het kabinet kan concretiseren wat de maatstaven voor crypto-agility zijn. Wanneer kan een organisatie er met een hoge mate van zekerheid op van op aan dat zij voldoende cryptografisch wendbaar is?

De leden van de NSC-fractie vragen het kabinet nader toe te lichten hoe zij de invulling van (PQC-) expertisecentra binnen Nederland voor zich ziet. Zijn deze expertisecentra specifiek bedoeld ter ondersteuning van het Rijk in de PQC-migratie of kan ook het bedrijfsleven en het maatschappelijk middenveld hiervan gebruikmaken? Indien het eerste het geval is, wat is de visie van het kabinet over hoe de in Nederland aanwezige expertise de gehele samenleving ten goede kan komen?

II Antwoord/reactie van de bewindspersoon

Vragen en opmerkingen van de leden van de GroenLinks-PvdA-fractie

De leden van de GroenLinks-PvdA-fractie hebben kennisgenomen van het Fiche Aanbeveling Routekaart Post-Quantumcryptografie. Deze leden erkennen het belang van cryptografisch veilige communicatie binnen het digitale domein voor de samenleving als geheel en de uitdagingen die quantum computing met zich meebrengt voor traditionele manieren van asymmetrische cryptografie. Deze leden juichen het dan ook toe dat zowel de Europese Commissie als de Minister zich inzet voor technologieën die ook in een post-quantum wereld nog bestand zijn tegen kraken. Wel

hebben de leden van de GroenLinks-PvdA-fractie enkele vragen en opmerkingen over het fiche.

2. Essentie voorstel

De leden van de GroenLinks-PvdA-fractie juichen het toe dat de Europese Commissie lidstaten aanraadt om reeds na te denken over een post-quantum wereld.

Deze leden zijn benieuwd naar de juridische en praktische gevolgen van een Routekaart Post-Quantum Cryptografie waar de Europese Commissie op aanstuurt. Kan de Minister aangeven wat een dergelijke routekaart in de praktijk zal betekenen?

De routekaart zal een handvat bieden om de gezamenlijke transitie naar Post-Quantumcryptografie gecoördineerd vorm te geven. De precieze invulling van de routekaart is nog niet bekend, waardoor niet alle juridische en praktische gevolgen nu al bekend zijn. Dit is in te vullen door een nog op te richten lidstatenforum onder de reeds bestaande NIS-werkstroom die geleid zal worden door een co-voorzitterschap. Frankrijk, Duitsland en Nederland zullen dit co-voorzitterschap op zich nemen.

Kan Nederland eigenstandig andere mogelijke technologieën onderzoeken die in een post-quantum wereld cryptografisch van nut zouden kunnen zijn indien die niet in de routekaart zijn opgenomen?

Ja, Nederland kan andere mogelijke technologieën onderzoeken. In hoeverre deze technologieën dan toegepast kunnen worden naast de routekaart, moet per casus bekeken worden. Het is aan te bevelen om gestandaardiseerde protocollen en algoritmen in producten te gebruiken om interoperabiliteit te garanderen. Alternatieve technologieën zijn mogelijk ook niet overal toepasbaar, bijvoorbeeld door de lage mate van standaardisatie of beschikbare producten. Mochten alternatieve technologieën nodig zijn, dan is het noodzakelijk om na te gaan hoe deze dan een betere bescherming kunnen bieden.

Kan de Minister aangeven hoe zij een dergelijke routekaart waardeert?

Het kabinet staat positief tegenover een dergelijke routekaart omdat deze kan bijdragen aan een gesynchroniseerde en gecoördineerde migratie tussen lidstaten. Digitalisering stopt niet bij de grenzen van organisaties en landen. Daarom moet internationaal samengewerkt worden om interoperabiliteit te waarborgen in de toekomst. Een routekaart kan lidstaten die minder ver gevorderd zijn in de transitie stimuleren, en ervoor zorgen dat interoperabiliteit tussen lidstaten geborgd wordt. Bovendien is de transitie naar Post-Quantumcryptografie een complexe, wereldwijde uitdaging en is kennis en capaciteit schaars. Dit maakt samenwerking op EU-niveau noodzakelijk. Ten slotte kan de routekaart als communicatiemiddel fungeren: enerzijds richting leveranciers, die dankzij de routekaart gestimuleerd kunnen worden producten te leveren die weerbaar zijn tegen quantumtechnologie en passen binnen de routekaart, en anderzijds richting beleidsmakers, die kaders opstellen waarbinnen een organisatie de transitie moet vormgeven.

Daarnaast zijn de leden van de GroenLinks-PvdA-fractie van mening dat Europese samenwerking op het gebied van post-quantum cryptografie zeer nuttig kan zijn. Deze leden zijn dan ook verheugd dat de Europese Commissie oproept om de acties te coördineren via een op te richting

toegewijd lidstatenforum. Tegelijk is Nederland lid van de Appropriately Qualified Authorities (AQUA) Reference Group.

Kan de Minister aangeven hoe zij dit op te richten toegewijd lidstatenforum waardeert ten opzichte van de AQUA Reference Group? Is Nederland voorstander van een op te richten lidstatenforum? Is zij van plan om toe te treden tot het lidstatenforum en blijft Nederland in dat geval óók lid van de AQUA Reference Group? Welke rol ziet zij daarin voor Nederland weggelegd? Hoe beoordeelt zij de overeenkomsten en verschillen tussen beiden gremia?

De deelname van Nederland aan het toegewijd lidstatenforum staat los van het lidmaatschap aan de AQUA Reference Group. Dit zijn verschillende gremia met verschillende doelstellingen. Nederland is voorstander van het op te richten lidstatenforum en neemt het co-voorzitterschap samen met Duitsland en Frankrijk op zich. Daarnaast zal Nederland ook bijdragen aan de routekaart en expertise leveren ten aanzien van de te vormen Europese standaarden.

Nederland zal ook lid blijven van de AQUA Reference Group. De AQUA Reference Group richt zich op de bescherming van EU-gerubriceerde informatie. Om beveiligingsproducten te gebruiken voor het beschermen van EU-gerubriceerde informatie, dienen deze ook geëvalueerd te worden door een lid van de AQUA Reference Group. Nederland is één van de slechts vijf EU-lidstaten die deze tweedelandsevaluaties mogen uitvoeren op producten die EU-gerubriceerde informatie beschermen.

Het lidstatenforum richt zich primair op de transitie van digitale infrastructuren en diensten voor overheidsdiensten en andere kritieke infrastructuren naar Post-Quantumcryptografie. In de AQUA Reference Group is deze transitie slechts een onderdeel van de taken.

3. Nederlandse positie ten aanzien van het voorstel

a) Essentie Nederlands beleid op dit terrein

De leden van de GroenLinks-PvdA-fractie vinden het prettig dat reeds in 2021 is begonnen met het Rijksbrede programma Quantumveilige Cryptografie Rijk en dat er sinds 2014 aandacht is voor de dreiging van de quantumcomputer.

In dat kader zijn deze leden benieuwd naar hoe de Minister kijkt naar de *store now decrypt* later problematiek, waarin datasets die eerder verzameld zijn op een later moment nog door een krachtige computer worden ontsleuteld. Welke risico's brengt deze problematiek met zich mee, hoe kunnen deze worden gemitigeerd?

Informatie die met de huidige cryptografie vercijferd is, loopt het risico onderschept te worden zodat deze in de toekomst ontcijferd kan worden met behulp van quantumtechnologie. Dit tast de vertrouwelijkheid van de informatie aan.

In onder andere het PQC-migratiehandboek van de AIVD, TNO en CWI en de gezamenlijke handreiking van de AIVD en het NCSC, staan verschillende maatregelen beschreven om bovenstaand risico te mitigeren.[1] Een

[1] *«Het PQC-migratiehandboek: richtlijnen voor het migreren naar post-quantumcryptografie» (https://www.aivd.nl/documenten/publicaties/2023/04/04/pqc-transitie-handboek) en «Maak je organisatie quantumveilig» (https://www.ncsc.nl/documenten/publicaties/2023/september/18/maak-je-organisatie-quantumveilig).*

van de maatregelen is het doen van een risicoanalyse: ga na welke informatie het betreft, hoe deze beschermd wordt en hoe het de organisatie kan schaden als deze informatie over bepaalde tijd (wanneer quantumtechnologie beschikbaar is met de capaciteit om te ontsleutelen) ingezien kan worden door andere partijen.

b) Beoordeling + inzet ten aanzien van dit voorstel

De leden van de GroenLinks-PvdA-fractie delen de positieve houding van het kabinet ten aanzien van de voorgestelde acties uit de aanbeveling van de Commissie om de transitie EU-breed aan te pakken. Deze leden zijn echter wel verrast over de kritiekpunten van het kabinet op het voorstel van de Commissie. Zij snappen de keuze van de Commissie om zowel post-quantum cryptografie (PQC) als quantum key distribution (QKD) onder hybride constructies te verstaan. Kan de Minister aangeven waarom zij dit anders ziet?

Binnen de cryptografie wordt de term hybride cryptografie meestal gebruikt voor de combinatie van asymmetrisch en symmetrische cryptografie. Meer recentelijk wordt hybride cryptografie ook als term gebruikt voor het gebruik van zowel huidige asymmetrische cryptografie als post-quantumcryptografie. Daarom is het gebruik van de term hybride verwarrend als men zou doelen op een combinatie van Post-Quantum-cryptografie (PQC) en Quantum Key Distribution (QKD).

Hoewel PQC en QKD beide tegenmaatregelen zijn tegen aanvallen via quantumtechnologie, zijn het verschillende technologieën. PQC is gebaseerd op onderliggende wiskundige problemen die niet gekraakt kunnen worden met de bekende quantumalgoritmes, zoals Shor en Grover. QKD is gebaseerd op het uitwisselen van quantumtoestanden. QKD zit nog in een ontwikkelfase en biedt momenteel nog onvoldoende informatiebeveiliging, ook indien dit in combinatie wordt gebruikt met PQC[2]

Wat is het risico als QKD ook wordt opgenomen in de Europese routekaart?

QKD is een technologie die nog in de ontwikkelfase zit. Naar inschatting van de informatiebeveiligingsautoriteiten in Nederland, is de technologie op dit moment en in de nabije toekomst nog niet volwassen genoeg om ingezet te worden voor informatiebeveiliging. De Europese routekaart dient over twee jaar beschikbaar te zijn en gevolgd te worden. Als QKD wordt opgenomen in de routekaart is het risico dat organisaties er onterecht van uitgaan dat QKD bij het ingaan van de routekaart voldoende beveiligingswaarde biedt voor het beveiligen van informatie.

QKD zit niet in de Europese Routekaart voor PQC omdat de routekaart een hoge urgentie heeft om op tijd weerbaar te zijn tegen aanvallen met quantumtechnologie.

Wat zijn de voor- en nadelen van het investeren in QKD naast PQC?

Het kabinet acht het van belang dat organisaties zo snel mogelijk PQC inzetten. PQC biedt oplossingen die de acute dreiging van quantumtechnologie mitigeren.

---

[2] *Position Paper over Quantum Key Distribution | Publicatie | AIVD.*

Daarnaast steunt het kabinet de ontwikkeling van QKD. Het is een technologie die volop in ontwikkeling is en mogelijk kansen biedt voor verschillende toepassingen. In de toekomst zou QKD mogelijk gebruikt kunnen worden voor informatiebeveiliging.

Daarvoor is het belangrijk dat er standaardisatie plaatsvindt, zodat er evaluatiemethodiek en -criteria beschikbaar gemaakt kunnen worden. Als in deze aspecten geïnvesteerd wordt, zou de technologie zich verder kunnen ontwikkelen naar een hogere Technology Readiness Level (TRL) en een meer volwassen beveiligingsniveau.

De leden van de GroenLinks-PvdA-fractie snappen dat QKD zich nog in een ontwikkelfase bevindt en dat PQC al verder ontwikkeld is, waarbij QKD tevens praktische bezwaren kent als dure en weinig beschikbare benodigde hardware. Deze leden zijn echter vooral benieuwd naar de redenen om QKD als technologie op voorhand af te wijzen, waarbij op dit moment nog niet duidelijk is of de use-case van QKD naast PQC wél van nut kan zijn in de toekomst.

Deelt het kabinet de visie dat praktische bezwaren van QKD die er op korte termijn zijn, op langere termijn wellicht wél weggenomen kunnen worden?

Het kabinet deelt deze visie en hecht eraan te benadrukken dat het QKD als technologie niet op voorhand afwijst. Het is mogelijk dat een deel van de praktische bezwaren tegen de toepassing van QKD op termijn wordt weggenomen.

Mede daarom heeft het kabinet als aanvulling op de aanbeveling de wens opgenomen dat de routekaart aanpasbaar is. Als QKD in de toekomst wel bewezen meerwaarde biedt voor informatiebeveiliging, daarnaast ook praktisch toepasbaar is, en de technologie gestandaardiseerd en geëvalueerd kan worden, zou QKD ingezet kunnen worden. Mede daarom volgt het kabinet de ontwikkelingen in de Europese Unie, en de strategie voor de ontwikkeling van quantumtechnologieën.

Waarom zou QKD niet genoemd kunnen worden in de aanbeveling als de EU hier samen met lidstaten wel in investeert, onder andere in het kader van de European Quantum Communication Infrastructure?

Het kabinet verwacht dat QKD niet voldoende ontwikkeld is binnen de termijn van twee jaar die staat voor het opstellen van de routekaart voor de transitie. Het kabinet ziet het noemen van QKD als mogelijke oplossing binnen de routekaart als een risico, omdat er onduidelijkheid kan ontstaan over de inzet van PQC.

Hierdoor zouden sommige organisaties onterecht kunnen wachten op QKD en niet migreren naar PQC terwijl dat wel noodzakelijk is op zo kort mogelijke termijn. Investeringen in onderzoek naar QKD kunnen leiden tot een dusdanige volwassenheid van de technologie, dat QKD eventueel alsnog kan worden opgenomen in het Europese traject.

Welke lidstaten delen de visie van de inlichtingendiensten van Nederland, Frankrijk, Duitsland en Zweden t.a.v. het niet opnemen van QKD in de aanbeveling en in de gezamenlijke Europese Routekaart en welke niet? Welke redenen geven de lidstaten die wél voorstander zijn van het opnemen van QKD in de aanbeveling?

De verbindingsbeveiligingsautoriteiten van Nederland, Frankrijk, Duitsland en Zweden hebben in een position paper een gezamenlijke visie gepubliceerd over de inzet van QKD. Deze autoriteiten representeren vier van de vijf leden van de AQUA Reference Group en zijn toonaangevend in Europa voor de bescherming van EU-gerubriceerde informatie. De gesprekken over de Europese routekaart moeten nog starten in het op te richten lidstatenforum. De positie van andere lidstaten is nog niet duidelijk.

Ondersteunt het kabinet op dit moment onderzoeksprojecten op het gebied van de praktische toepassing van QKD? Zo ja, welke projecten zijn dat? Zo nee, welke praktische, inhoudelijke en principiële redenen liggen daaraan ten grondslag?

Het kabinet ondersteunt onderzoeksprojecten naar QKD op nationaal en Europees niveau via Quantum Delta NL (QDNL)[3] Een voorbeeld hiervan is het initiatief European Quantum Communication Infrastructure (EuroQCI)[4], dat zich richt op het bouwen van een beveiligde quantum-communicatie-infrastructuur in de EU, waarin QKD een belangrijke rol speelt via het project OpenQKD[5]

Daarnaast hebben verschillende ministeries zelf ook onderzoeksprojecten en samenwerkingen lopen. Een voorbeeld is een onderzoek van het Ministerie van Buitenlandse Zaken en het Ministerie van Justitie en Veiligheid naar quantumnetwerken en QKD op basis van EuroQCI, samen met QDNL.

Wat is een mogelijk nadeel als de EU – in navolging van de wens van Nederland – in dit stadium nog niet inzet op QKD en andere grootmachten wel? Kan de Minister in de breedste zin van het woord op reflecteren op bovenstaande vragen?

Het kabinet hecht eraan te benadrukken dat het blijft inzetten op QKD en de verdere ontwikkeling van de technologie voor toepassing op de langere termijn. Dit is ook noodzakelijk in het licht van de geopolitieke positie van Nederland en de EU. Andere grootmachten zoals China zetten immers stevig in op onderzoek naar QKD. In het kader van de aanbeveling van de Commissie vindt het kabinet het echter van het grootste belang dat organisaties PQC nu zo snel mogelijk inzetten, omdat deze technologie momenteel het verst ontwikkeld is om de acute dreiging van quantum-technologie op het gebied van informatiebeveiliging te mitigeren.

Een verminderde inzet op onderzoek naar QKD zou een aantal risico's met zich meebrengen.

Ten eerste zou een risico zijn dat de EU en Nederland een technologische achterstand oplopen ten aanzien van andere grootmachten en big tech. Hierdoor kan Nederland in de toekomst afhankelijk worden van grootmachten en big tech op het gebied van QKD. Het is niet wenselijk dat de EU en Nederland strategisch afhankelijk worden van belangrijke technologie van buiten de EU in het kader van strategische autonomie en digitale soevereiniteit.

---

[3] *About Quantum Delta NL | Quantum Delta NL.*
[4] *The European Quantum Communication Infrastructure (EuroQCI) Initiative | Shaping Europe's digital future (Europa.eu).*
[5] *Home – OpenQKD.*

Ten tweede, als het communicatienetwerk in handen is van een statelijke actor (eventueel via big tech) met een offensief programma tegen de EU en de EU-lidstaten, is de vertrouwelijkheid en integriteit van de informatie niet te garanderen. Dit zou zeer schadelijk zijn voor Europese en Nederlandse belangen.

Ten derde zou het opgebouwde ecosysteem in de EU, betaald door de EU, geen mogelijkheid meer hebben om in de EU te groeien. Daarmee zou dit een nadelige impact hebben op de eerder gemaakte financiële investering, vanuit economisch perspectief.

Ten vierde is QKD slechts een onderdeel van quantumcommunicatietechnologie. QKD is een opstap naar andere use cases met quantumcommunicatie en quantum computing. Als we nu niet op QKD investeren, dan raken we achter op quantumcommunicatietechnologie in het algemeen.

Het is daarom van belang om de onderzoeksprojecten op het gebied van QKD voort te zetten op zowel nationaal, als op Europees niveau.

Daarnaast snappen de leden van de GroenLinks-PvdA-fractie de wens van het kabinet tot het volgen van standaardisatieorganisaties zoals de ISO, NIST, en IETF. Deze leden hebben hier echter nog wel enkele vragen over. Ten eerste vragen zij hoe het kabinet de invloed van andere geopolitieke grootmachten binnen dergelijke standaardisatieorganisaties beoordeelt. Hoe ziet het kabinet de relatieve invloed van grootmachten als de Verenigde Staten, de Europese Unie, China en anderen binnen dergelijke standaardisatieorganisaties op het gebied van Post Quantum Cryptografie en Quantum Key Distribution?

Er zijn verschillende gremia waarin wordt gewerkt aan standaarden voor Post-Quantumcryptografie. In de praktijk zien we dat veel van deze gremia naar elkaar kijken en dezelfde algoritmen accepteren. Verschillende grootmachten hebben in meer of mindere mate invloed op standaardisatieorganisaties. Het is daarom belangrijk om binnen Nederland en de EU een eigen weloverwogen strategie te ontwikkelen en een keuze te maken ten aanzien van de standaarden die worden gebruikt. Of binnen Nederland en de EU cryptografie en technologieën gebruikt worden die nog niet als standaard erkend zijn, moet per casus bekeken worden. Het kabinet wil daarom enkel standaarden gebruiken die op een transparante manier worden ontwikkeld en breed gesteund worden binnen de EU door de wetenschap en cybersecurityexperts.

Wat zijn de mogelijke gevolgen wanneer andere grootmachten binnen dergelijke standaardisatieorganisaties hun invloed laten gelden en – bijvoorbeeld – QKD als primaire technologie naar voren schuiven? Wat zijn de mogelijke gevolgen voor het Nederlandse beleid? Kan de Minister hier in de breedste zin op reflecteren?

Er is algemene consensus dat QKD geen totaaloplossing biedt voor verbindingsbeveiliging. QKD is in potentie een bouwblok dat gebruikt kan worden in aanvulling op PQC. Op dit moment worden voorbereidingen getroffen voor een standaardisatieproces op het gebied van QKD.[6] Het kabinet moedigt onderzoek naar het standaardiseren van QKD aan. Als een grootmacht QKD naar voren zou schuiven, zal dit weinig effect hebben op de standaardisatie van PQC. NIST is een van de belangrijkste organisaties met betrekking tot het standaardiseren van PQC. Hiervoor is in 2016 een open academisch proces begonnen waarin in verschillende ronden beoordeeld is welke algoritmen geschikt zijn voor standaardisatie.

---

[6] *https://www.etsi.org/committee/1430-qkd.*

Vanwege het open karakter van dit standaardisatieproces is er veel vertrouwen in dit proces, en is de verwachting dat deze standaarden breed geaccepteerd worden. Een grootmacht die in dit stadium nog zijn invloed wil laten gelden zal naar verwachting een gering effect hebben op deze standaardisatieronde, omdat dit proces in een afrondende fase zit.

Daarnaast vragen de leden van de GroenLinks-PvdA-fractie of er ook Europese standaardisatie-organisaties zijn die kaders ontwikkelen voor de transitie naar PQC en/of QKD? Kunnen deze op achterstand raken als alleen de kaders van de ISO, NIST en IETF genoemd worden in de aanbeveling?

Op dit moment zijn de in het fiche genoemde organisaties de meest toonaangevende standaardisatieorganisaties. Binnen andere Europese standaardisatieorganisaties zijn op dit moment geen substantiële ontwikkelingen op het gebied van PQC. NIST is in 2016 een open academisch proces begonnen waarin in verschillende ronden beoordeeld is welke algoritmen geschikt zijn voor standaardisatie. Vanwege het open karakter van dit standaardisatieproces is er veel vertrouwen in dit proces, en is de verwachting dat deze standaarden over de hele wereld breed geaccepteerd worden. Dit proces zit inmiddels in een afrondende fase en de uiteindelijke standaarden uit de eerste ronde worden dit jaar nog verwacht. Binnen ISO worden enkele alternatieve algoritmen uit het proces van NIST gestandaardiseerd, die in een late fase van het NIST-standaardisatieproces zijn afgevallen omdat deze niet in alle use-cases bruikbaar zijn. De EU-lidstaten en universiteiten zijn ook nauw betrokken geweest bij de totstandkoming van de relevante PQC-standaarden. Nederland omarmt deze standaarden en de verwachting is dat deze ook binnen de EU worden geaccepteerd.

Hoe beoordeelt de Minister het idee om de genoemde organisaties als een niet-uitputtende lijst op te nemen in de aanbeveling? Wat zou het nadeel zijn als uitsluitend de door het kabinet voorgestelde standaardisatie-organisaties worden genoemd in de aanbeveling?

Het kabinet ziet deze lijst niet als uitputtend. Op dit moment zijn dit de meest toonaangevende standaardisatieorganisaties. Mocht in de toekomst een ander gremium een bruikbare standaard leveren die breed gedeeld wordt in Europa, zal deze ook overwogen worden.

Ook lezen de leden van de GroenLinks-PvdA-fractie dat het kabinet van mening is dat de Routekaart naar post-quantum cryptografie aanpasbaar is, onder andere omdat de technologie nog volop in beweging is en er dus ook nog geen definitieve EU-breed gedeelde post-quantumcryptografie standaarden zijn. Deze leden prijzen de wil tot flexibiliteit van het kabinet. Tegelijk zijn zij verbaasd dat deze wil van flexibiliteit niet lijkt te gelden bij de keuze voor een specifieke technologie, gezien de voorkeur van het kabinet voor PQC ten opzichte van QKD. De leden van de GroenLinks-PvdA-fractie willen nogmaals benadrukken dat zij geen specifieke voorkeur hebben voor een van beide technologieën, maar dat zij ook graag met een open blik wensen te kijken naar beide opties.

Hoe beoordeelt het kabinet de eigen wil tot flexibiliteit ten aanzien van PQC met de keuze om bij de Commissie expliciet niet in te zetten op QKD? Kan de Minister hier in de breedste zin van het woord op reflecteren?

Het kabinet ziet op dit moment niet voldoende informatiebeveiligingswaarde in QKD voor dit specifieke traject. Als QKD in de toekomst wel bewezen meerwaarde biedt op het gebied van informatiebeveiliging, daarnaast ook praktisch toepasbaar is, en de technologie gestandaardi-

seerd en geëvalueerd kan worden, dan zou QKD eventueel alsnog opgenomen kunnen worden in dit specifieke traject.

De leden van de GroenLinks-PvdA-fractie lezen ook dat het kabinet vindt dat de Europese routekaart uit moet gaan van een risico-gehanteerde aanpak. Wat bedoelt het kabinet hiermee? Hoe ziet het kabinet het concreet voor zich om dit voor elkaar te krijgen?

Het kabinet is van mening dat de transitie moet worden ingevuld op een manier die verschillende risico's minimaliseert. Hierbij wordt niet alle cryptografie in één keer vervangen, maar wordt eerst een inschatting gemaakt welke cryptografie met de hoogste urgentie vervangen moet worden. Organisaties die gevoelige data verwerken of kritieke of langlevende infrastructuren aanbieden, moeten zo snel mogelijk de eerste migratiestappen zetten. Daarnaast biedt een risico-gebaseerde aanpak ruimte voor organisaties om andere beschermende maatregelen te treffen waar het vervangen van cryptografie nog niet mogelijk is. Het doel is om voldoende weerstand te kunnen bieden tegen aanvallen met quantumtechnologie. Dit is een race tegen de klok: maatregelen moeten tijdig getroffen worden om aanvallen met quantumtechnologie, die huidige cryptografie kunnen breken, het hoofd te bieden.

Vragen en opmerkingen van de leden van de VVD-fractie

De leden van de VVD-fractie zien de quantumcomputer als een veelbelovende technologie en tegelijkertijd als een groot risico voor onze (informatie)veiligheid vanwege «store now, decrypt later». Deze leden hebben kennisgenomen van het Fiche aanbeveling Routekaart Post-Quantumcryptografie en hebben hierover nog enkele vragen.

Uit antwoord op schriftelijke vragen «Het bericht «NIST kiest wapens tegen quantumcomputer als cryptokraker» (Kamerstuk 4064) van het lid Rajkowski (VVD) blijkt dat er wordt gewerkt aan een veelzijdig programma ter bescherming van staatsgeheimen en andere informatie. Hoe verhoudt dat programma zich tot de kabinetsinzet op dit fiche, zo vragen de leden van de VVD-fractie?

Dit betreft het programma Quantumveilige Cryptografie Rijk. Dit programma is nauw betrokken bij de totstandkoming van de kabinetsinzet op dit fiche en de ontwikkeling van de Europese routekaart. Het zal ook invulling geven aan de implementatie van de aanbeveling van de Commissie.

Ziet het kabinet Quantum Key Distribution (QKD) als een technologie waarbij het van belang om in te investeren? Zo nee, waarom niet? Zo ja op welke manier wenst zij dit vorm te gaan geven?

Zoals ik eerder heb gezegd in antwoord op de vragen van de GroenLinks-PvdA-fractie, hecht het kabinet eraan te benadrukken dat het blijft inzetten op QKD en de verdere ontwikkeling van de technologie voor toepassing op de langere termijn. Dit is ook noodzakelijk in het licht van de geopolitieke positie van Nederland en de EU. Andere grootmachten zoals China zetten immers stevig in op onderzoek naar QKD. In het kader van de aanbeveling van de Commissie vindt het kabinet het echter van het grootste belang dat organisaties PQC nu zo snel mogelijk inzetten, omdat deze technologie momenteel het verst ontwikkeld is om de acute dreiging van quantumtechnologie op het gebied van informatiebeveiliging te mitigeren.

Een verminderde inzet op onderzoek naar QKD zou een aantal risico's met zich meebrengen.

Ten eerste zou een risico zijn dat de EU en Nederland een technologische achterstand oplopen ten aanzien van andere grootmachten en big tech. Hierdoor kan Nederland in de toekomst afhankelijk worden van grootmachten en big tech op het gebied van QKD. Het is niet wenselijk dat de EU en Nederland strategisch afhankelijk worden van belangrijke technologie van buiten de EU in het kader van strategische autonomie en digitale soevereiniteit.

Ten tweede, als het communicatienetwerk in handen is van een statelijke actor (eventueel via big tech) met een offensief programma tegen de EU en de EU-lidstaten, is de vertrouwelijkheid en integriteit van de informatie niet te garanderen. Dit zou zeer schadelijk zijn voor Europese en Nederlandse belangen.

Ten derde zou het opgebouwde ecosysteem in de EU, betaald door de EU, geen mogelijkheid meer hebben om in de EU te groeien. Daarmee zou dit een nadelige impact hebben op de eerder gemaakte financiële investering, vanuit economisch perspectief.

Ten vierde is QKD slechts een onderdeel van quantumcommunicatietechnologie. QKD is een opstap naar andere use cases met quantumcommunicatie en quantum computing. Als we nu niet op QKD investeren, dan raken we achter op quantumcommunicatietechnologie in het algemeen.

Het is daarom van belang om de onderzoeksprojecten op het gebied van QKD voort te zetten op zowel nationaal, als op Europees niveau.

Gezien de snelle ontwikkelingen rondom QKD en de leidende rol van onder andere China, vragen de leden van de VVD-fractie waarom QKD niet genoemd zou kunnen worden in de aanbeveling als de EU hier samen met lidstaten wel in investeert, onder andere in het kader van de European Quantum Communication Infrastructure?

Het kabinet verwacht dat QKD niet voldoende ontwikkeld is binnen de termijn van twee jaar die staat voor het opstellen van de routekaart voor de transitie. Het kabinet ziet het noemen van QKD als mogelijke oplossing binnen de routekaart als een risico, omdat er onduidelijkheid kan ontstaan over de inzet van PQC. Hierdoor zouden sommige organisaties onterecht kunnen wachten op QKD en niet migreren naar PQC terwijl dat wel noodzakelijk is op zo kort mogelijke termijn. Investeringen in onderzoek naar QKD kunnen leiden tot een dusdanige volwassenheid van de technologie, dat QKD eventueel alsnog kan worden opgenomen in het Europese traject.

De leden van de VVD-fractie vragen welke lidstaten de visie delen van de inlichtingendiensten van Nederland, Frankrijk, Duitsland en Zweden t.a.v. het niet opnemen van QKD in de aanbeveling en in de gezamenlijke Europese routekaart. Welke doen dit niet? Wordt er samen met deze landen opgetrokken? Zo ja, hoe uit dit zich?

Zoals ik eerder heb gezegd in antwoord op de vragen van de GroenLinks-PvdA-fractie hebben de verbindingsbeveiligingsautoriteiten van Nederland, Frankrijk, Duitsland en Zweden in een position paper een gezamenlijke visie gepubliceerd over de inzet van QKD. Deze verbindingsbeveiligingsautoriteiten representeren vier van de vijf leden van de AQUA Reference Group en zijn toonaangevend in Europa voor de bescherming van EU-gerubriceerde informatie. De gesprekken over de Europese

routekaart moeten nog starten in het op te richten lidstatenforum. De positie van andere lidstaten is nog niet duidelijk.

De leden van de VVD-fractie zijn van mening dat het belangrijk is om zich te kunnen beschermen tegen de ontwikkelingen op het gebied van QKD in grootmachten als China en de VS en hierin niet achter te lopen. Is het kabinet het hiermee eens? Wat is een mogelijk nadeel als de EU in dit stadium nog niet inzet op QKD en grootmachten als China en de VS al wel? Hoe gaat het kabinet hiermee om?

Zoals hierboven reeds benoemd, hecht het kabinet eraan te benadrukken dat het blijft inzetten op QKD en de verdere ontwikkeling van de technologie voor toepassing op de langere termijn. Dit is ook noodzakelijk in het licht van de geopolitieke positie van Nederland en de EU. Andere grootmachten zoals China zetten immers stevig in op onderzoek naar QKD. In het kader van de aanbeveling van de Commissie vindt het kabinet het echter van het grootste belang dat organisaties PQC nu zo snel mogelijk inzetten, omdat deze technologie momenteel het verst ontwikkeld is om de acute dreiging van quantumtechnologie op het gebied van informatiebeveiliging te mitigeren.

Een verminderde inzet op onderzoek naar QKD zou een aantal risico's met zich meebrengen.

Ten eerste zou een risico zijn dat de EU en Nederland een technologische achterstand oplopen ten aanzien van andere grootmachten en big tech. Hierdoor kan Nederland in de toekomst afhankelijk worden van grootmachten en big tech op het gebied van QKD.

Het is niet wenselijk dat de EU en Nederland strategisch afhankelijk worden van belangrijke technologie van buiten de EU in het kader van strategische autonomie en digitale soevereiniteit.

Ten tweede, als het communicatienetwerk in handen is van een statelijke actor (eventueel via big tech) met een offensief programma tegen de EU en de EU-lidstaten, is de vertrouwelijkheid en integriteit van de informatie niet te garanderen. Dit zou zeer schadelijk zijn voor Europese en Nederlandse belangen.

Ten derde zou het opgebouwde ecosysteem in de EU, betaald door de EU, geen mogelijkheid meer hebben om in de EU te groeien. Daarmee zou dit een nadelige impact hebben op de eerder gemaakte financiële investering, vanuit economisch perspectief.

Ten vierde is QKD slechts een onderdeel van quantumcommunicatietechnologie. QKD is een opstap naar andere use cases met quantumcommunicatie en quantum computing. Als we nu niet op QKD investeren, dan raken we achter op quantumcommunicatietechnologie in het algemeen.

Het is daarom van belang om de onderzoeksprojecten op het gebied van QKD voort te zetten op zowel nationaal, als op Europees niveau

Hoe verhouden ontwikkelingen en innovaties die in Nederland plaatsvinden zich tot de Europese ambities en doelstellingen met betrekking tot post-quantumcryptografie (PQC)? De leden van de VVD-fractie vragen in hoeverre we Nederlandse ontwikkelingen kunnen versterken en beschermen met Europese doelstellingen.

Nederland heeft een sterke crypto-industrie met veel actieve organisaties. Dit ecosysteem, dat zich kenmerkt door korte lijnen tussen onderzoek, productie en afnemers, wordt actief versterkt door het Rijksbrede programma NCS (Nationale Crypto Strategie). De Europese doelstellingen kunnen de Nederlandse industrie versterken, omdat de crypto-industrie producten kan leveren die bruikbaar zijn in de transitie. Vanwege de korte lijnen tussen onderzoek en productie, kunnen de PQC-standaarden goed toegepast worden in beveiligingsproducten die gebruikt kunnen worden door Nederlandse organisaties die moeten voldoen aan de EU-aanbeveling.

Vragen en opmerkingen van de leden van de NSC-fractie

De leden van de NSC-fractie hebben kennisgenomen van het fiche over de aanbeveling Routekaart Post-Quantumcryptografie. Daarbij hebben deze leden nog enkele vragen en opmerkingen.

De leden van de NSC-fractie constateren dat het kabinet van inzicht verschilt van de Europese Commissie in enerzijds de betekenis van de term «hybride cryptografische constructies» en anderzijds de beoogde rol van Quantum Key Distribution (QKD) binnen die constructies. Deze leden steunen het kabinetsstandpunt in dat het onwenselijk is om in dit stadium in te zetten op het gebruik van QKD voor beveiliging tegen de quantumdreiging en het in plaats daarvan verstandiger is om ons te richten op de migratie naar post-quantumcryptografie (PQC).

Zij vragen daarbij wat het kabinet verwacht dat de potentiële toekomstige use cases zullen zijn voor vormen van quantumcommunicatie, waaronder QKD.

De ontwikkeling van QKD is een opstap voor volwaardige quantumnetwerken. De kennis en kennisinfrastructuur die we opbouwen met onderzoek naar QKD is essentieel om daarna netwerken te maken waarmee quantuminformatie kan worden uitgewisseld. Andere kansen voor inzet van quantumcommunicatietechnologie zijn de mogelijkheid tot het verbinden van quantumsensoren, verbinden van quantumcomputers (distributed quantum computing) en quantum satellietcommunicatie. Ook daarvoor is het essentieel dat er efficiënte quantumnetwerken bestaan.

Verder bieden quantumtechnologieën ook oplossingen voor andere sectoren zoals energie en gezondheid. Om die reden is quantumtechnologie als sleuteltechnologie opgenomen in de Nationale Technologiestrategie (NTS[7]). Kansrijke quantumtechnologieën zijn quantum computing, quantumcommunicatie en quantum sensing. Quantum computing *maakt berekeningen mogelijk die met klassieke computers ondenkbaar zijn, bijvoorbeeld voor het begrijpen van moleculair gedrag en het ontwikkelen van nieuwe materialen.* Quantumcommunicatie *maakt langeafstandscommunicatie mogelijk.* Quantum sensing *stelt ons in staat tot ongekend nauwkeurige metingen. Het is goed om op te merken dat QKD slechts een mogelijke technologie is binnen het quantum communicatie onderzoeksveld. De potentiële mogelijkheden die quantumcommunicatie biedt, zijn voor veel use cases geavanceerder dan QKD en liggen daarmee verder in de toekomst.*

Dit aangezien quantumcommunicatie als onderdeel van quantumtechnologieën in de Nationale Technologiestrategie wel wordt beschouwd als strategisch aandachtspunt. Zo heeft Nederland een trekkers- en coördine-

[7] De Nationale Technologiestrategie. Bouwstenen voor strategisch technologiebeleid | Rapport | Rijksoverheid.nl.

rende rol in internationale initiatieven als de Quantum Internet Alliance. Is de verwachting dat quantumcommunicatie in de toekomst wel toegevoegde waarde zal hebben voor informatiebeveiliging, of zal PQC in alle voorziene gevallen volstaan?

De verwachting is dat PQC in alle voorziene gevallen zal volstaan. Algehele cryptografische wendbaarheid is cruciaal voor de informatiebeveiliging nu en in de toekomst. Daarom is het onderhouden van volwaardige en passende cryptografische maatregelen om de dreigingen het hoofd te bieden essentieel. De migratie naar PQC is daarnaast noodzakelijk om huidige en toekomstige kwetsbaarheden in te perken.

Ondanks dat PQC in theorie veilig wordt geacht voor aanvallen met quantumtechnologie, kunnen systemen nog steeds kwetsbaar zijn wanneer de implementatie niet goed op orde is. Echter, dit is altijd een risico voor elk type systeem, ongeacht de dreiging.

De belofte van QKD is dat het meerwaarde biedt op informatiebeveiliging door informatietheoretische afluisterdetectie. Dit is een krachtige theoretische eigenschap.

Welke use cases buiten het domein van informatiebeveiliging voorziet het kabinet voor quantumcommunicatie en quantumnetwerken?

Zoals hierboven reeds benoemd, is de ontwikkeling van QKD een opstap voor volwaardige quantumnetwerken. De kennis en kennisinfrastructuur die we opbouwen met onderzoek naar QKD is essentieel om daarna netwerken te maken waarmee quantuminformatie kan worden uitgewisseld. Andere kansen voor inzet van quantumcommunicatietechnologie zijn de mogelijkheid tot het verbinden van quantumsensoren, verbinden van quantumcomputers (distributed quantum computing) en quantum satellietcommunicatie. Ook daarvoor is het essentieel dat er efficiënte quantumnetwerken bestaan.

Verder bieden quantumtechnologieën ook oplossingen voor andere sectoren zoals energie en gezondheid. Om die reden is quantumtechnologie als sleuteltechnologie opgenomen in de Nationale Technologiestrategie (NTS)[8]. Kansrijke quantumtechnologieën zijn quantum computing, quantumcommunicatie en quantum sensing. Quantum computing maakt berekeningen mogelijk die met klassieke computers ondenkbaar zijn, bijvoorbeeld voor het begrijpen van moleculair gedrag en het ontwikkelen van nieuwe materialen. Quantumcommunicatie maakt langeafstandscommunicatie mogelijk. Quantum sensing stelt ons in staat tot ongekend nauwkeurige metingen. Het is goed om op te merken dat QKD slechts een mogelijke technologie is binnen het quantum communicatie onderzoeksveld. De potentiële mogelijkheden die quantumcommunicatie biedt, zijn veel voor veel use cases geavanceerder dan QKD en liggen daarmee verder in de toekomst.

Het kabinet benoemt terecht het belang van inzetten op wendbaarheid van cryptografie, ook wel crypto-agility genoemd. De leden van de NSC-fractie vragen of het kabinet kan concretiseren wat de maatstaven voor crypto-agility zijn. Wanneer kan een organisatie er met een hoge mate van zekerheid op van op aan dat zij voldoende cryptografisch wendbaar is?

---

[8] De Nationale Technologiestrategie. Bouwstenen voor strategisch technologiebeleid | Rapport | Rijksoverheid.nl.

De werkgroep Crypto Agility van Quantumveilige Cryptografie Rijk houdt zich bezig met dit onderwerp. Vooralsnog zijn er nog geen concrete maatstaven om te bepalen in welke mate een organisatie cryptografisch wendbaar is. Uit literatuuronderzoek blijkt dat een veelheid van aspecten onder dit begrip kan worden verstaan, waardoor verschillende expertises nodig zijn om tot oplossingen te komen. Verschillende vormen van cryptografische wendbaarheid en wat dat in de praktijk betekent worden momenteel in deze werkgroep verder uitgewerkt.

De leden van de NSC-fractie vragen het kabinet nader toe te lichten hoe zij de invulling van (PQC-) expertisecentra binnen Nederland voor zich ziet. Zijn deze expertisecentra specifiek bedoeld ter ondersteuning van het Rijk in de PQC-migratie of kan ook het bedrijfsleven en het maatschappelijk middenveld hiervan gebruikmaken? Indien het eerste het geval is, wat is de visie van het kabinet over hoe de in Nederland aanwezige expertise de gehele samenleving ten goede kan komen?

Quantumveilige Cryptografie Rijk zal invulling geven aan de aanbeveling vanuit de Commissie. Tot op heden richtte het programma Quantumveilige Cryptografie Rijk zich op primair op de Rijksoverheid, maar het programma bereidt nu uitbreiding naar overheid en kritieke en vitale infrastructuren voor. Het Ministerie van Economische Zaken speelt een nadrukkelijke rol in het gezamenlijk werken aan een publiek-private samenwerking tussen overheid, onderzoek/wetenschap en bedrijfsleven om onderzoek en innovatie rondom PQC-migratie te bevorderen. Van de hierin opgedane kennis, ervaring en geleerde lessen kunnen dan ook andere, niet-vitale organisaties en bedrijven profiteren. Zo zal dit de gehele Nederlandse samenleving ten goede gaan komen.