Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

4064

Vragen van het lid **Rajkowski** (VVD) aan de Ministers van Justitie en Veiligheid en van Economische Zaken en Klimaat en de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties over *het bericht «NIST kiest wapens tegen kwantumcomputer als cryptokraker»* (ingezonden 27 juli 2022).

Antwoord van Staatssecretaris **Van Huffelen** (Binnenlandse Zaken en Koninkrijksrelaties), mede namens de Staatssecretaris van Justitie en Veiligheid (ontvangen 19 september 2022).

Vraag 1
Bent u bekend met het bericht «NIST kiest wapens tegen kwantumcomputer als cryptokraker»?[1]

Antwoord 1
Ja.

Vraag 2 en 5
Bent u het ermee eens dat kwantumcomputers een serieus gevaar kunnen vormen voor het Nederlandse briefgeheim en veilige communicatie tussen o.a. veiligheidsdiensten, Nederlandse burgers onderling en voor onze ondernemers in het kader van bedrijfsgeheimen? Zo ja, hoe beoordeelt u dit gevaar? Zo nee, waarom niet?
Welke gevolgen ziet u voor de rijksoverheid en lagere overheden met de komst van kwantumcomputers wat betreft het inrichten van de systemen?

Antwoord 2 en 5
Ja. De komst van de kwantumcomputer brengt risico's met zich mee op het gebied van informatiebeveiliging. Sommige cryptografische standaarden die nu veilig worden geacht, zullen door de komst van kwantumcomputers niet meer veilig zijn, waaronder cryptografie die nu veelvuldig wordt gebruikt voor het beveiligen van internetverkeer.
Zoals ook benoemd in de AIVD-brochure «*Bereid je voor op de dreiging van kwantumcomputers*», achten experts de kans klein maar reëel dat kwantumcomputers in 2030 al krachtig genoeg zullen zijn om de huidige cryptografi-

[1] AGConnect: 6 juli 2022 NIST kiest wapens tegen kwantumcomputer als cryptokraker – AG Connect

ah-tk-20212022-4064
ISSN 0921 - 7398
's-Gravenhage 2022

sche standaarden te breken.[2] Informatie die gedurende een langere periode vertrouwelijk moet blijven, waaronder staatsgeheimen, moet daarom zo snel mogelijk al beschermd worden tegen *store now, decrypt later*-aanvallen[3]. Deze dreiging wordt ook gesignaleerd door het NCSC, dat de afgelopen jaren heeft opgeroepen tot het starten met het voorbereiden op de komst van kwantumcomputers, bijvoorbeeld via de NCSC-factsheet «Postkwantumcryptografie».[4]
Voor de rijksoverheid en medeoverheden, maar ook voor de private sector, betekent dit dat zij zullen moeten migreren naar kwantumveilige systemen en technologieën. Deze migratie is omvangrijk, en zal zo snel mogelijk gestart moeten worden om op tijd voorbereid te zijn op de dreiging van kwantumcomputers.

Vraag 3, 4 en 6
Op welke wijze borgt u tijdig met oplossingen te komen tegen de komst van kwantumcomputers zodat inwoners van Nederland veilig digitaal kunnen communiceren en persoonsgegevens en bedrijfs- en staatsgeheimen goed beveiligd kunnen blijven? Welke concrete stappen zijn hier de afgelopen jaren voor gezet en welke stappen bent u nog voornemens te zetten?
Welke voorbereidingen neemt u op de komst van de kwantumcomputers? Welke voorbereidingen worden hier getroffen, ook eventueel in samenwerking met private sectoren?
Bent u samen met bedrijven en experts op zoek naar oplossingen om encryptie bestendig te maken tegen de komst van kwantumcomputers? Zo ja, wat is de status van deze gesprekken? Zo nee, waarom niet?

Antwoord 3, 4 en 6
Gezien de hierboven gesignaleerde veiligheidsrisico's voor de overheid, burgers en bedrijven, zet het kabinet zich, met partners uit de private sector en wetenschap, op verschillende wijzen in om maatregelen en technologieën te ontwikkelen die deze risico's kunnen helpen mitigeren.
Voor de verwerking van gerubriceerde gegevens zijn al geruime tijd kwantumveilige producten beschikbaar. Volgend uit het Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie (VIRBI) is kwantumveiligheid sinds 2020 een harde eis voor producten waarmee gerubriceerde gegevens verwerkt worden. Het gaat dan om gegevens gerubriceerd als departementaal vertrouwelijk en hoger. Om te borgen dat de rijksoverheid ook in de toekomst kan beschikken over beveiligingsproducten voor vertrouwelijke informatie, wordt er in het kader van de Nationale Cryptostrategie (NCS) geïnvesteerd in de ontwikkeling van deze producten. Dit maakt het mogelijk om in te spelen op risico's rondom kwantumcomputing voor wat betreft de rijksoverheid. Hierbij wordt in samenwerking met bedrijven en experts onder meer gewerkt aan de ontwikkeling van nieuwe beveiligingsproducten en het doorontwikkelen van bestaande producten.
Deze producten zullen gebruikmaken van post-quantumcryptografie (PQC). Dit is een vorm van cryptografie die gebaseerd is op wiskundige problemen die niet effectief te kraken zijn met een kwantumcomputer. In 2023 zal de AIVD in samenwerking met TNO en het Centrum voor Wiskunde en Informatica (CWI) een *kwantum Migratie Handleiding* publiceren die overheden, bedrijven en burgers kunnen gebruiken als handvat voor migratie naar kwantumveilige communicatie. Deze handleiding beschrijft de verschillende doelgroepen en bijbehorende (technische) stappen die genomen kunnen worden.
Investeringen en onderzoek
Het kabinet investeert via het Nationaal Groeifonds fors in de Nationale Agenda kwantumtechnologie (zie beneden het antwoord op vraag 10). Naast de inzet vanuit het Groeifonds hebben departementen een aantal jaar geleden gezamenlijk het initiatief genomen om binnen de Nationale Wetenschapsagenda (NWA) uit 2018 met het programma «Cybersecurity – naar een veilig en betrouwbaar digitaal domein» aan de slag te gaan om oplossingen te vinden voor vraagstukken rond internetveiligheid. Daarbinnen is een project

[2] Bereid je voor op de dreiging van quantumcomputers | Publicatie | AIVD
[3] In een *store now, decrypt later*-aanval wordt vercijferde informatie nu onderschept, om deze in de toekomst met hulp van kwantumcomputers te ontcijferen.
[4] Factsheet Postkwantumcryptografie | Factsheet | Nationaal Cyber Security Centrum (ncsc.nl)

gefinancierd tegen het gevaar van het breken van versleutelingsschema's door kwantumcomputers.[5] Daarnaast werkt de overheid samen met private partijen en wetenschappers, onder leiding van het ECP, aan het ontwikkelen van werelds eerste kwantum Impact Assessment (QIA). Organisaties die met kwantumtechnologie willen gaan werken, kunnen dan het QIA doen, om te bepalen wat juridische, ethische en maatschappelijke consequenties zijn van het inzetten van deze technologie. De kennis en producten ontwikkeld via deze trajecten zullen door overheid, bedrijven en burgers benut kunnen worden om zich te beveiligen en om kwantumtechnologie op een verantwoorde wijze te gebruiken.
Er wordt niet alleen op nationaal niveau geïnvesteerd en samengewerkt, maar ook op Europees niveau. Die Europese inzet is uiteengezet in het antwoord op vraag 9.
Inzet voor de (Rijks)overheid
Binnen de rijksoverheid zijn departementen vanuit hun eigen verantwoordelijkheid voor informatiebeveiliging ook verantwoordelijk om hun belangrijkste processen en andere belangen te beschermen tegen de dreiging van de kwantumcomputer op de toegepaste cryptografie. Om de departementen hierbij te helpen wordt er momenteel op verzoek van het CIO-beraad vanuit de I-strategie Rijk 2022 – 2025, interdepartementaal gewerkt aan een plan voor een gezamenlijke aanpak van deze dreiging, zodat kennis en kunde gedeeld worden, centraal een beeld ontstaat hoe ver de departementen zijn en om de krachten te bundelen onder andere met betrekking tot leveranciersmanagement. BZK zal de medeoverheden wijzen op het belang van spoedige inzet op kwantumcryptografie, en de door de rijksoverheid opgedane ervaring met hen delen, om hen snel op gang te helpen. Er is daarnaast ook een kwantum InnovatieHub rijksoverheid. Dit is een netwerk van geïnteresseerden in kwantumtechnologie en de impact voor de rijksoverheid. Dit netwerk heeft de afgelopen jaren een grote rol gespeeld in het vergroten van het bewustzijn omtrent de impact van kwantumtechnologie binnen de rijksoverheid.

Vraag 7 en 8
Heeft u al een selectie gemaakt van alternatieve cryptografische methoden die niet vatbaar zijn voor het kwantumrekengeweld? Zo ja, welke methoden vallen binnen deze selectie? Zo nee, wanneer verwacht u met een selectie te komen?
Bent u het met de experts uit het artikel eens dat het verstandig kan zijn alvast in te zetten op een combinatie van traditionele cryptografie en de nieuwe, nog niet volledig uitontwikkelde, postkwantummethoden? Zo ja, hoe gaat u dit vormgeven? Zo nee, waarom niet?

Antwoord 7 en 8
Zoals aangegeven in het antwoord op vragen 3, 4 en 6, wordt voor wat betreft het adresseren van de risico's van kwantumcomputing, door de overheid fors geïnvesteerd. Daarnaast werken cybersecurity experts en cryptologen van de rijksoverheid ook nauw samen met experts uit de private sector en wetenschap. Hierbij wordt breder gekeken naar het vraagstuk dan sec de ontwikkeling van cryptografie, maar ook de implementatie in beveiligingsproducten, standaardisering en migratie-adviezen. Die brede inzet moet de komende jaren leiden tot adviezen en producten die overheid, bedrijven en burgers kunnen gebruiken om zich te beveiligen tegen de dreiging van kwantumcomputing.
Naar aanleiding van de selectie van NIST heeft het NCSC in juli 2022 beveiligingsrichtlijnen gepubliceerd.[6] In deze beveiligingsrichtlijnen adviseert het NCSC over het gebruik van specifieke algoritmes waar organisaties gebruik van kunnen maken bij het inrichten van hun architectuur die gebruik

[5] De call «Cyber Security heeft de Ministeries van Binnenlandse Zaken en Koninkrijksrelaties, Buitenlandse Zaken, Economische Zaken en Klimaat, Defensie, Justitie en Veiligheid, Infrastructuur en Waterstaat, en Volksgezondheid, Welzijn en Sport als initiatiefnemers. NWO | 10 miljoen euro toegekend voor het oplossen van vraagstukken over cybersecurity
[6] https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2022/juli/guidelines-for-quantum-safe-transport-layer-encryption/guidelines-for-quantum-safe-transport-layer-encryption/Guidelines_for_PQC_-_Kyber.pdf

maakt van een combinatie van traditionele en kwantum-veilige algoritmes. Daarnaast publiceerde het NCSC in 2017 al de factsheet postkwantumcryptografie.
De AIVD heeft voor het gebruik van cryptografie voor het versleutelen van gerubriceerde informatie klassieke en nieuwe cryptografische methoden beoordeeld op mogelijk gebruik als post-quantum cryptografie (PQC), en daarover gepubliceerd in de brochure «*Bereid je voor op de dreiging van kwantumcomputers*». Hierin wordt een combinatie van traditionele cryptografie en PQC, een zogeheten hybride constructie, aangeraden voor die systemen waar niet gewacht kan worden op standaardisatie van PQC. Ook is het voor alle organisaties die werken met gevoelige informatie belangrijk om te beginnen met de migratie hiervan naar kwantumveilige systemen. In de eerste fasen van deze migratie kan een inventarisatie plaatsvinden van systemen die voor de komst van een kwantumcomputer al gemigreerd moeten worden, en wanneer deze migratie moet plaatsvinden.
Een ander veelgenoemde technologie voor het beveiligen van communicatie is *kwantum key distribution* (QKD). Echter, in de eerdergenoemde AIVD-brochure, beoordeelt de AIVD, QKD zonder het gebruik van PQC als ongeschikt voor het beveiligen van gevoelige informatie. De reden hiervoor is dat QKD sommige, maar niet alle benodigde veiligheidsfuncties vervult. Daarom adviseert de AIVD in alle gevallen om voor de verwerking van gevoelige informatie ook PQC te gebruiken. Onderzoek naar QKD zorgt wel voor kennisopbouw over de onderliggende kwantumtechnologieën. Daarom is het alsnog belangrijk om ook onderzoek te doen naar QKD, ondanks dat QKD op zichzelf ongeschikt is voor het beveiligen van gevoelige communicatie.
In het kader van het plan van aanpak dat voor de rijksoverheid wordt ontwikkeld, is een van de elementen waar binnen het migratieplan naar wordt gekeken de zogenaamde «crypto-agitatie». Dit concept maakt het mogelijk om flexibel en gemakkelijk over te schakelen op verschillende soorten cryptografie, bijvoorbeeld door hardware te gebruiken die dit mogelijk maakt. Dit zou de overstap voor een deel kunnen versnellen. Daarnaast kan dit concept worden ingezet voor producten en diensten die nu worden ontwikkeld en gebruik gaan maken van cryptografie.

Vraag 9
Is Nederland aangesloten bij de Europese programma's die betrekking hebben op kwantumcomputers? Zo ja, op welke manier heeft Nederland dit vormgegeven? Wat heeft dit concreet tot nu toe opgeleverd? Zo nee, waarom niet?

Antwoord 9
Ja, Nederland neemt deel aan Europese programma's die ook betrekking hebben op kwantumcomputers, zoals Digital Europe en Horizon Europe. Tijdens het Nederlandse EU-voorzitterschap in 2016 heeft de Europese Commissie het EU kwantum Technologies flagship gelanceerd, een R&D programma voor Europese consortia met een budget van 1 miljard euro. Van de totaal 146 miljoen euro uit de eerste fase van het flagship onder Horizon 2020 (2014–2020) namen Nederlandse kennisinstellingen deel voor 10,6 miljoen euro, een percentage van 7,28% – ruim meer dan het gemiddelde Nederlandse aandeel in Horizon 2020. Voor twee consortia op het gebied van kwantum Internet (TU Delft) en kwantum sensing (UvA) is Nederland penvoerder.
Daarnaast heeft Nederland een belangrijke rol in EuroQCI, het Europese programma voor kwantum-communicatie, waar QKD als technologie centraal staat. De Nederlandse inzet in dit EuroQCI programma wordt door het Ministerie van Economische Zaken en Klimaat en kwantumDeltaNL interdepartementaal afgestemd met vertegenwoordigers van onder meer J&V, DEF, BZ en BZK.
In de eerste fase van dit EuroQCI programma, ontvangt een Nederlands consortium met Stichting kwantum Delta als penvoerder cofinanciering van 5 miljoen euro uit het Digital Europe Programma. Het gaat hierbij om het project «QCINed: Towards a National kwantum Communication Infrastructure in The Netherlands» waarbij een experimenteel kwantum communicatienetwerk wordt opgezet door Nederlandse kennisinstellingen met participatie door verschillende ministeries en Rijksuitvoeringsorganisaties.

Deze projecten zitten momenteel in hun eerste fases, en zullen de komende jaren hun resultaten gaan opleveren. Wel heeft de projectontwikkelfase al bijgedragen aan meer samenwerking tussen Nederlandse en Europese partners op dit gebied.

Vraag 10
Hoeveel geld is tot op heden uit het groeifonds beschikbaar gesteld voor de ontwikkeling van kwantum technologie? Welk deel van dit budget is de afgelopen jaren, of zal de komende jaren ook worden geïnvesteerd in het ontwikkelen van deze technologie?

Antwoord 10
In de eerste ronde van het Nationaal Groeifonds is 615 miljoen euro gereserveerd voor de uitvoering van de Nationale Agenda kwantumtechnologie. Het voorstel kwantumDeltaNL richt zich op het versterken van Nederlands kwantum-ecosysteem, door te investeren in (1) kwantumcomputing, (2) kwantumnetwerken en (3) kwantumsensing. Behalve investeringen in R&D wordt het budget ook gebruikt voor een valorisatieprogramma, voor campusontwikkeling, en voor versterking van de nationale onderzoeksinfrastructuur via NanolabNL. Tevens is er aandacht voor de maatschappelijke impact van deze nieuwe technologie.
Van het bedrag van 615 miljoen uit het nationaal groeifonds is 54 miljoen euro direct toegekend voor Fase 1 van dit programma, welke is gestart in september 2021. Na positieve beoordeling van de uitvoering van Fase 1 is door het kabinet inmiddels ook de voorwaardelijke toekenning voor Fase 2 omgezet in een definitieve toekenning voor het bedrag van 228 miljoen euro. Na een tussentijdse evaluatie in 2025 zal een besluit worden genomen over de reservering van 333 miljoen euro voor Fase 3 van dit programma.

Vraag 11
Bent u het ermee eens dat de Nederlandse economie kan profiteren van de mogelijkheden van kwantumcomputers? Zo nee, waarom niet? Zo ja, op welke manier?

Antwoord 11
Ja, het kabinet is het hier mee eens. Om deze reden heeft de Adviescommissie Nationaal Groeifonds destijds positief geadviseerd om het kwantumDeltaNL project te honoreren. Kwantum is een ontwikkelende technologie, die een «game-changer» kan zijn op het gebied van rekenkracht en daarmee voor nieuwe verdienmodellen en oplossingen voor maatschappelijke problemen kan zorgen.
Op dit moment zien we een snelle groei van bedrijvigheid rondom deze sleuteltechnologie. Het ecosysteem van kwantumDeltaNL breidt zich snel uit met Nederlandse en buitenlandse startups en scale-ups die werken aan innovatieve componenten en services voor kwantumcomputers en kwantuminternet.
In het kader van het publiek-private samenwerkingsplatform voor cybersecurity kennis en innovatie dcypher wordt door de overheid, het bedrijfsleven en kennisinstellingen samengewerkt aan de ontwikkeling van innovatieve producten en diensten op het gebied van cryptocommunicatie. In aanvulling op de Nationale Crypto Strategie richt deze routekaart cryptocommunicatie zich voornamelijk op het ontwikkelen van het Nederlandse verdienvermogen met betrekking tot cryptografie op zoals dat binnen de overheid en het bedrijfsleven worden toegepast. Post-kwantum cryptografie is hier een belangrijk onderdeel van.