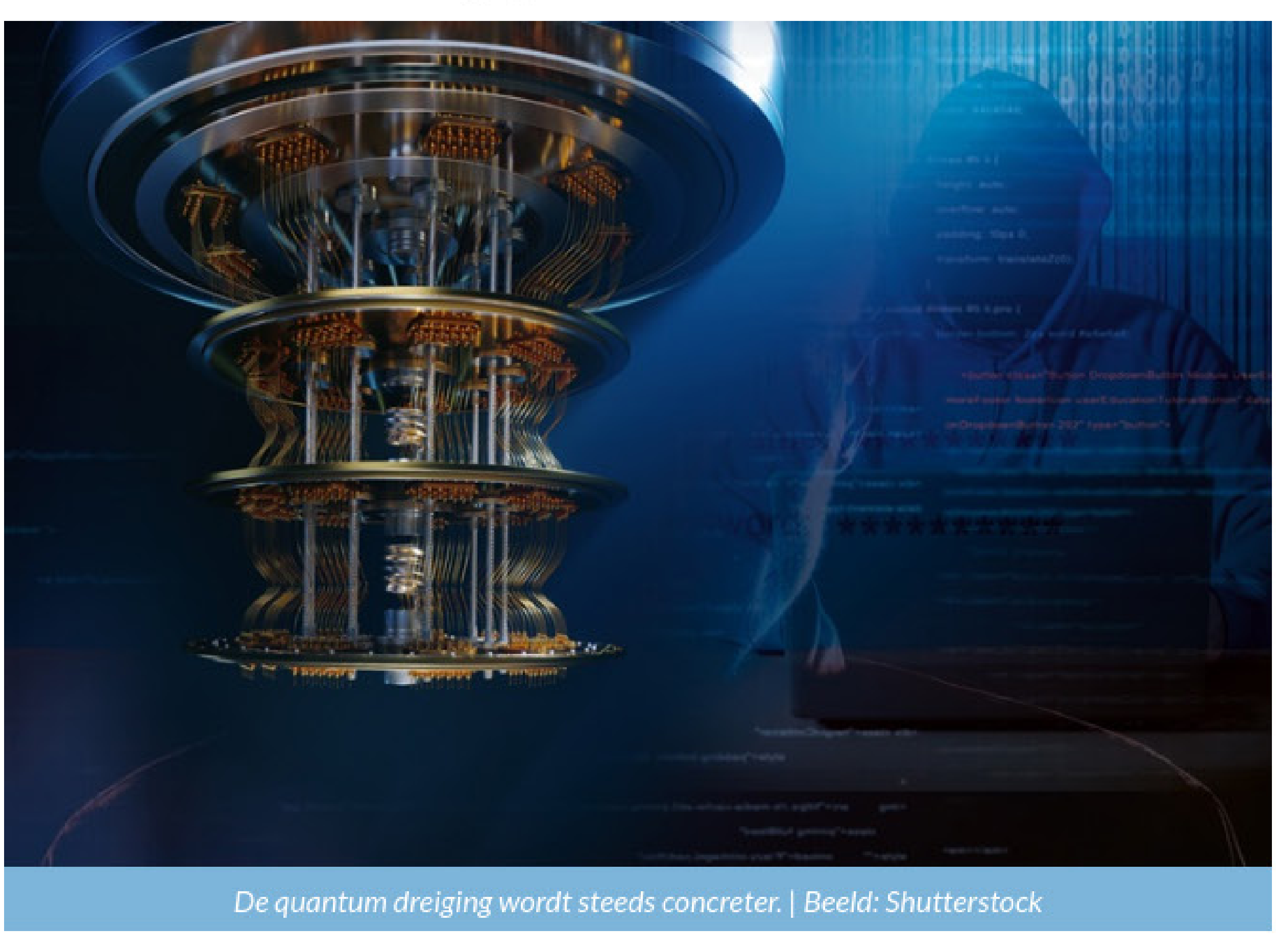
Urgentie quantumdreiging blijft in Nederland onopgemerkt



De quantum dreiging wordt steeds concreter. | Beeld: Shutterstock

29 januari 2025 ai, cybersecurity, europa, politiek, quantumtechnologie

Al vijf jaar is duidelijk dat overheden en bedrijven actie moeten ondernemen om hun IT-systemen te beschermen tegen aanvallen met een quantumcomputer. Vijandig gezinde landen steken miljarden in de ontwikkeling van quantumtechnologie. Ze kunnen daarmee mogelijk nu al onze cryptografische beveiliging breken of dat lukt binnenkort. Maar Nederland, en eigenlijk heel Europa, blijft als een konijn in de koplampen kijken.

Plat gezegd wonnen de geallieerden de Tweede Wereldoorlog door Alan Turing. De computerpionier kraakte de code waarmee de Duitse eenheden hun communicatie versleutelden. Hierdoor konden zij onopgemerkt meeluisteren en hun strategie aanpassen.
Die situatie dreigt zich weer voor te doen, maar nu zijn de kaarten opnieuw geschud. Wanneer we data versturen, worden die standaard door onze systemen cryptografisch versleuteld. Een aantal methoden waarmee dat gebeurt, is met de massale rekenkracht van quantumcomputers eenvoudig te kraken. Ook al lukt dat misschien nu nog niet, alle gegevens die we vandaag digitaal uitwisselen, worden onderweg ergens afgetapt en opgeslagen. Die informatie kan op een later tijdstip worden ontcijferd. Voor kwaadwillende mogendheden zijn niet alleen staatsgeheimen interessant. De kleinste brokjes, schijnbaar onschuldige informatie kunnen, gecombineerd met andere informatie, leiden naar strategisch waardevolle bronnen.

Te weinig actie

De AIVD publiceerde vorig jaar een handleiding voor de overstap naar quantumveilige communicatie, samen met TNO en het Centrum Wiskunde & Informatica (CWI). Ondanks deze en andere aanmoedigingen wordt in Nederland nog heel weinig actie ondernomen, constateert Dimitri van Esch. Hij is business consultant bij Quantum Amsterdam en CEO en oprichter van de Quantum Gateway Foundation. Deze organisatie maakt producten waarmee organisaties hun systemen onder meer kunnen doorlichten en beveiligen tegen aanvallen met quantumtechnologie. Het hele proces van opsporen en aanpassen van de kwetsbaarheden kost al snel tien tot vijftien jaar, is zijn ervaring. ‘Ik ben jaloers op Amerika, waar het Witte Huis eist dat organisaties binnen zes maanden een plan hebben en in 2030 quantumveilig zijn.’

> ***‘ Ik ben jaloers op Amerika, waar het Witte Huis eist dat organisaties binnen zes maanden een plan hebben en in 2030 quantumveilig zijn. ’***
>
> ***Dimitri van Esch, Quantum Gateway Foundation***

Top-down forceren

Zonder stok achter de deur, komen overheden, maar ook de vitale bedrijven, niet in beweging. ‘We moeten het top-down forceren’, stelt Van Esch. Hij heeft ervaring bij een grote bank waar geprobeerd is het proces bottom-up op gang te krijgen. ‘Er gaat niks gebeuren. Er wordt al snel gedacht: ‘Waarom zou ik iets doen waarmee mijn opvolger over tien of vijftien jaar mee kan *shinen?* Dan doe je het gewoon niet.’

Het probleem is dat de veiligheidsdreiging zich waarschijnlijk sneller dan gedacht aandient. *Non-friendly countries*, zoals Rusland en China, investeren zwaar in de ontwikkeling van quantumtechnologie. ‘We hebben onvoldoende zicht op wat daar precies gebeurt. Het enige wat we bijvoorbeeld kunnen volgen, is de ontwikkeling van patenten op dit gebied en ze zijn daar enorm aan het versnellen’, constateert Jesse Robbers, bestuurslid van Quantum Delta NL, de organisatie die de samenwerking rond quantumtechnologie in Nederland coördineert. ‘We weten één ding, ze gaan snelheid maken en proberen ons in te halen. Dat betekent dat wij in Nederland, in Europa, in de gelijkgezinde landen, echt stappen met elkaar moeten zetten. Het is belangrijk dat er urgentie wordt gecreëerd in het overheidsdomein.’

Dreiging van BRICS-landen

Ferdinand Griesdoorn van de Quantum Innovation Hub Rijksoverheid maakt de urgentie nog duidelijker. Hij spreekt over een dreigende “quantum-cyberoorlog”, waarbij Rusland en China op dit vlak kunnen samenwerken met India in het BRICS-verband, de tegenhanger van de NAVO. ‘Rusland en China lopen voor op Europa met quantumcommunicatie. India heeft een enorm potentieel en verwacht binnen acht jaar al *quantum supremacy* te bereiken.’ Dit is de situatie waarbij een quantumcomputer berekeningen kan maken die met de grootste supercomputer niet redelijkerwijs meer te simuleren is. Een quantumcomputer moet dan beschikken over minimaal duizend gevalideerde qubits. Met die computerkracht wordt het waarschijnlijk mogelijk de huidige encryptiemethoden te kraken. De quantumcomputers werken nu met circa 100 qubits. ‘Rusland, China en India spelen niet volgens onze regels’, waarschuwt Griesdoorn. ‘We zijn een wedstrijd ingegaan waarbij wij onszelf zwaardere regels hebben opgelegd dan de andere teams. Elke honderd meter moeten wij een hink-stap-sprong doen. En dat is problematisch, want daardoor vloeit onze innovatieve capaciteit in Europa weg.’

> ***‘ We zijn een wedstrijd ingegaan waarbij wij onszelf zwaardere regels hebben opgelegd dan de andere teams. ’***
>
> ***Ferdinand Griesdoorn, Quantum Innovation Hub Rijksoverheid***

Kafkaiaanse weg naar veiligheid

Griesdoorn doelt op Europese regelgeving die een snelle ontwikkeling van quantumveilige systemen in de weg staat. ‘In Europa wil elke lidstaat zelf zo veel mogelijk uit de ruif eten. Waar is de quantum visie in Europa? Waar is de blauwdruk, de architectuur?’ Hij is overigens geen voorstander van het ontwikkelen en blind volgen van wereldwijde standaarden. Europese bedrijven laten zich dan door vijandig gezinde mogendheden te makkelijk in de kaart kijken. ‘Ik heb liever dat veiligheidssystemen geen opgelegde standaarden gebruiken en eigenlijk propriëtair zijn als het even kan. Het hele idee van standaarden in het kader van veiligheid lijkt soms op een absurde, bijna kafkaiaanse weg naar veiligheid. Prima in een wereld die stabiel is, maar we zitten nu eenmaal in een geopolitieke gespannen wereld.’

Griesdoorn vindt dat in de beeldvorming over beschermende maatregelen de nadruk te veel ligt op quantumveilige encryptie. Die is complex en neemt veel tijd in beslag bij de implementatie. Bovendien heeft deze zogeheten postquantum encryptie ook zwakke plekken. Hij pleit voor gelijktijdig toepassen van postquantum crytografie, quantum key distribution (QKD) en het quantum internet (zie kader). ‘Snel aan de slag gaan met postquantum encryptie geeft ons tijd technologieën te combineren en een hoger veiligheidsniveau te verkrijgen voordat sterke aanvallen met quantumcomputers mogelijk worden.’

Kansen voor Nederland

Nederland kan profiteren door een voortrekkersrol te pakken in Europa. Onderzoeksorganisaties in Delft, Leiden, Amsterdam, Eindhoven en Twente hebben samen met een aantal startersbedrijven een unieke positie wereldwijd. ‘Er is een ecosysteem rond quantumtechnologie waarbij alle componenten binnen een straal van 100 kilometer zijn gevestigd’, zegt Robbers. Vanuit het Nationaal Groeifonds en de Europese Commissie wordt dit goed ondersteund. We moeten wel met elkaar bedenken hoe we hier dan echt de voordelen uit gaan halen. Straks gaat het verder dan ontwikkelen en moeten we bijvoorbeeld quantumchips gaan produceren. Ook daar ligt een urgentie bij de overheid om na te denken hoe we productiefaciliteiten gaan creëren.’

> ***‘ Er is in Nederland een ecosysteem rond quantumtechnologie waarbij alle componenten binnen een straal van 100 kilometer zijn gevestigd. ’***
>
> ***Jesse Robbers, Quantum Delta***

Van Esch wijst op noodzakelijke veranderingen in het investeringsklimaat in Europa. Wanneer daar niets aan gebeurt, voltrekt zich hetzelfde scenario als met kunstmatige intelligentie. ‘Nu al loopt talent weg naar de webgiganten. Ze zitten echt te wroeten bij al onze instituten. Zie die maar eens te behouden als ze opeens een drie keer zo hoog salaris krijgen aangeboden met een appartement in New York.’
Quantum Delta is in gesprek met onder meer overheden en de Europese investeringsbank. ‘Daar zit wel een enorme uitdaging. Wil je echt groot uitbouwen de komende periode, dan heb je voor één zo’n bedrijf al 200 miljoen nodig. Dat zijn bedragen die niet standaard op de markt liggen in Europa.’

De quantumdreiging wordt steeds concreter. Nederland heeft de kennis, het talent en de infrastructuur om een leidende rol in Europa te spelen. Alleen door nu verder te investeren in quantumveilige systemen en de ontwikkeling van quantumtechnologie kan ons land niet alleen de eigen weerbaarheid versterken, maar ook internationaal koploper worden. Maar dat vereist visie, daadkracht en nog betere publiek-private samenwerking.

Op zoek naar kwetsbaarheden

Voordat je systemen quantumveilig kunt maken, moet je eerst onderzoeken wat de kwetsbaarheden zijn en waar ze zich in de systemen bevinden. Het meest kwetsbaar is een aantal methoden gebaseerd op asymmetrische encryptie:
- Digitale handtekeningen op basis van het RSA-algoritme
- Communicatieprotocollen zoals gebruikt in een https-verbinding.
- Uitwisseling van encryptiesleutels op basis van het Diffie-Helman protocol

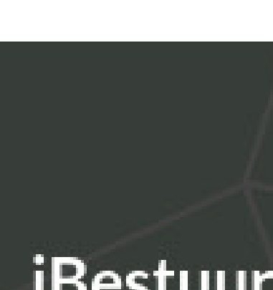
Daarnaast wordt AES, de ‘gouden standaard’ van symmetrische encryptie, zwakker omdat quantumcomputers sleutelruimtes effectiever kunnen doorzoeken.

Wat is de oplossing?

De veiligheid van datatransport kan eigenlijk alleen op het hoogste niveau worden gebracht met een combinatie van twee methoden:
- Postquantum cryptografie. Er zijn inmiddels drie cryptografische methoden gestandaardiseerd die bestand zijn tegen het rekengeweld van de quantumcomputer.
- Quantum key distribution (QKD). Met QKD kunnen cryptografische sleutels veilig uitgewisseld worden met behulp van principes uit de quantum mechanica.
- Dit is een breder concept dat een volledig netwerk van quantumcomputers en -apparaten omvat, met mogelijkheden voor diverse toepassingen.

Hoewel al deze technologie nog in ontwikkeling is, zijn er al toepassingen die daadwerkelijk de benodigde bescherming bieden. De eerste stap voor elke organisatie is echter aan de slag te gaan met de inventarisatie van de zwakke plekken en de risico-inventarisatie.

Dit artikel is ook gepubliceerd in iBestuur #53 van januari 2025.



Over Thijs Doorenbosch
Freelance IT-journalist
Lees meer van Thijs Doorenbosch »

LEES OOK

Data en AI | NIEUWS
RADIO wint aanmoedigingsprijs Nederlandse Privacy Awards

Data en AI | NIEUWS
Italiaanse toezichthouder wil antwoorden van DeepSeek

Digitalisering en Democratie | NIEUWS
Wel of niet van X? Overheden hakken de knoop door