



**Algemene Inlichtingen - en
Veiligheidsdienst**

Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties



**Bescherm je nu tegen
de dreiging van
quantumcomputers**

Jouw organisatie quantumveilig maken?

Start nu!

Al jaren wordt de komst van de quantumcomputer voorspeld die bepaalde cryptografie kan breken. Dit brengt risico's op het gebied van informatiebeveiliging met zich mee. De Algemene Inlichtingen- en Veiligheidsdienst (AIVD) volgt de ontwikkelingen op de voet en doet onderzoek om tijdig producten en oplossingen te kunnen bieden tegen deze beveiligingsrisico's.

Ben jij verantwoordelijk voor de informatiebeveiliging binnen jouw organisatie? Dan kan deze brochure jou helpen inzichtelijk te maken welke dreigingen van quantumcomputers van toepassing zijn op jouw organisatie, en welke stappen je kunt nemen om je hiertegen te beschermen. In deze publicatie deelt de AIVD haar visie op dit vlak, gesteund op eerdere publicaties.

Deze publicatie gaat voornamelijk in op de invloed van quantumcomputers op vertrouwelijkheid van informatie, en in mindere mate op de invloed van quantumcomputers op authenticatie. In onze eerdere publicatie van het handboek uit 2024¹ benoemen we dat de migratie van quantumkwetsbare cryptografie naar quantumveilige cryptografie een tijdrovend en kostbaar proces is. We adviseren organisaties in het handboek daarom de quantumdreiging te mitigeren via een driestappenplan. In deze publicatie geven we je een korte toelichting op deze stappen en vertellen we je wat er zowel op nationaal als internationaal vlak gebeurt.

Deze brochure is een herziene versie van de brochure 'Bereid je voor op de dreiging van quantumcomputers'² uit 2021, zodat het advies in deze brochure aansluit bij de stappen die geadviseerd worden in het handboek¹.

¹ AIVD, CWI, TNO. 'Het PQC-migratie handboek' (2024).

² AIVD. 'Bereid je voor op de dreiging van quantumcomputers' (2021).

Quantumcomputers: een reëel risico?

Al tientallen jaren is bekend dat inzichten vanuit de quantummechanica gebruikt kunnen worden om de meestgebruikte asymmetrische cryptografie (zie kader) aan te vallen met een quantumcomputer. Deze vorm van cryptografie wordt veel gebruikt in hedendaagse IT oplossingen, zoals het gebruik van HTTPS voor internetverkeer. De nu al werkende quantumcomputers hebben nog niet voldoende rekenkracht om een serieuze bedreiging te zijn voor deze veelgebruikte hedendaagse cryptografie. De ontwikkelingen van een 'Cryptografisch Relevante Quantum Computer' (CRQC)³ gaan echter hard. Een CRQC is een geavanceerde quantumcomputer die veelgebruikte hedendaagse asymmetrische cryptografie kan breken. In deze brochure bedoelen wij met een quantumcomputer een CRQC.

Schattingen wanneer een quantumcomputer beschikbaar is lopen sterk uiteen. Experts schatten de kans dat deze er in 2029 al is tussen de 5 en 14%. Voor 2034 stijgt deze kans al naar tussen de 19% en 34%⁴. Voor de bescherming van gevoelige informatie is een kleine kans al voldoende om passende maatregelen te nemen. Daarom adviseert de AIVD maatregelen te nemen voor het geval deze er in 2030 al zou kunnen zijn.

Er zijn nu al risico's voor de informatie die met veelgebruikte, quantumkwetsbare cryptografie, beveiligd wordt. De informatie die je nu gecijferd verstuurt of opslaat, is kwetsbaar voor 'store-now, decrypt-later'-aanvallen (zie kader). Daarnaast hebben organisaties vaak te maken met systemen of apparatuur met een lange levensduur waarbij het moeilijk of zelfs onmogelijk is om deze na ingebruikname nog bij te werken zodat ze quantumveilig worden. Denk hierbij aan complexe IT-infrastructuren met veel afhankelijkheden of industriële besturingsystemen, zoals OT-systemen of SCADA-systemen. Ten slotte kan een volledige migratie naar een quantumveilige oplossing vele jaren duren, afhankelijk van de complexiteit van de migratie⁵.

Daarom adviseert de AIVD je om op tijd te werken aan een migratieplan voor een quantumveilige oplossing. Bepaal met Mosca's ongelijkheid (zie kader) of jouw data nu al kwetsbaar is voor een aanval met een quantumcomputer. Houd je hier geen rekening mee of neem je te laat maatregelen? Dan loop je het risico dat gevoelige of vertrouwelijke informatie van jouw organisatie later alsnog ontcijferd wordt.

³ BSI, 'Status of quantum computer development' v2.1 (2024).

⁴ M. Mosca, M. Piani. 'Quantum threat Timeline report 2024' (2024).

⁵ BSI, KPMG. 'Market Survey on Cryptography and Quantum Computing' (2023).

Asymmetrische cryptografie

Asymmetrische cryptografie, ook wel publieke sleutel-cryptografie genoemd, maakt gebruik van twee verschillende sleutels: een publieke en een private sleutel. Bij het creëren van een dergelijk sleutelpaar wordt de publieke sleutel openbaar gemaakt zodat iedereen een bericht kan versleutelen of digitale handtekeningen kan verifiëren. Met de private sleutel kan de ontvanger van het versleutelde bericht deze ontsleutelen of een digitale handtekening zetten.

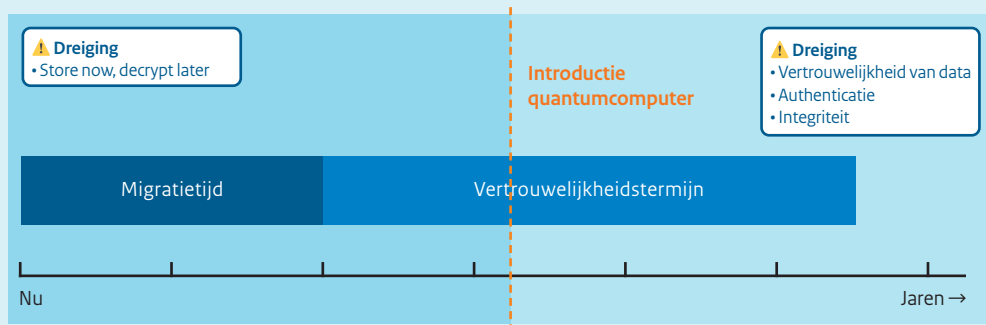
Store now, decrypt later

Omdat vertrouwelijke informatie vaak een lange geheimhoudingstermijn heeft, is de dreiging van een quantumcomputer reëel. Versleutelde data die nu onderschept en opgeslagen wordt, kan op een later moment ontsleuteld worden met een quantumcomputer. Dat kan gebeuren voordat de geheimhoudingstermijn van je informatie verloopt.

Mosca's ongelijkheid

Voor gevoelige data kan de tijd die jouw data veilig moet blijven tientallen jaren zijn. Je kunt Mosca's ongelijkheid gebruiken om te bepalen wanneer jouw data kwetsbaar wordt. Dit is afhankelijk van de tijd die jouw data veilig moet blijven (vertrouwelijkheidstermijn) en de tijd die een migratie naar PQC (migratietijd) in beslag neemt. Deze totale tijd moet kleiner zijn dan de tijd dat een quantumcomputer beschikbaar is. Anders is jouw data nu al kwetsbaar voor een (latere) aanval met een quantumcomputer. Zie figuur hieronder.

Authenticatieoplossingen zijn meestal niet kwetsbaar voor "store now, decrypt later" aanvallen omdat de vertrouwelijkheidstermijn hier kort is. Daarom is de migratie van deze oplossingen op dit moment nog minder urgent. Er moet wel zorg gedragen worden dat ook authenticatie-oplossingen gemigreerd zijn voordat er een quantumcomputer beschikbaar is. Voor bijvoorbeeld Public Key Infrastructures (PKI's) kan een root certificaat wel een lange geldigheidsduur hebben. Hiervoor adviseren we om een migratieplan op te stellen.



Hoe kun je je organisatie beveiligen tegen de dreiging van quantumcomputers?

De AIVD adviseert het gebruik van Post-Quantum Cryptografie

Om je gevoelige of vertrouwelijke data quantumveilig te beschermen, adviseert de AIVD het gebruik van Post-Quantum Cryptografie (PQC) in combinatie met de huidige (quantumkwetsbare) cryptografie. Dit noemen we een ‘hybride constructie’ (zie kader). PQC is een vorm van cryptografie die gebaseerd is op andere wiskundige problemen die niet effectief te kraken zijn met een quantumcomputer. De AIVD ziet dit als dé manier om je te beveiligen tegen aanvallen van quantumcomputers.

Vertrouwen door jarenlang proces van standaardisatie

Dankzij jarenlang open wetenschappelijk onderzoek is er veel vertrouwen in deze vorm van cryptografie. Om zeker te zijn van de veiligheid van cryptografie, is er namelijk tijd nodig om volwassen te worden. Met wetenschappelijk onderzoek en standaardisatie wordt het vertrouwen in de veiligheid van cryptografie vergroot. Dit is een proces dat veel tijd kost. Sinds 2024 wordt het vertrouwen in PQC ondersteund met standaarden van het National Institute of Standards and Technology (NIST)⁶, en aanvullend in 2026 met standaarden van het International Organization for Standardization (ISO)⁷.

De standaarden van NIST zijn tot stand gekomen via een ‘PQC-competitie’. Daarin zijn voorstellen van onderzoekers in verschillende rondes, verspreid over tien jaar, door de cryptografische gemeenschap publiekelijk geanalyseerd. De standaarden van ISO zijn een uitbreiding op de door het NIST gekozen standaarden voor diversifiëring van algoritmen, zodat deze toepasbaar zijn voor verschillende use cases. Het NIST doet zelf ook nog onderzoek naar nieuwe algoritmen ter diversifiëring van hun portfolio (zie kader).

De cryptografische gemeenschap heeft de afgelopen tien jaar veel onderzoek verricht naar de PQC-algoritmen die verwerkt zijn tot deze standaarden en blijft dat op de dag van vandaag nog steeds doen. De AIVD heeft daarom veel vertrouwen in de veiligheid en het toepassen van deze vorm van cryptografie.

⁶ NIST. ‘Module-Lattice-Based Key-Encapsulation Mechanism Standard’ (2024).

⁷ ISO. ‘ISO/IEC 18033-2:2006/DAMd 2: Information technology – Security techniques – Encryption algorithms – Part 2: Asymmetric ciphers, Amendment 2’ (2026).

Hybride constructies

Er is voldoende zekerheid over de veiligheid van de PQC-algoritmen, maar de implementaties zijn nog onvolwassen. Dat betekent dat het nog niet zeker is dat er in de implementaties geen fouten zijn gemaakt, waardoor het algoritme alsnog gebroken kan worden.

Een oplossing om je nu al te beschermen tegen dreigingen van een quantumcomputer, zonder verlies van veiligheid, is een hybride constructie. Dit is een combinatie van vertrouwde (quantumkwetsbare) cryptografie met PQC. Om deze constructie te breken zou een aanvaller beide algoritmen moeten breken. Daarom is de hybride constructie als geheel minimaal even veilig als elk algoritme afzonderlijk.

Standaardisatie

In 2024 zijn door het NIST verschillende PQC-standaarden uitgebracht, waaronder ML-KEM⁸. ML-KEM vervangt de algoritmes voor sleuteluitwisseling, zoals RSA en elliptische krommen. In 2026 gaat ISO in aanvulling ook nog twee standaarden uitbrengen voor quantumveilige sleuteluitwisseling, namelijk FrodoKEM en McEliece⁹.

Voor sleuteluitwisselingen adviseert de AIVD het gebruik van ML-KEM of FrodoKEM. Voor toepassingen waarbij meer zekerheid in de cryptografische constructie gewenst is, heeft FrodoKEM de voorkeur. In FrodoKEM worden namelijk minder wiskundige aannames gedaan, waardoor eventuele toekomstige aanvalsscenario's die ML-KEM zouden kunnen raken, niet per definitie van toepassing zijn op FrodoKEM.

⁸ NIST. 'Module-Lattice-Based Key-Encapsulation Mechanism Standard' (2024).

⁹ ISO. 'ISO/IEC 18033-2:2006/DAMd 2: Information technology – Security techniques – Encryption algorithms – Part 2: Asymmetric ciphers, Amendment 2' (2026).

Hoe migreer je naar een quantumveilige organisatie?

Het is belangrijk om als organisatie op tijd met de migratie te starten. Wanneer je hier te laat mee begint, loop je het risico dat je gevoelige informatie kwetsbaar is. Daarom adviseert de AIVD de volgende drie migratiestappen.

1

Stap 1: stel een diagnose van quantumkwetsbaarheid op

Voordat je met de PQC-migratie start is het belangrijk om eerst te beoordelen hoe groot de urgentie is voor jouw organisatie om te migreren. Aan de hand van deze urgentie kan een zekere diagnose van quantumkwetsbaarheid opgesteld worden. Hiervoor is het belangrijk dat je een inventarisatie maakt van je te beschermen data, welke cryptografische componenten je gebruikt, welke cryptografische afhankelijkheden je hebt en ten slotte een risicobeoordeling van deze informatie. Hiermee krijg je een goed inzicht in je te beschermen informatie, gegevens en systemen.

2

Stap 2: plan je migratie

Met dit inzicht is het mogelijk om een planning te maken van de uit te voeren migratie. Als eerste is het belangrijk een inschatting te maken hoeveel tijd het kost om over te gaan naar PQC om zo te bepalen wanneer de migratie moet plaatsvinden. Daarna kun je controleren of de apparatuur die je organisatie gebruikt overgezet kan worden naar PQC of dat ze vervangen moeten worden. Op deze manier breng je in kaart wat er nodig is voor de migratie en welke knelpunten je mogelijk gaat tegenkomen. Voorbeelden hiervan zijn lastig te updaten apparatuur, benodigde interoperabiliteit met verschillende partijen, lage bandbreedte of beperkte rekenkracht. De laatste twee voorbeelden kunnen mogelijk knelpunten veroorzaken doordat PQC-algoritmen vaak minder efficiënt zijn dan klassieke algoritmen. Voor de meeste toepassingen levert dit geen grote problemen op.

3 Stap 3: voer de migratie uit

Ten slotte is het tijd voor het uitvoeren van de migratie. Er is een compleet beeld van de organisatie over de te migreren cryptografische componenten en welke quantumveilige alternatieven deze kwetsbare componenten kunnen vervangen. Merk op dat een IT-landschap altijd in verandering is. Het is dus belangrijk om de inventarisatie continu up-to-date te houden.

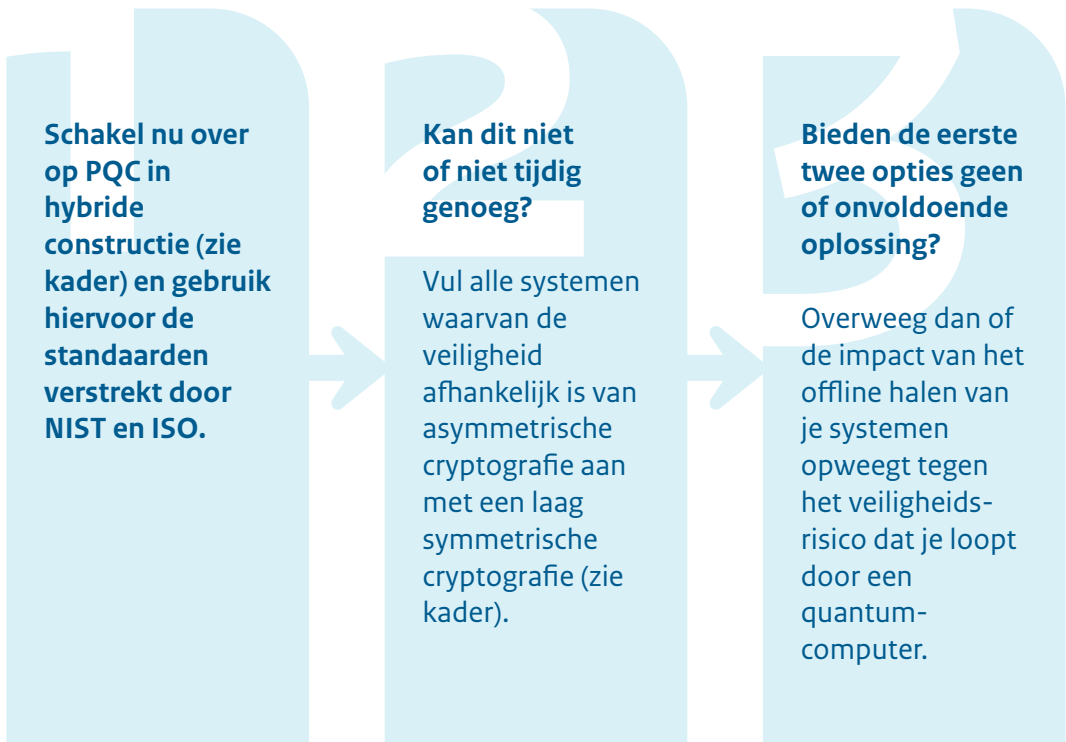
Bij het aanschaffen van nieuwe apparatuur kun je rekening houden met de overgang naar PQC, als onderdeel van je lifecyclemanagement. Houd bij de aanschaf ook rekening met de flexibiliteit van je apparatuur om met verschillende cryptografische algoritmen en sleutellengtes om te gaan. Dit wordt ook wel crypto-agility genoemd. Voor bestaande apparatuur kun je contact opnemen met de leverancier van jouw beveiligingsproducten over wanneer hun producten quantumveilig zijn.

Bovenstaande migratiestappen staan uitgebreid beschreven in het PQC-migratiehandboek¹⁰ dat de AIVD in samenwerking met het CWI en TNO in 2024 heeft uitgebracht.

¹⁰ AIVD, CWI, TNO. 'Het PQC-migratie handboek' (2024).

Wat als mijn data nu al quantumveilig moet zijn?

Heb je vastgesteld dat je vertrouwelijke informatie nu al quantumveilig moet zijn? Dan adviseren we je dit:



Merk op dat je bij bovenstaand advies de eerste stappen van de PQC-migratie overslaat. We adviseren daarom ook om naast bovenstaande noodoplossingen zo snel mogelijk parallel te starten met de eerste stappen van de migratie.

Symmetrische cryptografie

In tegenstelling tot asymmetrische cryptografie (zie kader: asymmetrische cryptografie), maakt symmetrische cryptografie slechts gebruik van één sleutel voor zowel het versleutelen als het ontsleutelen.

Met symmetrische cryptografie is je informatie minder kwetsbaar voor aanvallen met een quantumcomputer. Een veelgebruikt van symmetrische cryptografie is de Advanced Encryption Standard (AES). Met een sterk algoritme zoals AES geeft symmetrische cryptografie met een sleutellengte van 256 bits voldoende cryptografische weerstand tegen een quantumcomputer. Binnen je organisatie kun je de bestaande symmetrische sleutellengtes verhogen naar 256 bits.

Symmetrische cryptografie kun je ook gebruiken als aanvulling op je bestaande beveiliging. Met sommige VPN-producten is het bijvoorbeeld mogelijk om een extra laagje beveiliging toe te voegen met een symmetrisch gedeeld geheim. Ook kun je door asymmetrische cryptografie beveiligde verbindingen tunnelen door een symmetrisch beveiligde verbinding. Op die manier is eventueel onderschepte informatie alsnog beveiligd tegen een aanvaller met een quantumcomputer. Hierbij is het van belang dat het gedeelde symmetrische geheim op een quantumveilige manier wordt uitgewisseld, bijvoorbeeld offline.

Wat gebeurt er al op nationaal en internationaal vlak?

Zowel nationaal als internationaal worden er verschillende migratiestrategieën opgesteld om ervoor te zorgen dat overheden en organisaties gelijktijdig migreren naar een quantumveilige organisatie.

Zo is er binnen de Rijksoverheid het programma Quantumveilige Cryptografie Nederland (QvC NL) ingericht om de Rijksoverheid en andere organisatie binnen Nederland te helpen de risico's van quantumtechnologie op cryptografie op tijd te beheersen¹¹.

De Europese Commissie heeft een aanbeveling gepubliceerd waarin lidstaten wordt aangemoedigd een PQC-migratiestrategie op te stellen¹². Daarnaast hebben lidstaten, aangemoedigd door de Europese Commissie om de migratie gecoördineerd uit te voeren, gezamenlijk een routekaart te ontwikkelen met tijdslijnen voor de migratie naar PQC¹³.

Aanbevelingen van andere landen

Al sinds 2022 hebben de Verenigde Staten via een memorandum van het Witte Huis¹⁴ organisaties verplicht gesteld tot het oprichten van PQC-migratieprojecten en het nemen van extra beveiligingsmaatregelen voor National Security Systems (NSS)¹⁵. Ook het Verenigd Koninkrijk heeft in hun Cyber Security Strategie¹⁶ beschreven dat het vervangen van de huidige cryptografie door PQC de meest effectieve maatregel is in het tegengaan van de quantumdreiging en dat ze deze maatregel binnen de overheid zullen doorvoeren wanneer dit nodig is.

¹¹ Digitale Overheid. 'Bereid je voor' Beschikbaar op <https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/quantumveilige-cryptografie/bereid-je-voor/>, geraadpleegd op 31 juli 2025.

¹² Europese Commissie. 'Commission recommendation on a Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography' (2024).

¹³ NIS Cooperation Group. 'A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography' (2025).

¹⁴ US White House. 'National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems' (2022).

¹⁵ NSA. 'Commercial National Security Algorithm Suite 2.0' https://media.defense.gov/2022/sep/07/2003071836/-1/-1/o/CSI-CNSA_2.0_FAQ.PDF (2025).

¹⁶ US White House. 'National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems' (2022).

Ook binnen de Europese Unie hebben verschillende lidstaten al aanbevelingen en adviezen uitgebracht ten opzichte van een PQC-migratiestrategie. Zo heeft Duitsland (BSI) in 2021 aanbevelingen¹⁷ uitgebracht hoe te beginnen met de migratie en heeft Frankrijk (ANSSI) in 2022 haar visie¹⁸ op de Post-Quantum Cryptografie migratie uiteengezet.

Ondanks dat er kleine nuanceverschillen bestaan tussen Duitsland, Frankrijk en Nederland op het gebied van de PQC-migratie, zijn de landen het over het algemeen eens met elkaar en met de aanbevelingen zoals beschreven in de aanbeveling van de Europese Commissie. In 2025 hebben deze drie landen samen met vijftien andere Europese lidstaten een gezamenlijke verklaring¹⁹ uitgebracht over het mitigeren van de urgente quantumdreiging door te migreren naar PQC.

De unit Weerbaarheid van de AIVD

Bij de AIVD heeft de unit Weerbaarheid als taak om Nederland veilig te houden tegen statelijke dreigingen. Zij combineren hun specialistische beveiligingskennis met de bijzondere inlichtingenpositie die de AIVD heeft. Op deze manier helpt de unit Weerbaarheid organisaties binnen de Rijksoverheid, vitale sectoren en hightechsector om weerbaarder te worden en bijzondere en gevoelige informatie zoals staatsgeheimen en kritieke processen te beschermen. Dit gebeurt onder andere door advies te geven over (quantumveilige informatiebeveiligingsproducten.

Als er vragen zijn neem dan contact op met de accountmanager van de unit Weerbaarheid.

Daarnaast wijzen we organisaties nog graag op het PQC-migratiehandboek 2.0²⁰, waarin meer gedetailleerde informatie te vinden is.

¹⁷ BSI. 'Migration to Post Quantum Cryptography' (2021).

¹⁸ ANSSI. 'ANSSI views on the Post-Quantum Cryptography transition' (2022).

¹⁹ BSI, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, ANSSI, +15 Europese lidstaten. 'Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptography' (2025).

²⁰ AIVD, CWI, TNO. 'Het PQC-migratie handboek' (2024).

Lees ook onze andere publicaties

Op www.aivd.nl/publicaties vind je meer publicaties, hieronder enkele voorbeelden.



Publicatie: PQC migratiehandboek



Publicatie: Maak je organisatie quantumveilig



Publicatie: Verdedigbaar netwerk hoe doe je dat?



Publicatie: Cybersecuritybeeld Nederland 2025

Algemene Inlichtingen- en Veiligheidsdienst
Postbus 20010 | 2500 EA Den Haag
aivd.nl

April 2026