# Cybersecurity Technologies

*In 2035 heeft Nederland een concurrerende cybersecuritymarkt met voldoende talent ontwikkeld, en middels een multidisciplinaire aanpak een internationaal leidende positie in innovatieve cybersecuritytechnologieën verworven. Deze technologieën leveren een essentiële bijdrage aan de beveiliging van infrastructuren en IT- en OT-netwerken, de transitie naar post-quantum cryptografie en meer automatische detectie en verdediging door inzet van AI. Middels onderzoek en meer publiek-private samenwerking, op nationaal en internationaal niveau, is de kennispositie versterkt en is kennisvalorisatie toegenomen. Hiermee is cybersecurity een geïntegreerd onderdeel van de Nederlandse sectoren door het toepassen van security-by-design, security-by-default, cybersecurity in de toeleveringsketen van organisaties en bedrijfsketens. Dit alles draagt bij aan een digitaal veilig, weerbaar, autonoom en welvarend Nederland.*

## 1.1 Definitie

### 1.1.1 Belang van de sleuteltechnologie

Door de toenemende digitalisering van de samenleving is cybersecurity een essentiële randvoorwaarde om de nationale veiligheid, het verdienvermogen en andere maatschappelijke belangen van Nederland te kunnen beschermen.[1] Cybersecuritytechnologieën dragen bij aan digitale veiligheidsuitdagingen in alle sectoren van de maatschappij. Door technologische ontwikkelingen zoals kunstmatige intelligentie (AI) en quantum computing zal het belang en de afhankelijkheid van digitale processen blijven toenemen. Dit maakt de samenleving kwetsbaar voor cyberincidenten zoals uitval van (kritieke) systemen en activiteiten van kwaadwillende actoren. Daarnaast bieden technologische ontwikkelingen nieuwe manieren voor kwaadwillende actoren om cyberaanvallen uit te voeren op organisaties.

De digitale dreiging voor de Nederlandse samenleving neemt sterk toe. Zo blijkt uit het Cybersecuritybeeld 2023[2] (CSBN) dat Nederland geconfronteerd wordt met een toenemende dreiging van statelijke actoren die cyberactiviteiten inzetten, waaronder beïnvloeding, spionage, verstoring en sabotage. Deze dreiging wordt zichtbaar door een toenemend aantal digitale aanvallen op operationele technologieën (OT), waarbij sectoren zoals de gezondheidszorg, high-tech, energievoorziening, vervoer en defensie het risico lopen op ernstige verstoringen.[3]

Tevens dragen nieuwe sleuteltechnologieën bij aan de toenemende digitale dreiging. Een voorbeeld hiervan is de opkomst van quantumtechnologie. Quantumtechnologie biedt niet alleen kansen voor (cybersecurity)innovaties, maar vormt ook een bedreiging voor bestaande data encryptie methoden en kan daarmee de vertrouwelijkheid van digitale communicatie in gevaar brengen. Ook brengt de snelle ontwikkeling van kunstmatige intelligentie (AI) nieuwe uitdagingen met zich mee voor het detecteren van digitale indringing en de verdediging daartegen. Als gevolg van deze ontwikkelingen groeit de urgentie om effectieve cybersecuritymaatregelen te ontwikkelen die inspelen op de technologische en internationale ontwikkelingen van de komende jaren. Het ontwikkelen van organisatiemaatregelen, menselijke vaardigheden en effectieve wetgeving zijn essentiële bouwstenen voor het opbouwen van de nationale cyberweerbaarheid. Ondanks inspanningen om de digitale weerbaarheid te verhogen, is sprake van een scheefgroei tussen de toenemende dreiging en de ontwikkeling van de weerbaarheid.[4] Om die reden is de kabinetsbrede Nederlandse Cybersecuritystrategie 2022 – 2028 (NLCS)[5] opgesteld om Nederland digitaal veilig te maken door de digitale weerbaarheid te verhogen en dreigingen tegen te gaan.

Naast deze cybersecuritymaatregelen is kennis en innovatie rondom cybersecuritytechnologieën nodig voor de digitale weerbaarheid en het verdienvermogen van Nederland. Pijler 2 van de NLCS 2022 – 2028[6] benadrukt de noodzaak van gerichte investeringen in kennis- en innovatieontwikkeling van cybersecuritytechnologieën en toepassing ervan in onze economie en samenleving om nieuwe digitale dreigingen het hoofd te bieden. Dit verhoogt onze cyberweerbaarheid, vermindert de afhankelijkheid van buitenlandse bedrijven en oplossingen en bevordert de Nederlandse digitale open strategische autonomie.[7]

Het feit dat *'cybersecurity technologies'* als agenda is opgenomen in de Nationale Technologiestrategie (NTS) past goed bij deze inzet. Deze agenda is een nadere uitwerking van pijler 2 van de NLCS en daarmee gericht op het stimuleren van cybersecurity kennisontwikkeling en -innovatie. Tegelijkertijd is het essentieel dat deze agenda de verbinding zoekt en in samenhang wordt bezien met andere vraagstukken. Zo is het is noodzakelijk om de Nederlandse cybersecurityarbeidsmarkt aantrekkelijker te maken voor nieuw talent om deze doelstellingen te realiseren.[8] Daarnaast is een multidisciplinaire aanpak nodig voor cybersecurityuitdagingen, waarbij ook technische en niet-technische kennis worden gebundeld, om de juiste lange termijn keuzes te maken. Ook is het belangrijk om samenwerking te zoeken met vertegenwoordigers van Nederlandse sectoren waar grote transities plaatsvinden zoals de energiesector, logistiek, chips- en maakindustrie en de maritieme sector. In die transities is het essentieel dat cybersecurityprincipes zoals *cybersecurity-by-design*, *cybersecurity-by-default* en *cybersecurity in de toeleveringsketen* worden meegenomen zodat deze sectoren inherent cyberweerbaar worden.

### 1.1.2 Definitie[9]

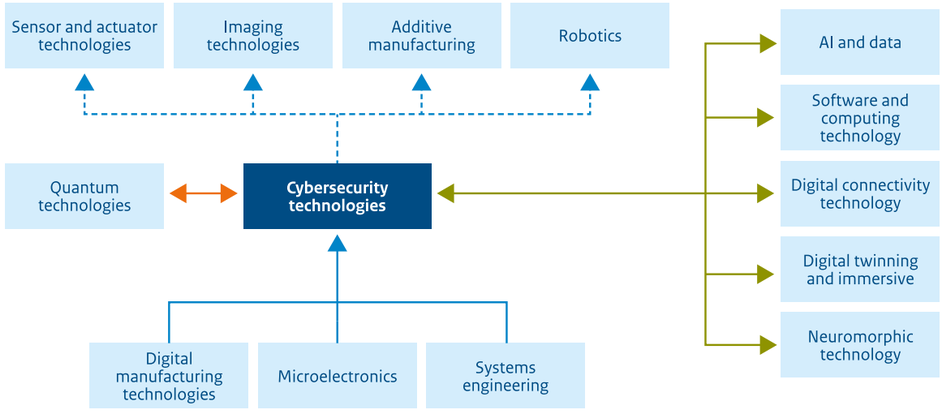
Cybersecuritytechnologieën zijn de digitale technische toepassingen die bedoeld zijn om relevante digitale risico's te verkleinen. Dit omvat ook het omgaan met risico's op schade of uitval van digitale systemen en de beschikbaarheid, integriteit en vertrouwelijkheid van gegevens. Daarnaast zijn cybersecuritytechnologieën gericht op het voorkomen van cyberincidenten en, wanneer cyberincidenten zich hebben voorgedaan, deze te ontdekken, schade te beperken en herstel eenvoudiger te maken. Wat een aanvaardbaar niveau is, is veelal de uitkomst van een risico-afweging.

### 1.1.3 Gerelateerde sleuteltechnologieën

Cybersecurity is een randvoorwaarde voor de ontwikkeling en succesvolle toepassing van alle digitale sleuteltechnologieën. Dit zijn met name de sleuteltechnologieën die tot het cluster *digital and information technologies* behoren en vallen onder de vlag van de Kennis- en Innovatieagenda Digitalisering (KIA)[10]: *AI and Data*, *software technologies and computing*, *digital connectivity technologies*, *digital twinning and immersive technologies* en *neuromorphic technologies*. Producten die ontwikkeld worden op basis van deze sleuteltechnologieën zullen vanwege hun digitale karakter inherent cybersecurity risico's kennen. Tegelijkertijd zijn deze digitale sleuteltechnologieën ook essentieel voor de ontwikkeling van cybersecuritytoepassingen. Denk aan het gebruik van AI en data voor geautomatiseerde detectiesystemen en softwaretechnologie voor toepassingen in softwarebeveiliging. In de figuur hieronder zijn deze digitale technologieën te herkennen aan de groene lijnen.

De sleuteltechnologieën *digital manufacturing technologies*, *microelectronics* en *systems engineering* zijn nodig voor cybersecuritytoepassingen. Sleuteltechnologieën zoals *sensor and actuator technologies*, *imaging technologies*, *additive manufacturing* en *robotics* hebben *cybersecurity technologies* ook nodig om deze mogelijk te maken. Echter, vanwege de digitale component in deze sleuteltechnologieën dient rekening gehouden te worden met cybersecurityrisico's en zijn *cybersecurity technologies* wel van belang. *Quantum technologies* bieden risico's voor de bestaande cryptografische protocollen, maar tegelijkertijd kansen voor nieuwe manieren van beveiliging (oranje lijn).

Gerelateerde sleuteltechnologieën




*Bron: TNO Rapport Herijking Sleuteltechnologieën 2023 (kia-st.nl)*

## 1.2 Positie, sterktes/zwaktes

### 1.2.1 Ontwikkelingsfase technologie

Cybersecuritytechnologieën bevinden zich in een fase van doorlopende ontwikkeling. Mede vanwege het snel veranderende cyberdreigingslandschap zijn innovatie en aanpassing voortdurend nodig. Door de toenemende digitalisering, nieuwe technologische ontwikkelingen en de geopolitieke situatie neemt de afhankelijkheid van digitale processen steeds meer toe[11], en daarmee ook de impact op de samenleving. De ontwikkeling en toepassing van cybersecuritytechnologieën hangt dan ook nauw samen met de ontwikkeling van andere (sleutel)technologieën, die zowel risico's als kansen bieden voor cybersecurity.

Een van deze technologieën is de ontwikkeling van AI, dat kwaadwillende actoren mogelijkheden biedt om snel en gemakkelijk cyberaanvallen uit te voeren. Zo kan generatieve AI gebruikt worden voor phishing-aanvallen die voor ontvangers niet meer te onderscheiden zijn van onschuldige communicatie.[12] Tegelijkertijd biedt het gebruik van AI mogelijkheden voor betere cybersecurity en draagt AI bij aan de verhoging van de arbeidsproductiviteit van een organisatie.[13]

Een andere ontwikkeling is de conversie van OT-netwerken naar IT/OT integratie in verschillende bedrijfssectoren. Het aantal cyberaanvallen op deze netwerken neemt steeds meer toe, en daarmee ook het risico op uitval van bijvoorbeeld ziekenhuisapparatuur of industriële systemen van fabrieken. Dit geldt eveneens voor consumentenapparaten zoals koelkasten en TV's die verbonden zijn aan het internet (Internet of Things). Vanwege deze ontwikkelingen is de Europese Unie (EU) actief in het opstellen van meer cybersecurityeisen via de Cyber Resilience Act (CRA)[14] en de herziening van de netwerk- en informatiebeveiligingsrichtlijn (NIS2-richtlijn).[15]

Daarnaast is post-quantum cryptografie (PQC) een andere belangrijke ontwikkeling die steeds meer aandacht krijgt. De Europese Commissie heeft een aanbeveling opgesteld waarin de urgentie van PQC staat beschreven.[16] De verwachting is dat de quantumcomputer veel mogelijkheden biedt, maar eveneens een dreiging vormt voor cybersecurity. De quantumcomputer zal in staat zijn om veel gebruikte vormen van cryptografie te ontsleutelen. Er is onderzoek en innovatie nodig om een betrouwbare transitie naar quantumveilige protocollen mogelijk te maken. Vervolgens hebben organisaties die IT-systemen en -producten beheren de tijd nodig om vanuit de bestaande cryptografie naar PQC te migreren. Tijdige voorbereidende stappen voor PQC-migratie en innovatie rondom PQC en de transitie naar *security-by-design* zijn daarom cruciaal.

### 1.2.2 Internationale positie en omvang

De mondiale cybersecuritymarkt heeft een totale omvang van 153 miljard dollar[17]. In 2019 kwam van de 500 meest verkopende cybersecuritybedrijven 75 procent uit de VS, 15 procent uit de EU en 7 procent uit Israël.[18] Op het gebied van innovatie en investeringen hebben vooral de VS en China een sterke positie.[19] Naar verwachting zal de cybersecuritysector in ieder geval in het komend decennium sterk blijven groeien.

Enkele globale spelers en bedrijven zijn o.a. Palo Alto, IBM, Broadcom, Check Point Software Technologies.[20]

Op het gebied van wetenschappelijk onderzoek heeft de EU een sterke positie, maar op innovatie en investeringen is dat minder het geval. Nederland heeft een sterke positie in Europa en is met name toonaangevend op het gebied van kennis, bijvoorbeeld rondom cryptografie. Voor cybersecuritydienstverlening zijn er verschillende Nederlandse en Europese leveranciers, ook voor het testen en certificeren van producten. Daarnaast zijn er Nederlandse en Europese bedrijven actief op de wereldwijde markt voor cryptografische producten.

Europa stelt financiering beschikbaar voor de ontwikkeling van de cybersecuritysector via de programma's Horizon Europe en Digital Europe. Ook heeft het Europees Cybersecurity Competence Center (ECCC) een belangrijke rol in het versterken van de industriële en technologische capaciteit van de sector, onder meer door financiering beschikbaar te stellen voor de ontwikkeling van ecosystemen en het stimuleren van kennis en innovatie in het cybersecuritydomein in Europa.

### 1.2.3 Europese wet- en regelgeving

Op Europees niveau is recentelijk een aanzienlijk pakket aan regelgeving voor cybersecurity vastgesteld. De herziende netwerk- en informatiebeveiligingsrichtlijn (NIS2-richtlijn)[21] is sinds 16 januari 2023 van kracht. De lidstaten hebben een termijn van 21 maanden (tot 17 oktober 2024) om deze EU-richtlijn om te zetten in nationale wetgeving. De NIS2-richtlijn schrijft voor dat cybersecurity een verplicht onderdeel wordt van de bedrijfsvoering van de middelgrote en grote ondernemingen in 18 specifieke sectoren. Alle Europese landen beschikken over een nationale cybersecuritystrategie. Ook is er inmiddels een politiek akkoord bereikt over de Cyber Resilience Act (CRA). Die verordening bouwt voort op de cybersecuritymaatregelen voor digitaal verbonden apparaten uit de Radioapparatenrichtlijn (RED). De CRA maakt dat digitaal verbonden producten die op de interne markt worden aangeboden aan cybersecurityvereisten moeten voldoen, en tijdens de redelijk te verwachten levensduur veilig moeten blijven. De reeds ingevoerde Cybersecurity Act (CSA) voorziet in de ontwikkeling van certificeringsschema's voor ICT-producten, diensten en processen. Naar verwachting zal een secundair effect van Europese wet- en regelgeving zijn dat de vraag van organisaties naar (geautomatiseerde) cybersecurityoplossingen toeneemt om te kunnen voldoen aan de gestelde eisen, wat cybersecurityinnovaties in de hand kan werken.

### 1.2.4 Nationale positie en omvang

In het onderzoek van Dialogic naar economische kansen van de Nederlandse cybersecuritysector (2023)[22] is een duidelijke groei van de (geschatte) omzet en het aantal werknemers te zien. In 2021 kent de Nederlandse cybersecuritysector een geschatte omzet van circa €16 miljard en een werknemersaantal van circa 94.600. De toegevoegde waarde ligt rond de € 7,5 miljard, wat overeenkomt met 0,94% van het bruto binnenlands product (BBP). De onderstaande tabel geeft een kwantitatieve inschatting van de omvang en groei van de cybersecuritysector weer.

*Tabel 3: onderzoek dialogic*

| | 2017 | 2018 | 2019 | 2020 | 2021 | $CO_2$ |
|---|---|---|---|---|---|---|
| Omzet (€ mld.) | 12,1 | 13,5 | 14,7 | 16,4 | 16 | |
| Toegevoegde waarde (€ mld.) | 6,7 | 7 | 7,5 | 7,5 | | |
| Aandeel van het BBP (%) | 0,91% | 0,91% | 0,92% | 0,94% | | 6-7 |
| Aantal werknemers (X1000) | 93,1 | 86,5 | 93,8 | 86,3 | 94,6 | |

*Bron: onderzoek Dialogic naar de economische kansen van de Nederlandse cybersecuritysector (2023)*

Naast de groeiende cybersecuritysector is er in Nederland een sterke kennisbasis in cybersecuritytechnologieën. Nederlandse kennisinstellingen en innovatieve bedrijven richten zich op veel aspecten van cybersecurity, maar staan in het bijzonder bekend om de ontwikkeling van cryptografie. Nederland heeft binnen de EU en NAVO als een van de weinige landen de status van *cryptoproducing nation*.[23] Doordat Nederland zelf in staat is om cryptografische producten te produceren, is Nederland niet afhankelijk van andere landen als het gaat om het beschermen van staatsgeheimen. Deze autonome positie staat echter onder druk vanwege een beperkte marktomvang en de sterke internationale concurrentie. Dit wordt echter, zoals aangegeven in de Nederlandse Cybersecuritystrategie 2022-2028, door implementatie van de Nationale Cryptostrategie (NCS) geadresseerd. De NCS stimuleert de overheid bij de ontwikkeling van cryptografische producten voor staatsgeheimen en is het doel om bedrijven in deze nichemarkt te laten floreren. Dit moet op termijn ook zorgen voor *spin-off* producten die voor minder zware toepassingen geschikt zijn, zoals in de netwerken van vitale organisaties.

Ondanks de sterke kennisbasis loopt Nederland relatief achter als het gaat om investeringen in innovatieve cybersecurity-technologieën. De terughoudendheid van investeerders en bedrijven om te investeren in cybersecurity verzwakt de Nederlandse cybersecuritymarkt, en versterkt de afhankelijkheid van buitenlandse producenten van cybersecurityproducten. Ook wordt er weinig Research & Development (R&D) op het gebied van cybersecurity uitgevoerd door bedrijven: de uitgaven van Nederlandse bedrijven aan R&D in het algemeen liggen relatief laag: met circa 1,4% van het BBP ten opzichte van bijvoorbeeld Duitsland (2,2%), VS (2,0%) en Zuid-Korea (3,5%).[24]

Via het programma Cybersecurity voor Nederland (CS4NL), uitgevoerd onder regie van het samenwerkingsplatform dcypher in samenwerking met Topsector ICT, wordt gewerkt aan meer cybersecurityinnovatie door het versterken van de samenwerking tussen het bedrijfsleven (o.a. topsectoren) en kennisinstellingen. Dit gebeurt door het uitzetten van onderzoeksubsidies op cybersecurityinnovatie-thema's waarop consortia kunnen inschrijven. Deze subsidies worden ontwikkeld in samenwerking met de Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO) en Topconsortium voor Kennis en Innovatie (TKI).

### 1.2.5 Specifieke toepassingsgebieden

Cybersecuritytechnologieën worden in een scala aan toepassingsgebieden gebruikt om digitale systemen, netwerken en gegevens te beschermen tegen bedreigingen en aanvallen. Enkele toepassingsgebieden zijn:

- **Netwerkbeveiliging:** Dit omvat het beschermen van computernetwerken tegen ongeautoriseerde toegang, aanvallen en misbruik. Technologieën zoals firewalls, intrusion detection/prevention systems (IDS/IPS), virtual private networks (VPN) en beveiligingsprotocollen zoals SSL/TLS worden hier veel gebruikt.
- **IT/OT security:** Dit omvat de bescherming van meet- en regelsystemen die voor de aansturing van industriële processen of gebouwbeheersystemen worden gebruikt. Internationaal wordt de term IACS (*Industrial Automation and Control Systems*) veel gehanteerd.
- **Endpoint-beveiliging:** Dit omvat het beschermen van individuele apparaten zoals computers, smartphones en tablets tegen malware, ransomware, en andere bedreigingen. Antivirussoftware, antimalwarescanners en endpoint detection and response (EDR) oplossingen worden hier vaak ingezet.
- **Cloudbeveiliging:** Met het toenemende gebruik van van cloud computing platformen, zijn technologieën nodig om gegevens en applicaties in de cloud te beschermen tegen aanvallen en datalekken. Encryptie, identity and access management (IAM), en cloud security posture management (CSPM) zijn enkele voorbeelden van cloudbeveiligingstechnologieën.
- **Gegevensbescherming:** Dit omvat het beschermen van gevoelige gegevens tegen ongeautoriseerde toegang, diefstal en manipulatie. Technologieën zoals encryptie, tokenisatie en databeveiligingsoplossingen worden gebruikt om gegevens te beschermen, zowel in rust als in transit.
- **Webbeveiliging:** Dit omvat het beschermen van websites en webapplicaties tegen aanvallen zoals SQL-injecties, cross-site scripting (XSS) en distributed denial-of-service (DDoS) -aanvallen. Web application firewalls (WAF's), content security policies (CSP's) en vulnerability scanners worden hier vaak gebruikt.

### 1.2.6 Risico's voor nationale veiligheid

Uit het Cybersecuritybeeld Nederland (CSBN) 2023[25] blijkt dat de cybersecuritydreiging voor Nederland onverminderd groot blijft en voortdurend groeit. De geopolitieke spanningen nemen toe onder andere vanwege de Russische oorlog tegen Oekraïne. Deze oorlog heeft geleid tot een opleving van op ontwrichting gerichte cyberaanvallen. Deze digitale dreiging kan abrupt veranderen, bijvoorbeeld bij verdere escalatie van de oorlog, en Nederlandse belangen kunnen worden geraakt.

Het CSBN 2023 benadrukt daarnaast de voortdurende uitdagingen op het gebied van risicobeheersing. Nieuwe Europese wetgeving legt extra eisen op voor digitale veiligheid, terwijl de verzekerbaarheid van digitale risico's onder druk staat, vanwege de toename van digitale risico's en de mogelijkheid van cyberincidenten om uit te groeien tot een systemische crisis. Daarnaast benadrukken de onderlinge verwevenheid binnen het bredere ecosysteem en de gelegenheidsstructuur voor cyberaanvallen de complexiteit van de digitale dreiging.

Het verkleinen van de scheefgroei tussen digitale dreiging en weerbaarheid blijft een grote uitdaging. Deze spanning is nadrukkelijk aanwezig op het gebied van OT. OT is een kwetsbare bouwsteen voor vitale processen, doordat deze een centrale rol speelt in het aansturen, monitoren en beheren van fysieke processen van organisaties. Daarmee fungeert OT als motor van vitale sectoren en vereist voortdurende aandacht voor cybersecurity. Tot slot vragen de bijzondere kenmerken van digitale risico's om een bredere benadering van risicobeheersing, waarbij digitale risico's worden beschouwd als integraal onderdeel van de nationale veiligheid, zoals ook aangegeven in de recent gepubliceerde 'Cybercheck: ook jij hebt supply chain risico's'.[26]

Voor de Nederlandse cybersecuritymarkt houdt dit in dat verdere investeringen, innovaties en absorptiecapaciteit van cruciaal belang zijn om de onverminderd hoge cyberdreiging het hoofd te kunnen bieden. Integratie van andere technologieën zoals AI kunnen daar een impuls aan geven en de Nederlandse cybersecuritymarkt onderscheiden van het buitenland. Te grote afhankelijkheid van cybersecuritybedrijven uit andere landen kan namelijk op termijn een zorg zijn, bijvoorbeeld in het kader van *vendor lock-in*. Daarnaast is het tekort aan cybersecuritypersoneel een punt van zorg: zonder de beschikbaarheid van voldoende talent zullen organisaties in Nederland (van grote bedrijven en overheidsorganisaties tot het mkb) onvoldoende hun digitale weerbaarheid op orde kunnen krijgen.

### 1.2.7 SWOT[27]

De Nederlandse cybersecuritysector vertoont een aantal sterke kanten met in 2020 een omzet van €16 miljard. De sector voldoet goed aan de binnenlandse vraag naar diensten en heeft vooralsnog een solide kennisbasis in cryptografisch onderzoek. Echter, er is een gebrek aan cybersecurity R&D-activiteiten en beperkte opschaal- en exportmogelijkheden van diensten wat leidt tot meer afhankelijkheid van buitenlandse leveranciers, wat de slagkracht van Nederlandse bedrijven beperkt. Kansen voor de Nederlandse cybersecuritysector omvatten een diepere integratie van wetenschappelijke en toegepaste kennis in bedrijfs-R&D, zoals over toepassing van AI voor cybersecurity en PQC. Uitdagingen waar bedrijven rekening mee moeten houden zijn bijvoorbeeld het tekort aan cybersecuritytalent, een beperkte bewustwording van het belang van cybersecurity bij afnemende partijen, belemmeringen op de Europese interne markt, overnames van innovatieve midden en kleinbedrijven (mkb) door buitenlandse partijen en gebrek aan durfkapitaal en overheidsinvesteringen.

| Sterkte | Zwakte |
|---|---|
| • Sterke kennisbasis cybersecuritytoepassingen (AI, PQC)<br>• Sterke groei cybersecuritysector | • Versnipperd onderzoeksveld en weinig cyber R&D<br>• Te weinig aandacht innovatie<br>• Afhankelijkheid buitenlandse partijen (big tech) |
| **Kans** | **Bedreiging** |
| • Groeiende mogelijkheden van AI<br>• Stevig en duurzame concurrentiepositie groeisectoren<br>• Groei van verdienvermogen | • Krapte cybersecurityarbeidsmarkt<br>• Gebrek durfkapitaal en overheidsinvesteringen<br>• Overnames start-ups door grote buitenlandse partijen |

Bron: *Ronde tafels en onderzoek Dialogic (De economische kansen van de cybersecuritysector, 2023)*

## 1.3 Ambitie

### 1.3.1 Hoofdambitie

In 2035 heeft Nederland een concurrerende cybersecuritymarkt met voldoende talent ontwikkeld, en middels een multidisciplinaire aanpak een internationaal leidende positie in innovatieve cybersecuritytechnologieën verworven. Deze technologieën leveren een essentiële bijdrage aan de beveiliging van infrastructuren en IT- en OT-netwerken, de transitie naar post-quantum cryptografie en meer automatische detectie en verdediging door inzet van AI. Middels onderzoek en meer publiek-private samenwerking, op nationaal en internationaal niveau, is de kennispositie versterkt en is kennisvalorisatie toegenomen. Hiermee is cybersecurity een geïntegreerd onderdeel van de Nederlandse sectoren door het toepassen van *security-by-design*, *security-by-default*, *cybersecurity in de toeleveringsketen* van organisaties en bedrijfsketens. Dit alles draagt bij aan een digitaal veilig, weerbaar, autonoom en welvarend Nederland.

### 1.3.2 Deelambities

De hoofdambitie wordt uiteengezet aan de hand van de uitdagingen uit de kabinetsstrategie "Versterken van onderzoeks- & innovatie ecosystemen"[28] die relevant zijn voor cybersecuritytechnologieën. Per uitdaging wordt een deelambitie geformuleerd die bijdraagt aan de hoofdambitie.

**Lange termijn blik en samenhang bij investeringen in onderzoek en innovatie**

In Nederland wordt nog onvoldoende geïnvesteerd in onderzoek en innovatie rondom cybersecurity. Het volume van investeringsprojecten vanuit private en publieke partijen is nog te klein. Hiervoor is meer samenhang tussen onderzoeks- en innovatieactiviteiten, en goede samenwerking tussen alle daarbij betrokken partijen cruciaal. Een multidisciplinaire benadering van kennis- en innovatieontwikkeling rondom cybersecurity, waarbij specialisten van andere werkgebieden en sleuteltechnologieën worden betrokken, zorgt voor meer samenhang en innovatieve inzichten en oplossingen. Innovatieve partijen hebben kritieke marktmassa nodig om succesvol te zijn. Als grote afnemer speelt de overheid hier een grote rol in.

**Deelambitie:** In 2035 is middels een multidisciplinaire aanpak meer samenhang gecreëerd tussen investeringen in cybersecurity en andere disciplines, zoals quantumtechnologie en AI en andere relevante sleuteltechnologieën, maar ook niet-technische disciplines zoals gedragswetenschappen en economie. De overheid is een belangrijke afnemer van deze producten.

**Investeringen in onderzoeks- en testfaciliteiten**

De onderzoeks- en testfaciliteiten zijn een onmisbaar element van cybersecurityinnovaties: goede faciliteiten maken onderzoek mogelijk en helpen bedrijven bij het oplossen van uitdagingen in de pre-competitieve fase. Voldoende cybersecurity-talent is hierbij een randvoorwaarde. De huidige faciliteiten in het cybersecuritydomein zijn veel gericht op het voldoen aan wet- en regelgeving en het adresseren van cybersecuritydreigingen en -risico's van (sleutel)technologieën, en minder op het gebruikmaken van de kansen van (sleutel)technologieën. Hiervoor is het van belang dat principes zoals security-by-design worden meegenomen in onderzoeks- en testfaciliteiten van andere (sleutel)technologieën. Het delen van data draagt daarnaast ook bij aan goed wetenschappelijk onderzoek.

**Deelambitie:** In 2035 is cybersecurity (*security-by-design en security-by-default*) een vanzelfsprekend onderdeel van onderzoeks- en testfaciliteiten van verschillende (sleutel)technologieën. Verder heeft Nederland voldoende faciliteiten en de juiste infrastructuur voor cybersecurityonderzoeken, zodat bedrijven en academische onderzoekers gemakkelijker onderzoek kunnen doen en uitdagingen in de pre-competitieve fase kunnen oplossen.

**Financiering voor startups en scale-ups: vroege fase financiering en doorgroei**

Vergeleken met de VS, waar de meest toonaangevende cybersecuritybedrijven gevestigd zijn, wordt in de EU relatief weinig geïnvesteerd in innovatieve cybersecurity startups en scale-ups.[29] Wanneer het gaat om investeringen die benodigd zijn voor opschaling van cybersecurity bedrijven wordt vaak uitgeweken naar het buitenland.[30] Veelbelovende cybersecurity startups in Nederland worden snel overgenomen door buitenlandse partijen, waardoor de sector zich beperkt ontwikkelt.[31]

**Deelambitie:** In 2035 is de kennis bij Nederlandse investeerders ten aanzien van cybersecurity vergroot, is er voldoende toegang tot durfkapitaal voor cybersecurity bedrijven, worden bestaande financieringsinstrumentaria nog steeds effectief ingezet en zijn er geen belemmeringen op de interne markt voor duurzame groei van de cybersecuritysector. Cybersecuritybedrijven hebben een optimaal groeiperspectief en er vinden meer lange-termijn investeringen plaats.

**Betrekken van afnemers bij onderzoek en innovatie en marktcreatie**

Het betrekken van afnemers bij onderzoek, innovatie en marktcreatie is belangrijk voor succesvolle innovatieontwikkeling van cybersecuritytechnologieën. De huidige en potentieel afnemende markt is nog niet voldoende betrokken bij cybersecurity-onderzoeksprojecten. In de huidige situatie werkt wetenschap/onderzoek nog onvoldoende samen met het (cybersecurity-)bedrijfsleven. Er vindt hiermee onvoldoende valorisatie plaats: wetenschappelijke onderzoeken en kennis worden niet omgezet in producten die aansluiten bij de behoeften en mogelijkheden van de markt. Dit komt doordat het mkb onvoldoende tijd heeft om te werken aan lange termijnuitdagingen rondom cybersecurityinnovatie. Tevens hebben belemmeringen op het gebied van datadelen negatieve gevolgen voor de kwaliteit en mogelijkheden van onderzoek.

**Deelambitie:** In 2035 worden meer Nederlandse marktpartijen betrokken bij onderzoek en innovatie van cybersecuritytechnologieën en worden oplossingen meer vraaggestuurd ontwikkeld, bijvoorbeeld door promovendi tijdelijk te laten werken in het bedrijfsleven en bedrijfsexperts in te zetten in onderzoeksprojecten. Middels een multidisciplinaire aanpak zijn cybersecurityprincipes *security-by-design* en *security-by-default* een voorwaarde voor onderzoeksprojecten van andere sleuteltechnologieën en zal er ook gekeken worden naar andere mogelijkheden voor de invulling van onderzoeksprojecten en financiering.

**Vaardigheden en absorptiecapaciteit in het mkb**

Door gebrek aan vaardigheden en kennis, en de krapte op de arbeidsmarkt is het voor het mkb een uitdaging om de juiste cybersecurity-maatregelen te nemen. Hiermee blijft het lastig voor het mkb om nieuwe innovaties rondom cybersecurity toe te passen. Daarnaast zijn cybersecurityproducten en -diensten niet goedkoop en is de vraag vanuit het mkb naar deze producten en diensten klein en het investeringsbereidheid laag.

**Deelambitie:** In 2035 vindt meer samenwerking plaats tussen het mkb, de grote bedrijven, overheden en kennisinstellingen om kennis en vaardigheden in het mkb te vergroten. Daarnaast worden grote bedrijven gestimuleerd om kennis te delen met mkb'ers. Tevens wordt gewerkt aan de schaalbaarheid van cybersecuritytechnologieën zodat er meer betaalbare cybersecurityproducten en -diensten beschikbaar zijn voor het brede mkb (bijv. door het toepassen van AI voor automatisering).

**Ontwikkelen, aantrekken en behoud van (top)talent**

Het aantrekken van het brede cybersecuritytalent – van technische specialisten tot mensen uit alfa en gamma-disciplines – is een grote uitdaging, mede door de grote arbeidskrapte en concurrentie met internationale bedrijven. Het is ook ingewikkeld om het talent te behouden: voor veel overheden, bedrijven en onderwijsinstellingen is het niet makkelijk om te concurreren met grote bedrijven uit het buitenland die veel middelen hebben. Ook zouden de onderwijs- en arbeidsmarktbehoeften beter op elkaar moeten worden aangesloten.

**Deelambitie:** In 2035 zijn de vraag en aanbod in het cybersecurity onderwijs en arbeidsmarkt beter op elkaar aangesloten en is de keten van onderwijs naar arbeidsmarkt versterkt. Dit draagt bij aan adequate onderwijsvorming en onderzoek, het verbeteren van de startpositie van afgestudeerd talent, laagdrempelig bij- en omscholingstrajecten en het stimuleren van Leven Lang Ontwikkelen trajecten.

**Betrekken innovatie bij de ontwikkeling van wet- en regelgeving**

De wet- en regelgeving rondom cybersecurity biedt kansen doordat organisaties verplicht zijn meer cybersecuritymaatregelen te nemen die zullen leiden tot de afname van meer cybersecurityproducten en -diensten. Dit zorgt tegelijkertijd voor dat afnemende organisaties enkel bezig zijn om de verplichte middelen in huis te hebben, zonder de eigen risico's goed te begrijpen. Daarnaast gaan technologische ontwikkelingen snel en worden wet- en regelgeving ingehaald door de werkelijkheid.

**Deelambitie:** In 2035 worden innovatiepartners in een vroeg stadium betrokken bij de ontwikkeling en uitvoering van wet- en regelgeving, zodat het belang van cybersecurityinnovatie hierin wordt meegenomen.

## Geraadpleegde deskundigen

*Deelnemers Ronde tafel 1*

- Bibi van den Berg – Universiteit Leiden, ACCSS
- Roland van Rijswijk-Deij – Universiteit Twente
- Jelle Niemantsverdriet – Microsoft
- Berry Vetjens – TNO
- Liesbeth Holterman – Cyberveilig Nederland
- Vincent Ossewaarde – Fortytwo
- Nort van Schayik – Compumatica
- Frits Grotenhuis – Topsector ICT
- Pieter Jansen – Darktrace
- Eddy Boot – dcypher

*Deelnemers Ronde tafel 2*

- Jelmer Schreuder – NLdigital
- Roland van Rijswijk-Deij – Universiteit Twente
- Jelle Niemantsverdriet – Microsoft
- Berry Vetjens – TNO
- Tim de Wolf – Technolution
- Christo Butcher – FOX-IT
- Vincent Ossewaarde – Fortytwo
- Nort van Schayik – Compumatica

*Overige bijdrage*

- Erik de Jong – Thales

# Bronnen


1 Hoofdlijnen beleid voor digitalisering (Kamerstukken II, 2021-22, 26 643, nr. 842 herdruk).
2 Cybersecuritybeeld Nederland 2023 NCTV
3 Dit zijn operationele systemen met een digitaal component die worden gebruikt voor de fysieke wereld, denk aan systemen die sluizen aansturen.
4 Strategie Digitale Economie - Voortgangsrapportage 2023 (overheid.nl)
5 Nederlandse Cybersecuritystrategie 2022 - 2028
6 Pijler 2 van de Nederlandse Cybersecuritystrategie 2022 – 2028, is gericht op veilige en innovatieve producten en diensten
7 Agenda Digitale Open Strategische Autonomie (2023)
8 Dialogic, de economische kansen van de cybersecuritysector (2023)
9 Gebaseerd op TNO Rapport Herijking Sleuteltechnologieën 2023 (kia-st.nl) (zie p. 20) en Nederlandse Cybersecuritystrategie 2022 - 2028
10 Zie: www.kia-digitalisering.nl
11 Cybersecuritybeeld Nederland 2023 NCTV
12 Why cybersecurity is on the frontline of our AI future | World Economic Forum (weforum.org)
13 Dialogic, De economische kansen van de cybersecuritysector (2023)
14 Zie: EUR-Lex - 52022PC0454 - EN - EUR-Lex (europa.eu)
15 Zie: EUR-Lex - 02022L2555-20221227 - EN - EUR-Lex (europa.eu)
16 Zie: Commission publishes Recommendation on Post-Quantum Cryptography | Shaping Europe's digital future (europa.eu)

17 Cyber Security Market Share, Forecast | Growth Analysis [2030] (fortunebusinessinsights.com); Cyber Security Market Share, Forecast | Growth Analysis [2030] (fortunebusinessinsights.com)
18 Europese Commissie: EU strategic dependencies and capacities: second stage of in-depth review
19 Ibid.
20 Gebaseerd op Canalys' 2021 Cybersecurity Leadership Matrix (2021)
21 Zie: EUR-Lex - 02022L2555-20221227 - EN - EUR-Lex (europa.eu)
22 Dialogic, De economische kansen van de cybersecuritysector (2023)
23 Agenda Digitale Open Strategische Autonomie (DOSA)
24 Het Dialogic-onderzoek verwijst naar deze data uit 2019
25 Cybersecuritybeeld Nederland 2023 NCTV
26 https://www.aivd.nl/binaries/aivd_nl/documenten/publicaties/2024/04/18/cybercheck-ook-jij-hebt-supply-chain-risicos/Cybercheck+ook+jij+hebt+supply+chain+risicos.pdf
27 Dialogic, De economische kansen van de cybersecuritysector (2023)
28 Kabinetsstrategie Versterken van onderzoeks- en innovatieecosystemen (2020)
29 Europese Commissie, EU strategic dependencies and capacities: second stage of in-depth reviews, februari 2022
30 Dialogic, Het Nederlandse investeringsklimaat, juni 2021, p44. Zie ook: Timmers en Dezeure, Nederlandse strategische autonomie en cybersecurity, januari 2021. Dit beeld kwam ook naar voren bij rondetafels met experts.
31 Dialogic, De economische kansen van de Cybersecuritysector, april 2023, p 59