De economische kansen van de cybersecuritysector

ir. ing. Reg Brennenraedts MBA, dr. Pim den Hertog, Sonja Kleter MSc, Jasper Ott MSc, Adriaan Smeitink MSc, drs. Robbin te Velde, ir. Arthur Vankan

Opdrachtgever:
Ministerie van EZK

Publicatienummer:
2022.130.2308

Datum:
Utrecht, 6 april 2023

Inhoudsopgave

Managementsamenvatting

1 Inleiding

Het Ministerie van Economische Zaken en Klimaat heeft in 2016 onderzoek laten uitvoeren naar de economische kansen voor de cybersecuritysector. Cybersecurity blijkt de afgelopen jaren steeds vaker een kritische succesfactor voor het realiseren van een succesvolle digitale transitie in steeds meer organisaties, sectoren en domeinen. Actuele cijfers over de cybersecurity activiteiten en over de toegevoegde waarde van de cybersecurity activiteiten voor het verdienvermogen van Nederland zijn belangrijk om daar meer zicht op te krijgen. Daarom heeft het ministerie aan Dialogic gevraagd om dit onderwerp opnieuw te onderzoeken. Hierbij staan de volgende onderzoeksvragen centraal:

1. Wat is op dit moment het economisch verdienvermogen van Nederland op het gebied van cybersecurity?

2. Wat is het potentieel van de cybersecuritysector? Welke toekomstige trends op het gebied van cybersecurity zullen naar verwachting effect hebben op het verdienvermogen?

3. Wat kan de overheid doen om bovengenoemd economisch potentieel te realiseren?

In dit rapport worden de bovenstaande vragen via een SWOT-analyse gestructureerd. De eerste vraag draait om de sterktes en zwaktes; de tweede vraag om de kansen en bedreigingen en de derde vraag om de confrontatie tussen deze twee aspecten. Er is gekozen voor een SWOT-analyse om binnen het onderwerp relevante aanknopingspunten te prioriteren, omdat het volledige onderwerp m.b.t. 'de cybersecuritysector, economische kansen en de rol van de overheid' te groot is om volledig te vangen met één onderzoek. Door de belangrijkste kansen, bedreigingen, sterktes en zwaktes te identificeren signaleren we de meest logische aanknopingspunten voor eventueel beleid.

2 Conceptueel model en onderzoeksopzet

Conceptueel model

In dit rapport wordt de waardeketen van cybersecurity nader uitgewerkt. Op basis van interviews, eigen inzichten en literatuurstudie is een conceptueel model ontwikkeld dat verschillende typen actoren in de 'cybersecurity-waardeketen' en hun onderlinge relatie typeert. De waardeketen bestaat volgens het conceptuele model uit vier categorieën actoren:

A. Partijen die actief zijn in cybersecurity R&D, zoals universiteiten, onderzoeksinstellingen en bedrijven. Dit is de primaire bron van vernieuwing die door andere delen van de waardeketen wordt gebruikt om te innoveren. We rekenen deze partijen alleen tot de cybersecuritysector indien er activiteiten worden uitgevoerd die als primair doel hebben te worden toegepast in cybersecurity.

B. Producenten van cybersecurityproducten en -diensten. De harde kern van de cybersecuritysector zijn de partijen die cybersecurityproducten en -diensten produceren. Deze categorie kan worden opgesplitst in acht soorten activiteiten: educatie, software, hardware, distributie, consulting, implementatie, managed services en certificering.

C. Partijen die cybersecurityproducten en diensten integreren in niet cybersecurityproducten en diensten. Alleen het deel van de organisaties dat zich primair bezighoudt met deze integratie valt wordt betrokken in dit onderzoek, het deel dat zich hier niet (primair) mee bezighoudt valt erbuiten

D. Gebruikers van cybersecurityproducten en diensten zijn de uiteindelijke afnemers van producten en diensten van partijen die cybersecurityproducten en -diensten produceren of integreren. Deze groep valt buiten de cybersecuritysector.

Een centraal aspect van dit onderzoek is de focus op economische kansen. De wijze waarop deze kansen zich voordoen, verschilt voor verschillende partijen in de waardeketen. Partijen die actief zijn in cybersecurity R&D zorgen bijna alleen indirect voor een hoger verdienvermogen. Producenten van cybersecurityproducten en -diensten kunnen uiteraard economische kansen pakken en een flinke groei doormaken als zij meer afzetten. Echter vanuit een macro-economisch perspectief is vooral de verhouding tussen import en export van deze producten en diensten relevant. Voor partijen die cybersecurityproducten en -diensten integreren draait het vooral om de mate waarin zij concurrentievoordelen behalen met de integratie hiervan in hun primaire diensten en producten. Voor gebruikers van cybersecurityproducten en -diensten is cybersecurity vanuit een macro-economisch perspectief vooral een kostenpost.

Onderzoeksaanpak

Het meten van deze waarde in de waardeketen is lastig, vooral doordat er geen duidelijke lijst is met bedrijven die in cybersecurity actief zijn. De onderzoeksopzet is gebaseerd op een analyse van de inhoud van websites van alle Nederlandse bedrijven. Op basis hiervan wordt een lijst gemaakt van bedrijven die in deze sector actief zijn. Van deze bedrijven is een analyse gemaakt op basis van CBS-microdata en al deze bedrijven hebben een enquête ontvangen. Naast deze methodes zijn interviews uitgevoerd, is er literatuuronderzoek gedaan, heeft er een kwantitatieve analyse van vacatures plaatsgevonden en is er een validatiesessie uitgevoerd. Een beperking aan de aanpak in dit onderzoek is dat bedrijven die mogelijk wel iets met cybersecurity doen, maar dat niet expliciet op de website aangeven, buiten beeld vallen.

3 Sterktes en zwaktes van de Nederlandse cybersecuritysector

De Nederlandse cybersecuritysector kent verschillende sterktes. Ten eerste kent de sector een flinke groei van 10% tot 15% per jaar. In 2020 draaide de sector een omzet van €26 miljard, behaalde een toegevoegde waarde van bijna €13 miljard en kende de sector ruim 130.000 werknemers. De cybersecuritysector omvat daarmee circa 0,9% van de Nederlandse economie. Ten tweede kan de sector goed voldoen aan de binnenlandse vraag naar diensten. Ook kent Nederland een sterke kennisbasis in onderzoek naar cryptografie. Het heeft decennia geduurd om deze positie op te bouwen. Tenslotte bevat de sector hoogwaardige integrators kunnen cybersecurity gebruiken om een competitief voordeel te realiseren. Nederland heeft een hoogwaardige economische structuur waarin de integratie van cybersecurity een competitief voordeel kan zijn.

De Nederlandse cybersecurity sector heeft echter ook enkele zwaktes. Zo kent de sector weinig private cyber R&D, en is er sprake van een sector die sterk R&D-intensief is, maar Nederlands bedrijven doen hier relatief beperkt aan. Daarnaast is de output van de sector is beperkt te exporteren. De Nederlandse sector is gericht op diensten en deze laten zich minder goed exporteren dan software, hardware en managed services. Door de focus op diensten is de sector kent grote afhankelijkheid van buitenlandse leveranciers. Om de nationale markt te kunnen bedienen wordt er sterk geleund om buitenlandse leveranciers van hardware, software en managed services. Tot slot bestaat de markt overwegend uit MKB en ZZP'ers. Hierdoor kent de sector een relatief beperkte slagkracht.

4 Kansen en bedreigingen voor de Nederlandse cybersecuritysector

De Nederlandse cybersecuritysector kent veel kansen, waaronder het feit dat Nederland goed is in de integratie van alfa-, bèta- en gammawetenschappen. Met een groeiende cybersecuritysector wordt een interdisciplinaire insteek steeds belangrijker. Daarnaast biedt de opkomst van AI groeiende mogelijkheden om mensenwerk via AI uit te voeren. De kansen die AI biedt zijn de afgelopen jaren sterk toegenomen. Ook heeft Nederland een sterke kennisbasis in kwantumtechnologie. Dit kan worden ingezet voor nieuwe vorm van encryptie. Op Europees niveau biedt de invoering van de NIS en de CRA kansen

doordat het nieuwe eisen stelt aan de marktpartijen waarop de sector kan anticiperen. Tenslotte is Nederland een aantrekkelijke vestigingsplaats voor NGO's en IO's. Toekomstige, nog op te richten, organisaties die zich richten op vrede en veiligheid in het digitale domein kunnen zich wellicht in Den Haag vestigen.

Daarnaast kent de Nederlandse cybersecuritysector enkele bedreigingen. De (mogelijk) grootste dreiging komt door het flinke tekort aan personeel met een cybersecurityprofiel. Ook de beperkte awareness bij organisaties en consumenten over risico's waardoor er meer risico wordt gelopen dan nodig is. Een andere bedreiging is het feit dat bedrijven die schaal krijgen snel worden overgenomen door externe (buitenlandse) partijen. Hierdoor kan de sector in Nederland zich beperkt ontwikkelen. Ook het gebrek aan venture capital werkt mee aan een tekort aan scale-ups omdat de conversie van startup naar scale-up lastig is. Een andere bedreiging ligt bij de overheid, welke niet zwaar investeert. Er zijn andere landen waar de overheid, als gevolg van een externe dreiging, sterk investeert waardoor een de sector zich goed ontwikkeld. Tot slot wordt er momenteel geen eenduidige visie overheid op cybersecurity ervaren. Er is sprake van fragmentatie van beleid. Met de publicatie van de NLCS wordt hieraan gewerkt, dit is echter nog te recent om een effect hiervan te ervaren.

5 Beleidsopties

Vanuit de SWOT-analyse komen vier aspecten naar voren waar het voeren van beleid het meest voor de hand ligt.

1. Met ontwikkelingen op het gebied van AI is het mogelijk om meer te kunnen doen met minder mensen. Op deze manier kan de sector blijven groeien ondanks krapte op de arbeidsmarkt. Bovendien biedt dit kansen voor exporteerbare producten. De brug tussen AI en cybersecurity moet vaker gelegd worden. Dit kan bijvoorbeeld via SBIR-aanvragen en de aansluiting bij het Groeifonds.

2. Zorgen voor kwantitatief en kwalitatief voldoende cybersecurityprofessionals. Er wordt al veel beleid gevoerd op dit onderwerp en het is opgenomen in de doelstellingen van de NLCS. Hoewel er mogelijkheden zijn om deze inspanningen verder te intensiveren, is het aanvullend belangrijk dat de visie op de aanpak van arbeidsmarkttekorten op het gebied van cybersecurity gaat passen binnen een meer integraal perspectief over hoe verschillende arbeidsmarkttekorten zich tot elkaar verhouden en wat we daar binnen Nederland aan willen doen. Er is nu immers sprake van 'beleidsconcurrentie' ten aanzien van het schaarse menselijk kapitaal waar de arbeidsmarkt in brede zin (ICT- en niet-ICT) over beschikt.

3. Voorkomen dat veelbelovende cybersecuritybedrijven in buitenlandse handen vallen zodat de Nederlandse sector zich beter kan ontwikkelen en afhankelijkheden worden beperkt, bijvoorbeeld door inzet van wet- en regelgeving en/of door het stimuleren van beschikbaar kapitaal voor de betreffende bedrijven. Wederom zou dit in een breder kader van sectoraal industriebeleid geplaatst moeten worden. Hierbij speelt ook inkoopbeleid van het Rijk en Europese afstemming een grote rol.

4. Versterken van bewustzijn bij gebruikers. Er zijn al veel initiatieven op allerlei geografische en sectorale niveaus. Optimalisatie kan vooral plaatsvinden door betere afstemming in het ecosysteem.

6 Conclusies

In hoofdstuk 6 worden de onderzoeksvragen systematisch beantwoord aan de hand van de drie hoofdvragen. Hieronder wordt de kern van de antwoorden gegeven; voor een meer gedetailleerd antwoord verwijzen we u door naar het volledige hoofdstuk 6.

Hoofdvraag 1: wat is op dit moment het economisch verdienvermogen van Nederland op het gebied van cybersecurity? In 2021 kent de Nederlandse

cybersecuritysector een geschatte omzet van circa 16 miljard euro en een werknemersaantal van circa 94.600. De toegevoegde waarde ligt rond de 7,5 miljard euro, wat overeenkomt met 0,94% van het BBP. Naast het verdienvermogen van de sector zelf (producenten cyberproducten en -diensten) is cybersecurity voor cyber integrators, partijen een schakel verder in de keten, een belangrijke randvoorwaarde die ook als competitief voordeel kan dienen. Voor uiteindelijke gebruikers van cybersecurityproducten en -diensten is het puur randvoorwaardelijk. Het economisch belang voor deze spelers later/laat in de keten is kwalitatief beschreven, maar is moeilijk te kwantificeren.

Hoofdvraag 2: wat is het potentieel van de cybersecuritysector? Welke toekomstige trends op het gebied van cybersecurity zullen naar verwachting effect hebben op het verdienvermogen? Er zijn diverse trends geïdentificeerd, waarbij de volgende vijf de meest prominente zijn: [1] sterke groei van de sector zelf, [2] de doorzettende ontwikkeling van AI, [3] de introductie van NIS2 en CRA, [4] de overname van potentievolle cybersecuritybedrijven door externe partijen, en [5] tekorten op de arbeidsmarkt. Trends [1], [2] en [3] hebben een positief effect op het toekomstig verdienvermogen van de sector. Trends [4] en [5] hebben een negatieve of remmende werking op het verdienvermogen.

Hoofdvraag 3: wat kan de overheid doen om bovengenoemd economisch potentieel te realiseren? De overheid heeft al veel beleid ontwikkeld om knelpunten waar de sector mee te maken heeft te adresseren. Het goed stroomlijnen van al het beleid dat reeds bestaat is een hoge prioriteit. Met de NLCS wordt hier al stevig aan gewerkt, en het beeld dat in dit onderzoek naar voren komt is dat die lijn doorgezet mag en zelfs moet worden. Daarnaast worden op vier concrete aanknopingspunten voor beleid suggesties gedaan voor eventueel aanvullende inspanningen. Een overkoepelende observatie is dat voor diverse onderwerpen, zoals arbeidsmarkt en buitenlandse overnames, men deze op een cybersecuritysector-overstijgende wijze zou moeten aanvliegen. De fundamentele onderliggende problemen zijn vaak immers niet specifiek voor deze sector, en een integrale visie en aanpak kan hier waardevol zijn. Hoewel dit laatste op onderdelen al gebeurt, kunnen hier nog verdere stappen gezet worden.

1 Inleiding

Het Ministerie van Economische Zaken en Klimaat heeft in 2016 onderzoek laten uitvoeren naar de economische kansen voor de cybersecuritysector[1]. Cybersecurity blijkt de afgelopen jaren steeds vaker een kritische succesfactor voor het realiseren van een succesvolle digitale transitie in steeds meer organisaties, sectoren en domeinen. Actuele cijfers over de cybersecurity activiteiten en over de toegevoegde waarde van de cybersecurity activiteiten voor het verdienvermogen van Nederland zijn belangrijk om daar meer zicht op te krijgen. Daarom heeft het ministerie aan Dialogic gevraagd om dit onderwerp opnieuw te onderzoeken. Hierbij staan de volgende onderzoeksvragen centraal:

1. Wat is op dit moment het economisch verdienvermogen van Nederland op het gebied van cybersecurity?

2. Wat is het potentieel van de cybersecuritysector? Welke toekomstige trends op het gebied van cybersecurity zullen naar verwachting effect hebben op het verdienvermogen?

3. Wat kan de overheid doen om bovengenoemd economisch potentieel te realiseren?

In dit rapport worden de bovenstaande vragen via een SWOT-analyse gestructureerd. De eerste vraag draait om de sterktes en zwaktes; de tweede vraag om de kansen en bedreigingen en de derde vraag om de confrontatie tussen deze twee aspecten. Er is gekozen voor een SWOT-analyse om binnen het onderwerp relevante aanknopingspunten te prioriteren, omdat het volledige onderwerp m.b.t. 'de cybersecuritysector, economische kansen en de rol van de overheid' te groot is om volledig te vangen met één onderzoek. Door de belangrijkste kansen, bedreigingen, sterktes en zwaktes te identificeren signaleren we de meest logische aanknopingspunten voor eventueel beleid.

1.1 Aanleiding

Het Ministerie van Economische Zaken en Klimaat heeft in 2016 onderzoek laten uitvoeren naar de economische kansen voor de cybersecuritysector, om zicht te krijgen op de kracht en zwakte van de sector, de potentiële bijdrage van de sector aan (ICT-gerelateerde) economische bedrijvigheid en de mogelijke overheidsmaatregelen om het vestigings- en ondernemingsklimaat voor de sector in Nederland te versterken.

In het Cyber Security Beeld Nederland 2022 (CSBN, 2022[2]) wordt duidelijk dat de digitale weerbaarheid aandacht blijft behoeven. De maatschappelijke en economische schade van incidenten kan enorm zijn. Zo vormen cyberaanvallen een aantrekkelijk verdienmodel voor criminelen. Cybersecurity blijkt daarom steeds vaker een kritische succesfactor voor het realiseren van een succesvolle digitale transitie in steeds meer organisaties, sectoren en domeinen. De groei van de (digitale) economie vraagt om vertrouwen in ICT en veilig datagebruik, en daarmee een goed ontwikkelde cybersecuritysector en een sterk R&D-ecosysteem. Actuele cijfers over cybersecurity activiteiten en over de toegevoegde waarde van de cybersecurity activiteiten voor het verdienvermogen van Nederland zijn belangrijk

[1] https://www.seo.nl/wp-content/uploads/2020/04/2016-56_Economische_kansen_Nederlandse_Cybersecurity_sector.pdf

[2] NCTV, (2022). Cybersecuritybeeld Nederland 2022. *CSBN2022*

om daar meer zicht op te krijgen. Een recent rapport van McKinsey[3] toont dat Europa achterloopt op het gebied van cybersecurity in vergelijking met de Verenigde Staten. Europa scoort lager op innovatie (gemeten aan de hand van patenten), productie (gemeten aan de hand van markt aandeel) en adoptie (gemeten door middel van publieke investering en eindmarktaandeel). Daarnaast worden de wettelijke kaders in relatie tot cybersecurity Europees momenteel flink aangescherpt. De herziening van de **Netwerk- en informatiebeveiligingsrichtlijn (NIS2)** maakt dat in alle EU-lidstaten en dus ook Nederland veel meer sectoren en organisaties wettelijke verplichtingen krijgen opgelegd voor de beveiliging van hun netwerk- en informatiesystemen. Naast de NIS2 wordt ook onderhandeld over de **Cyber Resilience Act (CRA)** om cybersecurity van digitale producten te vergroten. Om deze redenen wil het Ministerie van Economische Zaken en Klimaat een actualisering van het eerdere onderzoek laten uitvoeren.

1.2 Doelstelling en onderzoeksvragen

Het onderzoek kent drie doelstellingen: 1) ontwikkelingen in beeld krijgen met betrekking tot de sterktes en zwaktes van de Nederlandse uitgangspositie voor het realiseren van de economische kansen van cybersecurity; 2) de relatie tussen cybersecurity en economische activiteiten duiden, en beschrijven in hoeverre een hoger niveau van cybersecurity leidt tot meer economische bedrijvigheid; 3) een duiding over welke rol de (rijks)overheid kan spelen in de cybersecurity, op basis van de conclusies van doelstelling 1 en doelstelling 2 van het onderzoek.

Gebaseerd op bovenstaande doelstellingen zijn de volgende onderzoeksvragen geformuleerd:

1. **Wat is op dit moment het economisch verdienvermogen van Nederland op het gebied van cybersecurity?**
    a. Trek de vergelijking met het SEO-onderzoek in 2016.
    b. Kwantificeer (waar mogelijk): aantal werknemers, omzet, deel van BBP.
    c. Differentieer tussen verdienvermogen en randvoorwaardelijkheid van cybersecurity.
2. **Wat is het potentieel van de cybersecuritysector? Welke toekomstige trends op het gebied van cybersecurity zullen naar verwachting effect hebben op het verdienvermogen?**
    a. Benoem relevante trends.
    b. Beschrijf het te verwachten effect op het Nederlandse verdienvermogen.
    c. Omschrijf (kwantitatief waar mogelijk) het potentieel op basis van vraag 1.
3. **Wat kan de overheid doen om bovengenoemd economisch potentieel te realiseren?**
    a. Welke middelen kan de overheid gebruiken om – wanneer nodig - te interveniëren?
    b. Welk effect kunnen we verwachten door de inzet van deze middelen?
    c. Relateer aan de ontwikkelingen zoals omschreven bij vraag 2.

Dialogic vat de onderzoeksvragen op als een onderzoek met een SWOT-analyse. De eerste onderzoeksvraag betreft een interne analyse en dus de sterktes en zwaktes. De tweede onderzoeksvraag betreft een analyse van de externe omgeving en dus de kansen en bedreigingen. De derde onderzoeksvraag vraagt om de acties die op basis van de antwoorden op de voorgaande vragen kunnen worden ingezet. Het uitzetten van de sterktes en zwaktes

[3] https://www.mckinsey.com/capabilities/strategy-and-corporate-finance/our-insights/securing-europes-competitiveness-addressing-its-technology-gap

tegen de kansen & bedreigingen biedt hier een goede aanzet voor. Bij de uitvoering van dit onderzoek redeneren we vanuit het perspectief van een SWOT-analyse.

1.3 Leeswijzer

Hoofdstuk 2 geeft een uiteenzetting van de onderzoeksaanpak en de verschillende gebruikte databronnen. Hoofdstukken 3 en 4 zijn opgebouwd aan de hand van respectievelijk de sterktes en zwaktes, kansen en bedreigingen van de Nederlandse cybersecuritysector. Per onderdeel worden de resultaten aan de hand van de verschillende relevante onderzoekstappen beschreven. Bij de sterktes en zwaktes maken we onderscheid tussen de onderdelen van het conceptuele model: cyber R&D, cyberproducenten en cyberintegrators. In de bijlagen presenteren we de uitkomsten van de kwantitatieve analyses integraal. In de hoofdtekst halen we dit aan waar nodig. Dat betekent dat sommige uitkomsten van de kwantitatieve analyses niet in de hoofdtekst voorkomen, maar wel in de bijlagen. Andersom zijn er bepaalde uitkomsten die meer dan eens in de hoofdtekst voorkomen. We proberen zo min mogelijk herhaling in te bouwen, maar sommige uitkomsten van kwantitatieve analyse dragen nu eenmaal bij aan de onderbouwing van meerdere sterktes, zwaktes, kansen en bedreigingen. In hoofdstuk 5 sluiten we af met vier (groepen van) beleidsopties waarbij een kans of een bedreiging (derhalve kolommen in de SWOT) als uitgangspunt is genomen.

2 Conceptueel model en onderzoeks-opzet

Conceptueel model

In dit rapport wordt de waardeketen van cybersecurity nader uitgewerkt. Op basis van interviews, eigen inzichten en literatuurstudie is een conceptueel model ontwikkeld dat verschillende typen actoren in de 'cybersecurity-waardeketen' en hun onderlinge relatie typeert. De waardeketen bestaat volgens het conceptuele model uit vier categorieën actoren:

A. Partijen die actief zijn in cybersecurity R&D, zoals universiteiten, onderzoeksinstellingen en bedrijven. Dit is de primaire bron van vernieuwing die door andere delen van de waardeketen wordt gebruikt om te innoveren. We rekenen deze partijen alleen tot de cybersecuritysector indien er activiteiten worden uitgevoerd die als primair doel hebben te worden toegepast in cybersecurity.

B. Producenten van cybersecurityproducten en -diensten. De harde kern van de cybersecuritysector zijn de partijen die cybersecurityproducten en -diensten produceren. Deze categorie kan worden opgesplitst in acht soorten activiteiten: educatie, software, hardware, distributie, consulting, implementatie, managed services en certificering.

C. Partijen die cybersecurityproducten en diensten integreren in niet cybersecurityproducten en diensten. Alleen het deel van de organisaties dat zich primair bezighoudt met deze integratie valt wordt betrokken in dit onderzoek, het deel dat zich hier niet (primair) mee bezighoudt valt erbuiten

D. Gebruikers van cybersecurityproducten en diensten zijn de uiteindelijke afnemers van producten en diensten van partijen die cybersecurityproducten en -diensten produceren of integreren. Deze groep valt buiten de cybersecuritysector.

Een centraal aspect van dit onderzoek is de focus op economische kansen. De wijze waarop deze kansen zich voordoen, verschilt voor verschillende partijen in de waardeketen. Partijen die actief zijn in cybersecurity R&D zorgen bijna alleen indirect voor een hoger verdienvermogen. Producenten van cybersecurityproducten en -diensten kunnen uiteraard economische kansen pakken en een flinke groei doormaken als zij meer afzetten. Echter vanuit een macro-economisch perspectief is vooral de verhouding tussen import en export van deze producten en diensten relevant. Voor partijen die cybersecurityproducten en -diensten integreren draait het vooral om de mate waarin zij concurrentievoordelen behalen met de integratie hiervan in hun primaire diensten en producten. Voor gebruikers van cybersecurityproducten en -diensten is cybersecurity vanuit een macro-economisch perspectief vooral een kostenpost.

Onderzoeksaanpak

Het meten van deze waarde in de waardeketen is lastig, vooral doordat er geen duidelijke lijst is met bedrijven die in cybersecurity actief zijn. De onderzoeksopzet is gebaseerd op een analyse van de inhoud van websites van alle Nederlandse bedrijven. Op basis hiervan wordt een lijst gemaakt van bedrijven die in deze sector actief zijn. Van deze bedrijven is een analyse gemaakt op basis van CBS-microdata en al deze bedrijven hebben een

enquête ontvangen. Naast deze methodes zijn interviews uitgevoerd, is er literatuuronderzoek gedaan, heeft er een kwantitatieve analyse van vacatures plaatsgevonden en is er een validatiesessie uitgevoerd. Een beperking aan de aanpak in dit onderzoek is dat bedrijven die mogelijk wel iets met cybersecurity doen, maar dat niet expliciet op de website aangeven, buiten beeld vallen.

2.1 Inleiding

We beginnen de inhoudelijke kern van deze rapportage met een vrij uitvoerige uiteenzetting van het conceptueel model, onze visie op economische kansen, onze visie op operationalisering en tot slot de onderzoeksaanpak. Dit heeft een aantal redenen:

- Ten eerste is de cybersecuritysector een vrij breed en ambigue concept. We moeten dit allereerst goed definiëren en conceptualiseren voordat we dit kunnen meten. Hierbij spelen vragen als:
    - Wat is de cybersecuritysector in Nederland?
    - Wat is de kern van de sector?
    - Wat zijn aanpalende activiteiten en sectoren?
    - Wat valt buiten de sector?
    - Welke soorten activiteiten worden er ontplooid (door welke soort actoren)?
- Ten tweede hebben we hier te maken met een sector waarbij het perspectief dat draait om economische kansen niet evident is. Cybersecurity is een randvoorwaarde voor het functioneren van andere sectoren. Het is daarmee geen winstgevende factor, maar draagt bij aan de weerstand van sectoren, organisaties en domeinen.
- Ten derde is het meten van cybersecurity niet eenvoudig, ook gezien de relatief beperkte leeftijd van de sector. Om dit toch te realiseren hebben we gekozen voor een onderzoeksaanpak die enige toelichting behoeft.

De lezer die geen interesse heeft in de onderzoeksopzet, kan dit hoofdstuk overslaan. De vervolghoofdstukken van het rapport zijn zelfstandig leesbaar.

2.2 Conceptueel model

De Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) definieert cybersecurity in het Cybersecuritybeeld Nederland (CSBN) 2020[4] als volgt: "*Cybersecurity is het geheel aan maatregelen om schade door verstoring, uitval of misbruik van ICT te voorkomen en, indien er toch schade is ontstaan, het herstellen hiervan. Die schade kan bestaan uit de aantasting van de beschikbaarheid, vertrouwelijkheid of integriteit van informatiesystemen en informatiediensten en de daarin opgeslagen informatie.*"

Het aanhouden van deze definitie leidt niet tot een scherpe afbakeningen van bedrijven die cybersecurity activiteiten ontplooien. Bijna elk serieus bedrijf ontplooit in enige mate *maatregelen om schade door verstoring, uitval of misbruik van ICT te voorkomen*. Toch zal de bakker op de hoek die een veilige PIN-terminal heeft, doorgaans niet als onderdeel van de cybersecuritysector worden beschouwd. Daartegenover staan de organisaties die hoogwaardig onderzoek uitvoeren naar cryptografie. Er is best wat te zeggen om onderzoek niet te zien als *maatregelen om schade door verstoring, uitval of misbruik van ICT te voorkomen,* of op zijn minst om dit als een sterk indirecte maatregel te zien. Toch zouden we deze categorie organisaties wellicht wel willen betrekken in het overzicht van cybersecurity

[4] https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2020/juni/29/csbn-2020/CSBN+2020.pdf

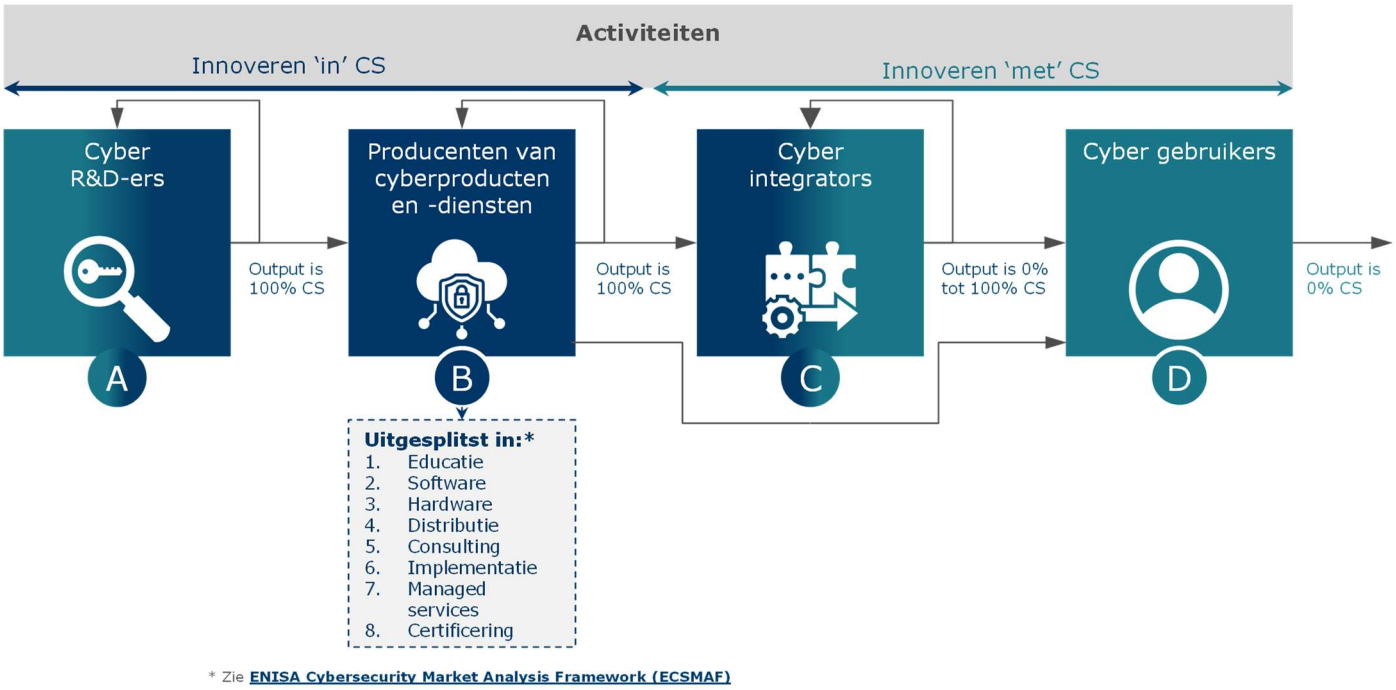
activiteten. Een bedrijf wordt beschouwd als cybersecurity bedrijf wanneer het bovengenoemde activiteiten ontplooit uit een *economisch* oogpunt.

Een ander aspect, in het verlengde van het voorgaande, is dat er sterk verschillende soorten actoren zijn in de cybersecuritysector, hoe we deze ook afbakenen. Er worden allerlei soorten activiteiten uitgevoerd die sterk van elkaar verschillen. Op basis van interviews, onze eigen inzichten en literatuurstudie komen we tot het onderstaande conceptueel model in Figuur 1. In dit model zien we vier soorten actoren:

- **A. Partijen die actief zijn in cybersecurity R&D**. Er is een aantal organisaties, zoals universiteiten en onderzoeksinstellingen, die zich bezighouden met onderzoek en ontwikkeling van cybersecuritytechnologie. Dit is de primaire bron van vernieuwing die door andere delen van de waardeketen wordt gebruikt om te innoveren. Voorbeelden van deze actoren zijn TNO en TU Delft.
- **B. Producenten van cybersecurityproducten en -diensten.** Dit zijn de bedrijven die cybersecurityproducten en -diensten produceren. Zij maken deels gebruik van de R&D die door de actoren in categorie A wordt uitgevoerd. Op basis van een onderzoek van ENISA kan deze categorie worden opgesplitst in acht soorten activiteiten: educatie, software, hardware, distributie, consulting, implementatie, managed services en certificering.[5] Binnen deze groep is sprake van veel afhankelijkheid. Een producent van cybersecurityhardware kan ook gebruik maken van de output van een partij die cybersecuritysoftware maakt. Vervolgens is er een partij die de implementatie hiervan doet, et cetera.
- **C. Partijen die cybersecurityproducten en diensten integreren** in niet cybersecurityproducten en diensten. Dit is een groep actoren die wordt gekenmerkt door het feit dat hun output niet primair het aanbieden van cybersecurityproducten of diensten betreft, maar producten en diensten waarin cybersecurityproducten of diensten worden geïntegreerd. Alle producten die gekoppeld kunnen worden aan digitale netwerken (laadpalen, MRI-scanners, slimme magnetrons, auto's, et cetera) moeten op een bepaald niveau cyberveilig zijn. Zij maken gebruik van de output van de partijen die onder B genoemd worden.
- **D. Gebruikers van cybersecurityproducten en diensten** zijn de uiteindelijke afnemers van producten en diensten van partijen die onder B en C genoemd worden. Hierbij gaat het om consumenten, maar ook bedrijven en publieke organisaties. De output van deze bedrijven en publieke organisaties bevat geen cybersecuritycomponent, maar zij hebben wel cybersecurityproducten en -diensten nodig om hun processen veilig te houden.

In het conceptuele model, dat we in Figuur 1 tonen, onderscheiden we verschillende soorten actoren en activiteiten. In de praktijk kan het uiteraard voorkomen dat organisaties op meerdere plekken in de waardeketen actief zijn.

[5] https://www.enisa.europa.eu/publications/enisa-cybersecurity-market-analysis-framework-ecsmaf/@@download/fullReport



Figuur 1. Conceptueel model dat centraal staat in deze studie

2.3 Afbakening van cybersecurity activiteiten

Op basis van het bovenstaande conceptuele model kunnen we een afbakening maken van de bedrijven die cybersecurity activiteiten ontplooien. De kleuren in deze afbeelding tonen onze visie hierop: Blauwe vakken rekenen we tot de cybersecurity activiteiten, blauwgroene vakken niet en vakken met beide kleuren deels. Beschouwen we de vierdeling dan nogmaals dan ontstaat het volgende beeld:

- **A. Partijen die actief zijn in cybersecurity R&D** rekenen we tot de cybersecuritysector indien er activiteiten worden uitgevoerd die als primair doel hebben te worden toegepast in cybersecurity. Onderzoeken naar cryptografie zijn hier een goed voorbeeld van. Er is echter ook veel onderzoek dat niet primair gericht is op cybersecurity, maar hier wel in toegepast wordt. Dit valt buiten onze afbakening van de cybersecuritysector. Een moderne hardwarematige firewall zit bijvoorbeeld vol met technologie die generiek voor de IT-sector is ontwikkeld en niet primair voor firewalls.
- **B. Producenten van cybersecurityproducten en -diensten**. Onder cybersecurityproducten vallen hardware en software. Onder cybersecuritydiensten vallen educatie, distributie, consulting, managed services, implementatie en certificering.
- **C. Partijen die cybersecurityproducten en -diensten integreren** vallen deels binnen de cybersecurity in deze studie. Het deel van de organisaties dat zich primair bezighoudt met deze integratie valt binnen de cybersecurity in deze studie, het deel dat zich hier niet mee bezighoudt valt erbuiten (zoals grote delen van de afdelingen financieel, juridisch en verkoop).
- **D. Gebruikers van cybersecurityproducten en -diensten** vallen buiten de cybersecurity in deze studie.

Tot slot willen we aangeven dat het conceptuele model bepaalde activiteiten toont. In de praktijk kan een organisatie een actor zijn in meerdere activiteiten.

2.4 Economische kansen

Een centraal aspect van dit onderzoek is de focus op economische kansen. Dit wijkt af van het primaire perspectief op cybersecurity dat draait om veiligheid; niet voor niets heet het cyber*security*. Het feit dat de focus op economische kansen ligt, neemt uiteraard niet weg dat we erkennen dat veiligheid een belangrijk element is in de discussie over cybersecurity. Met name bij het opstellen van beleidsopties is het van belang dit veiligheidsaspect in het achterhoofd te houden.

In de interviews die we uitgevoerd hebben, hebben we respondenten relatief vaak zien worstelen met de focus op economische kansen. De primaire focus blijkt bij veel personen toch te liggen op veiligheid. In een aantal gevallen werd er een parallel getrokken met andere sectoren waarin veiligheid een rol speelt en waarbij de overheid een grote rol speelt. Denk aan de brandweer en de politie. "*Wat zijn de economische kansen van de brandweer?"*, is in deze visie een vreemde vraag. We begrijpen dit perspectief, maar aan de andere kant kunnen we door middel van deze analogie ook redeneren dat er aan de brandveiligheid ook een economische kant zit. Bedrijven installeren zelf sprinklerinstallaties, hebben een brandblusser, trainen hun medewerkers hoe om te gaan met brand, gebruiken brandwerende materialen, richten hun gebouwen zo in dat brand zich niet kan verspreiden en hebben in sommige gevallen zelfs de verplichting[6] om een bedrijfsbrandweer te hebben.

Om de economische kansen goed te kunnen duiden, sluiten we weer aan bij het conceptuele model dat soorten actoren onderscheid. De wijze waarop deze kansen zich voordoen verschilt immers tussen actoren.

- **A. Partijen die actief zijn in cybersecurity R&D** zorgen alleen indirect voor een hoger verdienvermogen. De output die zij genereren kan worden gebruikt door de partijen onder B om steeds betere producten en diensten op de markt te brengen. Een uitzondering kan zijn als het gaat om organisaties die door middel van octrooien hun R&D direct kunnen valoriseren. Gezien de aard van de sector ligt dit gecompliceerd: Software is in Nederland lastig te octrooieren en wiskundige formules - bijvoorbeeld die ten grondslag liggen aan encryptie- zijn überhaupt niet te octrooieren.
- **B. Producenten van cybersecurityproducten en -diensten** kunnen uiteraard economische kansen pakken en een flinke groei doormaken. Als we kijken vanuit een macro-economisch perspectief dan zouden we vooral moeten kijken naar import en export van cybersecuritydiensten en -producten. Met andere woorden: Is Nederland een netto-exporteur of netto-importeur van cybersecurityproducten en -diensten? In het eerste geval levert het een positief effect op het bruto binnenlands product, in het tweede geval is er sprake van een negatief effect. Als we kijken naar soorten output, dan zullen er aanzienlijke verschillen liggen in de "*exporteerbaarheid*". Cybersecurityproducten zijn eenvoudig te exporteren. Managed services en software kunnen via het internet worden aangeboden. Ook hardware is relatief eenvoudig te exporteren al moet het apparaat hier wel fysiek voor verplaatst worden. Diensten (als in: personen die activiteiten verrichten) zijn lastiger te exporteren dan producten, al heeft de recente acceptatie van werken op afstand dit vereenvoudigt. Om diensten te exporteren moet een persoon die in Nederland werkt geregeld naar het buitenland gaan. Gezien de hoge kosten hiervan komt al snel de vraag naar voren, waarom men deze personen in het buitenland niet hiertoe opleidt. Daarnaast kunnen tijdzones, taal en cultuur een drempel zijn.

[6] https://wetten.overheid.nl/BWBR0004694/2007-01-01

- **C. Partijen die cybersecurityproducten en -diensten integreren** hebben indirect te maken met cybersecurity aangezien hun product of dienst wel een cybersecuritycomponent bevat, maar geen cybersecurityproduct of -dienst is. De mate waarin bedrijven in staat zijn cybersecurity te integreren in hun output bepaalt de economische impact. Voor steeds meer producten en diensten wordt het verplicht om cybersecurity te integreren. De mate waarin integrators hierin succesvol zijn, heeft impact op hun concurrentiepositie. Doordat er steeds meer cybersecurity regelgeving komt, moeten bedrijven aan bepaalde standaarden voldoen om hun activiteiten te kunnen ontplooien. Bovendien kan het in sommige markten zorgen voor een competitief voor- of nadeel als de diensten of producten cyberveilig (en dus toekomstvaster) zijn en aanbieders van deze diensten en producten hier proactief op inspelen.
- **D. Gebruikers van cybersecurityproducten en -diensten** zijn de uiteindelijke afnemers van de producten en diensten. Vanuit een macro-economisch perspectief is cybersecurity hier vooral een kostenpost. Zij moeten extra middelen alloceren om hun activiteiten te kunnen uitvoeren. Met andere woorden: indien er geen cyber dreigingen zouden zijn (en er dus op deze manier geen schade kan worden aangericht), dan zouden zij evident beter af zijn. In de 19e eeuw werd door Bastiat dit effect al herkend in de vorm van de parabel van de gebroken ruit.[7] Het breken van ruiten om werk te genereren voor de glazenmaker is niet goed voor de economie. Het is beter om geen ruiten te breken.

2.5 Uitdagingen om cybersecurity-activiteiten te meten

In de bovenstaande paragrafen werd duidelijk uit welke actoren cybersecurity activiteiten ontplooien. Ook werd duidelijk hoe we vanuit economisch perspectief naar cybersecurity kunnen kijken. Nu duidelijk is *wat* we willen meten, komt de vraag naar voren *hoe* we dit gaan meten. Er is een aantal routes verkend en niet uitgevoerd om uiteenlopende redenen:

- **Standaard Bedrijfsindeling** (SBI-codes) geven aan onder welke code bedrijven zich ingeschreven hebben in het Handelsregister van de Kamer van Koophandel. SBI-codes voor cybersecurity bestaan simpelweg niet, daar is de sector te jong voor. De bedrijven die in cybersecurity opereren staan vaak geregistreerd onder codes die vooral door IT-bedrijven worden gebruikt. Bovendien kennen SBI-codes ook methodologische uitdagingen onder meer doordat ze initieel niet altijd up to date zijn, doordat bedrijven andere activiteiten zijn gaan ontplooien (en hun SBI-code niet hebben bijgewerkt) en doordat bedrijven een breed scala aan activiteiten ontplooien. De cybersecuritysector definiëren op basis van SBI-codes is hiermee geen optie.
- Een tweede optie die verkend is, is om in te zetten op **bestaande lijsten met cybersecuritybedrijven**. Hier zijn enkele voorbeelden van, zoals het ISO Register. In dit register staan bedrijven met ISO 27001 certificering, een wereldwijde norm op het gebied van informatiebeveiliging. Maar hiermee krijgen we slechts een deel van de bedrijven die actief zijn in dit domein in beeld, want mogelijk heeft niet elk bedrijf deze certificering. We zouden de afbakening ook kunnen doen op basis van lijsten van cybersecuritybedrijven die we vinden bij koepelorganisaties of overzichten op websites, zoals bij Cyberveilig Nederland of SecuriGuide. Wederom brengen we hier alleen een deel van de bedrijven in kaart, al zullen de grotere partijen waarschijnlijk goed vertegenwoordigd zijn.
- Een derde optie die we verkend hebben is het **uitzenden van een enquête** naar een doelgroep waarvan verwacht kan worden dat ze wellicht tot de cybersecurity

[7] Zie http://bastiat.org/fr/cqovecqonvp.html

activiteiten zullen uitvoeren. Deze aanpak is gekozen door SEO en VKA toen zij in 2016 een eerste iteratie van dit onderzoek uitvoerden.[8] Deze aanpak kan leiden tot goede resultaten als de doelgroep goed is afgebakend. Als de doelgroep te smal gedefinieerd is dan verliezen we bedrijven. Als de doelgroep te breed benaderd dan wordt een te grote groep bedrijven benaderd.[9] Dat laatste is methodologisch geen probleem, maar zorgt wel voor administratieve lasten bij veel bedrijven. Bovendien moet de response hoog genoeg zijn om conclusies te kunnen trekken op sectorniveau. In onze ervaring ligt de response bij dit type enquêtes op 5% à 10% als het goed wordt uitgevoerd. In het onderzoek van SEO en VKA werd de enquête uitgestuurd naar 3.868 ICT-bedrijven. Dat lijkt ons een prima opzet gegeven de mogelijkheden die er toentertijd waren. Het is echter aannemelijk dat veel bedrijven die niet geregistreerd staan als ICT-bedrijf toch actief zijn in cybersecurity. Daarmee is het mogelijk dat een groot aandeel van de cybersecurity bedrijven niet zijn benaderd. Ook kent een enquête de beperking van een selectieve non-response, zeker met betrekking tot de cybersecurity markt omdat het niet duidelijk is wat de populatie nu eigenlijk is.[10] Daarnaast heeft het onderzoek van SEO en VKA zijn resultaten gebaseerd op een sample van slechts 266 bedrijven. Dit is ons inziens een te klein sample om de omvang van cybersecurity activiteiten te bepalen.

De bovenstaande opties hebben dus allen beperkingen. In de volgende paragraaf maken we duidelijk hoe wij ons onderzoek hebben opgezet om deze beperkingen te ondervangen.

2.6 Onderzoeksaanpak

De onderstaande afbeelding toont een schematisch overzicht van de onderzoeksmethodes die we hebben gehanteerd en de wijze waarop ze onderling samenhangen. Om de economische kansen van de cybersecuritysector in kaart te brengen is het van belang een afbakening te maken: welke bedrijven voeren cybersecurity activiteiten uit, en welke niet? Deze afbakening is gemaakt aan de hand van een inhoudelijke analyse van de teksten op de websites van alle Nederlandse bedrijven. Vervolgens is voor deze bedrijven administratieve data opgehaald van het CBS en is er een enquête uitgestuurd onder bedrijven waarvan het emailadres bekend is in de database van Innovatiespotter. Parallel hebben we een literatuurstudie uitgevoerd en vacatureonderzoek gedaan. Alle gedefinieerde trends zijn vervolgens getoetst en aangevuld in een ronde interviews (n=16). De uitkomsten van alle onderzoekstappen zijn getoetst en verrijkt in een validatiesessie.

Wij zijn ons ervan bewust dat deze onderzoeksmethode, het identificeren van cybersecuritybedrijven aan de hand van zoektermen op hun websites, ook zijn beperkingen kent. Ondanks dat wij van mening zijn dat het mogelijk is om via deze methode een groot deel van de cybersecuritybedrijven in Nederland te identificeren, bevat het sample ruis en missen er mogelijk cybersecuritybedrijven.

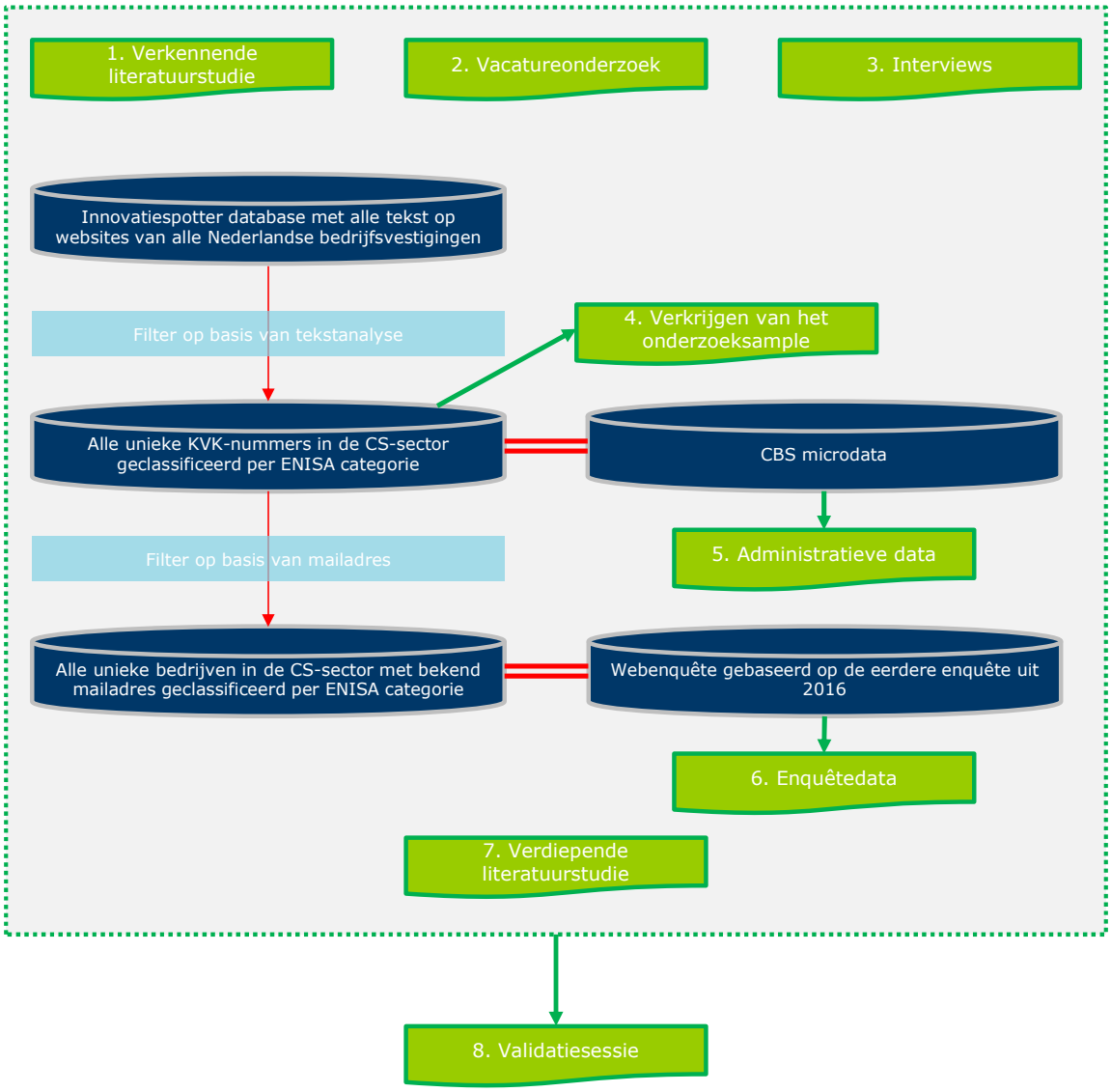
Een uitgebreide beschrijving van de verschillende onderdelen uit de onderzoeksaanpak is beschreven in Bijlage 1.

---

[8] https://www.seo.nl/wp-content/uploads/2020/04/2016-56_Economische_kansen_Nederlandse_Cybersecurity_sector.pdf

[9] Of erger nog toch toegeschreven aan de cybersecuritysector, wat leidt tot een overschatting.

[10] Met andere woorden: waardevolle uitspraken over selectiviteit in de respons zijn lastig te maken, omdat het niet duidelijk is welke populatie beschreven wordt.



Figuur 2. Onderzoeksaanpak en onderlinge samenhang van onderzoeksmethodes.

3 Sterktes en zwaktes van de Nederlandse cybersecuritysector

De Nederlandse cybersecuritysector kent verschillende sterktes. Ten eerste kent de sector een flinke groei van 10% tot 15% per jaar. In 2020 draaide de sector een omzet van €26 miljard, behaalde een toegevoegde waarde van bijna €13 miljard en kende de sector ruim 130.000 werknemers. De cybersecuritysector omvat daarmee circa 0,9% van de Nederlandse economie. Ten tweede kan de sector goed voldoen aan de binnenlandse vraag naar diensten. Ook kent Nederland een sterke kennisbasis in onderzoek naar cryptografie. Het heeft decennia geduurd om deze positie op te bouwen. Tenslotte bevat de sector hoogwaardige integrators kunnen cybersecurity gebruiken om een competitief voordeel te realiseren. Nederland heeft een hoogwaardige economische structuur waarin de integratie van cybersecurity een competitief voordeel kan zijn.

De Nederlandse cybersecurity sector heeft echter ook enkele zwaktes. Zo kent de sector weinig private cyber R&D, en is er sprake van een sector die sterk R&D-intensief is, maar Nederlands bedrijven doen hier relatief beperkt aan. Daarnaast is de output van de sector is beperkt te exporteren. De Nederlandse sector is gericht op diensten en deze laten zich minder goed exporteren dan software, hardware en managed services. Door de focus op diensten is de sector kent grote afhankelijkheid van buitenlandse leveranciers. Om de nationale markt te kunnen bedienen wordt er sterk geleund om buitenlandse leveranciers van hardware, software en managed services. Tot slot bestaat de markt overwegend uit MKB en ZZP'ers. Hierdoor kent de sector een relatief beperkte slagkracht.

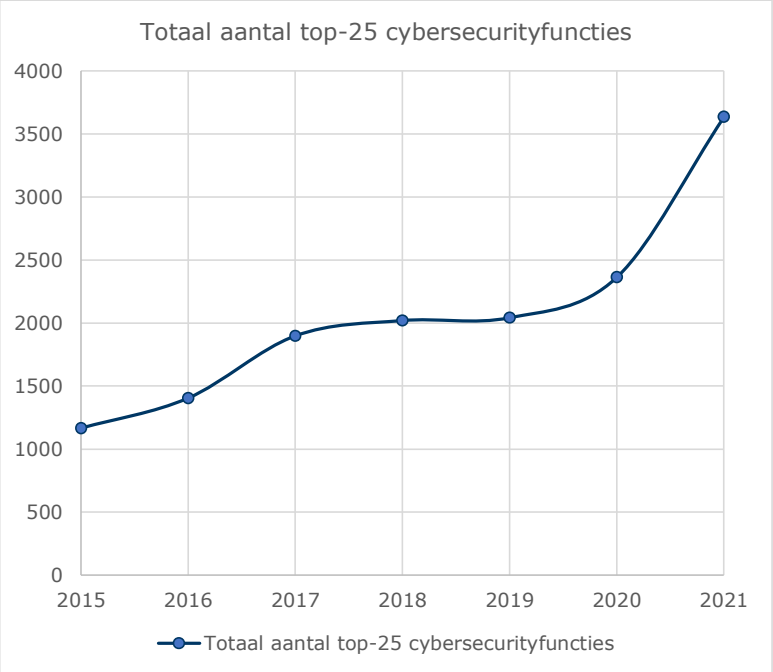
3.1 Sterktes van de Nederlandse Cybersecuritysector

3.1.1 Sector kent een flinke groei

De cybersecuritysector heeft de afgelopen jaren een flinke groei doorgemaakt. Dit wordt onderbouwd door een groot aantal bronnen in de literatuur, de interviews, de vacatureanalyse, de enquête en administratieve data van het CBS.

Analyse van vacatures

Om een beeld te krijgen van de groei van de sector, hebben we gekeken naar de vacatures die worden uitgezet naar cybersecurityfuncties. Als we de aantallen sommeren, dan ontstaat Figuur 3. Het is duidelijk dat er sprake is van een flinke groei in de vacatures, een goede indicator van de groei van de sector. We kunnen op basis van deze data een inschatting maken van de gemiddelde jaarlijkse groei (CAGR). Voor de periode 2015-2020 was dit 13% en dit komt overeen met de uitkomsten van de cijfers uit de literatuur die we eerder noemden. Als we de spectaculaire groei van 2021 meenemen dan komen we op een CAGR van 18%. Een uitsplitsing naar functies is te vinden in Bijlage 6, Tabel 57.



Figuur 3. Ontwikkeling van het totaal aantal vacatures in de Top 25 cybersecurityfuncties. Bron: Dialogic o.b.v. data Jobdigger[11]

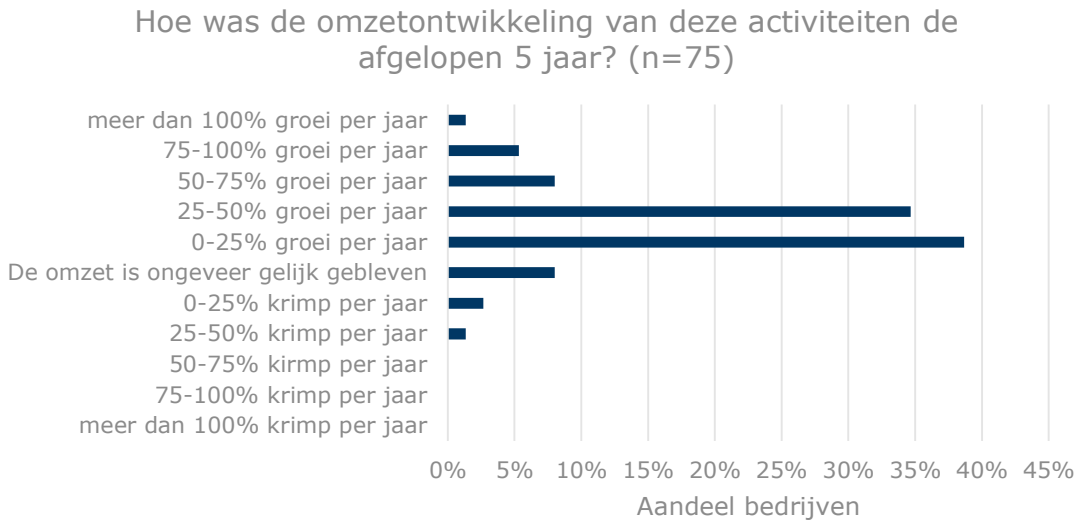
Hierboven keken we naar vacatures van cybersecurityfuncties. Een ander perspectief is het kijken naar vacatures met cybersecurityvaardigheden. Er zijn immers ook allerlei functies die niet primair gericht zijn op cybersecurity, maar waarbij dit wel een component is. Op basis van dezelfde bron kunnen we ook een uitsplitsing maken van de meest gevraagde cybersecurityvaardigheden, zie Bijlage 6 Tabel 5858. Hier komen we op een jaarlijkse groei van functie met hierin cybersecurityvaardigheden van circa 14%.

Enquête

In de enquête is specifiek gevraagd naar de omzetontwikkeling van de cyberproducten en -diensten van de afgelopen vijf jaar. In totaal hebben 75 bedrijven antwoord gegeven op deze vraag. Uit de reacties van deze bedrijven komt naar voren dat er sprake is van een zeer sterke groei. Bijna 40% van de respondenten kent een groei van 0 tot 25%. Bijna 35% heeft een jaarlijkse groei van 25% tot 50%.[12] Enkele weinig bedrijven kenden een dalend omzet. Figuur 4 toont het volledige overzicht.

[11] Exclusief de vacatures van de bemiddelingsinstellingen. Van de vacatures die via bemiddelingsinstellingen (onder andere uitzendbureaus) worden uitgezet kan, door een beperkte omschrijving van de vacature, niet goed worden bepaald of hij al eerder is uitgezet. Om te voorkomen dat er vacatures dubbel worden meegenomen, is daarom besloten om de vacatures die worden uitgezet door bemiddelingsinstellingen niet mee te nemen. Specifiek is gekeken of één van de volgende woorden voorkomt: 'cyber', 'security', 'beveiliging' of 'hacker'

[12] Voor alle duidelijkheid een groei van 50% per jaar over een periode van 5 jaar betekent dat de omzet in 2022 7,5x hoger lag dan in 2017. Een groei van 75% per jaar over een periode van 5 jaar betekent dat de omzet met een factor 16 omhoog ging.

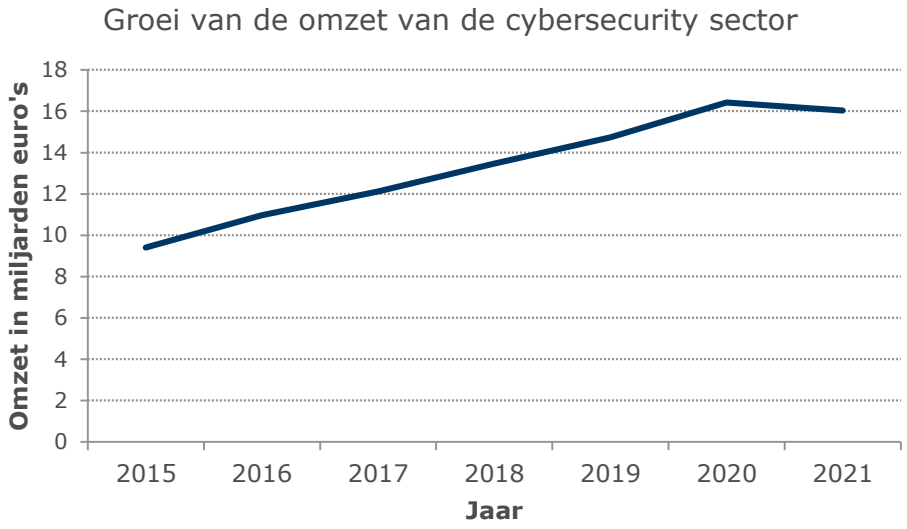


Figuur 4. Omzetontwikkeling van cybersecurityproducenten

CBS microdata

Op basis van de CBS-microdata kunnen we een uitsplitsing maken van de omzetontwikkeling van de zeven onderzochte ENISA-categorieën. Onderstaande figuur toont de ontwikkeling van de omzet van bedrijven die onder meer cybersecurity-activiteiten ontplooien. Een belangrijke kanttekening hierbij is dat dit ook omzet betreft die is gegenereerd uit niet-cybergerelateerde producten en diensten (onderstaand figuur is dus vooral informatief voor de groei en niet voor de absolute omzet van de sector). Hieruit komt naar voren dat er sprake is van een flinke groei. In de periode 2015-2020 verdubbelde de totale bedrijfsomzet ongeveer van 32 miljard naar 56 miljard. Dat betekent een jaarlijkse groei van circa 15% per jaar.[13] Opvallend is dat er in 2021 sprake is van een daling. We kunnen niet met zekerheid verklaren waar deze daling door komt. Een mogelijke verklaring is dat de omzet van bedrijven in 2021 is gedaald in verband met de coronacrisis (deze daling kan ook plaats hebben gevonden in de omzet die is gegenereerd uit niet-cyber-gerelateerde producten en diensten).

[13] De groei over de periode 2015-2021 was 13% per jaar.



Figuur 5 Ontwikkeling van de omzet van bedrijven die onder meer cybersecurity-activiteiten ontplooien[14]

Zoals gezegd bevat de omzet in bovenstaande figuur ook omzet gegenereerd uit niet-cyber-gerelateerde producten en diensten. Om een goede indicatie te krijgen van de omzet die uitsluitend gerelateerd is aan cybersecurity, kunnen we gebruik maken van de enquête. Op basis hiervan komen we tot de conclusie dat 29% van deze bovenstaande omzet afkomstig is van cybersecuritydiensten en -producten. Dit percentage van de omzet afkomstig van cybersecurity hebben we vermenigvuldigd met de totale omzet, toegevoegde waarde en aantal werknemers van de CBS-microdata van de set aan bedrijven (zie Bijlage 4 voor de achterliggende data). Uit onderstaande tabel komt de belangrijke uitkomst naar voren dat de cybersecuritysector een aanzienlijke omzet en toegevoegde waarde kent.

Tabel 1. Geschatte omzet, toegevoegde waarde, aandeel in BBP en aantal werknemers van de cybersecuritysector

	2015	2016	2017	2018	2019	2020	2021
Omzet (€ mld.)	9,4	11,0	12,1	13,5	14,7	16,4	16,0
Toegevoegde waarde (€ mld.) [15]	5,5	6,0	6,7	7,0	7,5	7,5	
Aandeel van het BBP[16]	0,80%	0,85%	0,91%	0,91%	0,92%	0,94%	
Aantal werknemers	82.580	108.802	93.112	86.510	93.799	86.348	94.628

Aanpak van de schatting van de omzet, toegevoegde waarde, aandeel in BBP en aantal werknemers van de cybersecuritysector

De schatting van de omzet, toegevoegde waarde, aandeel in BBP en aantal werknemers van de cybersecuritysector in Tabel 1 hebben we als volgt gemaakt. In de uitgezette enquête hebben bedrijven aangegeven welk deel van hun omzet voortkomt uit cybersecurityproducten en -diensten. Van de 127 bedrijven die de survey hebben

[14] In Bijlage 4 is de achterliggende data te vinden.

[15] Voor 2021 zijn er geen gegevens over de toegevoegde waarde beschikbaar uit de CBS-microdata.

[16] Bron: [Eurostat]

ingevuld, zijn er 90 actief in de cybersecuritysector. De overige 37 bedrijven hebben aangegeven geen R&D uit te voeren op het gebied van cybersecurity, geen cybersecurityproducten en/of -diensten te leveren en geen integratie uit te voeren van cybersecurity in diensten of producten. Van de 90 bedrijven actief in de cybersecuritysector hebben 75 bedrijven ingevuld welk deel van de omzet voorkomt uit de levering van cybersecuritydiensten en -producten. Doorgaans is immers niet 100% van de omzet van deze bedrijven toe te schrijven aan cybersecurity-producten en/of diensten; daarom dienen we een 'correctiefactor' toe te passen op de totale omzet van de bedrijven die (onder andere) cybersecurity-producten en/of diensten leveren.

Op basis van enquêteresultaten is de correctiefactor als volgt bepaald: bedrijven met minder dan 10 werknemers halen ~50% van hun omzet uit cybersecurity-activiteiten, bedrijven met 10-99 werknemers halen ~40% van hun omzet uit cybersecurity-activiteiten en bedrijven met 100 werknemers of meer halen ~25% van hun omzet uit cybersecurity-activiteiten. Dit komt overeen met een gewogen gemiddelde van ~29%. Indien de uitsplitsingen naar grootteklasse in tabellen aanwezig zijn, hebben we de drie separate percentages gehanteerd. In de andere tabellen hebben we het gewogen gemiddelde van 29% gebruikt.

Het economisch verdienvermogen van de sector uit dit onderzoek kunnen we vergelijken met het onderzoek dat in 2016 door SEO en VKA werd uitgevoerd, hoewel de methoden van de onderzoeken enigszins verschillen.[17] De uitkomsten van dit vorige onderzoek zijn te vinden in Tabel 2. Als we 2014 en 2015 vergelijken dan valt direct op dat dit onderzoek grofweg in lijn ligt met de resultaten van het eerdere onderzoek, ervan uitgaande dat de cybersecuritysector een groeiende sector is. Enkel het aantal werknemers dat zich bezighoudt met cybersecurity activiteiten ligt aanzienlijk hoger. Voor een deel wordt dit verklaard doordat SEO en VKA alleen bedrijven (1) uit de ICT-sector (2) met minimaal 5 FTE onderzochten. Uit ons onderzoek komt naar voren dat bedrijven met andere SBI-codes ook actief zijn in dit domein, zie Bijlage 12. Verder zien we dat kleinere bedrijven in deze sector ook een rol spelen, zie Bijlage 4, Tabel 19. SEO en VKA geven dit ook al aan in hun onderzoek: "*Alleen het deel binnen de ICT-sector is reeds 0,6% van het BBP. Deze uitkomst is daarom een conservatieve schatting van de cybersecurity-sector.*"[18]

Tabel 2. Uitkomsten van het onderzoek over hetzelfde onderwerp uit 2015. [19]

	2010	2014
Omzet (€ mld.)	4,8	7,5
Toegevoegde waarde (€ mld.)	2,6	4,1
Aandeel van het BBP	0,41%	0,62%
Aantal werknemers	12.000	13.500

[17] https://www.seo.nl/wp-content/uploads/2020/04/2016-56_Economische_kansen_Nederlandse_Cybersecurity_sector.pdf

[18] https://www.seo.nl/wp-content/uploads/2020/04/2016-56_Economische_kansen_Nederlandse_Cybersecurity_sector.pdf

[19] https://www.seo.nl/wp-content/uploads/2020/04/2016-56_Economische_kansen_Nederlandse_Cybersecurity_sector.pdf

Wat verder opvalt is dat het aantal werknemers zeer sterk verschilt tussen beide studies. We kunnen dit verifiëren door het te toetsen aan een derde bron: de gemiddelde toegevoegde waarde per medewerker per jaar. Wij komen in onze analyse op een toegevoegde waarde van (€7,5 miljard / 86.348≈) €86.857 per werknemer per jaar in 2020. Voor heel Nederland was de toegevoegde waarde €76.000 per werkzaam persoon in 2020 in alle sectoren.[20] Voor de bedrijven met de SBI-code *J Informatie en communicatie* was dit €109.000.[21] Onze schatting lijkt ons daarmee redelijk; we weten immers dat een deel van de bedrijven in de cybersecuritysector niet deze SBI-code hanteren. Als we kijken naar de schatting van het eerdere onderzoek uit 2016 dan komen we voor 2014 op een toegevoegde waarde per medewerker per jaar van (€4,1 miljard / 13.500≈) €300.000 per werknemer per jaar. Dit lijkt ons aan de hoge kant, zeker omdat we ook nog eens rekening moeten houden met inflatie. Wij vermoeden daarom dat in het vorige onderzoek het aantal medewerkers onderschat is.

Literatuur

Er zijn talloze studies die schattingen maken van de **groei van de cybersecuritysector**. McKinsey heeft het over een groei van ruim 12% per jaar[22], Grandview spreekt over een groei van 8% per jaar[23], Next Move Strategy Consulting over bijna 13%[24], Statista van 11%[25], Strategic Market Research van 9,5%[26], Mordor van ruim 13%[27], Polaris van bijna 10%[28], Global Data van bijna 9%[29] en Zion van ruim 10%.[30] Omdat de uitgangspunten (regio, marktafbakening, periode) verschillen, zullen de uitkomsten ook verschillen. Desalniettemin is het algemene beeld dat er duidelijk sprake is van een markt met een flinke jaarlijkse groei van rond de 10% per jaar.

Doordat we als samenleving **steeds afhankelijker worden van ICT**, neemt de relevantie van cybersecurity toe. De versnelling als gevolg van de COVID-19 pandemie heeft recent een extra impuls gegeven.[31] We zijn veel meer hybride of thuis gaan werken en business processen gebeuren steeds vaker in de cloud. Beide trends leveren nieuwe

---

[20] https://opendata.cbs.nl/#/CBS/nl/dataset/84180NED/table

[21] https://opendata.cbs.nl/#/CBS/nl/dataset/84180NED/table

[22] https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2-trillion-dollar-market-opportunity-for-cybersecurity-technology-and-service-providers#/

[23] https://www.grandviewresearch.com/industry-analysis/cyber-security-market

[24] https://www.globenewswire.com/news-release/2023/01/30/2597604/0/en/Global-Cyber-Security-Market-to-Generate-USD-657-02-billion-by-2030-Next-Move-Strategy-Consulting.html

[25] https://www.statista.com/outlook/tmo/cybersecurity/worldwide

[26] https://www.strategicmarketresearch.com/market-report/cyber-security-market

[27] https://www.mordorintelligence.com/industry-reports/cyber-security-market

[28] https://www.polarismarketresearch.com/industry-analysis/cyber-security-market

[29] https://www.globaldata.com/store/report/cybersecurity-market-analysis/

[30] https://www.prnewswire.com/news-releases/at-10-1-cagr-of-global-cyber-security-market-size-to-report-spectacular-growth-revenue-to-hit-us210-billion-by-2028---zion-market-research-301530191.html

[31] World Economic Forum. Global Cybersecurity Outlook 2022. Insight Report January 2022. https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf

veiligheidsuitdagingen op.[32,33,34] Het aanvalsoppervlak is immers sterk uitgebreid. Dit blijkt ook uit de zorgen van zogenaamde 'cyberleiders', ofwel de belangrijkste leidinggevenden binnen de cybersector. Uit een survey van het World Economic Forum onder *cyberleaders* blijkt dat 42% vreest voor uitval van infrastructuur door een cyberaanval, 24% voor identiteitsdiefstal, 20% voor ransomware en 10% voor verlies van vermogen.[35] Daar waar het specifiek gaat om cyberaanvallen zijn organisaties het meest bang voor (1) ransomware, (2) social engineering en (3) kwaadwillende insideractiviteit.[36]

Een andere trend is de **toenemende dreiging van statelijke actoren**.[37] Statelijke actoren kunnen onder meer de volgende middelen inzetten: 1) beïnvloeding en inmenging, 2) spionage (waaronder technologiediefstal) en 3) voorbereidingshandelingen voor een daadwerkelijke verstoring en sabotage. Nederland is doelwit gebleken van een offensief cyberprogramma van landen als Rusland en China.[38] Statelijke actoren kunnen cybercriminelen inhuren, gedogen of onder druk zetten om cyberaanvallen op gewenste doelwitten uit te voeren.[39] De oorlog tussen Rusland en Oekraïne in het bijzonder heeft een sterke invloed (gehad) op trends in cyberdreigingen.[40] Enkele interessante ontwikkelingen waren de aanzienlijke toename van hacktivistische activiteiten, cyberactoren die operaties uitvoeren in combinatie met kinetische militaire actie, de mobilisatie van hacktivisten, cybercriminaliteit en hulp van nationale staten tijdens dit conflict. Het werd ook duidelijk dat geopolitiek een grote invloed blijkt te hebben in dit domein. Destructieve aanvallen bleken een prominent onderdeel te zijn van de acties van statelijke actoren (combinatie met militaire actie). Daarnaast bleek desinformatie een belangrijke tool in cyberwarfare. Het werd bijvoorbeeld al gebruikt voordat de "fysieke" oorlog begon als een voorbereidende activiteit voor de inval van Rusland in Oekraïne.

Mobiele cyberbeveiliging wordt steeds belangrijker.[41,42] De trend naar werken op afstand versnelt de groei van mobiele cyberveiligheid. Voor werknemers is het inmiddels normaal om te schakelen tussen een reeks mobiele apparaten, zoals tablets en telefoons, met behulp van openbare Wi-Fi-netwerken en tools voor samenwerking op afstand. Als gevolg hiervan blijven mobiele bedreigingen groeien en evolueren. De uitrol van 5G-technologie en de

---

[32] Gartner Report (2022). Top Trends in Cybersecurity 2022. https://www.gartner.com/en/doc/760806-top-trends-in-cybersecurity

[33] https://www.forbes.com/sites/bernardmarr/2022/11/11/the-top-five-cybersecurity-trends-in-2023/?sh=321ecc171785

[34] https://www.kaspersky.com/resource-center/preemptive-safety/cyber-security-trends

[35] World Economic Forum. Global Cybersecurity Outlook 2022. Insight Report January 2022. https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf

[36] World Economic Forum. Global Cybersecurity Outlook 2022. Insight Report January 2022. https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf

[37] NCTV (2022). Cybersecuritybeeld Nederland 2022. https://www.nctv.nl/onderwerpen/cybersecuritybeeld-nederland/documenten/publicaties/2022/07/04/cybersecuritybeeld-nederland-2022

[38] AIVD, 'Tweede Kamer geïnformeerd over prioriteiten en accenten AIVD voor 2022', 17 december 2021. https://www.aivd.nl/actueel/nieuws/2021/12/17/tweede-kamer-geinformeerd-over-aivd-prioriteiten-en-accenten-voor-2022.

[39] 'Cybersecuritybeeld Nederland 2021', NCTV, juni 2021. https://www.nctv.nl/binaries/nctv/documenten/publicaties/2021/06/28/cybersecuritybeeld-nederland-2021/CSBN2021_def_interactieve+pdf_web.pdf

[40] ENISA (november 2022). Threat Landscape 2022. DOI: 10.2824/764318 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022/@@download/fullReport

[41] https://www.kaspersky.com/resource-center/preemptive-safety/cyber-security-trends

[42] https://www.simplilearn.com/top-cybersecurity-trends-article

afhankelijkheid van snelle toegang tot grote gegevensbestanden zorgen voor mogelijke nieuwe kwetsbaarheden.[43] Steeds meer producten en diensten worden gedigitaliseerd, van slimme televisies tot verbonden auto's en medische apparatuur.[44] En door de komst en groei van 5G-netwerken wordt een nieuw tijdperk van interconnectiviteit werkelijkheid met het Internet of Things (IoT).[45] Deze communicatie tussen meerdere apparaten opent ook de weg voor kwetsbaarheden door beïnvloeding van buitenaf, aanvallen of een onbekende softwarebug. Zelfs de meest gebruikte browser ter wereld, Chrome, bleek ernstige bugs te bevatten.[46] De architectuur van 5G is relatief nieuw en vereist veel onderzoek naar het vinden van mazen om zo de systeembeveiliging te verbeteren.

Digitale aanvallen op **operationele technologie (OT)** komen vaker voor en worden onder meer gebruikt in cyberoorlogsvoering. Dit zijn digitale systemen die bijvoorbeeld sluizen aansturen of de productie in fabrieken reguleren. De stijgende vraag naar betere connectiviteit van systemen, sneller onderhoud van apparatuur en betere inzichten in het gebruik van middelen heeft geleid tot OT-systemen met internetverbinding, waaronder industriële besturingssystemen (ICS) en andere systemen zoals SCADA-systemen (Supervisory Control and Data Acquisition), gedistribueerde besturingssystemen (DCS), remote terminal units (RTU's) en PLC's (Programmable Logic Controllers). Nu alles via internet en de cloud wordt beheerd, worden de productiesector en de kritieke infrastructuursectoren (d.w.z. sectoren als gezondheidszorg, farmacie, chemie, energieopwekking, olieproductie, vervoer, defensie, mijnbouw, levensmiddelen en landbouw) blootgesteld aan ernstige bedreigingen met een grote impact. Vanuit de NLCS wordt ingezet op het vergroten van kennis en bewustzijn van de risico's bij organisaties die gebruik maken van deze systemen.

Cyberaanvallen op leveranciersketens (supply chain attacks) door criminelen zijn een groeiend probleem.[47] Incidenten hebben namelijk niet alleen impact op de directe slachtoffers, maar ook op ketens van leveranciers, klanten en burgers die gebruik maken van de dienstverlening.[48] Kwetsbaarheden die diep zijn ingebed in de digitale toeleveringsketen zijn vaak uiterst moeilijk te detecteren, en duizenden toepassingen of apparaten kunnen tegelijkertijd worden getroffen.[49][50] Criminelen zijn ook steeds beter in staat tot aanvallen op

---

[43] https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/cybersecurity-trends-looking-over-the-horizon

[44] NCTV (2022). Nederlandse Cybersecuritystrategie 2022-2028 Ambities en acties voor een digitaal veilige samenleving. https://www.nctv.nl/onderwerpen/nederlandse-cybersecuritystrategie-2022-2028

[45] https://www.simplilearn.com/top-cybersecurity-trends-article

[46] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-3075

[47] Zie bv. https://publications.tno.nl/publication/34638899/zNP6Av/buningh-2021-als.pdf

[48] Dialogic (2022). Verkenning risicofactoren ransomware-aanvallen. In opdracht van WODC, Den Haag. https://www.dialogic.nl/wp-content/uploads/2022/04/3275-verkenning-risicofactoren-ransomware-aanvallen-volledige-tekst.pdf

[49] Gartner Report (2022). Top Trends in Cybersecurity 2022. https://www.gartner.com/en/doc/760806-top-trends-in-cybersecurity

[50] Recente voorbeelden zijn SolarWinds en REvil in Kaseya remote access software, en URGENT/11 and Log4j.

Managed Services Providers (MSP's).[51] De risico's van de digitale toeleveringsketen vallen doorgaans uiteen in vier hoofdcategorieën:[52]

1. De mogelijke openbaarmaking van gevoelige informatie die wordt gedeeld met ketenpartners.
2. Compromittering van met ketenpartners gedeelde infrastructuur zoals netwerken, software, cloud service en managed services providers.
3. Aanvallen via gangbare commerciële en open-source software die bij bedrijfs- en IT-activiteiten wordt gebruikt.
4. De exploitatie van beveiligingsfouten in de digitale producten die aan klanten worden verkocht.

Voor de markt betekent dit dat er vermoedelijk meer risicobeperkende maatregelen komen om de impact van cyberaanvallen op leveranciersketens te verkleinen. Zulke maatregelen zijn bijvoorbeeld een meer doelbewuste segmentatie en scoring van leveranciers en partners op basis van risico's, meer verzoeken aan leveranciers en partners omtrent bewijs van beveiligingscontroles en veilige *best practices*. Eén eerste trend binnen deze categorie is dat de door organisaties gebruikte systemen steeds complexer worden en er minder zicht op is, waar criminelen slim gebruik van maken.[53] Deze complexe systemen zijn afhankelijk van een veelheid aan leveranciers en de selectie en het beheer van deze leveranciers wordt bepaald door een groot aantal factoren. Om het nog ingewikkelder te maken, hebben verschillende afdelingen binnen dezelfde organisatie soms verschillende protocollen om diensten van leveranciers af te nemen. Dit maakt het voor organisaties bijna onmogelijk om een volledig overzicht te krijgen van hun relaties met derden en de hieruit voortvloeiende afhankelijkheden en risico's. En naast deze relaties is er niet altijd een goed overzicht waar gegevens zich bevinden en welke partner toegang heeft tot deze gegevens (zowel in online als offline vorm). Het is vrijwel zeker dat criminelen verder misbruik zullen maken van dit gebrek aan zicht op afhankelijkheden, alsmede van de toegenomen complexiteit en het vertrouwen van organisaties en hun leveranciers, om voet aan de grond te krijgen binnen organisaties. Ook zullen criminelen waarschijnlijk gaan investeren in onderzoek naar kwetsbaarheden in veelgebruikte bedrijfstechnologieën, zoals e-mailservers of kennisbeheersoftware. Een kwetsbaarheid (of een keten van kwetsbaarheden) in één technologie geeft hun immers toegang tot meerdere omgevingen tegelijk.[54] Tot slot zijn cybersecurityonderzoekers binnen organisaties steeds vaker zelf het doelwit van criminelen.[55] De laatsten hoeven zo niet zelf al het onderzoek te doen, maar kunnen de resultaten simpelweg stelen.

---

[51] ENISA (november 2022). Threat Landscape 2022. DOI: 10.2824/764318 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022/@@download/fullReport

[52] Gartner Report (2022). Top Trends in Cybersecurity 2022. https://www.gartner.com/en/doc/760806-top-trends-in-cybersecurity

[53] ENISA (november 2022). Threat Landscape 2022. DOI: 10.2824/764318 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022/@@download/fullReport

[54] ENISA (november 2022). Threat Landscape 2022. DOI: 10.2824/764318 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022/@@download/fullReport

[55] Black Hat Keynote: Supply Chain Infections and the Future of Contactless Deliveries https://www.blackhat.com/us-21/briefings/schedule/#keynotesupply-chain-infections-and-the-future-of-contactless-deliveries-24987

Interviews

In de interviews wordt uitvoerig gesproken over de flinke groei die de sector heeft doorgemaakt. Hierbij worden vanuit verschillende perspectieven gekeken naar de groei van de sector:

- De **toegenomen economische en maatschappelijke afhankelijkheid** van de ICT heeft ervoor gezorgd dat cybersecurity steeds belangrijker is geworden. Voorheen werd cybersecurity als een technisch thema beschouwd. In het afgelopen decennium is het echter veranderd in een bestuurlijk thema. Het is daarmee veranderd van een nevenactiviteit naar een belangrijk onderdeel van het functioneren van een organisatie en daarmee randvoorwaardelijk voor de bedrijfscontinuïteit. Cybersecurity is niet langer een nichemarkt, maar een brede sector. De groei en het besef van het belang van cybersecurity is gelijk opgegaan met het besef dat digitalisering ook in de haarvaten van de samenleving terecht is gekomen.
- In het verlengde hiervan wordt door verschillende respondenten specifiek gewezen op de kwetsbaarheid van **supply chains**. Doordat organisaties steeds meer onderlinge (digitale) koppelingen hebben, nemen kwetsbaarheden toe. Wanneer het mis gaat bij één partij, gaat het fout bij alle digitale partners in diezelfde keten. Grote bedrijven eisen steeds vaker van hun toeleveranciers dat zij hun informatiebeveiliging op orde hebben, anders vormt deze toeleverancier een kwetsbare plek. Over het algemeen is het mkb niet het primaire doel van een cybersecurityaanval. Maar als een dergelijk middelgroot of klein bedrijf deel uitmaakt van een gedigitaliseerde keten, dan worden de afhankelijkheden groter en wordt cybersecurity belangrijker.
- Een ander aspect dat respondenten benoemen is de **kwalitatieve en kwantitatieve toename van cyberaanvallen**. Er wordt onderscheid gemaakt tussen twee soorten aanvallers. Enerzijds zijn er criminele organisaties die veelal financieel gewin als hoofddoel hebben; anderzijds zijn er statelijke actoren die vaak uit zijn op spionage en verstoring. Echter kunnen deze agressors ook in elkaars verlengde liggen en is het onderscheid soms lastig te maken omdat ze dezelfde aanvalstechnieken gebruiken. De afgelopen jaren zijn beide soorten aanvallers steeds professioneler gaan werken. Als het gaat om criminele organisaties, dan komt vooral ransomware naar voren als grote bedreiging. Doordat deze aanvallen vanaf elke locatie kunnen worden uitgevoerd en de pakkans klein is, is het een aantrekkelijk *businessmodel* voor de intelligente crimineel. Als het gaat om statelijke actoren, dan komt specifiek een zorg voor maatschappelijke ontwrichting als gevolg van aanvallen op vitale sectoren naar voren.
- In de afgelopen jaren heeft de sector zich verder **gediversifieerd en gespecialiseerd**. Er worden niet alleen meer cyberproducten en -diensten afgenomen, er worden ook andere, nieuwe producten en diensten afgenomen. Het meest in het oog springende voorbeeld dat genoemd wordt zijn cybersecurityverzekeringen. Deze bestonden enige tijd geleden niet of nauwelijks en worden nu op flinke schaal afgenomen. Dit betekent dat bedrijven zich meer bewust zijn van de risico's van de impact die cyberaanvallen kunnen hebben. Ook allerlei vormen van certificering worden in deze context genoemd.

3.1.2 Sector kan goed voldoen aan binnenlandse vraag naar diensten

De Nederlandse cybersecuritysector is een sector die goed in staat is om te voldoen aan de binnenlandse vraag naar diensten (hier bedoelen we diensten van personen, niet managed services). Dit komt uit de enquête en de interviews naar voren. Het in staat zijn om te voldoen aan de vraag is een sterkte, maar kent ook een keerzijde. Bij de zwaktes zullen we zien dat andere delen van de binnenlandse vraag (de vraag naar cybersecurityproducten)

niet goed kunnen worden bediend door Nederlandse aanbieders. In Nederland gebruikt men internationale producten om de dienstenmarkt te voorzien.

Uitkomsten van enquête

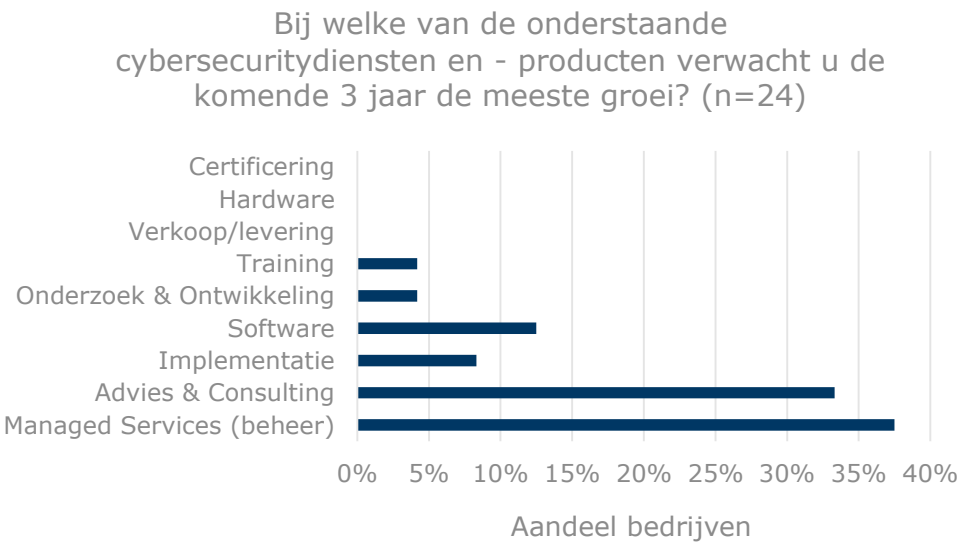
Uit de enquête komt naar voren dat de dienstensector in Nederland veruit het grootste deel van de markt behelst. Diensten als advies & consulting, implementatie en training komen sterk naar voren. Hardware en software komen veel minder sterk naar voren. Dit kan wellicht deels verklaard worden doordat organisaties die diensten leveren, met een kleinere schaalgrootte kunnen opereren dan producenten van software en zeker hardware. Concreet: een expert kan zich voor één dag per week laten inhuren als cybersecurityconsultant, maar een bedrijf dat hardware produceert heeft veel meer FTE nodig om haar output te kunnen genereren.

Figuur 6. Verdeling van activiteiten van de Nederlandse cybersecuritybedrijven[56]

Ook als we kijken naar de verwachte groei van de Nederlandse sector, dan komt de dienstenkant sterk naar voren. Advies en consulting wordt door een derde van de respondenten genoemd als sector waar men de meeste groei verwacht.[57]

[56] Wij zijn ons ervan bewust dat de categorie managed services (beheer) op twee manieren geïnterpreteerd kan worden. Als het aanbieden van managed services, maar ook als het aanbieden van het beheer van managed services die door een andere partijen worden geleverd. Wij verwachten echter dat het merendeel van de respondenten het als de eerste optie (het aanbieden van deze diensten) geïnterpreteerd heeft. Dit komt omdat we diensten als advies, consulting, training en implementatie separaat benoemd hebben.

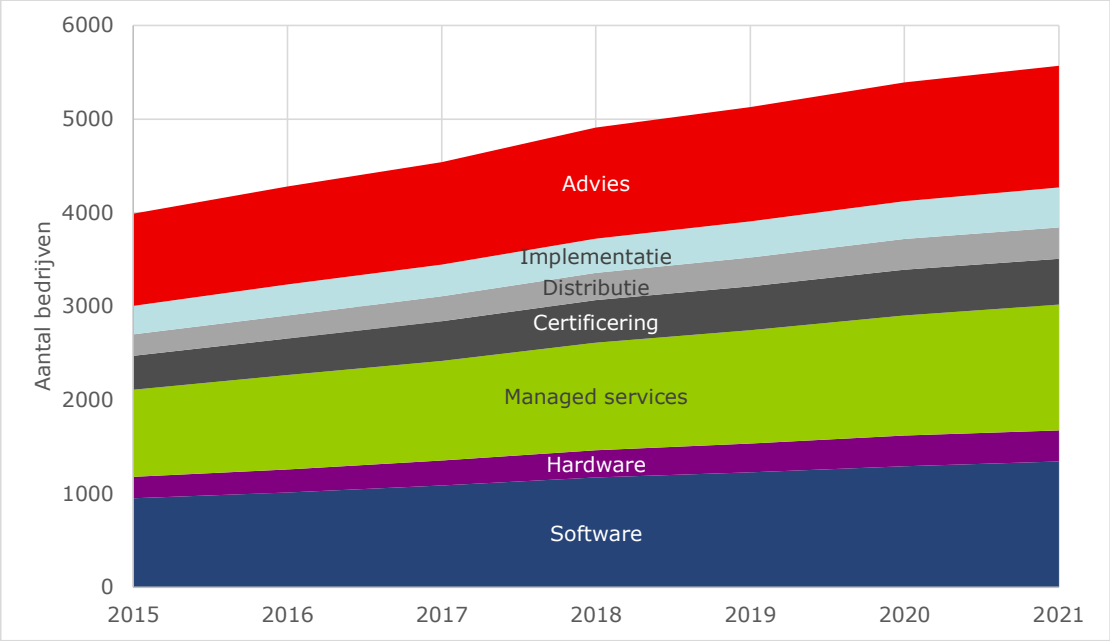
[57] Opvallend is dat certificering niet wordt genoemd door respondenten. Een mogelijke verklaring is dat respondenten hier uit één van de categorieën moesten kiezen. Het kan dus zijn dat men wel groei verwacht bij certificering, maar dat men niet verwacht dat hier de *meeste* groei plaats zal vinden.



Figuur 7. Sectoren waar de meeste groei wordt verwacht door respondenten

CBS microdata

Ook op basis van de CBS microdata kunnen we een uitsplitsing maken over de ENISA-categorieën. Ook hier komen de diensten sterk naar voren. Advies, implementatie, distributie en certificering zijn een substantieel deel van de sector, zoals uit Figuur 8 duidelijk naar voren komt. Opvallend is dat de bedrijfsverdeling vanuit de microdata een groter aandeel software bedrijven bevat ten opzichte van de bedrijven die de enquête hebben ingevuld. Dit kan erop duiden dat software bedrijven zijn ondervertegenwoordigd in de enquête.



Figuur 8. Ontwikkeling van het aantal cybersecurityproducenten uitgesplitst naar zeven categorieën

Interviews

In verschillende interviews komt naar voren dat de Nederlandse sector vooral gericht is op diensten voor de nationale markt. In Nederland zijn we vooral in staat om allerlei managed services, hardware en software die door buitenlandse partijen worden geleverd in te zetten

om Nederland veilig te houden. Het is een positief teken dat de Nederlandse cybersecurity-sector hiertoe in staat is, want dit betekent dat er absorptievermogen is om buitenlandse producten in te zetten waardoor de nieuwste ontwikkelingen kunnen worden toegepast. In de interviews werd vooral geredeneerd vanuit de zwakte van deze smalle scope, zie §3.2.2, §3.2.3 en §3.2.4. Er werd in de interviews aangegeven dat bij bedrijven de focus ligt op het veilig houden van de huidige situatie.

3.1.3 Sterke kennisbasis in cryptografie

Nederland heeft een sterke kennisbasis in onderzoek naar cryptografie. In de literatuur en de interviews komt dit duidelijk naar voren. Cryptografie is vrij fundamenteel van aard en op zichzelf geen cybersecurity, het is wiskunde. Cryptografie is de essentie van cybersecurity. Door de continuïteit van ontwikkelingen in ICT voorzieningen en cybercriminaliteit is continue verbetering van cryptografie noodzakelijk. Hierbij is het ook van belang naar de toekomst te kijken. Huidige cryptografie, waarvan het ontsleutelen op dit moment bijvoorbeeld 2 jaar duurt, kan met de komst van kwantumcomputers in slechts uren worden ontsleuteld. Een nieuwe vorm van encryptie gebaseerd op kwantum principes, en daarmee resistent tegen kwantumcomputers, is in ontwikkeling.

Literatuur

Encryptie biedt mogelijkheden als hulpmiddel, om integriteit en vertrouwelijkheid te kunnen bereiken, maar kan ook in negatieve zin worden ingezet (bijvoorbeeld doordat ransomwaresoftware bestanden zijn versleuteld). Nederland kent een lange traditie van onderzoek naar cryptografie.[58] Na de Tweede Wereldoorlog werden deze activiteiten door de PTT uitgevoerd. In het Dr Neher Lab werden versleutelingsapparaten ontwikkeld.[59] In 1957 werd deze tak voor Philips-USFA overgenomen.[60] In 1990 werden deze activiteiten doorgezet onder de naam Philips-Crypto. In 2003 werden deze activiteiten deels overgenomen door Compumatica en FOX-IT.[61] In deze periode werd een groot aantal apparaten ontwikkeld.[62] Nederland is nog steeds een van de weinige landen waar cryptografische producten en diensten worden ontwikkeld en vervaardigd, omdat deze zeldzame kennis en expertise in Nederland beschikbaar is.[63] Er is sprake van een sterke wetenschappelijke leiderschapspositie met veel internationaal erkende vooraanstaande wetenschappers.[64] Vanuit de overheid wordt de ontwikkeling binnen het cryptografische domein voortgezet door implementatie van de Nationale Crypto Strategie. De ontwikkelingen op dit gebied gaan snel en door de steeds verdergaande ontwikkeling van de kwantumcomputer wordt het noodzakelijk om ook op

---

[58] Oberman (2022) *Staatsgeheim, Beveiliging van overheidsberichten*.

[59] https://www.cryptomuseum.com/crypto/ptt/

[60] https://nl.wikipedia.org/wiki/Philips-USFA

[61] https://nl.wikipedia.org/wiki/Philips-Crypto

[62] Voor een goede overzicht zie: https://www.cryptomuseum.com/crypto/philips/index.htm

[63] NCTV (2022). Nederlandse Cybersecuritystrategie 2022-2028 Ambities en acties voor een digitaal veilige samenleving. https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2022/oktober/11/ncsc-onderzoeksagenda-2023---2026/Onderzoeksagenda+2023+-+2026+NCSC_NL_comp..pdf

[64] https://www.pnoconsultants.com/nl/wp-content/uploads/sites/2/2021/08/Nederland-Crypto-land_verkenning_202105.pdf

korte termijn nieuwe vormen van encryptie in te zetten. Dit is tevens een onderwerp in de NCSC Onderzoeksagenda 2023-2026.[65]

Interviews

Ook in verschillende interviews is aangegeven dat Nederland een goede positie heeft in dit domein. Er wordt onder meer aangegeven dat we internationaal gerespecteerd worden als een land dat veel kennis heeft over cybersecurityresearch en cybersecurity technologie. Nederland heeft nog steeds de naam een cryptografie expert te zijn. Het veilig houden van communicatie en encryptie is een punt waarop Nederland een historie heeft. Nederland beschikt over een aantal top-hoogleraren op dit gebied. Toch worden er ook kanttekeningen geplaatst door respondenten. Academische posities in dit domein blijken lastig in te vullen. Verder wordt aangegeven dat er een groot verschil is tussen het academisch onderzoek en de realiteiten waarin bedrijven opereren. Bedrijven zijn heel sterk gericht op het oplossen van hele concrete problemen die vandaag spelen, terwijl de academische sector op een langere termijn focust. Financiering van wetenschappelijk onderzoek door bedrijven is daardoor lastig.

3.1.4 Hoogwaardige integrators kunnen cybersecurity gebruiken om competitief voordeel te realiseren

Nederlandse bedrijven leveren hoogwaardige tech producten met een cybersecurity aspect. Voorbeelden hiervan zijn bank- en verzekeringsdiensten. Nederland is daarmee goed in het integreren van cybersecurity en heeft een beperkte focus op de technische kant van cybersecurity.

Literatuur

Nederland heeft een hoogwaardige economische structuur waarin de integratie van cybersecurity een competitief voordeel kan zijn. Nederland verdient het meest aan de export van machines en machineonderdelen als het gaat om toegevoegde waarde.[66] Dit zijn typisch sectoren waarbij de integratie van cybersecurity een belangrijk concurrentievoordeel kan bieden. Ook de toegevoegde waarde van "vervoer en opslag", met andere woorden de logistieke sector, is relatief groot in Nederland. Ook dit is een sector die de afgelopen jaren zeer sterk gedigitaliseerd is.[67] En ook hierbij speelt cybersecurity een relatief grote rol. Niet voor niets worden logistieke bedrijven relatief vaak aangevallen.[68] Als we kijken naar de grootste bedrijven van Nederland, dan zijn er relatief veel bedrijven waarvoor de integratie van

---

[65] NCSC Onderzoeksagenda 2023-2026 (oktober 2022). Doing Cybersecurity Research Together! https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2022/oktober/11/ncsc-onderzoeksagenda-2023---2026/Onderzoeksagenda+2023+-+2026+NCSC_NL_comp..pdf

[66] https://www.cbs.nl/nl-nl/nieuws/2019/45/hoogste-exportverdiensten-dankzij-machines

https://longreads.cbs.nl/nederland-handelsland-2022/nederlandse-verdiensten-aan-internationale-handel/

[67] Een deel van de digitalisering zit in het proces (en valt hiermee buiten de scope van het punt dat we willen maken), maar een flink deel ook in de dienst (en valt hiermee binnen de scope). Waar het exacte onderscheid ligt, is soms lastig te maken maar op het moment dat klanten er direct effect van ondervinden dan zouden wij het tot de dienst willen rekenen.

[68] https://www.tln.nl/nieuws/cybercriminaliteit-ook-dreiging-voor-transport-en-logistiek/ en https://www.ing.nl/zakelijk/sector/transport-logistics-mobility/sector-thema-update-transport-logistics-mobility-cybersecurity

cybersecurity in hun product of dienst belangrijk is. Denk bijvoorbeeld aan ASML, ING, Rabobank, NN, NXP en Adyen.

Enquête

Uit de enquête komt naar voren dat meer dan de helft van de respondenten cybersecurity integreert in hun diensten of producten. In Bijlage 3 bij Figuur 15 zijn nadere details te vinden.

De bedrijven die betrokken zijn bij integratie is gevraagd waarom zij dit doen, zie Bijlage 3, Figuur 26. Ruim 60% van de respondenten geeft aan dat het draait om het voldoen aan wet- en regelgeving en circa een derde geeft aan dat het gaat om het realiseren van een competitief voordeel. Relatief veel respondenten geven andere opties aan. We hebben deze uitkomsten geanalyseerd en geclusterd. Twee soorten antwoorden kwamen sterk naar voren. In een eerste cluster wordt aangegeven dat het inherent aan het product of dienst is. Met andere woorden: het product of dienst kan niet geleverd worden zonder een voldoende mate van cyberveiligheid. Een tweede cluster antwoorden draait om morele afwegingen: "omdat het ethisch de juiste optie is".

Aan de bedrijven die actief zijn met integratie is tevens gevraagd in welke mate hen dit een competitief voordeel oplevert, zie Bijlage 3, Figuur 27. Bijna 50% is van mening dat hen dit in (zeer) sterke mate een voordeel oplevert, terwijl dit voor bijna 25% van de bedrijven in (zeer) beperkte mate het geval is.

Interviews

Ook in enkele interviews is dit onderwerp aan bod gekomen. Er wordt erkend dat de integratie van cybersecurity in producten of diensten voor Nederland kansen kan opleveren voor de export. In de interviews komen verschillende punten naar voren:

- Er wordt **duidelijk onderscheid** gemaakt tussen producten en diensten waarvoor dit wel en niet relevant is. Voor verschillende producten die bijvoorbeeld Philips Medical Systems maakt zal dit een erg relevant onderwerp zijn, maar voor de productie van paprika's zal dit veel minder spelen. Het zou uiteraard wel kunnen dat voor het laatste cybersecurity steeds relevanter wordt in het productieproces, denk aan bescherming tegen ransomwareaanvallen die de onderneming kunnen verlammen, maar het zit niet in het product of de dienst zelf. Het hangt verder sterk af van het type product of dienst in hoeverre cybersecurity toegevoegde waarde heeft en de hogere prijs gerechtvaardigd is.
- Verschillende respondenten brengen het onderwerp *security by design* ter sprake. Met andere woorden: producten worden zo ontworpen dat de cyberveiligheid (tot een relatief hoog niveau) gewaarborgd is. Door een toenemende vraag van afnemers naar veilige producten, biedt het ontwikkelen van producten met *security by design* een competitief voordeel.

3.2 Zwaktes van de Nederlandse Cybersecuritysector

3.2.1 Weinig private cyber R&D

In Nederland wordt relatief weinig R&D op het gebied van cybersecurity uitgevoerd door bedrijven. De mate waarin private cybersecurity R&D in Nederland wordt uitgevoerd is nihil. Enkele (over het algemeen grote) bedrijven die cybersecurity R&D uitvoeren zijn tevens integrators, denk hierbij bijvoorbeeld aan ASML. Doordat wij in Nederland een gebrek hebben aan grote cybersecurity bedrijven zijn de mogelijkheden voor private R&D beperkt, de Nederlandse sector is grotendeels gefocust op het aanbieden van diensten.

Interviews

In de interviews is aangegeven dat de cybersecuritysector in het algemeen erg R&D intensief is en dat dit steeds meer ingebed raakt bij IT-bedrijven (echter vindt er in Nederland weinig private R&D plaats op het gebied van cybersecurity). Vooral bij de hoge TRL-niveaus is er sprake van een constante strijd tussen aanvallers en verdedigers en tussen cybersecurity-bedrijven onderling. Cybercriminelen kunnen relatief snel innoveren ten opzichte van bedrijven in de cybersecuritysector. Ze hebben geen last van regelgeving zoals de AGV; ze professionaliseren steeds meer en krijgen soms steun van statelijke actoren. In de gesprekken is ook aangegeven dat integrators soms moeite hebben om de R&D te "absorberen". Deze verwerken de cybersecurity kennis niet voldoende in hun hoogwaardige producten en diensten.

Literatuur

De uitgaven van Nederlandse bedrijven aan R&D zijn traditioneel laag.[69] We liggen weliswaar op het gemiddelde van de EU, met circa 1,4% van het BBP in 2019, maar in deze groep zitten ook allerlei landen met een minder ontwikkelde economie. Landen met een hoogontwikkelde economie scoren veel hoger op deze indicator. Voorbeelden zijn: Zuid-Korea 3,5%, Zweden 2,4%, Oostenrijk 2,2%, Duitsland 2,2%, USA 2,0%, België 1,9%[70].[71] Aan de andere kant moet wel gezegd worden dat de grote achterstanden die Nederland had wat zijn ingelopen. Het is uiteraard niet duidelijk in welke mate dit te generaliseren is voor uitgaven aan R&D voor cybersecurity, maar het is in ieder geval geen goed voorteken.

In de literatuur wordt vooral verwezen naar de private R&D op het gebied van cybersecurity en bedrijven in het kader van samenwerkingen. In de Nederlandse Cybersecurity Strategie (hierna: NLCS), die in 2022 is gepubliceerd, presenteert het kabinet haar plannen om de cybersecuritysector te versterken.[72] Hierin wordt aangegeven dat er wordt gestreefd naar een sterke cybersecuritykennis en -innovatieketen. "*Verschillende onderdelen van de keten - zoals fundamenteel en toegepast onderzoek, het bedrijfsleven en overheden – moeten elkaar beter gaan vinden en samenwerken aan concrete meerjarige projecten*."

CBS-microdata

Als wij kijken naar de uitgaven van cybersecuritybedrijven aan R&D dan zien we dat dit rond de 3,5% à 4% schommelt in de afgelopen jaren. Verder valt op dat hoe groter het bedrijf is, des te hoger de relatieve uitgaven aan R&D zijn. Als we kijken naar andere sectoren, dan valt op dat de R&D intensiteit van deze sector beperkt is. De R&D-intensiteit van bedrijven die hardware (ICT-producten) produceren in de EU en de VS ligt op bijna 10%.[73] Kijken we naar R&D-intensiteit van leveranciers van ICT-diensten dan ligt dit op bijna 5% in de EU en op 13% in de VS. Als we naar de onderstaande cijfers kijken, dan wordt het duidelijk dat de Nederlandse sector aanzienlijk lager scoort. Hier kunnen twee verklaringen voor zijn: de eerste is dat we in Nederland een sector hebben die getypeerd wordt door veel kleine bedrijven. Een tweede aspect is dat de eerder genoemde bron kijkt naar bedrijven die ICT-

---

[69] https://www.dialogic.nl/wp-content/uploads/2021/04/Dialogic-Ontwikkeling-RD-investeringen-in-Nederland-Final-21-april-2021.pdf

[70] Alle data betreft 2019

[71] https://www.dialogic.nl/wp-content/uploads/2021/04/Dialogic-Ontwikkeling-RD-investeringen-in-Nederland-Final-21-april-2021.pdf

[72] https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2022/oktober/10/nlcs-2022/NLCS_2022_19.pdf

[73] https://op.europa.eu/en/publication-detail/-/publication/fb50fc5e-570e-11ec-91ac-01aa75ed71a1/language-en

producten produceren of ICT-diensten leveren. Dit is een bredere scope dan cybersecurity en een sector waarin waarschijnlijk ook inherent meer R&D wordt gedaan.

Tabel 3. R&D-uitgaven als percentage van de totale omzet per grootteklasse

Grootteklasse	2015	2016	2017	2018	2019	2020
10 - 49	0,1%	0,2%	0,2%	0,2%	0,3%	0,2%
50 - 149	0,8%	0,9%	1,0%	0,8%	0,5%	0,3%
150 - 249	0,5%	0,2%	0,3%	0,3%	0,7%	0,8%
250 - 999	1,1%	1,1%	0,9%	1,2%	1,1%	1,6%
1000 of meer	11,0%	8,9%	10,0%	8,7%	10,4%	8,5%
Hele sector	3,8%	3,5%	4,3%	3,7%	4,3%	3,5%

Enquête

Ook in de enquête is uitgevraagd welk deel van de omzet besteed wordt aan R&D, zie Bijlage 3, Figuur 19. Doordat we dit uitvragen in intervallen, is het niet mogelijk om een gemiddelde te berekenen. Wat wel duidelijk opvalt, en in lijn is met de gegevens uit de microdata, is dat ongeveer een derde van de bedrijven minder dan 10% van hun omzet besteden aan R&D. Toch besteedt bijna de helft van de bedrijven meer dan 10% van hun omzet aan R&D activiteiten.

Aan de respondenten is verder gevraagd in hoe de uitgaven aan R&D zich ontwikkeld hebben over de tijd, zie Bijlage 3, Figuur 20. Hieruit komt duidelijk naar voren dat dit door de bank genomen toegenomen is over de tijd. Bijna de helft van de bedrijven geeft aan een toename te zien. Dit lijkt niet in lijn te zijn met de data van het CBS, waarin een relatief vlak patroon wordt weergegeven.[74]

Verder is in de enquête gevraagd naar het TRL-niveau waarop bedrijven hun R&D richten, zie Bijlage 3, Figuur 21. TRL staat voor Technology Readiness Level en geeft de mate van ontwikkeling van een technologie aan (TRL 1 staat aan het begin van de ontwikkeling en TRL 9 is technologie die technisch en commercieel gereed is).[75] Hierbij is TRL 1, 2 en 3 *verkennen*, met hierin fundamenteel onderzoek, toegepast onderzoek en toetsing. TRL 4, 5 en 6 draait om *ontwikkelen* waarin prototypes centraal staan. TRL 7 en 8 draaien om *demonstraties*. Het is duidelijk dat respondenten vooral aangeven gericht te zijn op demonstraties, aangezien meer dan de helft zich richt op TRL 7 en 8.

3.2.2 Output die beperkt exporteerbaar is

De activiteiten die de Nederlandse cybersecuritysector ontplooit zijn grotendeels niet goed te exporteren. We zijn een netto-importeur van cybersecurityproducten: Software, hardware en managed diensten worden vooral geïmporteerd. Deze zwakte is het spiegelbeeld van de sterkte dat Nederland goed in staat is om haar eigen dienstenmarkt te bedienen. Zoals eerder genoemd zijn Nederlandse cybersecurity bedrijven voornamelijk gefocust op het aanbieden van diensten. De vraag naar diensten is momenteel omvangrijk genoeg dat het exporteren van diensten geen noodzaak behoeft.

[74] Merk op dat de data van CBS gaat over R&D uitgaven en deze data over bedrijven die aan R&D doen. Dat betekent dat beide statements waar kunnen zijn, indien enkele bedrijven die veel aan R&D uitgeven minder zijn gaan uitgaven en veel kleine bedrijven meer zijn gaan uitgeven aan R&D.

[75] https://www.rvo.nl/onderwerpen/trl

CBS-microdata

Op basis van de CBS-microdata kunnen we een uitsplitsing maken over het aantal bedrijven actief in de ENISA-categorieën, zie Tabel 11 in Bijlage 4. Hieruit komt naar voren dat de categorieën die slecht te exporteren zijn (diensten als advies, certificering, distributie en implementatie) samen ruim 2.500 bedrijven kennen. Hardware (560 bedrijven), managed services (ruim 1300) en software (ruim 1300) kennen in deze telling toch ook een substantiële component.

Interviews

In verschillende interviews is een beeld geschetst dat wij herkennen van andere interviews die we uitvoerden voor onderzoeken over de Nederlandse IT-sector. Het is op de Nederlandse markt relatief aantrekkelijk om diensten aan te bieden en relatief onaantrekkelijk om schaalbare producten aan te bieden. Een expert op het gebied van cybersecurity kan zichzelf als ZZP'er relatief eenvoudig tegen een hoog tarief laten inhuren. Voor een cybersecuritybedrijf is het ook eenvoudig om diensten aan te bieden. Als een bedrijf of persoon een schaalbaar product wil ontwikkelen, dan is het beeld dat dit minder aantrekkelijk is vanwege drie redenen:

- Er is een **grote voorinvestering** voor nodig. Voordat het schaalbaar product gereed is moet er geruime tijd geïnvesteerd worden. In deze periode zullen er geen inkomsten zijn en de vraag is hoe deze periode overbrugd moet worden.
- Er is sprake van een **hoog risico**. De kans dat het lukt om een dergelijk schaalbaar product succesvol op de markt te brengen is gering. Er is sprake van zware concurrentie van andere oplossingen van grote leveranciers.
- Er zullen relatief **beperkte opbrengsten** zijn. Nederland kent een relatief kleine markt waardoor opschaling lastig is. Verder zijn de belastingen relatief hoog (op zijn minst ten opzichte van de VS) waardoor veel van de mogelijke inkomsten bij verkoop verloren gaan. Verder waren aandelenopties voor medewerkers voor 1 januari 2023 fiscaal onaantrekkelijk.

Het bovenstaande leidt er toe dat we in Nederland een marktstructuur hebben die sterk draait op diensten en beperkt op schaalbare producten (software, hardware en managed services). Het potentieel voor export van deze diensten is, zoals eerder genoemd (en benoemd in het eerdere onderzoek van SEO en VKA), beperkt. Het nadeel van deze structuur is dat voor bedrijven de marges relatief klein zijn. Het is weliswaar eenvoudig om diensten aan te bieden, maar de werknemers vragen hoge salarissen. De beste medewerkers hebben tevens de optie om als ZZP'er verder te gaan, waardoor zij een sterke positie hebben ten opzichte van werkgevers. Een gevolg van het voorstaande is ook dat de marktstructuur in Nederland gekenmerkt wordt door veel kleine bedrijven. Wat is het voordeel om veel schaal te hebben als je toch geen schaalbaar product aanbiedt?

Het Nationaal Bureau voor Verbindingsbeveiliging (NBV) evalueert beveiligingsproducten, zoals computersystemen, -netwerken en telecommunicatieapparatuur, die gebruikt kunnen worden voor (staatsgeheime) informatie van de overheid, vitale sectoren en de Nederlandse economie. Op haar website publiceert zij een overzicht van producten die goedgekeurd zijn.[76] Hier zijn verschillende voorbeelden te vinden van (van origine) Nederlandse producten van dit soort schaalbare producten. Initieel lijkt dit een interessante kans voor export van

[76] https://www.aivd.nl/onderwerpen/informatiebeveiliging/evalueren-van-veiligheidsproducten/geevalueerde-producten

producten. Het probleem is echter dat er sprake is van markt waarin wantrouwen een grote rol speelt.[77] Dat dit niet onterecht is blijkt uit de *cryptoleaks* van 2020 waarin duidelijk werd dat de Zwitserse marktleider van versleutelingsapparatuur achter de schermen decennialang (!) in handen bleek te zijn van de CIA en de Duitse inlichtingendienst BND.[78] In deze periode konden zij dus meeluisteren met vijanden en bondgenoten. Ook bij apparatuur van Philips zijn in sommige gevallen algoritmes bewust verzwakt.[79] Ondertussen luisterde NSA Angela Merkel tien jaar lang af[80] en hielpen de Duitsers tegelijkertijd de NSA om het Franse presidentieel paleis, het Élysée en de Europese Commissie af te luisteren.[81]

Er is dus niet voor niets sprake van nationale markten met extreem hoge entry barriers voor buitenlandse partijen. Nederland wil graag apparatuur kopen van Nederlandse leveranciers en buitenlandse partijen willen graag apparatuur kopen van hun nationale leveranciers. Hierdoor zijn entry barriers op deze markten heel hoog en is de exporteerbaarheid gering. Daarnaast speelt de vraag in welke mate er strategische afwegingen gemaakt moeten worden bij export. Willen we deze apparatuur verkopen aan landen waar anders tegen mensenrechten wordt aangekeken? Zorgt de export van deze apparatuur ervoor dat onze communicatie minder veilig wordt omdat duidelijk wordt hoe deze apparatuur exact werkt?

3.2.3 Grote afhankelijkheid van buitenlandse leveranciers van services, soft- en hardware

We zagen bij de sterktes al dat de Nederlandse cybersecuritysector goed in staat is om de eigen markt te bedienen. Om dit te kunnen doen zijn we echter wel sterk afhankelijk van buitenlandse leveranciers van services, soft- en hardware. Er worden wel services, soft- en hardware in Nederland ontwikkeld, maar dit is niet voldoende voor de nationale vraag. Wel worden er met de Europese wetgeving (CSA, CRA) eisen gesteld aan (buitenlandse) ICT-producten, -diensten en -processen middels certificeringen.

Literatuur

In het Cybersecuritybeeld Nederland 2022 en in het Cybersecuritybeeld Nederland 2020 wordt aangegeven dat Nederland op het gebied van productontwikkeling achterloopt, waardoor er afhankelijkheid van het buitenland ontstaat.[82] Daar komt bij dat enkele grote buitenlandse partijen het grootste deel van de markt in handen hebben. Denk hierbij aan leveranciers van besturingssystemen zoals Microsoft en Apple. Het kiezen voor een marktleider heeft ook voor afnemers veel voordelen (o.m. vereenvoudigde data-uitwisseling met

[77] Oberman (2022) *Staatsgeheim, Beveiliging van overheidsberichten*.

[78] https://tweakers.net/nieuws/163328/cia-en-bnd-waren-eigenaar-van-zwitserse-marktleider-cryptosystemen.html

[79] https://www.vpro.nl/argos/lees/onderwerpen/cryptoleaks/2020/cryptoleaks-in-the-netherlands-former-philips-top-cryptographer-admits-to-compromising-encryption-devices.html

[80] https://www.theguardian.com/world/2013/oct/26/nsa-surveillance-brazil-germany-un-resolution

[81] https://nos.nl/artikel/2033240-duitsers-hielpen-nsa-met-afluisteren-elysee

[82] NCTV, (2022). Cybersecuritybeeld Nederland. *CSBN2022;* NCTV, (2020). Cybersecuritybeeld Nederland. *CSBN2020*

andere organisaties). Toetredingsdrempels voor nieuwe bedrijven zijn, mede daarom, hoog.[83]

Daarnaast hebben we te maken met een **enorme toeleverancierskete**n. Digitale diensten, hardware, software en netwerken kunnen allemaal van andere leveranciers komen. Zo maken ook verschillende digitale dienstverleners gebruik van dezelfde ontwikkel- en monitoringstools en bestaat hardware uit verschillende componenten die door andere leveranciers worden gemaakt. Daardoor raken kwetsbaarheden in veelgebruikte diensten en een groot aantal organisaties over de hele wereld. Die **verwevenheid** maakt kwetsbaar (denk aan Apache Log4-j).[84]

Door het hybride en in de cloud werken, en door de beperkingen van *human capital*, is er meer en meer behoefte aan multifunctionele geïntegreerde producten en diensten die 'alles' beveiligen.[85] Daar speelt de cybersecuritymarkt goed op in. Steeds vaker worden 'oplossingen' verkocht, waarin beveiligingsfuncties in bredere beveiligingssystemen geconsolideerd worden. Dit zou moeten leiden tot een betere algemene veiligheid, maar brengt ook uitdagingen voor de markt met zich mee. Doordat er een hoge mate van integratie kunnen grotere partijen een sterkere positie op de markt innemen. Ook kan het leiden tot "single points of failure" waardoor er weer een hogere mate van kwetsbaarheid ontstaat.

Interviews

Ook in de interviews is dit aspect vaak aan bod gekomen. In verschillende gesprekken is benadrukt dat een heel groot deel van de cybersecurity-oplossingen komen van Microsoft, Apple en Google die simpelweg een heel groot deel van de besturingssystemen leveren. Dit geldt voor smartphones, tablets, laptops en in mindere mate ook voor servers. Een heel groot gedeelte van de markt bestaat dus uit deze drie partijen die simpelweg updates *pushen* naar hun klanten. Zoals een respondent aangaf: "*De updates op je Windows computer zijn misschien wel de grootste factor in cyberveiligheid*".

In interviews wordt aangegeven dat deze afhankelijkheid voor integrators een nieuw risico kan betekenen. De software moet in sommige gevallen gemaakt worden voor het Windows platform en de integrator moet geloven dat dit veilig is (en blijft) en heeft er verder geen invloed op. In het verlengde hiervan wordt ook aangegeven dat er een risico ontstaat doordat buitenlandse partijen via hun producten inzage krijgen in de werking van Nederlandse IT-systemen. Een partij die een geautomatiseerde pen-test uitvoert weet bijvoorbeeld exact waar de kwetsbaarheden liggen. Hoe weten we zeker dat dit niet gebruikt wordt voor spionage van bedrijfsgevoelige gegevens?

Verschillende geïnterviewden hebben aangegeven dat deze kwetsbaarheid ook een kans kan betekenen voor de Nederlandse cybersecuritysector. Er is in sommige gevallen simpelweg behoefte aan een Nederlandse leverancier. Het is alleen de vraag in welke markten dat ook realistisch is. We zullen in Nederland nooit een nieuw grootschalig besturingssysteem ontwikkelen als concurrent voor Windows of MacOS.

---

[83] NCTV (2022). Cybersecuritybeeld Nederland 2022. https://www.nctv.nl/onderwerpen/cybersecuritybeeld-nederland/documenten/publicaties/2022/07/04/cybersecuritybeeld-nederland-2022

[84] NCTV (2022). Cybersecuritybeeld Nederland 2022. https://www.nctv.nl/onderwerpen/cybersecuritybeeld-nederland/documenten/publicaties/2022/07/04/cybersecuritybeeld-nederland-2022

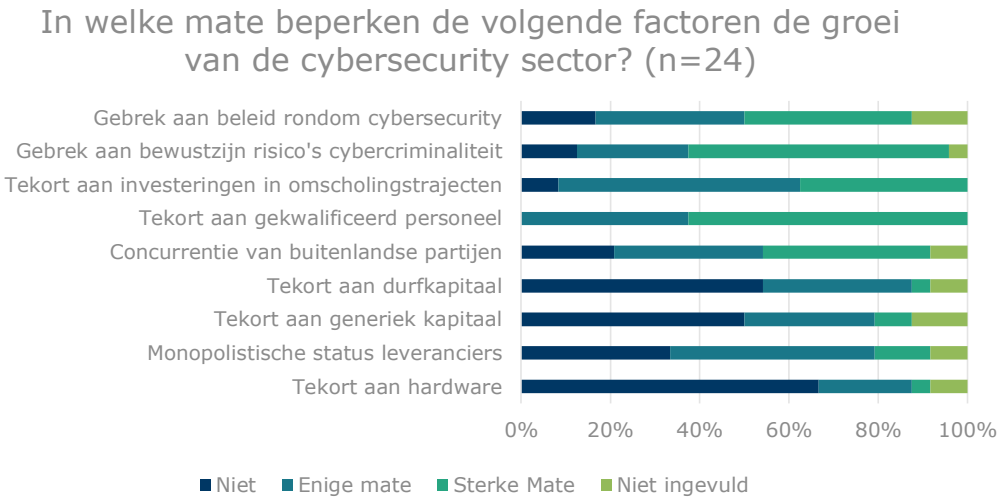
[85] Gartner Report (2022). Top Trends in Cybersecurity 2022. https://www.gartner.com/en/doc/760806-top-trends-in-cybersecurity

Eén geïnterviewde kwam met een verrassend perspectief op datacenters. Op dit moment ligt deze sector redelijk onder vuur, onder meer door de mogelijke komst van hyperscalers[86]. Het kan echter ook een additioneel risico betekenen als wij in Nederland sterk afhankelijk worden van buitenlandse datacenters. Dit argument is wellicht niet zo sterk voor hyperscalers, maar voor multi-tenant datacenters (grote datacenters waar meerdere partijen hun apparatuur plaatsen) geldt dit mogelijk wel. Immers, indien ook deze datacenters niet meer in Nederlandse handen zijn, staat Nederlandse data ook fysiek bij andere partijen.

In de interviews kwam verschillende keren naar voren dat er sprake is van een hoge mate van *vendor lock in* als gevolg van *switching costs*. Met andere woorden een afnemer is heel sterk gebonden aan zijn aanbieder, omdat overstappen hele hoge kosten kent. Doordat aanbieders dit weten, schuiven zij op in de waardeketen en gaan zij ook andere diensten aanbieden. Concurrentie wordt beperkt doordat diensten van andere leveranciers niet goed samenwerken met de systemen van de dominante aanbieder. Eén geïnterviewde verwijst naar een studie van ACM naar clouddiensten waarin dit onderwerp inderdaad wordt uitgewerkt.[87]

Enquête

In de enquête is gevraagd naar factoren die de groei van de cybersecuritysector beperken. Respondenten zijn onder andere gevraagd om aan te geven in welke mate concurrentie van buitenlandse partijen de groei beperkt, zie Figuur 12. Bijna 80% van de respondenten vond concurrentie van buitenlandse partijen in enige, of in sterke mate een beperking van de groei. Er is dus niet alleen sprake van afhankelijkheid van buitenlandse partijen, er is dus ook in enige mate verdringing door deze partijen.



Figuur 9 Antwoorden op enquêtevraag: In welke mate beperken de volgende factoren de groei van de cybersecuritysector?

[86] Hyperscalers zijn extreem grote datacenters die door de grote tech bedrijven overal ter wereld worden neergezet om hun diensten mondiaal te kunnen aanbieden. Voorbeelden zijn het datacenter van Microsoft in Middenmeer en die van Alphabet (Google) in Eemshaven. Het voorgenomen datacenter van Meta (Facebook) in Zeewolde gaat definitief niet door.

[87] https://www.acm.nl/system/files/documents/marktstudie-clouddiensten.pdf

3.2.4 Sector bestaat overwegend uit MKB en veel ZZP'ers

Als wij kijken naar de structuur van de Nederlandse markt, dan bestaat de sector vooral uit MKB en ZZP'ers (hoewel er enkele grotere spelers zijn). Uiteraard kent deze zwakte ook een relatie met de sterkte *focus op diensten* (die weinig schaalvoordelen kennen) en de geringe *export* (waardoor groei beperkt is). De dienstenmarkt bestaat typisch uit voornamelijk kleine bedrijven.

CBS Microdata

Als we kijken naar de data van CBS in Tabel 4 dan wordt duidelijk dat kleine partijen het overgrote deel van de sector uitmaken. In 2021 zijn er ruim 4000 bedrijven in onze sample; hiervan hebben slechts 136 bedrijven 250 of meer medewerkers. De andere bijna 4000 bedrijven zijn dus allemaal MKB. De data geven echter een vertekend beeld, want de grote bedrijven die in deze sample zitten zijn grote bedrijven die *ook* actief zijn op het gebied van cybersecurity. Een blik op de ledenlijst van de brancheverenigingen Cyberveilig Nederland geeft een aardig beeld. Een aantal leden van deze brancheverenigingen zijn zeer grote bedrijven die binnen de sector vallen, maar ook (en vaak zelfs *vooral*) veel activiteiten buiten de sector ontplooien. Nederlandse bedrijven met meer dan 250 medewerkers die zich uitsluitend op cybersecurity richten zijn wij niet of nauwelijks tegengekomen in ons onderzoek. [88]

Tabel 4. Aantal cybersecuritybedrijven per grootteklasse

Grootteklasse	2015	2016	2017	2018	2019	2020	2021
0	405	471	509	585	582	624	630
1	907	972	1036	1128	1219	1242	1310
2	236	221	236	236	252	298	290
3-4	214	225	224	237	244	257	274
5-9	297	328	327	330	360	371	386
10-19	311	305	338	344	321	328	327
20-49	262	289	303	332	348	374	393
50-99	144	141	148	162	176	175	175
100-149	53	60	66	78	81	69	73
150-199	32	37	34	37	34	50	49
200-249	15	18	25	23	26	29	31
250-499	40	47	45	47	55	64	68
500-999	27	25	26	29	32	30	26
1000 of meer	32	37	40	36	38	37	42
Eindtotaal	2975	3176	3357	3604	3768	3948	4074

Interviews

In de interviews is verschillende keren aangegeven dat de Nederlandse sector vooral uit mkb en ZZP'ers bestaat. Dit wordt gezien als een zwakte omdat het de slagkracht van de Nederlandse sector beperkt. Verder wordt ook benoemd dat het dunne lijntje tussen IT en cybersecurity het meten van de sector lastig maakt. Er zijn veel grote IT-bedrijven die ook

[88] Wellicht zou FOX-IT als voorbeeld genoemd kunnen worden. Echter is dit bedrijf in handen van een Brits bedrijf.

actief zijn op deze markt. Dat is logisch want cybersecurity is een onderdeel van IT. Het maakt het echter lastig om de sector goed af te bakenen en te meten.

4 Kansen en bedreigingen voor de Nederlandse cybersecuritysector

De Nederlandse cybersecuritysector kent veel kansen, waaronder het feit dat Nederland goed is in de integratie van alfa-, bèta- en gammawetenschappen. Met een groeiende cybersecuritysector wordt een interdisciplinaire insteek steeds belangrijker. Daarnaast biedt de opkomst van AI groeiende mogelijkheden om mensenwerk via AI uit te voeren. De kansen die AI biedt zijn de afgelopen jaren sterk toegenomen. Ook heeft Nederland een sterke kennisbasis in kwantumtechnologie. Dit kan worden ingezet voor nieuwe vorm van encryptie. Op Europees niveau biedt de invoering van de NIS en de CRA kansen doordat het nieuwe eisen stelt aan de marktpartijen waarop de sector kan anticiperen. Tenslotte is Nederland een aantrekkelijke vestigingsplaats voor NGO's en IO's. Toekomstige, nog op te richten, organisaties die zich richten op vrede en veiligheid in het digitale domein kunnen zich wellicht in Den Haag vestigen.

Daarnaast kent de Nederlandse cybersecuritysector enkele bedreigingen. De (mogelijk) grootste dreiging komt door het flinke tekort aan personeel met een cybersecurityprofiel. Ook de beperkte awareness bij organisaties en consumenten over risico's waardoor er meer risico wordt gelopen dan nodig is. Een andere bedreiging is het feit dat bedrijven die schaal krijgen snel worden overgenomen door externe (buitenlandse) partijen. Hierdoor kan de sector in Nederland zich beperkt ontwikkelen. Ook het gebrek aan venture capital werkt mee aan een tekort aan scale-ups omdat de conversie van startup naar scale-up lastig is. Een andere bedreiging ligt bij de overheid, welke niet zwaar investeert. Er zijn andere landen waar de overheid, als gevolg van een externe dreiging, sterk investeert waardoor een de sector zich goed ontwikkeld. Tot slot wordt er momenteel geen eenduidige visie overheid op cybersecurity ervaren. Er is sprake van fragmentatie van beleid. Met de publicatie van de NLCS wordt hieraan gewerkt, dit is echter nog te recent om een effect hiervan te ervaren.

4.1 Kansen voor de Nederlandse cybersecuritysector

4.1.1 Goed in integratie alfa-, bèta- en gammawetenschappen

Met een groeiende cybersecuritysector, wordt een interdisciplinaire insteek steeds belangrijker. Nederland lijkt een goede positie te hebben als het gaat om deze interdisciplinaire insteek met de integratie van alfa-, bèta- en gammawetenschappen.

Interviews

In meerdere interviews is dit onderwerp aan bod gekomen. Vanuit partijen die actief zijn op de markt en experts wordt aangegeven dat er een switch gaande is van een puur technologische benadering, naar een veel breder perspectief. Er is onder meer sprake van een sociologische insteek waarbij gedragsveranderingen binnen organisaties centraal staan. Ook juridische aspecten worden steeds belangrijker. De markt wordt volwassener en er zijn binnen een aanbieder meer specialismen nodig. Het beeld dat cyber alleen maar technisch is, moet dus veranderen. Een steeds groter deel van de werknemers van deze bedrijven heeft helemaal geen achtergrond in de IT meer. Als er wordt gekeken naar R&D dan wordt

geconstateerd dat radicale vormen van innovatie[89], binnen de cybersecuritysector (zoals een nieuwe vorm van cryptografie) vaak niet eens uit cybersecurityonderzoek komen, maar bijvoorbeeld vanuit de AI of wiskunde hoek. Dit geeft het belang aan van een interdisciplinaire insteek. Bovendien wordt aangegeven dat vooral de medewerkers met een multidisciplinaire insteek waardevol zijn. Men wil medewerkers die wel cybersecurity tot op een zeker niveau begrijpen, maar ook kennis hebben van een ander domein, zoals juridisch, marketing, sales, privacy, certificering, et cetera. Dit soort bruggenbouwers zijn relatief schaars en er is veel vraag naar dit soort expertise. Wellicht verhogen dit soort interdisciplinaire rollen de interesse in cybersecurityopleidingen en -banen.

Literatuur

De VU en met name de UvA zijn ook in internationaal opzicht toonaangevende hubs van interdisciplinair onderzoek op het gebied van IT.[9091] De twee universiteiten werken nauw samen met CWI en de HvA (die veel programmeurs opleidt). UvA doet, als algemene universiteit, al 30 jaar wetenschappelijk toponderzoek naar AI – veel langer dus dan de technische universiteiten in Nederland. De sterkte van de interdisciplinaire insteek komt ook duidelijk naar voren in de zeer succesvolle Innovation Centers for AI (ICAI-labs), waarvan er vanuit de UvA inmiddels landelijk 30 zijn uitgerold.[92] AI labs koppelen een concrete maatschappelijke opgave altijd aan state-of-the-art AI-onderzoek. CWI heeft van oudsher (o.a.) een erkende sterkte in cryptografie.[93] Samen met de UvA en TU Delft wordt in QuTech ook onderzoek gedaan naar next generation cryptografie, dat wil zeggen *cryptography on quantum computing*.[94]

4.1.2 Groeiende mogelijkheden om via AI mensenwerk uit te voeren

Kunstmatige intelligentie (AI) ontwikkelt zich snel. De [1] toenemende kracht van ICT in termen van informatie-opslag, -verwerking en transmissie in combinatie met [2] een toenemende hoeveelheid beschikbare data biedt meer en meer mogelijkheden om AI effectief in te kunnen zetten. Daarbij worden ook de algoritmen en modellen verfijnd, waardoor de data en rekenkracht ingezet kunnen worden om steeds complexere taken uit te voeren. ChatGPT is hier een recent bekend voorbeeld van. In steeds meer gevallen is het mogelijk om AI bestaande taken uit te laten voeren of nieuwe taken op te laten pakken. Het gaat bij AI specifiek om 'informatietaken'; taken waarbij *informatie verwerkt* wordt en dus ook betreffende 'competenties' benodigd zijn [95]. Het zijn exact deze informatie-gerelateerde competenties waar AI over beschikt en jaarlijks in blijft groeien. Dit biedt dus ook kansen voor de cybersecuritysector. De taken waarbij de bijdrage van een informatieverwerkingscompetentie groot is, zijn naar verwachting goede kandidaten om met AI aan te pakken[96]. De exacte impact die het op de cybersecuritysector en haar werkzaamheden zal hebben is onbekend, maar het is aannemelijk dat dit naar de toekomst toe aanzienlijk kan zijn. Ter

---

[89] Radicale innovatie verwijst naar zeer vernieuwende innovaties, in tegenstelling tot incrementele innovaties.

[90] https://iis.uva.nl/?cb

[91] https://vu.nl/nl/onderwijs/professionals/cursussen-opleidingen/master-it-audit-compliance-advisory/overzicht

[92] https://icai.ai/about/

[93] https://www.cwi.nl/en/groups/cryptology/

[94] https://qutech.nl/lab/quantum-cryptography-lab/

[95] Zie bijvoorbeeld McKinsey Global Institute (2017). A future that works: Automation, employment, and productivity.

[96] Deze benadering is met succes toegepast in 'Arbeidsmarktanalyse Rijk 2018-2025' (Dialogic, 2019)

illustratie: eerder onderzoek liet zien dat bedrijven die AI-gerelateerde innovaties doorvoerden 40% snellere omzetgroei kenden dan vergelijkbare bedrijven die dat niet deden[97].

Interviews

In de interviews worden er duidelijk twee perspectieven op AI genoemd. Aan de ene kant wordt duidelijk gemaakt dat aanvallers AI kunnen inzetten om snel en efficiënt kwetsbaarheden te vinden in systemen. Ook kan het bijvoorbeeld gebruikt worden om social engineering uit te voeren. Het manipuleren van mensen, bijvoorbeeld door *deep fakes*, wordt veel eenvoudiger door AI.

Aan de andere kant wordt ook erkend dat AI kansen biedt voor de cybersecuritysector. Het kan gebruikt worden om geavanceerde pentesten uit te voeren. Maar het kan ook worden ingezet om aanvallen te detecteren en netwerken te toetsen op *Indicators of Compromise*.[98] AI kan op deze manier worden ingezet om "*volumewerk weg te automatiseren*", zoals een respondent dit fraai verwoordde. Hierbij biedt het meteen een oplossing voor de krapte op de arbeidsmarkt. Een aanbieder van cybersecurity-diensten gaf aan dat het traditioneel werken op basis van use cases niet meer werkt omdat je dan achter de feiten aanloopt. Met AI kan er simpelweg veel sneller worden ingegrepen. In de interviews wordt verder aangegeven dat het uiteraard vooral de managed services zullen zijn die profiteren van de ontwikkeling van AI.

Literatuur

AI speelt ook in cybersecurity een steeds grotere rol. Dat geldt zowel aan de kant van de aanvallers als aan de kant van de verdedigers.[99] Aanvallers gebruiken bijvoorbeeld geavanceerde chatbots (*deep fakes, influence bots*) voor het verspreiden van desinformatie of phishing[100], of AI voor de analyse dan grote hoeveelheden data voor social engineering.

Aan de verdedigingskant kunnen AI algoritmes worden gebruikt om verdachte patronen te detecteren en te voorspellen (op basis van de eerdere aanvallen die zijn waargenomen), en daar (*near) real-time* op te acteren.[101] Het belang van het voorspellen van aanvallen wordt steeds groter omdat het volume cyber attacks steeds groter wordt.[102] Overigens is er op dit moment meestal nog geen sprake van volledig automatische systemen (zoals spamfilters). Bij meer geavanceerde vormen van cybercriminaliteit nemen menselijke *agents* nog steeds de beslissingen maar worden ze voor het inschatten van risico's daarbij in toenemende mate ondersteund door AI-systemen (vooral om in zeer grote data sets signaal van ruis te

---

[97] Alderucci et al. (2019), Quantifying the Impact of AI on Productivity and Labor Demand: Evidence from U.S. Census Microdata

[98] IoC's stellen organisaties in staat om snel zicht te krijgen op malafide activiteiten. https://www.ncsc.nl/binaries/ncsc/documenten/factsheets/2019/juni/01/factsheet-indicators-of-compromise/20161208+Factsheet-Indicators-of-Compromise.pdf

[99] Zie bv. Bonfanti, M.A. (2022) Artificial intelligence and the offense-defense balance in cyber security. in: Cavelty, M.D. & Wenger, A. (Eds). *Cyber Security Politics. Socio-Technological Transformtions and Political Fragmentation*. Abingdon:Routledge (Ch.5)

[100] Evans. K. (2022) *AI-based social engineering is the next-generation of hacking humans* (July 14). https://www.cybertalk.org/2022/07/14/ai-based-social-engineering-is-the-next-generation-of-hacking-humans/

[101] Dash, B., Sharma, P., Ansari, M.F., Ali, A. (2022). Threats and Opportunities with AI-based Cyber Security Intrusion Detection: A Review. *International Journal of Software Engineering & Applications, 13*(5). DOI: 10.5121/ijsea.2022.13502

[102] Conti, M., Ali Dehghantanha, A., Dargahi, T. (2018) Cyberthreat Intelligence: Challenges and Opportunities. https://arxiv.org/pdf/1808.01162.pdf

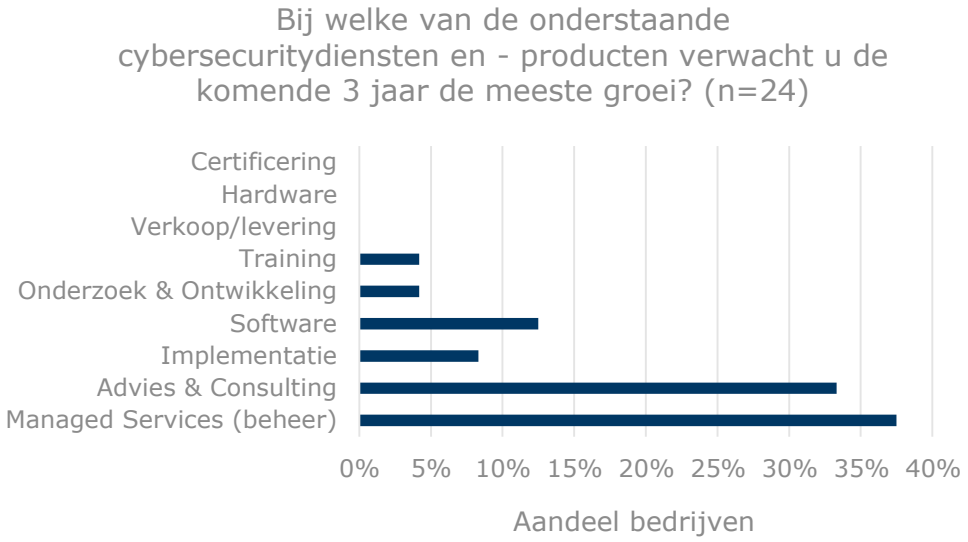
onderscheiden – elimineren van valse positieven). Een andere sterkte is uiteraard dat *AI-drive*n security-systemen 24/7 actief zijn.

De grootschalige inzet van AI in cybersecurity brengt ook nieuwe (soorten) kwetsbaarheden met zich mee. Een voorbeeld is het opzettelijk voeden van *AI-driven* security-systemen met verkeerde training data (‘*data poisoning*)[103] of het manipuleren van de input (‘ input/*evasion-attack*’)[104]. Het lerende vermogen van AI kan op dit moment ook al worden ingezet om (semiautomatisch) malware te ontwikkelen die steeds sneller evalueert, en zo aan detectie blijft ontkomen.[105] Om het nog weer complexer te maken: op hun beurt kunnen *AI defence* systemen weer worden getraind met kwaadaardige voorbeelden om eerder en beter aanvallen te kunnen herkennen.[106]

Enquête

In de enquête werd aan 31 partijen die R&D uitvoeren gevraagd wat hot-topics (opkomende gebieden) waren. Er was sprake van een open antwoordcategorie en respondenten moesten dus zelf een tekstveld invullen. Zeven respondenten (22%) gaven een antwoord dat in generieke zin betrekking had op kunstmatige intelligentie, zoals AI, Machine Learning en ChatGPT.

In de enquête kan ook een link gemaakt worden met de groei van managed services, die voor een deel wordt (en zal worden) veroorzaakt door AI. De onderstaande afbeelding toont dat 38% van de respondenten aangeven dat Managed Services het onderdeel van de sector is dat de meeste groei kent.



[103] Gu, T., Dolan-Gavitt, B. and Garg, S. (2019). *BadNets: Identifying Vulnerabilities in the Machine Learning Model Supply Chain*. https://arxiv.org/pdf/1708.06733.pdf

[104] Sadeghi, K., Banerjee, A. & Gupta, S.K. (2020). A system-driven taxonomy of attacks and defenses in adversarial machine learning. *IEEE transactions on emerging topics in computational intelligence*, 450-467.

[105] Violio, B. (2022) *Artificial intelligence is playing a bigger role in cybersecurity, but the bad guys may benefit the most* (Sept.13) https://www.cnbc.com/2022/09/13/ai-has-bigger-role-in-cybersecurity-but-hackers-may-benefit-the-most.html

[106] Brink, N. et al. (2023) *Adversarial AI in het cyberdomein*. TNO Whitepaper (februari 2023). https://publications.tno.nl/publication/34640579/Mf1Fda/TNO-2023-R10292.pdf

CBS microdata

Ook in de data van CBS kunnen we terugvinden dat de managed services een van de snelst groeiende onderdelen zijn. Het aantal bedrijven dat managed services aanbood, groeide in de periode 2015-2021 gemiddeld met 6,3% per jaar. Een deel hiervan wordt mogelijk gedreven door AI.

Tabel 5. Groei van de cybersecuritysector uit gesplitst op ENISA categorie

	2015	2016	2017	2018	2019	2020	2021	CAGR[107]
Advies	988	1046	1091	1185	1222	1271	1299	**4,7%**
Certificering	363	388	425	451	469	485	493	**5,2%**
Distributie	229	246	265	292	308	329	332	**6,4%**
Hardware	440	463	473	505	525	541	560	**4,1%**
Implementatie	303	333	342	367	387	404	427	**5,9%**
Managed services	931	1011	1063	1151	1209	1285	1342	**6,3%**
Software	947	1010	1087	1170	1226	1290	1342	**6,0%**
Eindtotaal	4201	4497	4746	5121	5346	5605	5795	**5,5%**

4.1.3 Sterke kennisbasis in kwantumtechnologie

Nederland heeft veel kennis van kwantumtechnologie. Dit kan worden ingezet binnen de cybersecuritysector. Huidige vormen van encryptie zijn gemakkelijk te kraken met een kwantumcomputer. De opkomst van kwantumtechnologie vraagt om de ontwikkeling van een nieuwe generatie cryptografie, gebaseerd op kwantum technologie. Kwantumencryptie kan in theorie nog steeds gekraakt worden door een kwantumcomputer, maar de zogenoemde 'kwantumstatus' van informatie veranderd wanneer het is ontsleuteld.

Interviews

In verschillende interviews is het onderwerp kwantumtechnologie aan bod gekomen. Net als bij AI wordt dit vanuit het perspectief van cybersecurity zowel als kans als bedreiging gezien.

Een kwantumcomputer maakt het mogelijk om veel van de encryptie die op dit moment gebruikt wordt te kraken. Inherente eigenschappen van de technologie maken het mogelijk om *brute force* hacks veel sneller uit te kunnen voeren. Dit kan een grote dreiging zijn omdat veel gegevens die nu veilig versleuteld worden, in de toekomst mogelijk uitgelezen kunnen worden door een derde partij. Sommige partijen ontwikkelen *quantum resistant* systemen die voorkomen dat dit gebeurt en hier ligt een interessante marktkans. Toch vraag een enkele respondent zich ook af of we hier wel op in zouden moeten zetten of dat dit al een gelopen race is.

Enquête

In de enquête werd aan 31 partijen die R&D uitvoeren gevraagd wat hot-topics (opkomende gebieden) waren. Er was sprake van een open antwoordcategorie en respondenten moesten dus zelf een tekstveld invullen. Twee respondenten (6%) gaven als antwoord kwantumtechnologie. Hoewel dit een beperkt aantal is, geeft het aan dat kwantumtechnologie door een gedeelte van de sector wel als interessant opkomend gebied wordt beschouwd.

[107] CAGR staat voor *compound annual growth rate* en dus de gemiddelde jaarlijkse groei over een bepaalde periode. Hier gaat het uiteraard om de periode 2015-2021.

Literatuur

Het QuTech initiatief is reeds eerder genoemd (zie 4.1.1). Dit is een missiegedreven onderzoeksinstituut dat werkt aan prototypes van een quantumcomputer en een quantuminternet[108] De Nederlandse overheid heeft de afgelopen jaren omvangrijke financiering (circa €150 miljoen vanaf 2012) aan QuTech toegekend.[109] Binnen QuTech werken de TU Delft, TNO en de UvA samen aan de ontwikkeling van kwantumcomputers. TUD en TNO richten zich daarbij vooral op de hardware (TU/e en UT doen ook samen met TUD onderzoek naar kwantumhardware), de UvA op software (Leiden doet op dit terrein ook vooraanstaand onderzoek, en werkt daarbij o.a. samen met Google Quantum AI). UvA werkt op haar beurt nauw samen met CWI. CWI doet al jarenlang onderzoek naar de impact van kwantumcomputing op cyber security. Die impact zou zeer groot kunnen zijn. Zo zijn decrypties die met conventionele computers eeuwen aan *computing capacity* zouden vergen, met een kwantumcomputer in enkele minuten te kraken.

4.1.4 Invoering van NIS2 en CRA

Nieuwe richtlijnen (de vervolgversie van *Network and Information Security*[110] en *Cyber Resilience Act*) vanuit Europa gaan (mogelijk) nieuwe eisen stellen aan de marktpartijen. Hier kan de sector op anticiperen en dit biedt kansen. Daarbij zal de cybersecuritysector als essentiële dienst onder de NIS2 vallen en daarmee meer informatie vanuit het NCSC ontvangen. Daarmee kan de sector zich gaan onderscheiden wat mogelijk kansen gaan bieden. Kort gezegd kunnen we stellen dat de NIS2 eisen stelt aan het veiliger maken van processen, waardoor de vraag vanuit de markt zal groeien. De CRA stelt eisen aan veiligere producten/diensten, welke kansen bieden voor met name integrators.

Literatuur

Sinds 2018 is de Wet beveiliging netwerk- en informatiesystemen (Wbni) in werking getreden.[111] Hiermee is onder meer geregeld dat aanbieders van essentiële diensten en digitale dienstverleners een plicht hebben om passende en evenredige technische en organisatorische maatregelen op het gebied van cybersecurity te nemen. Deze wet regelt onder meer een meldplicht van incidenten bij het Computer Security Incident Response Team voor digitale dienstverleners (CSIRT-DSP).

Als gevolg van de herziening van de Netwerk- en informatiebeveiligingsrichtlijn (NIB2) krijgen veel meer sectoren en organisaties te maken met wettelijke verplichtingen voor de beveiliging van hun netwerk- en informatiesystemen.[112] Deze organisaties dienen in het kader van een zorgplicht te voldoen aan een hoog niveau van cybersecurity en incidenten moeten tijdig gemeld worden. Met de implementatie van de richtlijn worden meer en andere organisaties (ruim 5000 bedrijven; momenteel slechts 200 organisaties) aangemerkt dan nu

---

[108] Zie bijvoorbeeld https://www.tudelft.nl/qutech en de website van QuTech.

[109] Soeteman, K. (2015) *Overheid investeert 135 miljoen euro in kwantumcomputers* (1 juni). https://tweakers.net/nieuws/103423/overheid-investeert-135-miljoen-euro-in-kwantumcomputers.html

[110] NIS2: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333

[111] https://www.rijksoverheid.nl/documenten/rapporten/2018/09/01/wet-beveiliging-netwerk--en-informatiesystemen-wbni-voor-digitale-dienstverleners

[112] Kamara, I., Van den Boom, J. (2022). Computer Security Incident Response Teams in the reformed Network and Information Security Directive: good practices.

onder de Wbni aangewezen zijn.[113] Er wordt ook toezicht gehouden op de naleving van de plichten. Met de implementatie van deze richtlijn is de vrijblijvendheid dus grotendeels voorbij.

Ook is het kabinet van plan om maatregelen te treffen om de digitale weerbaarheid van specifieke sectoren te verhogen.[114] Er komen extra normen voor de zorg- en onderwijssectoren, en gemeenten en provincies krijgen te maken met aangescherpte beveiligingseisen.

De onderhandelingen voor de Cyber Resilience Act zijn daarnaast aan de gang. Nederland maakt zich hier hard voor opname van een zorgplicht voor fabrikanten en leveranciers van alle ICT-producten, diensten en processen, die gedurende de hele levenscyclus geldt, inclusief bijbehorende standaarden en toezicht.[115]

Interviews

In een groot deel van de interviews komt dit onderwerp aan bod. Dit is een onderwerp dat duidelijk op de agenda staat bij respondenten. De sector ziet het als een kans dat steeds meer organisaties door de NIS2 gedwongen worden om voldoende maatregelen te treffen. Hierdoor gaat de bewustwording van de risico's en het algemene niveau van veiligheid omhoog. Bovendien zijn markpartijen uiteraard verheugd met de toename in vraag die dit zal veroorzaken. Er zijn echter ook zorgen in welke mate bedrijven hier al van op de hoogte zijn. Ook is er twijfel of het duidelijk is voor bedrijven aan welke eisen ze moeten voldoen. En welke marktpartijen daadwerkelijk aan de standaarden kunnen voldoen. Normering en certificering lijken nog beperkt te zijn uitgewerkt.

Het is op dit moment nog niet zeker in welke vorm de CRA realiteit wordt. Daarom wordt hier in de interviews minder over gesproken. De komst van de CRA wordt als een kans gezien omdat het zal voorkomen dat laagwaardige cybersecurityintegrators actief zijn op de Europese markt. Dit biedt een kans voor hoogwaardige Nederlandse cybersecurityintegrators.

Enquête

In de enquête zijn twee vragen gesteld aan integrators over de achterliggende reden voor de van integratie van cyberveiligheid in hun producten of diensten. Meer dan 60% van de respondenten gaf op dit moment al aan dat er een verplichting is vanuit regelgeving om dit te doen, zie Figuur 27. Motivatie van integratie cyberveiligheid in Enquête 3. Bovendien gaf meer dan de helft van de respondenten aan het als een (zeer) sterk competitief voordeel te zien. Dit is een goede indicatie dat de invoering van de CRA daadwerkelijk een voordeel kan zijn voor de Nederlandse sector.

4.1.5 Logische vestigingsplaats voor NGO's en IO's op gebied van vrede en veiligheid in het digitale domein

Nederland, en Den Haag in het bijzonder, heeft een reputatie als vestigingsplaats voor non-gouvernementele organisaties (NGO's) en internationale organisaties (IO's) op gebied van vrede en recht. Het zou een kans kunnen zijn om toekomstige, nog op te richten, organisaties die dit voor het digitale domein gaan doen in Den Haag te vestigen.

---

[113] NCTV (2022). Nederlandse Cybersecuritystrategie 2022-2028 Ambities en acties voor een digitaal veilige samenleving.

[114] NCTV (2022). Nederlandse Cybersecuritystrategie 2022-2028 Ambities en acties voor een digitaal veilige samenleving.

[115] NCTV (2022). Nederlandse Cybersecuritystrategie 2022-2028 Ambities en acties voor een digitaal veilige samenleving.

Literatuur

Den Haag profileert zich duidelijk als Stad van Vrede en Recht.[116] Hiermee heeft het een duidelijke en unieke internationale profilering.[117] In de stad zijn op dit moment tientallen NGO's en IO's gevestigd.[118] Als wij kijken naar Den Haag dan komen tot verschillende grotere IO's die mogelijk een raakvlak kunnen gaan krijgen met cybersecurity.

- *International Criminal Court.*[119]
- *Permanent Court of Arbitration*[120]
- *Eurojust*[121]
- *International Court of Justice*[122]
- *Europol*[123]
- *United Nations Interregional Crime and Justice Research Institute*[124]
- *Hague Conference on Private International Law*[125]
- *International Development Law Organization*[126]
- *Organisation for the Prohibition of Chemical Weapons*[127]
- *European Patent Office*[128]

Bovendien is in Den Haag het Global Forum on Cyber Expertise (GFCE) gevestigd dat als doel heeft om internationale samenwerking bij *cyber capacity building* te stimuleren. De vestiging van al deze organisaties heeft een aanzienlijke economische impact op de stad.[129]

Het is niet onredelijk om te veronderstellen dat op het gebied van cybersecurity de komende jaren nieuwe IO's worden opgericht. Het zou interessante kunnen zijn om te verkennen of deze niet in Den Haag gevestigd kunnen worden. De zwakte dat Nederland weinig grote bedrijven heeft in dit domein, kan nu ineens een kracht worden.

Interviews

In de interviews is dit onderwerp beperkt aan bod gekomen. Wel is benoemd dat het voor de overheid van belang is om Nederland op de kaart te zetten als interessante vestigingslocatie voor internationale bedrijven. Nederland heeft een goed ontwikkelde IT-sector en een goed opgeleide bevolking. Als relatief klein land in Europa heeft Nederland een goede

---

[116] https://www.denhaag.nl/nl/bestuur-en-organisatie/stad-van-vrede-en-recht.htm

[117] https://www.researchgate.net/publication/280254038_Den_Haag_Geneve_aan_de_Noordzee_Vergelijkend_beleidsonderzoek_rond_internationale_organisaties_en_ngo%27s_in_Den_Haag_en_Geneve

[118] Zie bijvoorbeeld https://denhaag.raadsinformatie.nl/document/3369851/1/RIS175444a

[119] https://www.icc-cpi.int/

[120] https://pca-cpa.org/en/home/

[121] https://www.eurojust.europa.eu/

[122] https://www.icj-cij.org/

[123] https://www.europol.europa.eu/

[124] https://unicri.it/about-unicri

[125] https://www.hcch.net/en/home

[126] https://www.idlo.int/about-idlo/about-idlo

[127] https://www.opcw.org/

[128] https://epo.org/

[129] https://www.researchgate.net/publication/280254038_Den_Haag_Geneve_aan_de_Noordzee_Vergelijkend_beleidsonderzoek_rond_internationale_organisaties_en_ngo%27s_in_Den_Haag_en_Geneve

uitgangspositie om op te staan als cybersecurity-zwaartepunt. Nederland staat er dus goed voor om zichzelf verder te profileren binnen de cybersecuritysector.

Enquête

In de enquête is één aanknopingspunt voor dit onderwerp. Het valt op dat ethisch gedrag in dit domein in Nederland in hoog aanzien staat. Op de vraag waarom aandacht werd besteed aan cyberveiligheid, gaf een relatief groot aandeel van de respondenten spontaan een antwoord dat gerelateerd is aan ethische overweging. Voorbeelden zijn: 'Dit is moreel juist. De dagelijkse onzichtbare dreiging treft iedereen en iedereen gebruikt techniek. Toch is de verdediging helaas niet zo sterk aanwezig als dat zou mogen idealiter' en 'aandacht besteden aan cybersecurity is ethisch de juiste optie is'.

4.2 Bedreigingen voor de Nederlandse cybersecuritysector

4.2.1 Tekorten aan personeel met cybersecurityprofiel

In Nederland zijn er in het algemeen tekorten op de arbeidsmarkt, maar als het om cybersecurity gaat dan zijn deze tekorten nog veel groter. Dit beperkt niet alleen het huidige functioneren, maar ook de potentiële groei van de sector.

Interviews

Het punt dat nagenoeg iedere respondent maakte, is dat er sprake is van de flinke tekorten op de cybersecurityarbeidsmarkt. Hoewel we geen kwantitatieve analyse van interviews gaan uitvoeren, is het toch veilig om stellen dat dit door de bank genomen als grootste probleem wordt gezien door respondenten. Er worden verschillende specifieke punten over dit onderwerp gemaakt.

- De **formele cybersecurityopleidingen zijn niet de voornaamste bron van talent**. De meeste werknemers worden (en zijn) op andere manieren opgeleid.
    - De personen die een opleiding als HBO-cybersecurity doen, zijn niet altijd de personen met de meeste kennis van dit onderwerp. Sommige specialisten zijn **autodidacten** die vanuit interesse kennis hebben opgedaan. Zij hebben mogelijk geen opleiding meer nodig en kunnen direct de arbeidsmarkt betreden.
    - **Opleidingen als wiskunde, AI, data science, ICT** zijn belangrijke toeleveranciers voor de cybersecurityarbeidsmarkt. Deze personen kunnen ook de technische kant van het onderwerp goed doorgronden. Maar ook mensen zonder een technische opleiding kunnen als bruggenbouwer een belangrijke rol spelen. Ook aan dit soort **interdisciplinaire kennis** is een tekort.
    - **Interne opleidingen** (bij binnenkomst bij een bedrijf) worden door sommigen beschouwd als de beste opleiding. Wanneer mensen met basisvaardigheden en talent bij elkaar worden gezet om van elkaar te leren kunnen zij hun kennis en interesse verder ontwikkelen. Er zijn weinig afgestudeerden die direct op het niveau zitten dat ze mee kunnen draaien in een cybersecuritybedrijf. Bedrijven hebben interesse om met opleiders samen te werken om zo samen mensen op te leiden.
    - **Zij-instromers** kunnen een enorm potentieel in zich hebben. Met kennis over bijvoorbeeld bedrijfsvoering kunnen sommige medewerkers relatief makkelijk worden omgeschoold tot een cybersecurityexpert.
- Er is twijfel of de formele opleidingsinstituten (WO, HBO en MBO) **wel voldoende uitgerust zijn** om cybersecurity-opleidingen te realiseren.

    - Er is sprake van een dynamische sector waardoor het lastig is om het **curriculum actueel** te houden. Voor een opleidingsinstituut is het moeilijk om een dynamische sector als die van de cybersecuritysector bij te houden wat betreft het onderwijsmateriaal. Het Ministerie van Onderwijs, Cultuur en Wetenschap ziet erop toe dat opleidingen zo flexibel mogelijk worden ingericht om aan te sluiten bij de vraag uit de markt. Het is hierbij van groot belang dat aanpassingen snel worden doorgevoerd. Het curriculum zou constant moeten veranderen en docenten moeten de ruimte krijgen om hun eigen kennis constant up-to-date te houden.
    - Er is twijfel of de onderwijssector wel **voldoende personeel** kan aantrekken. Zijn er wel voldoende docenten om voor de klas te staan? Zijn er personen die PhD plekken willen invullen?
- Er is op de arbeidsmarkt en bij opleidingen sprake van **concurrentie met buitenland**.
    - Er is een beeld dat veel **buitenlandse studenten in Nederland een** securityopleiding volgen. Maar hoeveel daarvan blijven er daadwerkelijk in Nederland werken? En geven we hiermee niet veel kennis en schaarse plekken weg?
    - Voor Nederlandse afgestudeerden binnen de cybersecuritysector is **het aantrekkelijk om voor een buitenlands bedrijf te werken.** Hier kan er sprake zijn van gunstigere arbeidsvoorwaarden en een sneller carrièrepad. Het is onduidelijk hoe de stroom van talent dat vertrekt naar het buitenland zich verhoudt tot de stroom talent die wij als Nederland binnenhalen. Omdat cybersecurity in het veiligheidsdomein valt is Nederland mogelijk terughoudender in het aannemen van buitenlands talent voor functies in deze sector. Dit maakt het vullen van deze posities nog lastiger. Defensie zoekt veel IT'ers met specifieke kennis van veiligheid[130], dit is lastig om in te vullen.
- Bedrijven **worden belemmerd in hun groei** door het tekort aan medewerkers. Het probleem van sommige bedrijven is dus niet (meer) een gebrek aan vraag. Er is concurrentie voor talent tussen verschillende soorten partijen, waarbij ook de partijen die wij buiten de cybersecuritysector vinden vallen (*de gebruikers*) flink trekken aan de arbeidsmarkt.

Literatuur

In de literatuur is veel informatie te vinden over tekorten op de arbeidsmarkt. In het algemeen is er sprake van een tekort aan expertise in de cybersecuritymarkt. [131] Cybersecurityteams blijven onderbemand en overbelast.[132] In 2020 onderzocht Dialogic de status van het investeringsklimaat van het Nederlandse cybersecuritydomein.[133] Het algehele beeld was dat Nederland er relatief goed voorstond, maar dat het geen koploper was op het gebied van cybersecurity. Ook ontbraken er een aantal essentiële elementen voor een goed investeringsklimaat. Het tekort aan capabele cybersecurity professionals om te kunnen voldoen aan de vraag uit het bedrijfsleven kwam ook hier sterk naar voren.

---

[130] Zie bijvoorbeeld https://www.binnenlandsbestuur.nl/carriere/slagveld-digitaliseert-dus-ook-defensie-gaat-digitaal

[131] Onderzoeksraad voor Veiligheid, 'Kwetsbaar door software: lessen naar aanleiding van beveiligingslekken door software van Citrix', 2021.

[132] https://securityboulevard.com/2022/01/emerging-cybersecurity-trends-in-2022/

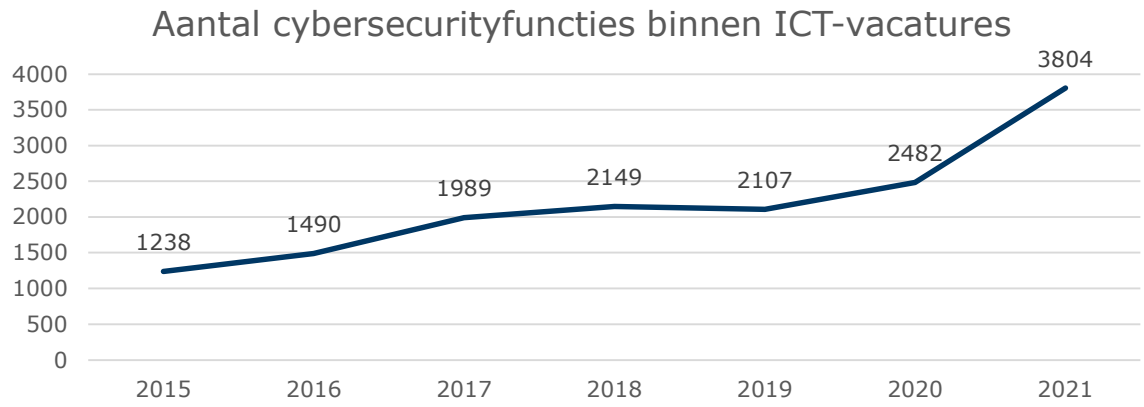
[133] https://www.dialogic.nl/wp-content/uploads/2021/06/Dialogic-2020.170-MinEZK-Het-Nederlandse-investeringsklimaat.pdf

Enquête

In de enquête is gevraagd naar de factoren die de groei van de cybersecuritysector belemmeren. Ruim 60% van de respondenten gaf aan dit het tekort aan personeel hier in sterke mate aan bijdraagt. Bijna 35% gaf aan dat hier in enige mate sprake van was. Geen enkele respondent gaf aan dat een tekort aan gekwalificeerd personeel geen beperkende factor is.

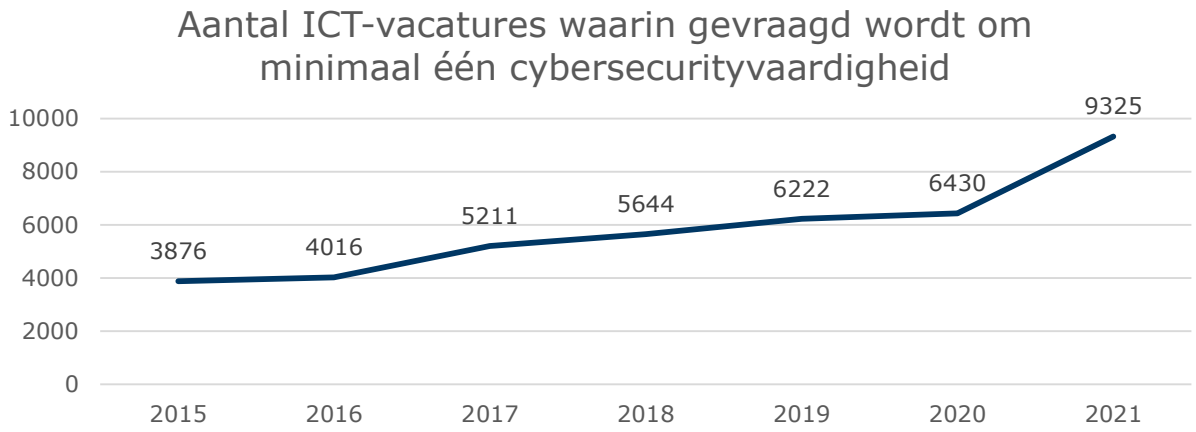
Analyse van vacatures

In het algemeen is er sprake van een tekort aan expertise in de cybersecuritymarkt. Om trends in deze arbeidsmarkt te identificeren, hebben we naar cybersecurityvacatures gekeken. Meegenomen zijn zowel 'harde' cybersecurity-functies, als vacatures waarin minimaal één relevante cybersecurityvaardigheid of cybersecurityvaardigheden in generieke zin wordt genoemd. Opvallend, maar wel in lijn met de verwachtingen, is het aantal cybersecurityvacatures sterk toegenomen sinds 2015. Voor zowel cybersecurityfuncties als functies waarin wordt gevraagd om cybersecurityvaardigheden, geldt dat het aantal vacatures hiervoor 2,5 tot 3 keer zo hoog ligt in 2021 als in 2015. Voor cybersecurityfuncties is dit in 2021 3,4% van het totaal aan ICT-vacatures (in 2015 was dit 1,7%). Voor ICT-functies waarin gevraagd wordt om minimaal één cybersecurityvaardigheid is dit in 2021 8,4% van het totaal aan ICT-vacatures (in 2015 was dit 5,4%).



Figuur 10. Aantal cybersecurityfuncties binnen ICT-vacatures. Om te bepalen of een ICT-vacature over een cybersecurityfunctie gaat is gekeken naar relevante trefwoorden in de functietitel. Bron: Dialogic o.b.v. data Jobdigger. De vacaturedata is afkomstige van Jobdigger en betreft vacatures in Nederland[134]

[134] Exclusief de vacatures van de bemiddelingsinstellingen. Van de vacatures die via bemiddelingsinstellingen (onder andere uitzendbureaus) worden uitgezet kan, door een beperkte omschrijving van de vacature, niet goed worden bepaald of hij al eerder is uitgezet. Om te voorkomen dat er vacatures dubbel worden meegenomen, is daarom besloten om de vacatures die worden uitgezet door bemiddelingsinstellingen niet mee te nemen.



Figuur 11. Aantal ICT-vacatures waarin gevraagd wordt om minimaal één cybersecurityvaardigheid. Bron: Dialogic o.b.v. data Jobdigger. De vacaturedata is afkomstige van Jobdigger en betreft vacatures in Nederland[135]

4.2.2 Beperkte awareness bij organisaties en consumenten over risico's

Doordat organisaties en consumenten zich niet goed bewust zijn van de risico's die zij lopen ontstaan er kwetsbaarheden. Dit is een bedreiging voor de sector in Nederland omdat er meer risico wordt gelopen dan nodig. Ook beperkt dit de groei van de sector. Daarnaast biedt het vergroten van awareness kansen voor de cybersecurity markt.

Interviews

In de interviews is zeer nadrukkelijk naar voren gekomen dat de beperkte awareness van afnemers een aanzienlijke bedreiging is. Een groot deel van de respondenten heeft dit onderwerp ter sprake gebracht. Het algemene beeld is dat de awareness toeneemt, maar nog steeds niet op voldoende niveau is. Een enkeling gaf aan *dat je bijna hoopt dat er eens iets groots gebeurt, dan worden we tenminste wakker en kunnen we nog grotere problemen voorkomen.* In deze discussie gaat het deels over kennis (we dachten dat deze oplossing veilig zou zijn), maar veel vaker over een gebrek aan zicht op de risico's. Marktpartijen zien dat sommige afnemers de risico's en dreigingen onderschatten *doordat* (!) ze op dit moment goede dienstverlening afnemen. Hebben we geen schade omdat de dreigingen beperkt zijn of omdat we goede dienstverlening afnemen? Voor veel afnemers is deze vraag niet goed te beantwoorden. Marktpartijen die heel goed zijn in het voorkomen van incidenten bij klanten ervaren dat de klant zich af gaat vragen waarom ze zoveel geld uitgeven aan cybersecurity. Er zijn immers geen cyberissues.

Enquête

In de enquête is gevraagd naar de factoren die de groei van de cybersecuritysector belemmeren. Ruim 60% van de respondenten gaf aan dat een gebrek aan bewustzijn van de risico's van cybercriminaliteit de groei van de cybersecuritysector beperkt. Bijna 25% gaf

[135] Exclusief de vacatures van de bemiddelingsinstellingen. Van de vacatures die via bemiddelingsinstellingen (onder andere uitzendbureaus) worden uitgezet kan, door een beperkte omschrijving van de vacature, niet goed worden bepaald of hij al eerder is uitgezet. Om te voorkomen dat er vacatures dubbel worden meegenomen, is daarom besloten om de vacatures die worden uitgezet door bemiddelingsinstellingen niet mee te nemen.

aan dat hier in enige mate sprake van was, zie Figuur 18. Redenen voor beperkingen aan groei. Ook vanuit de enquête komt dit aspect dus goed naar voren.

Literatuur

Uit recent onderzoek van I&O research naar het bedrijfsleven binnen de cybersecurity blijkt dat een derde van de medewerkers van Nederlandse bedrijven hun eigen kennisniveau over cyberveiligheid als slecht tot matig inschat (bij ICT-verantwoordelijken is dit een vijfde).[136] Echter onderneemt een kwart van de kleine bedrijven geen actie om veilig online te zijn. Ook uit eerder onderzoek komt naar voren dat ondernemers in Nederland het risico op cybercriminaliteit onderschatten.[137] In 2022 was 35% van de Nederlandse bedrijven voornemens om het budget voor cybersecurity te *verlagen* in 2023, tegenover 49% die het budget hiervoor wilden verhogen.[138]

4.2.3 Bedrijven die schaal krijgen worden snel overgenomen door externe partijen

In Nederland zijn de afgelopen jaren verschillende bedrijven tot wasdom gekomen. Bedrijven die een schaalbaar product of dienst ontwikkelen worden in veel gevallen echter snel overgenomen door buitenlandse partijen waardoor de Nederlandse sector zich beperkt kan ontwikkelen. Dit beperkt niet alleen de potentiële groei van de sector, ook vermindert het de autonomie van de sector.

Interviews

In de interviews is deze bedreiging expliciet benoemd. Hierbij wordt specifiek aandacht gegeven aan bedrijven die een schaalbaar product hebben ontwikkeld. Doordat zij een dergelijk product hebben ontwikkeld waren ze in staat om snel te groeien en een interessante kandidaat voor overname te zijn. Bovendien maken dit soort diensten het goed mogelijk om ook in het buitenland opgeschaald te kunnen worden. Het betekent echter ook dat de sector in Nederland wordt uitgekleed. De opschaalbare dienst verhuist naar het buitenland en in Nederland blijft weinig over. Hierdoor kan de cybersecuritysector zich beperkt ontwikkelen in Nederland. Ook worden strategische posities snel verlaten. Een laatste zorg is dat deze technologie terechtkomt bij partijen met een flinke marktmacht, waardoor Nederland afhankelijker wordt van buitenlandse partijen.

Literatuur

De recente empirische literatuur lijkt de stelling te onderbouwen dat Nederlandse hightech bedrijven boven een bepaalde schaal (in ieder geval de laatste jaren) relatief vaak worden overgenomen door (grote) buitenlandse bedrijven of investeerders. Dit geldt onverkort voor de Nederlandse cybersecurity bedrijven. We noemen hier bijvoorbeeld de overname van het Nederlandse cybersecurity 'kroonjuweel' Fox-IT door het Britse verzekeraar NCC Group in 2015[139] en in datzelfde jaar van SurfRight (zero days attacks) door het bekende Britse security bedrijf Sophos[140]; van Securelayers (IoT cyber security) door het Franse VINCI in 2018[141], en die van Motiv ICT security (tot die tijd een van de grootste onafhankelijke

[136] [Rijksoverheid.nl]

[137] [abnamro.nl]

[138] [pwc.nl]

[139] https://tweakers.net/nieuws/106470/nederlands-beveiligingsbedrijf-fox-it-overgenomen-door-brits-concern.html

[140] https://tweakers.net/nieuws/106838/sophos-neemt-nederlandse-hitmanpro-maker-surfright-over.html

[141] https://www.vinci-energies.nl/overname-cyber-sespecialist-securelayers/

managed security services aanbieders in Nederland) door de eveneens Franse multinational Atos in 2020[142] en die van Cybersprint (realtime vulnerability dashboards) door het Britse Darktrace in hetzelfde jaar[143]; en de overname van ION-IP (ook managed security services) door de Belgische telecomreus Proximus[144] en de overname van SecurIT (Identity & Access Management) door het Belgische Cegeka in 2021.[145] Daarentegen zijn er ook enkele voorbeelden van overnames door Nederlandse bedrijven; KPN heeft in 2017 onder andere Dearbytes[146] en QSight IT[147] overgenomen.

Deze dynamiek hoeft overigens vanuit beleidsoptiek niet altijd slecht te zijn – de winsten zullen veelal naar het buitenland stromen maar de werkgelegenheid blijft in sommige gevallen behouden. Recent spelen geopolitieke overwegingen wel een sterkere rol maar het gros van de overnames is door Europese bedrijven, niet door Amerikaanse, Israëlische, Chinese of Russische bedrijven.

4.2.4 Weinig Venture Capital en conversie van startup naar scale-up is lastig

Er is in Nederland relatief weinig venture capital (VC) beschikbaar. Er ontstaan wel startups, maar zij vinden het lastig om op te schalen naar scale-ups. De Nederlandse markt is vooraanstaand gefocust op het aanbieden van cybersecurity diensten. Gegeven de grote vraag en het beperkte aanbod is het voor ZZP'ers en ondernemers aantrekkelijk om diensten aan te bieden, zonder de ambitie te hebben zicht tot een scale-up te ontwikkelen. Daarnaast kent Europa een financieringsachterstand ten opzichte van de Verenigde Staten en China.[148] Zo bestaat het financieringsprogramma Horizon Europe uit slechts een tiende van de financiering die jaarlijks beschikbaar komt in het federale O&O-budget van de Verenigde Staten. Toch heeft Nederland een van de grootste ratio's cybersecurity marktomvang ten opzichte van de ICT marktomvang, vergeleken met andere Europese landen zoals België, Frankrijk en Italië.[149]

Interviews

In de interviews komt dit punt geregeld naar voren. Opvallend is echter dat niet alle respondenten op één lijn zitten. Men is het erover eens dat hier vroeger sterk sprake van was en dat het tegenwoordig beter gesteld is. Toch verschillen de meningen over de huidige situatie. Sommige partijen vinden het nog steeds problematisch, anderen zijn van mening dat het nu op een goed niveau is. Aangezien bij beide soorten partijen een ruime ervaring zit, ligt het waarschijnlijk in het soort kapitaal dat aangetrokken wordt. Wellicht zijn er tekorten van

---

[142] https://www.computable.nl/artikel/nieuws/security/7108253/250449/motiv-ict-security-onder-paraplu-van-atos.html

[143] https://ir.darktrace.com/regulatory-news/2022/2/23/1553096

[144] https://tweakers.net/nieuws/136719/proximus-neemt-nederlands-beveiligingsbedrijf-ion-ip-over.html

[145] https://www.cegeka.com/nl-nl/nieuws/cegeka-neemt-cybersecurityspecialist-securit-over

[146] https://www.overons.kpn/nieuws/kpn-koopt-cybersecuritybedrijf-dearbytes/

[147] https://www.computable.nl/artikel/nieuws/cloud-computing/6215686/250449/kpn-lijft-qsight-it-en-inspark-in.html

[148] https://www.mckinsey.com/~/media/mckinsey/business%20functions/strategy%20and%20corporate%20finance/our%20insights/securing%20europes%20competitiveness%20addressing%20its%20technology%20gap/securing-europes-competitiveness-addressing-its-technology-gap-september-2022.pdf

[149] https://advisory.eib.org/publications/attachments/cyber-technical-report.pdf

bepaalde vormen van financiering (of in bepaalde domeinen of voor bepaalde bedrijven), maar is dat niet zo in andere gevallen. Uit eigen ervaring weten we dat de verschillen per technologie groot kunnen zijn. Over het algemeen worden veelbelovende tech startups die al wat verder zijn (proven technology, omzet enkele miljoenen euro's) weldegelijk opgepikt door (veelal buitenlandse) investeerders. De bottleneck zit (nog steeds) in de fase daarvoor. Het is echter ook een gegeven dat er in de eerdere fasen van de evolutie nog veel 'selectie' plaatsvindt.

Enquête

Ook in de enquête is gevraagd of het tekort aan kapitaal een beperkende factor voor groei is. Zowel voor generiek kapitaal als durfkapitaal vindt circa 60% van de respondenten dat hier geen tekort aan is. Circa 30% van de respondenten vindt (voor beide gevallen) dat er in enige mate sprake van is. Het aandeel respondenten dat vindt dat er in sterke mate sprake van is, is dus in beide gevallen klein.

Literatuur

In de NLCS is opgenomen dat er **gewerkt moet worden aan het aanbod van kapitaal in Nederland voor investeringen:** op dit vlak lijken de ontwikkelingen beperkt. De Nederlandse (private) kapitaalmarkt op het gebied van cybersecurity is zeer beperkt.[150] Het belangrijkste fonds in Nederland is waarschijnlijk het Dutch Security TechFund van TIIN Capital. In 2021 is er door Invest-NL €5 miljoen euro in dit fonds geïnvesteerd, dat daarmee een totale omvang van €30 miljoen euro kreeg. De omvang blijft daarmee, zeker internationaal gezien, zeer beperkt en het risico voor buitenlandse overnames blijft daardoor hoog[151]. Het algehele beeld is dat het aanbod aan durfkapitaal in Nederland nog ontoereikend is.

In 2020 onderzocht Dialogic de status van het investeringsklimaat van het Nederlandse cybersecuritydomein.[152] Het algehele beeld was dat Nederland er relatief goed voorstond, maar dat het geen koploper was op het gebied van cybersecurity. Ook ontbraken er een aantal essentiële elementen voor een goed investeringsklimaat. Verdere knelpunten die in de Nederlandse cybersecuritysector werden gesignaleerd zijn: Gebrek aan toegang tot *start*kapitaal. De nadruk ligt hier op startkapitaal omdat er in de latere fasen genoeg interesse voor overnames lijkt te zijn (zie hiervoor, 4.2.3).

Dit is overigens geen typisch Nederlands maar een Europees probleem. In de VS wordt bijvoorbeeld aanzienlijk (drie keer) meer risicokapitaal geïnvesteerd in de technologiesector dan in de EU. Investeringen in startups zijn er makkelijker, vooral als de onderneming geen of weinig aantoonbare inkomsten heeft, de groei is ook sneller. Individuele investeringen hebben een transactieomvang die twee tot drie keer groter is in de VS en ook de waardering (*valuation*) is twee tot drie keer hoger.[153] Als wij kijken naar Israël dan is het beeld nog schever. In 2020 bedroeg het totale venture capital in Israël 15,0 miljard euro; tegen 0,8 miljard euro in Nederland (waarvan 0,5 miljard – 62% – buitenlandse VC's). Dat is een factor 19 lager dan het VC in Israël, dat economisch ruim 2x zo klein is als Nederland). In 2021

---

[150] https://www.ncsc.nl/onderwerpen/nederlandse-cybersecurity-strategie

[151] https://managementscope.nl/magazine/artikel/5260-roel-reijnen-cybersecurity

[152] https://www.dialogic.nl/wp-content/uploads/2021/06/Dialogic-2020.170-MinEZK-Het-Nederlandse-investeringsklimaat.pdf

[153] https://www.cybersecurityraad.nl/binaries/cybersecurityraad/documenten/rapporten/2021/02/18/onderzoeksrapport-digitale-autonomie/Onderzoeksrapport+%27Nederlandse+strategische+autonomie+en+cybersecurity%27.pdf.

neemt het VC in Nederland naar verhouding sterk toe – tot 1,9 miljard euro (waarvan 1,2 – 63% – buitenlands); tegen 21,6 miljard in Israël – nog steeds ruim een factor 11 lager.

Kijken we in meer detail naar de VC markt dat lijkt met name dat laatste punt (*valuation*) een zwakte van de Europese VC-markt te zijn. Dat wil zeggen, er is op zich wel voldoende risicokapitaal in Europa, alleen lijken de Europese 'durfinvesteerders' aanmerkelijk minder durf te hebben dan hun Amerikaanse collega's.[154]

4.2.5 Geen overheid die zwaar investeert

In Nederland is er geen sprake van een overheid die zwaar investeert in cybersecurity. In landen waar hier wel sprake van is, komt deze sector meer tot bloei en ontstaan er exportkansen. Echter zijn er maar weinig landen die zwaar investeren in cybersecurity zoals bijvoorbeeld Israël en Estland. In Nederland hebben vraagstukken met betrekking tot bijvoorbeeld klimaat en energie grotere prioriteit ten opzichte van cybersecurity. Het is daarom te verklaren waarom de Nederlandse overheid geen zware investeerder is in het cybersecurity domein. Wel zijn er veel subsidiemogelijkheden in dit domein.

Interviews

In meerdere interviews komt naar voren toe dat de Nederlandse cybersecuritysector op de internationale markt moet concurreren met bedrijven in landen waar de overheid veel geïnvesteerd heeft in deze sector. Het voorbeeld dat wordt aangehaald is Israël. Aan de andere kant wordt ook aangegeven dat hun situatie onvergelijkbaar is. Zij hebben een situatie met een dienstplicht van twee à drie jaar en waarbij de cybersecuritytalenten worden ingedeeld bij de Unit 8200 (de cybersecurityinlichtingendienst). Hier worden ze opgeleid en daarna wordt gestimuleerd om een startup te beginnen in dit domein. Hierdoor heeft Israël een heel goed cybersecurityecosysteem. In Israël zijn het bedrijfsleven en defensie sterker geïntegreerd waardoor kennisdeling snel gaat en innoveren wordt vergemakkelijkt. Een ander voorbeeld dat genoemd wordt is Estland. Nadat zij in 2007 een golf van Russische cyberaanvallen hebben ervaren, hebben zij sterk geïnvesteerd in dit domein. Zij wilden koploper worden in dit domein en dit lijkt vrij aardig te zijn gelukt.

In verschillende interviews ontstaat er een gesprek waarin parallellen met de Deltawerken worden getrokken.[155] In Nederland hadden wij in de jaren 50 een duidelijke *sense of urgency*. Om ons te beschermen tegen dreigingen moeten we nu flink investeren in een groot project. Dit is een duidelijke overeenkomst met Estland en Israël. Nadat wij de Deltawerken hadden gemaakt, bleken er ineens interessante exportkansen voor de watersector te zijn ontstaan. Dit was niet het primaire doel, maar een bijgevolg van de unieke investeringen die we gedaan hebben in de Deltawerken. Ook hier gaat de parallel met Estland en Israël op.

Literatuur

Exacte cijfers over overheidsuitgaven aan cybersecurity zijn lastig te vinden, maar een studie van het HCSS heeft enkele landen in kaart gebracht.[156] De onderstaande afbeelding toont enkele landen en de ontwikkeling van overheidsuitgaven aan cybersecurity. De verschillen

---

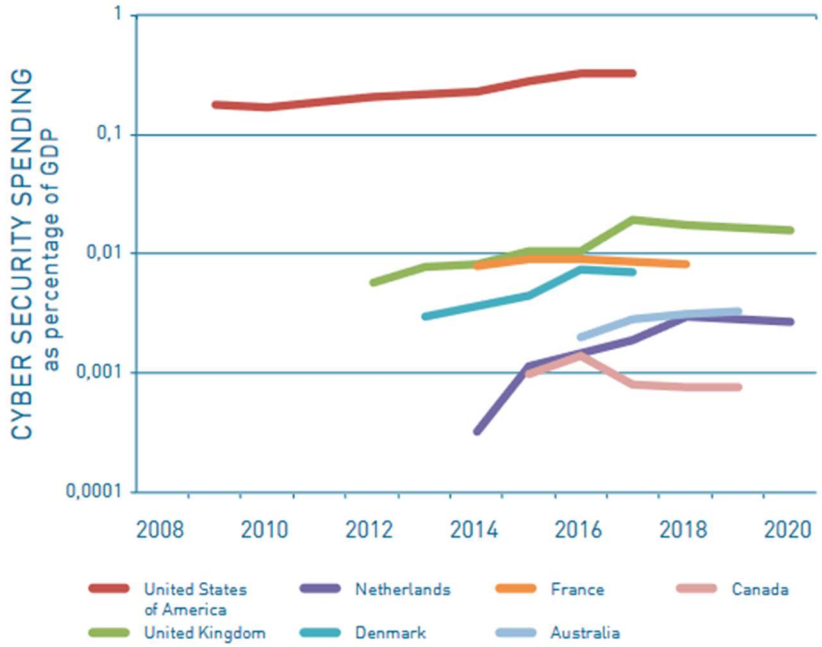
[154] https://www.cybersecurityraad.nl/binaries/cybersecurityraad/documenten/rapporten/2021/02/18/onderzoeksrapport-digitale-autonomie/Onderzoeksrapport+%27Nederlandse+strategische+autonomie+en+cybersecurity%27.pdf.

[155] In verschillende gesprekken hebben wij tijdens dit onderwerp gevraagd of zij deze analogie herkennen. Het is dus niet in alle gevallen spontaan genoemd.

[156] https://hcss.nl/wp-content/uploads/2017/03/HCSS_Dutch-Investments-in-ICT_0.pdf

lijken beperkt, maar merk de logaritmische y-as op. De daadwerkelijke verschillen zijn dus wezenlijk groter dan ze in eerste oogopslag lijken te zijn. In 2020 geeft het Verenigd Koninkrijk bijvoorbeeld niet grofweg het dubbele uit in vergelijking met Nederland, maar grofweg een factor 10 meer.

In de Nederlandse Cybersecurity Strategie (hierna: NLCS) 2022-2028 is een jaarlijks investering in cybersecurity van €92,6 miljoen euro begroot tot 2026. Vanaf 2027 is een investering van €111 miljoen euro begroot. Het Ministerie van Economische Zaken en Klimaat en Ministerie Justitie en Veiligheid dragen het grootste deel van deze structurele investering.



Figuur 12. Overheidsuitgaven aan cybersecurity. Bron HCSS.[157]

Israël heeft, vanwege zijn diaspora, van oudsher nauwe banden met zowel de VS als Rusland. In de periode 1989-2017 immigreerde er bijna één miljoen Russische joden naar Israël.[158] Zij hebben in de loop der jaren voor een fikse influx aan human capital gezorgd (ook en vooral in IT).[159] De nauwe banden met de VS hebben het land – dat qua BNP ongeveer de helft van Nederland is – in de loop der jaren ook heen windeieren gelegd. Helemaal vanzelf is dat niet gegaan. De Israëlische overheid heeft hier een instrumentele rol in gespeeld. Door gunstige belastingmaatregelen (vanaf 1993 verdubbelde de Israëlische overheid elke buitenlandse VC-investering) is het totale venture capital in het land tussen 1993 en 2000 een factor 60 gegroeid. Parallel daaraan heeft de Israëlische overheid zwaar geïnvesteerd in R&D. Israël heeft al decennialand het hoogste percentage R&D per GDP ter wereld: 5,4% in 2020. [160] Het enige land dat de tred van Israël enigszins kan bijhouden is Zuid-Korea (4,8% in 2020). Het percentage voor Nederland in dat jaar is 2,3%. Voor Israël

[157] https://hcss.nl/wp-content/uploads/2017/03/HCSS_Dutch-Investments-in-ICT_0.pdf

[158] https://en.wikipedia.org/wiki/1990s_post-Soviet_aliyah

[159] https://www.osw.waw.pl/sites/default/files/PV_The-Russian-street_net_0.pdf

[160] https://data.oecd.org/rd/gross-domestic-spending-on-r-d.htm

geldt daarbij de disclaimer dat een aanzienlijk deel van de R&D-uitgaven door de (omvangrijke) defensiesector wordt gedaan. En die uitgaven zijn niet in de cijfers meegenomen.

4.2.6 Geen (ervaren) eenduidige visie overheid

In Nederland wordt er middels de NLCS en zijn voorganger, de Nederlandse Cybersecurity Agenda (NCSA), al jaren gewerkt aan een uniform beleid vanuit de overheid. Echter, doordat [1] de verantwoordelijkheid voor aspecten van cybersecuritybeleid is belegd bij verschillende ministeries, en [2] er ook lokale/regionale initiatieven zijn die niet direct gekoppeld zijn aan het landelijk gecoördineerde beleid, ervaren partijen een fragmentatie van het beleid.

Interviews

In veel interviews is het gebrek aan eenduidige visie van de overheid als bedreiging aangegeven. Vanuit de sector wordt aangegeven dat er verschillende signalen van verschillende ministeries komen. Een eenduidige stem vanuit de overheid wordt gemist. Specifiek naar voren komt het onderscheid tussen het Ministerie van Economische Zaken en Klimaat (met een focus op economische kansen) en Justitie en Veiligheid (met een focus op veiligheid). Er lijkt geen integraal afwegingskader te zijn welke van deze doelen in welke gevallen prioriteit heeft. Een enkele respondent ziet echter ook dat dit een inherente eigenschap is van de bestuurscultuur die we in Nederland hebben (poldermodel) en een top-down aanpak (zoals in Frankrijk vaak het geval is) zou hier niet goed werken.

Eén van de commentaren die verder naar voren komt is dat de overheid reactief is. Een mogelijke verklaring hiervoor is de combinatie van de hoge mate van dynamiek in de sector en het gebrek aan kennis van deze sector bij beleidsmakers. Ook bij bestuurders en in de Tweede Kamer wordt weinig cyber-expertise herkend. De samenwerking tussen de overheid en het private sector wordt nog als te beperkt en te weinig geformaliseerd gezien. Aan de andere kant: dit geldt voor samenwerking in de hele keten.

Enquête

Ook in de enquête is gevraagd of een gebrek aan beleid rondom cybersecurity een beperkende factor voor groei is. Bijna 40% van de respondenten geeft aan dat dit in enige mate en ruim 40% zegt dat dit sterke mate speelt. Slechts 20% ziet het niet als beperking.

Literatuur

Het belangrijkste document om trends in het cybersecuritydomein (en haar investeringsklimaat) te identificeren is de NLCS, die in 2022 is gepubliceerd. In deze publicatie presenteert het kabinet haar plannen om de cybersecuritysector te versterken. De strategie krijgt concreet vorm in het Actieplan Cybersecuritystrategie 2022-2028.[161]

Hoewel de gehele NLCS relevant is in dit kader, zien we Pijler II ('Veilige en innovatieve digitale producten en diensten', Doel 2 ('Nederland heeft een sterke cybersecuritykennis- en innovatieketen') in het bijzonder relevant om hier te benoemen. Daar staan de volgende actielijnen vermeld:

- "De productontwikkeling voor *high assurance* producten wordt gestimuleerd middels versterkt en eensgezind opdrachtgeverschap vanuit de Rijksoverheid [zodat Nederland de beschikking houdt over betrouwbare cryptografische oplossingen]." Er wordt

[161] NCTV namens de Rijksoverheid (2022), *Actieplan Nederlandse Cybersecuritystrategie 2022-2028. Ambities en acties voor een digitaal veilige samenleving*.

dus geen additioneel budget voor investeringen ter beschikking gesteld – het gaat hier om vraagbundeling.

- "In samenwerking met bedrijven en wetenschappelijke instellingen wordt onderzoek uitgevoerd naar de ontwikkeling van moderne en hoogwaardige beveiligingsproducten." De eigenaar van deze actielijn is echter het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, dus niet het Ministerie van Onderwijs Cultuur en Wetenschappen en/of het Ministerie van Economische Zaken en Klimaat.
- "Defensie versterkt de *Cyber Innovation Hub* (CIH) om het innovatieportfolio uit te breiden en de landelijke positie in cybersecurity kennis- en innovatienetwerken te versterken." In 2018 heeft Defensie zijn jaarlijkse budget voor cyberonderzoek verhoogd van 3,9 miljoen naar 6,5 miljoen euro.[162]
- "NCSC voert onderzoeksactiviteiten uit onder een meerjarige agenda in samenwerking met diverse (kennis)instellingen op diverse domeinen gerelateerd aan de rol van het NCSC en haar doelgroep(en). Dit is wel een significante investering: 16 miljoen euro boven op het lopende budget van 6 miljoen euro, De voornaamste reden is om aan de aangescherpte Europese regels voor cybersecurity te kunnen (blijven) voldoen.[163]
- "Het kabinet zet meerjarige thematische routekaarten op aan de hand waarvan onderzoek wordt uitgevoerd of uitgezet middels het platform Dcypher." De thema's die zijn vastgesteld vormen de basis voor het programmeringsproces binnen Dcypher.
- "De cybersecurity kennis- en innovatiebehoefte van het bedrijfsleven en kennisinstellingen wordt onderdeel van het Nederlandse Topsectoren Programma.' Dit is het nieuwe CS4NL-programma, een instrument om de samenwerking tussen Dcypher en de Topsectoren op het gebied van cybersecurity innovatie te structureren. Er wordt vanuit het Ministerie van Economische Zaken en Klimaat een geschat budget van 27 tot 36 miljoen euro voor vrijgemaakt voor de periode 2023-2027.[164]

Ter vergelijking, het gaat hier dus om investeringen van enkele miljoenen tot maximaal 50 miljoen per jaar. Het totale venture capital in Nederland bedroeg 1.900 miljoen euro in 2021 (in Israël 21.600 miljoen euro, zie hiervoor, 4.2.5). Darktrace heeft in 2020 Cybersprint overgenomen voor 50 miljoen euro (zie hiervoor, 4.2.3). In datzelfde jaar hebben de Nederlandse directieleden van Fox-IT het bedrijf proberen terug te kopen van de NCC Group voor 100 miljoen euro.[165] Die overname is overigens niet gelukt. In plaats daarvan is Fox-IT "verder geïntegreerd" in de NCC Group.

---

[162] Sanders, R. (2018) *Defensie vergroot budget cyberonderzoek.* https://www.computable.nl/artikel/nieuws/security/6513456/250449/defensie-vergroot-budget-cyberonderzoek.html

[163] HSD Foundation (2022). *Dutch Government Reserves Millions in Funding for Cybersecurity* (Sept.22) https://securitydelta.nl/news/overview/dutch-government-reserves-millions-for-cybersecurity

[164] CS4NL (2022). Topsectoren bundelen innovatiekracht cybersecurity in CS4NL (Oct. 19). https://www.emerce.nl/wire/topsectoren-bundelen-innovatiekracht-cybersecurity-cs4nl

[165] Altorf, J. (2020) (26 mei) *'Couppoging moest Fox-IT in Nederlandse handen brengen'* https://www.techzine.nl/nieuws/security/441575/couppoging-moest-fox-it-in-nederlandse-handen-brengen/

5 Beleidsopties

Vanuit de SWOT-analyse komen vier aspecten naar voren waar het voeren van beleid het meest voor de hand ligt.

1. Met ontwikkelingen op het gebied van AI is het mogelijk om meer te kunnen doen met minder mensen. Op deze manier kan de sector blijven groeien ondanks krapte op de arbeidsmarkt. Bovendien biedt dit kansen voor exporteerbare producten. De brug tussen AI en cybersecurity moet vaker gelegd worden. Dit kan bijvoorbeeld via SBIR-aanvragen en de aansluiting bij het Groeifonds.

2. Zorgen voor kwantitatief en kwalitatief voldoende cybersecurityprofessionals. Er wordt al veel beleid gevoerd op dit onderwerp en het is opgenomen in de doelstellingen van de NLCS. Hoewel er mogelijkheden zijn om deze inspanningen verder te intensiveren, is het aanvullend belangrijk dat de visie op de aanpak van arbeidsmarkttekorten op het gebied van cybersecurity gaat passen binnen een meer integraal perspectief over hoe verschillende arbeidsmarkttekorten zich tot elkaar verhouden en wat we daar binnen Nederland aan willen doen. Er is nu immers sprake van 'beleidsconcurrentie' ten aanzien van het schaarse menselijk kapitaal waar de arbeidsmarkt in brede zin (ICT- en niet-ICT) over beschikt.

3. Voorkomen dat veelbelovende cybersecuritybedrijven in buitenlandse handen vallen zodat de Nederlandse sector zich beter kan ontwikkelen en afhankelijkheden worden beperkt, bijvoorbeeld door inzet van wet- en regelgeving en/of door het stimuleren van beschikbaar kapitaal voor de betreffende bedrijven. Wederom zou dit in een breder kader van sectoraal industriebeleid geplaatst moeten worden. Hierbij speelt ook inkoopbeleid van het Rijk en Europese afstemming een grote rol.

4. Versterken van bewustzijn bij gebruikers. Er zijn al veel initiatieven op allerlei geografische en sectorale niveaus. Optimalisatie kan vooral plaatsvinden door betere afstemming in het ecosysteem.

5.1 Integrale analyse van sterktes, zwaktes, kansen en bedreigingen

In de hoofdstukken 3 en 4 hebben we uitgebreid stil gestaan bij respectievelijk sterktes en zwaktes van (hoofdstuk 3) en kansen en bedreigingen voor de Nederlandse Cybersecuritysector (hoofdstuk 4). De kansen en bedreigingen hebben een signalerende functie voor beleid, omdat zij helpen bij het identificeren van de punten waarop inspanningen wenselijk geacht worden. Deze inspanningen kunnen zowel inspanningen vanuit de overheid (beleid) als inspanningen van andere partijen betreffen. Of overheidsbeleid specifiek wenselijk is, hangt af van de mate waarin er een legitieme rationale is voor dergelijke overheidsinterventie. Deze rationale kan geanalyseerd worden aan de hand van verschillende raamwerken, waarbij de perspectieven van marktfalen, systeemfalen en transformatiefalen gangbaar zijn, zie bijvoorbeeld de recente (EZK-)publicatie *'Durf te leren, ga door met meten'* (2022). De geïdentificeerde sterktes en zwaktes kunnen als 'bouwblokken' gezien worden die relevant zijn bij het inspelen op de kansen en bedreigingen.

De kansen, bedreigingen, sterktes en zwaktes zijn samengebracht in een confrontatiematrix, die waardevol kan zijn bij het uitvoeren van een SWOT-analyse, zie Figuur 13. De sterktes en kansen worden gepresenteerd met een **groene** kleur, de zwaktes en bedreigingen met een **rode** kleur. Hierin zijn vier kwadranten te onderscheiden die vier handelingsperspectieven reflecteren, te weten:

- Gebruiken van een bestaande **sterkte** om in te spelen op een **kans** (NW-kwadrant).
- Gebruiken van een bestaande **sterkte** om een **bedreiging** af te weren/te mitigeren (NO-kwadrant).
- **Zwakte** adresseren om zo beter in te kunnen spelen op een **kans** (ZW-kwadrant).
- **Zwakte** adresseren om zo een **bedreiging** af te weren/te mitigeren (ZO-kwadrant).

In de confrontatiematrix heeft het onderzoeksteam op basis van de informatie die is opgehaald met de verschillende ingezette onderzoeksmethoden, een inschatting gemaakt in welke cellen sprake is van een combinatie die urgent is om te adresseren. Lichtgrijs duidt op een combinatie die beperkt urgent lijkt, grijs op een combinatie die redelijk urgent lijkt en zwart op een combinatie die zeker urgent lijkt.

Voor het analyseren van beleidsopties bespreken we de kansen en bedreigingen (de kolommen) met de meeste zwarte cellen, omdat deze de meest relevante aanknopingspunten lijken te geven. Dit zijn de volgende vier kansen/bedreigingen:

1. Inzet van AI om arbeidsproductiviteit te vergroten
2. Tekorten aan personeel met CS-profiel
3. Overnames van groeiende bedrijven
4. Beperkt CS-bewustzijn bij gebruikers

Daarbij zullen we ook aangeven in hoeverre een overheidsinterventie hier gelegitimeerd is vanuit de perspectieven van markt-, systeem en transformatiefalen.[166] Die perspectieven worden (recentelijk) vaak als conceptueel kader gebruikt als het gaat om legitimatie van overheidsinterventie.[167]

Belangrijk is te noemen dat we hier primair kijken naar beleidsopties, maar dat dit andere actoren als bedrijven, kennisinstellingen, maatschappelijke organisaties en ook burgers niet ontslaat van de eigen verantwoordelijkheid om de cybersecuritysector (smalle economische betekenis van cybersecuritysector voor Nederland) alsook het bredere economische verdienvermogen van Nederland middels cybersecurity (bredere economische betekenis van cybersecurity voor Nederland) te versterken.

Hoewel de geïdentificeerde aanknopingspunten voor beleid uit dit onderzoek volgen, wil dit niet zeggen dat dit alle mogelijke aanknopingspunten zijn. Dit onderzoek is vertrokken vanuit de economische kansen voor de cybersecuritysector, en heeft daarmee al een nauwere scope dan cybersecurity in generieke zin. Daarnaast is dit onderzoek onderworpen aan beperkingen ten aanzien van de ingezette onderzoeksmethoden zoals de interviews en de literatuurstudie. Dus hoewel de geïdentificeerde aanknopingspunten binnen dit onderzoek naar ons oordeel relevant zijn, moedigen wij betrokken (beleids)professionals aan om in bredere zin te blijven reflecteren op aanvullende mogelijkheden voor beleid.

[166] Zie Dialogic (2020). Onderzoeks- en innovatieecosystemen in Nederland. In opdracht van EZK/OCW, Den Haag. https://www.dialogic.nl/wp-content/uploads/2020/11/Dialogic-Onderzoeks-en-innovatie-ecosystemen-in-Nederland-2020.pdf

[167] Ministerie Economische Zaken en Klimaat & SEO (2022). Durf te leren, ga door met meten. https://www.seo.nl/publicaties/durf-te-leren-ga-door-met-meten/

			KANSEN					BEDREIGINGEN					
			Sociaal	Technologisch	Technologisch	Politiek	Politiek	Sociaal	Sociaal	Economisch	Economisch	Politiek	Politiek
			Goed in integratie alfa, beta en gammawetenschappen	Groeiende mogelijkheden om via AI mensenwerk uit te voeren	Sterke kennisbasis in kwantumtechnologie	Invoering van NIS2 en CRA in het bijzonder	Logische vestigingsplaats voor NGO's en IO's	Tekorten aan personeel met CS profiel	Beperkte awareness bij organisaties en consumenten over risico's	Bedrijven die schaal krijgen worden snel overgenomen door externe partijen	Weinig VC en conversie van start-up naar scale-up is lastig	Geen overheid die zwaar investeert	Geen eenduidige visie overheid op CS
STERKTES	**Cyber R&D**	Sterke kennisbasis in cryptografie											
STERKTES	**Cybersector**	Sector kent een flinke groei											
STERKTES	**Cybersector**	Sector kan goed voldoen aan binnenlandse vraag naar diensten											
STERKTES	**Cyber-integrators**	Hoogwaardige integrators kunnen cybersecurity gebruiken om competitief voordeel te realiseren											
ZWAKTES	**Cyber R&D**	Weinig private cyber R&D											
ZWAKTES	**Cybersector**	Output die beperkt exporteerbaar is											
ZWAKTES	**Cybersector**	Grote afhankelijkheid van buitenlandse leveranciers van services, soft- en hardware											
ZWAKTES	**Cybersector**	Sector bestaat overwegend uit MKB en veel ZZP-ers											

Figuur 13. SWOT-analyse voor de economische kansen van de Nederlandse cybersecuritysector

5.2 Inzet van AI om arbeidsproductiviteit te vergroten

5.2.1 Aanknopingspunt voor beleid

De ontwikkeling van Artificial Intelligence (AI) heeft de laatste jaren een vlucht genomen. Belangrijke drivers hiervoor zijn [1] de toename in ICT-capaciteiten in informatieopslag (bijv. harde schijven), informatieverwerking (bijv. CPU's en GPU's), en informatietransmissie (bijv. mobiele upload-/downloadsnelheden) en [2] de toename van beschikbare data waar AI op gebouwd kan worden. Zie ook 4.1.2.

Ook in de cybersecuritysector zijn deze ontwikkelingen zichtbaar. Enerzijds heeft het betrekking op de aard van de cyberincidenten en het bestrijden daarvan, zoals de opkomst van '*deep fakes'*. Anderzijds kan ook de sector zelf AI op een innovatieve manier inzetten om het eigen werk te ondersteunen of zelfs (deels) te automatiseren. Dit laatste is een wenselijke toevoeging gezien het tekort aan gekwalificeerd personeel. AI kan als het ware gezien worden als een digitale collega met zeer sterke informatieverwerkingscompetenties, dus alle taken die baat hebben bij deze competenties zijn goede kandidaten om te ondersteunen of zelfs volledig uit te laten voeren door AI.

De slimme toepassingen van AI zitten onder andere in het geautomatiseerd testen en uitvoeren van andere taken binnen detectie. Daarnaast zien betrokkenen ook mogelijkheden ontstaan binnen de response. Hoewel het nog een relatief nieuw gebied is, kan de sector zichzelf vooruithelpen door zo slim en verantwoord mogelijk gebruik te maken van de kracht van AI. De exacte impact die AI kan gaan maken is nog onbekend, maar eerder onderzoek en de groei in de markt voor AI maken het aannemelijk dat het een substantiële impact kan hebben op de cybersecuritysector.

5.2.2 Legitimering overheidsingrijpen

Het ontdekken, ontwikkelen en toepassen van de kansen van AI voor de sector kent verschillende elementen, ieder met een eigen onderbouwing voor eventuele overheidsinterventie.

In het stadium van onderzoek en ontwikkeling (of R&D) speelt met name het marktfalen (positieve) **'externaliteiten'** een rol. Doordat er doorgaans bij R&D zogenaamde kennisspillovers plaatsvinden, profiteren ook andere partijen van de R&D-investeringen. Omdat een individueel bedrijf deze opbrengsten zich niet volledig toe kan eigenen, ontstaat er maatschappelijk gezien een onderinvestering in R&D. In deze vroege fase van onderzoek en ontwikkeling speelt vaak ook het marktfalen '**coördinatiefalen**' een rol. Partijen zijn gebaat bij gecoördineerde inspanningen met andere partijen, bijvoorbeeld vanwege synergie in hun expertises of netwerk, maar voor individuele partijen is het te kostbaar om de coördinatie op zich te nemen ('de business case kan niet uit'). Coördinatie kan daardoor uitblijven, evenals de resultaten die in theorie mogelijk waren geweest.

Op het moment dat de toepassingen er al (in enige vorm) zijn, verschuift het zwaartepunt naar adoptie, aanpassen aan de specifieke context, en implementatie. In deze fase spelen andere falens een rol. Zo is er allereerst doorgaans sprake van **'informatiegebreken'**; men weet niet wat er precies mogelijk is en onderneemt daardoor ook niet de juiste stappen. Ten tweede is er vaak beperkt absorptie vermogen binnen de organisatie (veelal vanwege te weinig kennis en kunde). Op dit vlak wordt HR-beleid, bijvoorbeeld in de vorm van werving en selectie en bij- en omscholing relevant. Voor het opleiden van mensen is het marktfalen '**externaliteiten**' vaak een reden voor maatschappelijke onderinvestering in menselijk kapitaal, zie ook §5.3. Ten derde zien we in de praktijk vormen van **coördinatiefalen** ontstaan. Organisaties weten niet bij wie ze moeten zijn en of geschikte partijen überhaupt

bestaan, waardoor in economische termen de zoekkosten te hoog zijn en markttransacties niet tot stand komen; hiervoor kunnen bijvoorbeeld coördinerende partijen en/of platformen uitkomst bieden.

5.2.3 Bestaand beleid

Er wordt in Nederland veel beleid ontwikkeld als het gaat om kunstmatige intelligentie. Dat loop van internationale verdragen over AI[168][169], hulpmiddelen voor het maken van een impact assessment [170] , mogelijkheden binnen het Groeifonds [171] en het hosten van conferenties.[172] Een van de eigenschappen van AI is dat het in veel domeinen kan worden toegepast en er zijn voor veel sectoren beleidsmaatregelen, zoals vervoer[173], onderwijs[174] en de zorg[175]. Toch zien we de doorsnede cybersecurity en AI relatief beperkt voorkomen in een beleidscontext. Er is een masteropleiding in Nijmegen[176] en een onderzoeksgroep in Delft[177], maar dit raakt slechts beperkt aan beleid. In de NLCS zijn we kunstmatige intelligentie dan ook niet tot nauwelijks tegengekomen.

5.2.4 Mogelijkheden voor (nieuw) beleid

Er zijn verschillende richtingen om beleid te ontwikkelingen als het gaat om cybersecurity en kunstmatige intelligentie. Hieronder geven we enkele mogelijkheden.

In de interviews wordt sterk verwezen naar de rol van de overheid als launching customer. De overheid is een grootafnemer van deze producten en diensten en kan een vraag naar AI-cybersecurityoplossingen uitzetten. Indien hiervoor een Nederlands bedrijf wordt geselecteerd, dan krijgt de Nederlandse sector een stimulans om zich verder te ontwikkelen. Zo kan productontwikkeling worden gestimuleerd. Een specifieke mogelijkheid die zou kunnen worden ingezet is het uitzetten van een SBIR[178] op dit onderwerp uit te zetten. Hoewel de SBIR 'slechts' tot het stadium van prototype reikt, kan de overheid het wel gebruiken om de vraag naar marktpartijen te articuleren en de ontwikkeling van nieuwe producten en diensten aan te jagen.

Een andere insteek die verkend kan worden, is die van het Groeifonds. Het AINed-voorstel uit de eerste ronde is gehonoreerd. De beschikbare middelen zijn niet als zodanig geoormerkt voor cybersecurity, maar er kan vanuit cybersecurity (meer) aansluiting gezocht worden bij initiatieven die binnen AINed ontplooid worden. Daarnaast zou ook naar nieuwe voorstellen gekeken kunnen worden, waarbij het raakvlak van AI en CS ingebed kan worden. Naast het

---

[168] https://www.rijksoverheid.nl/documenten/kamerstukken/2022/09/12/kamerbrief-over-mogelijke-elementen-ai-verdrag-raad-van-europa

[169] https://www.rijksoverheid.nl/actueel/nieuwsbrieven/regeringsnieuws/2022/176

[170] https://www.rijksoverheid.nl/onderwerpen/rijksoverheid/documenten/rapporten/2022/11/30/ai-impact-assessment-ministerie-van-infrastructuur-en-waterstaat

[171] https://www.rijksoverheid.nl/actueel/nieuws/2021/04/09/extra-impuls-voor-innovatie-vanuit-nationaal-groeifonds

[172] https://magazines.rijksoverheid.nl/bz/veiligheidsdiplomaat/2022/04/04

[173] https://nlaic.com/nieuws/ai-maakt-autorijden-veiliger-maar-zelf-sturen-voelt-nog-altijd-beter/

[174] https://communities.surf.nl/ai-in-education/artikel/artificial-intelligence-in-het-onderwijs-wat-is-het-en-wat-kun-je-ermee

[175] https://nictiz.nl/wat-we-doen/programmas/artificial-intelligence/

[176] https://www.ru.nl/opleidingen/masters/cyber-security-and-ai

[177] https://www.tudelft.nl/ewi/over-de-faculteit/afdelingen/intelligent-systems/cybersecurity

[178] https://www.rvo.nl/subsidies-financiering/sbir

NGF zijn er ook andere routes denkbaar om het raakvlak meer aandacht te geven, bijvoorbeeld in de vorm van PPS'en. Zo is het thema mogelijk in te bedden binnen voorstellen die momenteel ontwikkeld worden voor het gehonoreerde NGF-voorstel betreffende opschaling van PPS'en, of via andere bestaande kanalen.

Een derde mogelijke richting is het stimuleren van kruisbestuiving tussen de twee domeinen. In de interviews is aangegeven dat de AI en cybersecurity redelijk sterk als separate domeinen opereren. Door samenwerking aan te jagen kunnen nieuwe innovaties worden gedaan. In de woorden van de innovatie-econoom Schumpeter is innovatie niet meer dan "*Durchsetzung neuer Kombinationen*"

5.3 Zorgen voor kwantitatief en kwalitatief voldoende cybersecurity-professionals

5.3.1 Aanknopingspunt voor beleid

De cybersecuritysector is groeiende en heeft behoefte aan voldoende kwalitatief menselijk kapitaal om deze groei te faciliteren. Ook is hoogwaardige arbeid nodig om innovaties te ontwikkelen en te implementeren. Op zichzelf is het gebrek aan voldoende hoogwaardige arbeidskrachten geen 'nieuwe' uitdaging voor de sector, of cyber-specifiek; al jaren lijkt de vraag naar cyberprofessionals groter dan het aanbod. Toch lijkt de uitdaging in de huidige periode van brede arbeidsmarktkrapte groter geworden. Bedrijven moeten nóg meer inspanningen plegen om mensen aan te trekken én te behouden, en kosten lijken ook navenant op te lopen. Daarbij concurreren Nederlandse bedrijven met het buitenland als het gaat om de schaarse talenten.

Er zijn verschillende routes om de pool aan cyberprofessionals te vergroten. Veel genoemde routes zijn [1] het vergroten van de uitstroom in het reguliere (bekostigd) onderwijs, onder andere door meer cybersecurity-opleidingen aan te bieden en de aanwezigheid van cybersecurity in bestaande (ook niet cybersecurity) opleidingen te vergroten, [2] Leven Lang Ontwikkelen binnen organisaties, [3] het vergroten van de zijinstroom en [4] Nederland aantrekkelijker maken als vestigingslocatie voor internationale arbeidskrachten, denk hierbij aan de 30% regeling. Gesprekspartners in dit onderzoek geven daarbij aan dat men het onderwerp cybersecurity niet als puur technisch onderwerp moet positioneren, en ook in de werving breder moet kijken dan alleen mensen met een (cyber)technische achtergrond.

5.3.2 Legitimering overheidsingrijpen

Het interveniëren als overheid op het systeem van onderwijs en opleiding is niet nieuw, en kent een rijke beleidshistorie. Het beleid kan doorgaans ook goed gelegitimeerd worden aan de hand van diverse falens, zowel in het perspectief van markt- en systeemfalen als in het perspectief van transformatiefalen. Hieronder noemen we enkele veelvoorkomende falens die vaak gerelateerd zijn aan vraagstukken rondom opleiden.

Vanuit het perspectief van **marktfalen** is er veelal sprake van zogenoemde 'positieve externaliteiten'. In deze context betekent dit dat wanneer een bedrijf investeert in het opleiden van ('eigen') mensen, deze investering ook bijdraagt aan andere partijen. Dit kan bijvoorbeeld gebeuren doordat de kennis en expertise of de resultaten hiervan in het dagelijkse werk gedeeld worden met andere organisaties waardoor zij er ook profijt van hebben. Of, en dit is een vaker benoemd risico, dat de persoon die de opleiding genoten heeft van werkgever wisselt. Door deze dynamiek kunnen bedrijven vaak niet de volledige waarde van de investering in opleiding toe-eigenen, waardoor er maatschappelijk gezien ondergeïnvesteerd wordt in opleiding.

Gebruikt men het perspectief van **systeemfalen** om naar dit probleem en bijbehorende legitimatie voor overheidsinterventie te kijken, dan wordt vaak de *'capability failure'* genoemd. Het gaat hierbij om het ontbreken van kennis/vaardigheden die actoren nodig hebben om effectief mee te kunnen doen in een markt of systeem. In deze situatie zijn er niet de juiste (hoeveelheid) *'capabilities'* om de sector optimaal te laten ontwikkelen.

Tot slot is er het perspectief van **transformatiefalen**. Hoewel dat nog minder onderzocht is, zou in deze context gesteld kunnen worden dat er mogelijk sprake is van zogenaamd *'directionality failure'*: gebrek aan eenduidige richting in het laten cumuleren van veranderingen. Door expliciet als overheid te sturen op een digitale transitie waarin cybersecurity een integrale rol speelt kan deze 'stip op de horizon' helpen alle neuzen in dezelfde richting te krijgen. Allerlei spelers in het ecosysteem, waaronder onderwijsinstellingen, bedrijven, overheden en burgers, kunnen hun activiteiten aanpassen aan de gezamenlijke (grotere) doelstellingen. Op dit vlak zijn er verschillende geluiden. Enerzijds wordt er hard gewerkt aan het creëren van een gezamenlijke richting, bijvoorbeeld door de Nationale Cybersecurity Strategie en de NCSA, wat dit falen zou moeten adresseren. Anderzijds wordt er vaker benoemd dat het in Nederland ontbreekt aan centrale regie en richting en dat er sprake is van een hoge mate van versnippering.

Hoewel bovenstaande argumenten binnen de perspectieven van markt-, systeem- en transformatiefalens aanleiding geven om als overheid te interveniëren, geeft het nog niet per se aan in welke richting de overheid zou moeten bewegen. Met de huidige arbeidsmarktkrapte speelt er namelijk nog **een fundamenteler vraagstuk dat de cybersecuritysector overstijgt**: als er in vrijwel alle sectoren sprake is van arbeidsmarktkrapte, hoe bepalen we dan welke krapte 'prioriteit' krijgt? Er is vaak sprake van een *zero-sum-game*. Ter illustratie: op het moment dat de cybersecuritysector een ICT-gediplomeerde aantrekt, zal die persoon inherent niet gaan werken in een andere sector (bijv. software development, AI, financiële sector, overheid, et cetera). En andersom geldt dit natuurlijk net zo. Met name ICT-professionals en professionals met affiniteit voor ICT zijn al jaren schaars. Met andere woorden: afgezien van eventuele additionele arbeidskrachten uit het buitenland vissen we allen in dezelfde vijver. Dit vraagt van de overheid om een bredere visie op human capital te ontwikkelen en uit te dragen. Wanneer iedere sector dit voor zichzelf gaat uitwerken zal er veel energie en middelen 'verloren' gaan aan de onderlinge strijd, want iedereen komt logischerwijs op voor de eigen belangen en achterban. Hoewel dit proces beschouwd zou kunnen worden als een vorm van 'marktwerking' waarbij de sterkste partijen boven komen drijven, is de vraag of dit maatschappelijk wenselijk is. Vanuit een neoklassiek economisch perspectief zou gesteld kunnen worden dat de markt en bijbehorende lonen uit zichzelf naar een passend equilibrium bewegen, wat ook zal betekenen dat productievere banen en/of sectoren vanzelf boven komen drijven. De vraag hier is of dit daadwerkelijk zo is, en of aanverwante maatschappelijke waarden als veiligheid en autonomie hierbij niet het onderspit delven. Hoe dan ook is het waardevol om hier binnen Nederland een gezamenlijke visie op te ontwikkelen en uit te dragen. Zoals eerder aangegeven overstijgt dit het niveau van specifiek de cybersecuritysector, en zal dit ook binnen het Ministerie van Economische Zaken en Klimaat en de Rijksoverheid in brede zin een gezamenlijke inspanning moeten zijn.

5.3.3 Bestaand beleid

In het Actieplan Nederlandse Cybersecuritystrategie worden de volgende activiteiten benoemd om *'Doel 4. De Nederlandse arbeidsmarkt kan voldoen aan de toenemende vraag naar cybersecurity-experts'* te bereiken:

1. Onderwijsinstellingen werken aan bij- en omscholingsprogramma's om de cybersecurity-expertise van werknemers te vergroten. Daartoe werken zij samen met het

bedrijfsleven en andere relevante partijen. Hierbij worden o.a. knelpunten en beperkingen in die samenwerking voortvloeiend uit regelgeving geïnventariseerd en bezien welke oplossingen daarvoor nodig zijn.

2. Er wordt geïnvesteerd in hbo-opleidingen in de bètatechniek, waar cybersecurityopleidingen ook onderdeel van zijn. Middelen worden ingezet op (1) hogere instroom binnen de opleiding, (2) lagere uitval en switch, (3) hogere zijinstroom, (4) inductie/warme overgang van opleiding naar arbeidsmarkt. Het doel van deze maatregel is om de arbeidsmarkttekorten in te perken.
3. Voor een aantal specifieke onderwerpen in het WO wordt vanuit de sectorplannen geïnvesteerd in cybersecurity. Het doel van deze middelen is om samenwerking te stimuleren. Universiteiten maken per sector/domein een analyse waarin zij de kansen en knelpunten op het gebied van onderzoek en onderwijs in kaart brengen, en maatregelen voorstellen om hierop in te spelen. In het ingediende sectorplan Techniek wordt ook aandacht besteed aan cybersecurity. Via deze weg zullen ook de universitaire cybersecurity-opleidingen profiteren.
4. De kwalitatieve en kwantitatieve tekorten op de cybersecurityarbeidsmarkt worden onderzocht, inclusief aanbevelingen hoe deze tekorten aan te pakken.
5. Verkend wordt of de initiatieven voor inzicht in ICT-brede tekorten en de ontwikkeling van een onderwijs- en arbeidsmarktdashboard ICT ook voldoende inzicht bieden in regionale tekorten van cybersecurity-specialisten.
6. Het kabinet zet zich via de *Human Capital Agenda ICT* in om de instroom van cybersecurityspecialisten en ICT-specialisten te vergroten en de kwaliteit van de instroom te beïnvloeden. Dit wordt in nauwe samenwerking met het bedrijfsleven, regionale en lokale overheidsinstellingen en onderwijsinstellingen opgepakt.
7. Via thematische routekaarten en communities worden gesprekken gefaciliteerd tussen kennisinstellingen en het bedrijfsleven met betrekking tot de high-end kennisontwikkeling die nodig is om innovatieve productontwikkeling tot stand te brengen.

Deze activiteiten beslaan een grote variëteit aan onderliggende acties, en hebben betrekking op de inspanningen van een grote set aan betrokken actoren. Expliciet genoemde actoren binnen het actieplan zijn onder meer OCW, EZK, J&V, SZW, BZK, universiteiten, hogescholen, MBO-instellingen, werkgevers, CBS, en Dcypher.

Daarnaast wordt ook in aanpalende contexten aan het vraagstuk gewerkt, onder meer via het masterplan basisvaardigheden waar een focus is op digitale geletterdheid.

Een belangrijke conclusie is dat er al veel gebeurt om voldoende kwalitatief geschoolde professionals te scholen en om- of bij te scholen.

5.3.4 Mogelijkheden voor (nieuw) beleid

Met het Actieplan Nederlandse Cybersecuritystrategie wordt een breed pallet aan beleidsinterventies gedekt. Daarbij noemt activiteit [4] expliciet het nader onderzoeken van de tekorten en mogelijke aanbevelingen voor de aanpak hiervan. Het ligt voor de hand om eventuele aanvullende concrete initiatieven te ontplooien naar aanleiding van de resultaten van dat onderzoek. Wij adviseren om in dat onderzoek expliciet rekening te houden met de arbeidsmarktvraagstukken in brede zin c.q. om het vraagstuk op het gebied van cybersecurity als één specifieke manifestatie te zien van een generiek tekort aan menselijk kapitaal.

In lijn met het Actieplan stellen meerdere gesproken experts dat het ook zinvol is om IT eerder en sterker in te bedden in het basis- en voortgezet onderwijs. Wanneer de interesse voor dergelijke thematiek in een vroeg stadium aangewakkerd wordt, is de kans groter dat men later kiest voor een opleiding en beroep in deze sector. Ook in het wetenschappelijk

onderwijs kan meer aandacht voor cyber komen, bijvoorbeeld door het verhogen van het onderzoeksbudget voor cybersecurity. Deze acties zijn in gang gezet, maar in de perceptie van de gesproken experts mogelijk nog niet voldoende en kan het waardevol zijn om dit punt op de agenda te houden.

Aanvullend op het uitvoerige Actieplan stellen we voor om cybersecuritysector-overstijgend, en zelfs ICT-sector overstijgend, na te denken over hoe deze sector zich verhoudt tot andere sectoren met arbeidsmarktkrapte. Hoe prioriteren we verschillende werkzaamheden, functies, organisaties of sectoren? Hoe verhoudt de cybersecuritysector zich bijvoorbeeld tot de ICT-sector in brede zin, de zorg, het onderwijs, de installatietechniek of de AI-sector? Welke criteria hanteren we om keuzes en processen vorm te geven? Dit past ook goed binnen de opmerking vanuit verschillende respondenten dat er binnen de Nederlandse overheid beperkt sprake is van onderling afgestemd beleid.

In lijn hiermee zou het Ministerie van Economische Zaken en Klimaat en het Rijk in brede zin ook kunnen nadenken over het dynamisch laten aansluiten van generiek opleidingsinstrumentarium bij actuele behoeften op de arbeidsmarkt. Binnen een instrument zoals het STAP-budget zou bijvoorbeeld gedifferentieerd kunnen worden tussen opleidingen in de hoogte van het beschikbare budget naargelang de competenties en/of functies in kwestie aansluiten bij bestaande arbeidsmarktkrapte. Dit mechanisme zou onder andere gericht kunnen worden op benodigde competenties voor cybersecurityprofessionals, maar ook op andere functies met krapte zoals specifieke functies in de energie, installatietechniek, software development, zorg of vervoer.

Naast het vraagstuk 'in welke sectoren/beroepen' het schaarse menselijk kapitaal (bij voorkeur) moet gaan werken, is een tweede element hoe de bijbehorende opleidingen en curricula zich zo goed mogelijk kunnen blijven aanpassen aan de behoeften op de arbeidsmarkt. Hier is flexibiliteit benodigd en is contact met de arbeidsmarkt (bijv. via bestaande PPS'en) essentieel. Hier wordt al flink aan gewerkt, ook op het gebied van ICT in brede zin, en het is zinvol om die lijn door te zetten.

Tot slot wordt vaak genoemd dat cybersecurity in feite niet (alleen) een losstaand thema is, maar dat het verweven is met vrijwel alles dat een digitale component heeft. En vrijwel alles heeft tegenwoordig een digitale component. Dat betekent dat in de werving, naamsbekendheid, en activiteiten nóg meer aansluiting gezocht zou kunnen worden bij lopende initiatieven. Dit kan variëren van het borgen van cybersecurity bij allerhande Groeifondsvoorstellen tot het borgen van cybersecurity in lerarenopleidingen. Hoewel indirect, kunnen dergelijke inspanningen de sector mogelijk nog zichtbaarder en aantrekkelijker maken.

5.4 Voorkomen dat veelbelovende bedrijven in buitenlandse handen vallen

5.4.1 Aanknopingspunt voor beleid

In hoofdstuk 4 hebben we als een van de bedreigingen genoemd dat bedrijven die schaalbaar en veelbelovend zijn beperkte mogelijkheden hebben om met Nederlands durfkapitaal als Nederlands bedrijf op te schalen en internationaal de vleugels uit te slaan. Juist de briljante bedrijven die toch de eerste stappen maken, worden in de praktijk vaak snel overgenomen door buitenlandse partijen. Naar dit soort overnames kunnen we kijken vanuit een economisch perspectief, maar ook vanuit een perspectief dat vooral om veiligheid en geopolitiek draait.

Vanuit **economisch perspectief** willen we waar mogelijk een sterke kennisbasis ook internationaal kunnen vermarkten, hebben we baat bij export van, in dit geval,

cybersecuritybedrijvigheid en zijn we geïnteresseerd in een sterke cybersecuritysector die integrators en gebruikers van producten en diensten kan ondersteunen om cybersecurity te integreren in hun bedrijfsvoering. Binnen het economisch perspectief kennen we het smalle sectorbelang en de brede economisch belang. Vanuit het smalle sectorbelang beschikken we graag over internationaal competitieve bedrijven die cybersecurityservices, soft- en hardware internationaal vermarkten en sterk doorgroeien. Vanuit het bredere economische belang willen we kunnen over beschikken over *state of the art* cybersecurity dienstverleners, soft- en hardware producenten en leveranciers en doet hun herkomst er wellicht minder toe. Het beeld dat we eerder van de cybersecuritysector in smalle zin schetsten is er een van weliswaar een sterke kennisbasis, maar ook een van beperkte export en dominantie van buitenlandse big tech bedrijven en leveranciers van services, soft- en hardware. De Nederlandse partijen zijn, enkele uitzonderingen daargelaten, sterk gefocust op het bedienen van de nationale markt en behoren overwegend tot het mkb.

Vanuit een **geopolitiek en veiligheidsperspectief** wordt deels anders gekeken. Vanuit dit perspectief willen we enerzijds risicovolle afhankelijkheden voorkomen en anderzijds voorkomen dat strategische kennis van onder andere cybersecurity weglekt naar buitenlandse partijen. Het is niet voor niets dat delen van de cybersecuritymarkten feitelijk nationale (captive) markten zijn, simpelweg omdat men (1) vindt dat essentiële kennis niet in handen mag komen van buitenlandse mogendheden en (2) geen afhankelijkheid wil van buitenlandse partijen. Vanuit dit perspectief is het belangrijk juist op het vlak van cybersecurity niet te sterk afhankelijk te zijn van het buitenland en strategisch autonoom te zijn. Cybersecurity als sector wordt dan, zeker waar het unieke kennis betreft, een strategische industriële sector die anders behandeld moet worden dan andere sectoren en waar bijvoorbeeld veiligheid en autonomie boven economisch voordeel zouden kunnen gaan. Daarbij moet aangetekend worden dat: (1) niet alle kennis en economische bedrijvigheid als even strategisch moet worden beschouwd (een hoogwaardig kwantumtechnologiebedrijf wordt anders beoordeeld dan een meer standaard cybersecuritydienstverlener die bestaande oplossingen die in de markt beschikbaar zijn toepast bij klanten) en (2) vanuit veiligheidsperspectief niet per se Nederland, maar wellicht ook Europa het uitgangspunt kan zijn.

5.4.2 Legitimering overheidsingrijpen

Is het actief tegengaan dat Nederlandse cybersecurityparelтjes in handen vallen van buitenlandse partijen gelegitimeerd vanuit markt-, systeem- en transformatieperspectief? Er zijn naar ons idee diverse markt-, systeem- als transformatiefalen die het voorstelbaar maken dat, breder getrokken, een specifiek strategisch industriebeleid gericht op de ontwikkeling en bescherming van de cybersecuritysector wordt vormgegeven.

Vanuit het perspectief van **marktfalen** is het belangrijk dat de cybersecuritysector kenmerken heeft van een publiek goed. Een goede functionerende cybersecuritymarkt komt iedereen ten goede en is wellicht het beste te organiseren op systeemniveau waarbij geldt dat bij voorkeur iedereen er toegang toe heeft. De consumptie van cybersecurity door het ene bedrijf, organisatie of burger gaat niet ten koste van de anderen. Deels geldt dat niet-betalers soms moeilijk zijn uit te sluiten van de consumptie ervan (niet uitsluitbaar), hoewel goederen en diensten met een hogere ingebouwde cybersecurity ook gewoon hoger geprijsd kunnen worden. Vanuit strategische overwegingen geldt dat afhankelijkheid van een of enkele (buitenlandse) partijen met een grote marktmacht ook een reden kan zijn te interveniëren. Mogelijk geldt ook dat marktpartijen (vooral gebruikers) de waarde van voldoende investeringen in cybersecurity onvoldoende kunnen overzien of beoordelen (waardoor ze mogelijk onderinvesteren in cybersecurity). Dit laatste hangt uiteraard samen met onvoldoende bewustzijn bij gebruikers (zie §5.5).

Vanuit het perspectief van **systeemfalen** speelt mogelijk *infrastructural failures* een rol. Cybersecurity heeft kenmerken van een essentiële infrastructuur en het is aannemelijk dat deze niet zonder overheidsingrijpen voldoende tot stand komt. Ook het bestaan van onvoldoende afstemming in het systeem over hoe de essentiële cybersecurityinfrastructuur tot stand komt (*interactional failure*), legitimeert mogelijk overheidsingrijpen.

Tot slot kan er ook vanuit het perspectief van **transformatiefalen** aanleiding zijn te interveniëren. Het is opmerkelijk dat er een uitgebreide Nederlandse Cybersecuritystrategie tot stand is gekomen met een uitgebreid actieplan, maar dat de industriepolitieke component daar niet of nauwelijks onderdeel van uitmaakt. Dit wijst mogelijk op een gebrekkige afstemming tussen beleidsprikkels (*directionality failure*). Dit kan mogelijk de transitie belemmeren naar een markt en samenleving waarin voldoende wordt geïnvesteerd in cybersecurity en het scenario waarin er een Nederlandse/Europese cybersecurityindustrie voorhanden is die kan voorzien in cybersecurityoplossingen.

Vanuit het perspectief van verschillende falens is er tenminste aanleiding te bezien of er niet meer systematisch aandacht moet worden geschonken aan een specifiek strategisch industriebeleid voor cybersecurity. In zekere zin gaat het om een sector die net als bijvoorbeeld de defensie-industrie en in zekere zin de ruimtevaart specifieke kenmerken heeft waardoor het niet als een willekeurige economische sector kan worden behandeld.

5.4.3 Bestaand beleid

Er is geen sprake van een significant bestaand specifiek beleid noch vanuit economisch perspectief om actoren in de cybersecuritysector te beschermen of specifiek te stimuleren. Wel is in opdracht van NCTV onderzocht in welke mate de nationale veiligheid kan worden geschaad als gevolg van overnames door buitenlandse partijen[179], maar dit draaide primair om veiligheidsvraagstukken. Wel is er de afgelopen jaren door de toenemende geopolitieke spanningen, de noodzaak van verduurzaming en de verstoring van complexe internationale waardeketens (gebaseerd op ver doorgevoerde toelevering- en uitbesteding) sprake van een herwaardering van actieve industriepolitiek. Zo heeft de Adviesraad Internationale Vraagstukken (AIV) in maart 2022 een advies over slimme industriepolitiek[180] opgesteld waar expliciet gesproken wordt over overheden die ingrijpen in de markt met stimulansen en investeringen voor bijvoorbeeld specifieke bedrijfstakken of ecosystemen (verticale industriepolitiek), juist ook om strategische sectoren te beschermen c.q. te stimuleren. Daarbij speelt ook de vraag wat op Nederlandse schaal en wat op Europese schaal gedaan kan worden. De EU heeft ook een flinke duw gegeven aan het industriebeleid getuige bijvoorbeeld de European Chips Act en subsidiering om een versnelling aan te brengen in de verduurzaming van de industrie. In Nederland is dit recent duidelijk naar voren gebracht in de Kamerbrief strategisch en groen industriebeleid.[181] Hierin wordt expliciet ingegaan op zaken als economische veiligheid en open strategische autonomie en worden beschermings- en stimuleringsmaatregelen genoemd die mogelijk ook in relatie tot de cybersecuritysector kunnen worden ingezet, bijvoorbeeld (niet uitputtend):

- Wetgeving om ongewenste overnames te voorkomen. De Wet Veiligheidstoets investeringen fusies en overnames (Wet vifo) is vorig jaar mei aangenomen en zal

[179] Zie https://repository.wodc.nl/bitstream/handle/20.500.12832/2217/2609_Volledige_Tekst_tcm28-250320.pdf?sequence=2&isAllowed=y

[180] Zie https://www.adviesraadinternationalevraagstukken.nl/documenten/publicaties/2022/03/18/slimme-industriepolitiek

[181] Zie https://www.rijksoverheid.nl/documenten/kamerstukken/2022/07/08/het-verschil-maken-met-strategisch-en-groen-industriebeleid

naar verwachting op 1 juni in werking treden. Vooralsnog staan in de reikwijdte van de wet bedrijven die actief zijn op de volgende sensitieve technologieën: dual-use en militaire goederenlijst (exportcontrolelijsten), quantum, semicon, fotonica en high-assurance producten (cryptografie). Indien cybersecuritytechnologie onder één van deze categorieën valt, geldt de Wet vifo ook daarvoor.

- Strafbaarstelling van o.a. spionage gericht op (digitale) diefstal van technologie.
- Het gericht versterken van sectoren en waardeketens. Hier wordt onder andere gesproken over een hernieuwde aanpak voor de sleuteltechnologieën die meer focust op het gedachtengoed van open strategische autonomie.
- Ontwikkelen van een geo-economische monitor om een beter inzicht te verkrijgen in strategische afhankelijkheden van Nederland wat betreft kennis, goederen en diensten.
- Het toegang houden tot cruciale technologieën en toepassingen en strategische dialoog met EU en internationale partners over sensitieve industrie en wederzijdse afhankelijkheden.

In de Kamerbrief[182] (p. 30) wordt aangegeven dat er geen geoormerkte investeringen in open strategische autonomie zijn, maar worden wel diverse opties genoemd bijvoorbeeld investeringen via het Nationale Groeifonds of het *Deep Tech Fund* (via Invest-NL), de participatie in IPCEIs, via ruimtevaartbeleid, EU-defensiefonds, en middelen in het KIC. Ook vanuit het ministerie van Defensie zijn potentiële instrumenten voor "open strategische autonomie" beschikbaar.[183] Kortom, binnen het innovatie-instrumentarium van het Ministerie van Economische Zaken en Klimaat (en uiteraard ook van Defensie) ontstaat duidelijk meer aandacht voor veiligheid en strategische toegang tot cruciale technologieën. Gegeven bovenstaande is het opmerkelijk dat in het in oktober 2022 gepubliceerde Actieplan Nederlandse Cybersecuritystrategie 2022-2028 in geen van de vier pijlers aandacht is voor industriepolitieke overwegingen en acties die mogelijk gewenst zijn om bijvoorbeeld strategisch belangrijke cybersecuritykennis voor Nederland te behouden of ruimer toegang tot cruciale cybertechnologie en toepassingen zeker te stellen. De industriepolitieke component van cybersecurity komt in het actieplan niet expliciet aan de orde.

5.4.4 Mogelijkheden voor (nieuw) beleid

Het voorkomen dat veelbelovende cybersecuritybedrijven overgenomen worden door buitenlandse ondernemingen is een heel specifiek industriepolitiekvraagstuk. Moet bijvoorbeeld specifiek de sterkte van Nederland op kwantum niet beter worden beschermd, omdat juist de komst van kwantumcomputers de hele sector van cybersecurity op zijn kop kan zetten? In de interviews is onder andere genoemd dat de dreiging reëel is dat nu al data geoogst wordt die over bijvoorbeeld tien jaar met kwantumcomputers ontsleuteld kan worden.

Het beschermen van de parels onder de Nederlandse cybersecuritybedrijven is onderdeel van de ruimere vraag in hoeverre de Nederlandse overheid mede vorm zou moet geven aan de wijze waarop de Nederlandse cybersecuritysector zich ontwikkelt. Juist omdat cybersecurity zo'n belangrijke randvoorwaarde is voor het laten functioneren van bedrijven,

---

[182] Zie https://www.rijksoverheid.nl/documenten/kamerstukken/2022/07/08/het-verschil-maken-met-strategisch-en-groen-industriebeleid

[183] Zie bijvoorbeeld de Nota Defensie Industrie Strategie (2018) waarin door het Ministerie van Defensie is aangegeven dat (zie paragraaf 4.2) kritisch gekeken wordt naar fusies en overnames in vitale sectoren (waaronder Defensie gerelateerde sectoren). Er worden daartoe onder andere ex-ante analyses uitgevoerd in hoeverre beschermende maatregelen tegen ongewenste overnames en investeringen moeten worden genomen (https://open.overheid.nl/repository/ronl-77d21fe6-49b4-4d0d-ad98-ae5442e20bc5/1/pdf/Nota%20Defensie%20Industrie%20Strategie.pdf)

organisaties en uiteindelijk economieën, samenlevingen en staten is het redelijk om dit niet als een reguliere sector te beschouwen. Is het niet een dermate centrale sector dat een **specifieke industriestrategie of sectoraal industriebeleid** op zijn plaats is? Het voorkomen dat kansrijke scale-ups worden overgenomen door buitenlandse investeerders is dan slechts één van de vragen waarop mogelijk specifiek beleid gewenst is.

Dit dossier is complex, raakt aan andere dossiers en kent ook een meer generiek karakter in termen van de omgang met strategische producten, diensten en bedrijvigheid. Hoewel wij op basis van (dit) onderzoek geen antwoorden kunnen geven op primair politiek geladen vraagstukken, identificeren we wel de volgende vragen die relevant zijn voor de politieke en bestuurlijke discussie:

- Moet er op cybersecuritytechnologie die strategisch van grote waarde is niet simpelweg een exportverbod komen en voor de bedrijven die deze kennis ontwikkelen en toepassen in producten en diensten een beschermingsbeleid waardoor ze niet zondermeer door elke partij overgenomen kunnen worden (het tegengaan van ongewenst overnames)? Momenteel spelen dergelijke vraagstukken ook in de casus van ASML. Naast specifieke exportverboden zou de overheid ook een aandeel kunnen nemen in het kapitaal van betreffende strategische ondernemingen.
- Hoe groot is het probleem van strategische cybersecuritykennis die in buitenlandse handel valt eigenlijk? Tot zover is de bewijsvoering vooral anekdotisch. In hoeverre komt in Nederland ontwikkelde cybersecuritykennis ook op andere manieren in het buitenland terecht (bijvoorbeeld door internationale mobiliteit van experts)?
- Moet er niet meer groeigeld voor cybersecuritystarters en scale-ups beschikbaar komen als dit type bedrijven voor het verder schalen kennelijk makkelijker in het buitenland terecht kan?
- Zijn er voldoende kennis- en innovatieprojecten in Nederland die een voldoende voedingsbodem zijn voor het genereren van *top of the bill* cybersecuritykennis? Zou de Nederlandse cybersecuritycommunity (kennisinstellingen, bedrijven, belangrijke afnemende partijen) gebaat zijn bij enkele grootschalige kennis- en innovatieprojecten, bijvoorbeeld een Groeifondsproject dat expliciet gericht is op cybersecurity?
- Moet het inkoopbeleid van de overheid op het gebied van cybersecurity aangepast worden? De overheid heeft al inkooprichtlijnen geformuleerd, onder andere in de NLCS en de DVHS. Tegelijkertijd komt in de interviews herhaaldelijk naar voren dat de overheid als launching customer een grotere rol kan spelen in deze markt.
- Hoe gaan we om met de ontwikkelingen in/rondom de Europese federatieve data- en cloudinfrastructuur Gaia-X?[184]

Bij het ontwikkelen van dergelijk beleid moet ook rekening worden gehouden met de prikkels die toekomstige startups krijgen. Eén van de redenen dat ambitieuze ondernemers beginnen met een startup, is de optie om hun aandelen later voor veel geld te kunnen verkopen. Als dit niet meer mogelijk is, dan lopen we een kans dat er minder (succesvolle) startups in Nederland komen. Onze ambitieuze ondernemers vertrekken dan wellicht naar andere landen om hier een startup te beginnen.

[184] Toelichting Gaia-X: https://gaia-x.nl/

5.5 Versterken van bewustzijn bij gebruikers

5.5.1 Aanknopingspunt voor beleid

Het implementeren van de juiste maatregelen om als organisatie en de economie als geheel cyberweerbaar te werken, begint bij voldoende bewustzijn over de thematiek. Het gaat dan zowel om [1] bewustzijn van de risico's op het gebied van cyberveiligheid als om [2] bewustzijn van gepaste maatregelen en de wijze waarop deze geïmplementeerd kunnen of moeten worden. (Potentiële) gebruikers van cybersecurityproducten en -diensten zijn zich van bovenstaande niet altijd even bewust, wat ook blijkt uit de enquête en interviews binnen dit onderzoek. Het kan bijvoorbeeld concreet gaan om het onderschatten van de risico's (zowel de kans dat men wordt aangevallen als de impact daarvan) en de daarbij behorende lage betalingsbereidheid voor het verhogen van het cyberveiligheidsniveau, of om het niet weten wie binnen de organisatie exact welke stappen moet ondernemen.

Er is daarmee sprake van een latente vraag. Zouden deze gebruikers immers wél bewust zijn van alle risico's en mogelijke maatregelen, dan zou de vraag naar verwante cybersecurityproducten en -diensten toenemen, zou de cybersecuritysector (verder) groeien en zouden cyberrisico's effectiever afgewend worden. Althans, dat is de redeneerlijn die door veel experts gevolgd wordt. Het bewust maken van de vraagzijde van de markt is daarmee een belangrijke factor bij de ontwikkeling van de sector.

Belangrijk bij het onderwerp 'bewustzijn' is om dit concept niet als een binair concept te beschouwen (c.q. je bent wel of niet bewust), maar als een glijdende schaal. Bij lage mate van bewustzijn gaat het met name om het bewustzijn *dat* men iets met cybersecurity moet doen; bij hogere mate van bewustzijn is het 'dat' getackeld, en gaat het er primair om wat je dan exact zou moeten doen. Cybersecurity is een veelkoppig monster dat ook nog eens continu in ontwikkeling is, dus het is geen sinecure om continu (voldoende) bewust te zijn en te blijven.

5.5.2 Legitimering overheidsingrijpen

Het interveniëren als overheid op het beperkte 'cyberbewustzijn' van gebruikers kan zowel vanuit het perspectief van markt-, systeem- als transformatiefalen gelegitimeerd worden.

Vanuit het perspectief van **marktfalen** is belangrijk dat er sprake is van een informatiegebrek (en informatieasymmetrie). Doordat gebruikers niet voldoende informatie hebben over het onderwerp, zijn zij niet in staat hun (latente) vraag te articuleren en komen (wenselijke) transacties in de markt niet tot stand. Gebruikers kunnen als het ware niet voldoende effectief met hun 'eigen boodschappenlijstje' de markt op.

Vanuit het perspectief van **systeemfalen** speelt de *'capability failure'* een prominente rol: het ontbreekt aan ontwikkelingen van kennis/vaardigheden die actoren nodig hebben om effectief mee te kunnen doen in een markt of systeem.

Tot slot kan er ook vanuit het, relatief nieuwe, perspectief van **transformatiefalen** naar deze problematiek gekeken worden. Allereerst is er sprake van het falen van de vraagarticulatie. Afwezigheid van vraag naar de resultaten van een transitie, in dit geval cyberveiligheid en cyberweerbaarheid binnen een bredere digitale transitie, voorkomt optimale totstandkoming. Daarnaast is er in deze context ook (in zekere mate) sprake van een zogenaamd beleidscoördinatiefalen; er is sprake van gebrekkige afstemming tussen beleidsprikkels die een transitie dienen te bevorderen. Het risico hierop is groot wanneer veel verschillende partijen met eigen interventies aan de slag gaan; een fenomeen dat op dit thema zeker aanwezig is.

5.5.3 Bestaand beleid

Er bestaat al veel beleid om het bewustzijn bij gebruikers te versterken. Bewustzijn is daarbij ook een belangrijk onderdeel van Pijler 1 binnen de Nationale Cybersecurity Strategie.

Er zijn veel verschillende initiatieven, op zowel landelijk, regionaal als lokaal niveau. Denk bijvoorbeeld aan het ontwikkelen van nieuwe producten en diensten met onder andere aandacht voor inbedding van cybersecurity in het risicomanagementproces, crisispreparatie, incidentrespons en thematische advisering (NCSC en DTC), de MKB-werkplaatsen Digitalisering, een MKB Cybercampus of diverse voorlichtingscampagnes. Uit een recente 'Regioscan Digitalisering MKB', uitgevoerd in samenwerking met EZK en alle provincies komen *tientallen* (regionale) initiatieven naar voren die zich bezighouden met bewustwording bij het MKB. Het gaat dan om een divers palet aan typen beleidsinspanningen, variërend van (zelf)scans tot aan informatiesessies en aanpassingen in curricula en bijscholingsmodules.

Gezien de omvang en diversiteit in het bestaande beleid wordt breed erkend dat voldoende regie en coördinatie waardevol is voor de effectieve inzet van alle maatregelen. Hiertoe zijn ook al de nodige inspanningen gemaakt, niet in de laatste plaats door de ontwikkeling en implementatie van de NLCS. Een belangrijk element van de NLCS is om versnippering tegen te gaan en de bestaande en nieuwe inspanningen goed te coördineren. Dit neemt niet weg dat mensen in de praktijk inspanningen nog steeds als versnipperd kunnen percipiëren.

5.5.4 Mogelijkheden voor (nieuw) beleid

Zoals de vorige sectie laat zien gebeurt er al ontzettend veel op dit vlak. Een criticus zou zelfs kunnen beargumenteren dat er (op punten) te veel gebeurt. Het groot aantal initiatieven leidt regelmatig tot een gevoel van 'door de bomen het bos niet meer zien' en 'versnippering van overheidsbeleid'. Het enerzijds op peil houden van de inhoudelijke lijn (waar moet men bewust van zijn) en anderzijds het gestroomlijnd inrichten van het ecosysteem (de manieren waarop de kennis tot mensen en organisaties komt) vraagt om een strakke en goed gecoördineerde aanpak. **Met (o.a.) de NLCS wordt deze gewenste coordinatie vormgegeven**. Verschillende partijen in het ecosysteem zoals diverse departementen, brancheorganisaties en regionale stakeholders hebben daarmee de handen ineengeslagen om de 'gebruikers' cyberweerbaar te maken en te houden, en er lijkt nog winst mogelijk om deze inspanningen gezamenlijk nog effectiever vorm te geven. Aangezien de NLCS nog niet heel lang bestaat is het niet ondenkbaar dat men in de praktijk de stroomlijning nog niet volledig ervaart, maar belangrijk is dat er stappen worden gezet om het diverse beleid strakker te coördineren.

Gezien de diversiteit aan huidige beleidsinspanningen zouden we daarom niet willen adviseren om nóg (veel) meer nieuwe initiatieven te ontplooien, maar om verder te gaan met het stroomlijnen van datgeen er al gebeurt. Met name voor (klein) mkb kan het huidige ecosysteem zodanig gelaagd zijn dat (latente) behoeften op het gebied van cybersecurity niet vervuld worden. Het zinvol gebruiken van de landelijke schaal om bijvoorbeeld informatieproducten gezamenlijk te creëren en het gebruik van regionale en lokale structuren om organisaties effectief te bereiken lijkt voor de hand te liggen. Dit vraagt om een goede afstemming tussen spelers in het ecosysteem: wie doet wat exact en hoe maken we slim gebruik van elkaars competenties, netwerken en inspanningen?

In één interview wordt verder aangegeven dat veel bewustwordingscampagnes niet goed ontworpen worden en er te hoge verwachtingen van zijn. Ook in de literatuur komt dit punt

vrij sterk naar voren.[185] Meta studies laten zien dat slechts 8% van de doelgroep ook daadwerkelijk gedrag verandert en dat deze gedragsverandering niet altijd duurzaam is.[186] Hier kan de overheid een nadere (coördinerende) rol in oppakken. Naast deze bewustwording zou ook actiever gestuurd kunnen worden op beleid gericht op 'basisveiligheid' (bijvoorbeeld eisen rondom updates van Microsoft/iOS/Android, 2FA, automatische updates, etc.). Experts geven aan dat een coördinerende rol van de overheid ook essentieel is voor het beschermen van bedrijven, mogelijk in samenwerking met partijen als de inlichtingendienst en de nieuwe brancheverenigingen Cyberveilig Nederland. Tot slot dient de overheid in brede zin ook zelf aan de eigen cyberrichtlijnen te voldoen, wat nu nog niet altijd en overal het geval is.

5.6 Overige beleidsopties

Naast de bovenstaande beleidsopties zijn er tijdens het onderzoek meer relevante beleidsopties naar voren gekomen. Dit komt vooral voort uit de interviews en onze integrale analyse van de data. Deze willen we ook nog kort voor het voetlicht brengen.

- De enige positie in dit domein waarin Nederland echt een unieke positie heeft, is het vestigen van internationale organisaties (en NGO's) op het gebied van vrede en veiligheid (in de Den Haag) in het digitale domein. Het lijkt ons verstandig om hier actief op in te (blijven) zetten aangezien deze vestigingen waardevol voor de lokale economie kunnen zijn, zie 4.1.5.
- Aansluitend op de kans dat Nederland goed is in de integratie van alfa-, bèta- en gammawetenschappen, is in verschillende gesprekken benoemd dat Nederland een goede positie heeft als het gaat om IT-auditors. Er is sprake van een goede georganiseerde sector en met een beroepsorganisatie.[187] Bovendien is er een post-master opleiding: IT-auditing.[188]
- Een punt dat we verschillende keren zijn tegengekomen is het delen van *threat intel* (informatie over dreigingen). In Nederland is er een cultuur van (publiek-private) samenwerking en een marktstructuur zonder grote partijen waardoor onderling delen goed van de grond kan komen en georganiseerd kan worden/blijven. De overheid zou een trekkende rol hierin kunnen nemen en partijen bij elkaar kunnen brengen. Dit sluit aan bij in het delen van dreigingsinformatie binnen pijler 1 van de NLCS, en is gerelateerd aan onder meer de integratie van het DTC. Aansluiting bij CTI-initiatieven vanuit Europa (bijv. vanuit ECSO) lijkt waardevol.

[185] https://omooc.nl/wp-content/uploads/2016/11/Gedragsverandering-via-campagnes-MOOC-Slim-beleid-2016.pdf

[186] https://pubmed.ncbi.nlm.nih.gov/14960405/

[187] https://www.norea.nl/mission-statement

[188] https://www.eur.nl/esaa/postinitiele-opleidingen/it-auditing-advisory

6 Conclusies

In hoofdstuk 6 worden de onderzoeksvragen systematisch beantwoord aan de hand van de drie hoofdvragen. Hieronder wordt de kern van de antwoorden gegeven; voor een meer gedetailleerd antwoord verwijzen we u door naar het volledige hoofdstuk 6.

Hoofdvraag 1: wat is op dit moment het economisch verdienvermogen van Nederland op het gebied van cybersecurity? In 2021 kent de Nederlandse cybersecuritysector een geschatte omzet van circa 16 miljard euro en een werknemersaantal van circa 94.600. De toegevoegde waarde ligt rond de 7,5 miljard euro, wat overeenkomt met 0,94% van het BBP. Naast het verdienvermogen van de sector zelf (producenten cyberproducten en -diensten) is cybersecurity voor cyber integrators, partijen een schakel verder in de keten, een belangrijke randvoorwaarde die ook als competitief voordeel kan dienen. Voor uiteindelijke gebruikers van cybersecurityproducten en -diensten is het puur randvoorwaardelijk. Het economisch belang voor deze spelers later/laat in de keten is kwalitatief beschreven, maar is moeilijk te kwantificeren.

Hoofdvraag 2: wat is het potentieel van de cybersecuritysector? Welke toekomstige trends op het gebied van cybersecurity zullen naar verwachting effect hebben op het verdienvermogen? Er zijn diverse trends geïdentificeerd, waarbij de volgende vijf de meest prominente zijn: [1] sterke groei van de sector zelf, [2] de doorzettende ontwikkeling van AI, [3] de introductie van NIS2 en CRA, [4] de overname van potentievolle cybersecuritybedrijven door externe partijen, en [5] tekorten op de arbeidsmarkt. Trends [1], [2] en [3] hebben een positief effect op het toekomstig verdienvermogen van de sector. Trends [4] en [5] hebben een negatieve of remmende werking op het verdienvermogen.

Hoofdvraag 3: wat kan de overheid doen om bovengenoemd economisch potentieel te realiseren? De overheid heeft al veel beleid ontwikkeld om knelpunten waar de sector mee te maken heeft te adresseren. Het goed stroomlijnen van al het beleid dat reeds bestaat is een hoge prioriteit. Met de NLCS wordt hier al stevig aan gewerkt, en het beeld dat in dit onderzoek naar voren komt is dat die lijn doorgezet mag en zelfs moet worden. Daarnaast worden op vier concrete aanknopingspunten voor beleid suggesties gedaan voor eventueel aanvullende inspanningen. Een overkoepelende observatie is dat voor diverse onderwerpen, zoals arbeidsmarkt en buitenlandse overnames, men deze op een cybersecuritysector-overstijgende wijze zou moeten aanvliegen. De fundamentele onderliggende problemen zijn vaak immers niet specifiek voor deze sector, en een integrale visie en aanpak kan hier waardevol zijn. Hoewel dit laatste op onderdelen al gebeurt, kunnen hier nog verdere stappen gezet worden.

In dit slothoofdstuk sluiten we het rapport op concluderende wijze af door systematisch de onderzoeksvragen te beantwoorden. We stellen hierbij de drie hoofdvragen centraal, waarbij de deelvragen in de beantwoording meegenomen worden.

6.1 Hoofdvraag 1: wat is op dit moment het economisch verdienvermogen van Nederland op het gebied van cybersecurity?

1. Wat is op dit moment het economisch verdienvermogen van Nederland op het gebied van cybersecurity?
   a. Trek de vergelijking met het SEO-onderzoek in 2016.
   b. Kwantificeer (waar mogelijk): aantal werknemers, omzet, deel van BBP.
   c. Differentieer tussen verdienvermogen en randvoorwaardelijkheid van cybersecurity.

In 2021 kent de Nederlandse cybersecuritysector een geschatte omzet van circa 16 miljard euro en een werknemersaantal van circa 94.600. De toegevoegde waarde ligt rond de 7,5 miljard euro, wat overeenkomt met 0,94% van het BBP. Onderstaande tabel geeft de kwantitatieve inschatting van de sector weer, samen met de cijfers die uit eerder onderzoek van SEO naar voren zijn gekomen.

	Onderzoek SEO		**Onderzoek Dialogic**						
	2010	2014	2015	2016	2017	2018	2019	2020	2021
Omzet (€ mld.)	4,8	7,5	9,4	11,0	12,1	13,5	14,7	16,4	16,0
Toegevoegde waarde (€ mld.) [189]	2,6	4,1	5,5	6,0	6,7	7,0	7,5	7,5	
Aandeel van het BBP[190] (%)	0,41%	0,62%	0,80%	0,85%	0,91%	0,91%	0,92%	0,94%	
Aantal werknemers (x1000)	12	13,5	82,6	108,8	93,1	86,5	93,8	86,3	94,6

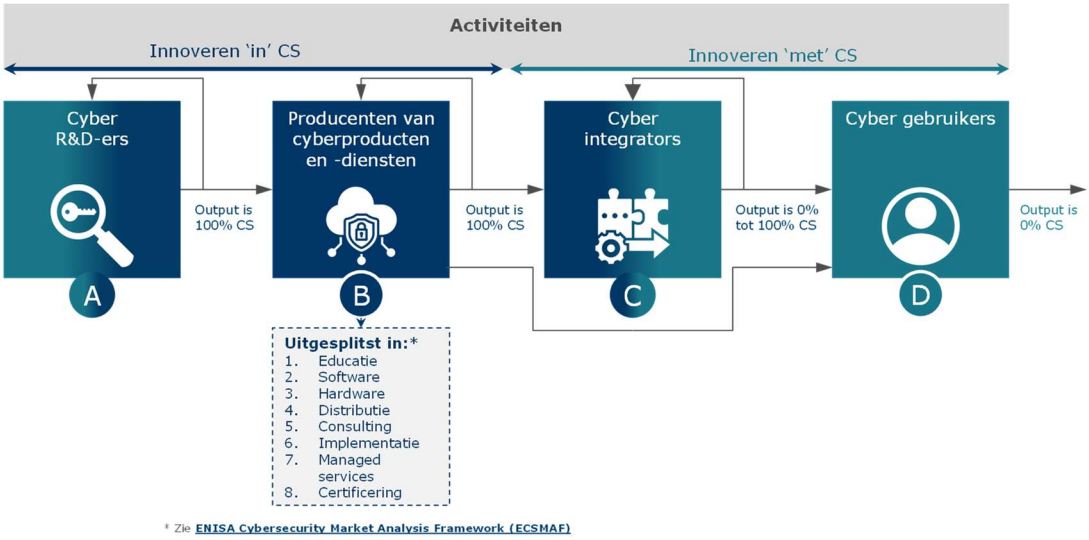
Het eerdere onderzoek van SEO en dit onderzoek hebben verschillende onderzoeksaanpakken gehanteerd, welke ook invloed hebben op de uitkomsten van de analyses. Een belangrijk verschil is dat SEO vanuit de SBI-codes vertrokken is die primair over ICT gaan, terwijl we in dit onderzoek vertrokken zijn vanuit bedrijven die op hun website aangeven bezig te zijn met cybersecurityproducten en/of -diensten. Een belangrijke beperking in de aanpak van het eerdere onderzoek door SEO is dat veel partijen die met cybersecurity bezig zijn niet in de desbetreffende SBI's vallen; in dit onderzoek valt 43% in SBI-code '*J: Informatie en communicatie'*, en hoewel dit de grootste SBI-code is kennen veel cybersecurity-bedrijven een andere SBI. Een belangrijke beperking aan de aanpak in dit onderzoek is dat bedrijven die mogelijk wel iets met cybersecurity doen, maar dat niet expliciet op de website aangeven, buiten beeld vallen. Hoewel beide aanpakken niet waterdicht zijn, zijn ze wel in staat om ons een inschatting te geven van de omvang van de sector. In termen van ordegrootte lijken de twee aanpakken op vergelijkbare uitkomsten te wijzen. Het enige fundamentele verschil zit in het aantal werknemers dat actief is in de sector; SEO komt op een substantieel lager aantal werknemers uit en daarmee ook op een stuk hogere arbeidsproductiviteit (~€300.000

[189] Voor 2021 zijn er geen gegevens over de toegevoegde waarde beschikbaar uit de CBS-microdata.

[190] Bron: [Eurostat]

per werknemer in 2014). In dit onderzoek komen we uit op een gemiddelde arbeidsproductiviteit van circa €90.000 per werknemer. Volgens het CBS was de gemiddelde bruto toegevoegde waarde per werkzaam persoon in 2018 €64.800[191], dus wij vermoeden dat de €90.000 een reëlere schatting is.

Bovenstaande cijfers hebben primair betrekking op de cybersecuritysector in 'nauwe' zin. In dit onderzoek hebben we verschillende typen partijen in de 'cybersecurity-waardeketen' gedefinieerd, zie nogmaals het conceptuele kader hieronder. De cijfers hierboven gaan dus primair over categorie B: de producenten van cyberproducten en -diensten. Dit is te beschouwen als het **directe verdienvermogen**.



Daarnaast zijn er andere spelers in de keten die primair andersoortige producten en diensten produceren, maar waarbij cybersecurity wel geïntegreerd wordt: de 'cyber integrators'. Denk bijvoorbeeld aan de (hoogwaardige) maakindustrie in Nederland. Voor hen is cybersecurity als een sterk relevante '**randvoorwaardelijkheid**' te beschouwen, waarbij goede integratie van cybersecurity ook als competitief voordeel kan dienen. Verderop in de keten zijn er tenslotte de gebruikers van cyberproducten en diensten. Dit zijn partijen waarbij er geen cybersecurity-element in hun output zit, maar die cybersecurity als een pure randvoorwaardelijkheid kunnen beschouwen. Hoe verder we de focus in de keten verleggen richting gebruikers, hoe kleiner de rol van cybersecurity maar ook om hoe meer partijen het gaat. Het bepalen van de rol van cybersecurity voor het verdienvermogen van deze partijen is moeilijk kwantitatief te bepalen, maar kan kwalitatief als belangrijke randvoorwaardelijkheid beschouwd worden.

[191] https://www.cbs.nl/nl-nl/longread/diversen/2021/het-nederlandse-midden-en-kleinbedrijf-europees-vergeleken/4-nederland-heeft-een-relatief-hoge-bruto-toegevoegde-waarde-per-werkzame-persoon

6.2 Hoofdvraag 2: wat is het potentieel van de cybersecuritysector? Welke toekomstige trends op het gebied van cybersecurity zullen naar verwachting effect hebben op het verdienvermogen?

2. Wat is het potentieel van de cybersecuritysector? Welke toekomstige trends op het gebied van cybersecurity zullen naar verwachting effect hebben op het verdienvermogen?

a. Benoem relevante trends.
b. Beschrijf het te verwachten effect op het Nederlandse verdienvermogen.
c. Omschrijf (kwantitatief waar mogelijk) het potentieel op basis van vraag 1.

In dit onderzoek zijn verschillende trends naar voren gekomen, zie ook hoofdstuk 3 en 4. Belangrijke trends zijn:

1. Sterke groei van de sector zelf
2. De doorzettende ontwikkeling van AI
3. De introductie van NIS2 en CRA
4. De overname van potentievolle cybersecuritybedrijven door externe partijen
5. Tekorten op de arbeidsmarkt

De huidige groei van de sector zelf, de doorzettende ontwikkeling van AI, en de introductie van NIS2 en CRA hebben een positief effect op het Nederlandse verdienvermogen. De overnames door externe partijen en de tekorten op de arbeidsmarkt hebben een negatief effect op het verdienvermogen.

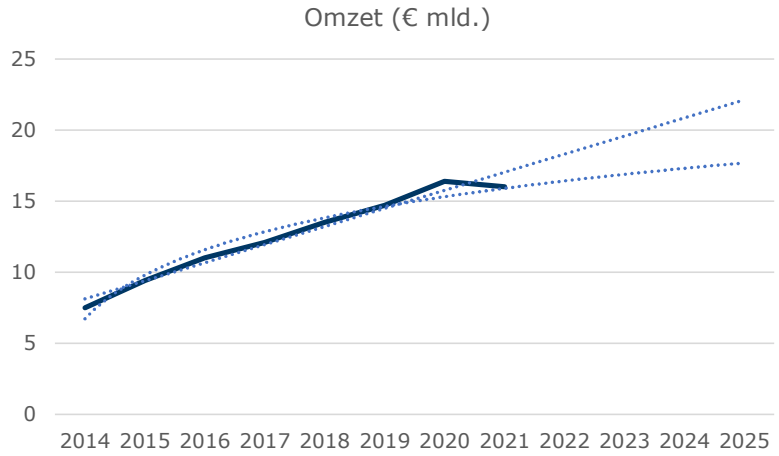
De toenemende mogelijkheden van AI stellen de sector in staat om de arbeidsproductiviteit te verhogen. Zo kunnen bepaalde taken sneller en/of beter uitgevoerd worden door AI op een slimme en verantwoorde wijze in te zetten. Dit geldt voor de 'informatietaken' binnen de sector, waar primair 'informatieverwerkingscompetenties' nodig zijn om de taken goed uit te voeren. Door [1] de toenemende kracht van ICT (informatie-opslag, -verwerking en -transmissie), [2] de toenemende hoeveelheid beschikbare data en [3] nieuwe en verbeterde algoritmen kunnen we een steeds breder palet aan (informatie-)taken laten uitvoeren of ondersteunen door computers en AI in specifieke zin. Gegeven de context waarin menselijk kapitaal schaars is, is meer kunnen doen met evenveel (of minder) mensen vrijwel een voorwaarde voor het vergroten van het verdienvermogen.

De introductie van NIS2 zal (vermoedelijk) leiden tot een toename in de vraag naar cybersecurityproducten en -diensten. Daarnaast zal de introductie van CRA mogelijkheden bieden voor integrators om het cyberelement als competitive edge te gebruiken. Gezien de sterkte in Nederland om verschillende disciplines bijeen te brengen en kennis en (deel)producten te integreren is het niet ondenkbaar dat Nederlandse bedrijvigheid relatief voordeel kan halen uit de CRA.

Een remmende werking op het verdienvermogen lijkt te komen vanuit de overnames van (potentievolle) jonge cybersecuritybedrijven. Hoewel deze bedrijven in de praktijk de facto nog steeds op Nederlandse bodem kunnen acteren, verliest Nederland wel de controle (en vermoedelijk een deel van de belastinginkomsten) van deze bedrijven. Daarnaast worden ook de tekorten op de arbeidsmarkt als belangrijke dimensie genoemd bij de randvoorwaarden voor succesvolle doorontwikkeling en groei van de cybersecuritysector. Dit wordt versterkt door de constatering dat veel cyberproducten en -diensten in Nederland ook direct afhankelijk zijn van menselijk kapitaal (dienstverlening door mensen), en in mindere mate

van schaalbare hard- en software-producten; dit betekent dat voldoende menselijk kapitaal een belangrijke voorwaarde voor groei is.

Hoe de verschillende trends en ontwikkelingen optellen tot een inschatting van het kwantitatieve effect op het verdienvermogen is (door ons) moeilijk te zeggen. Wel achten wij het aannemelijk dat de groei van de afgelopen jaren, met de benoemde trends inachtneming, in zekere zin kan doorzetten. Hieronder zijn twee verdedigbare (eenvoudige) extrapolaties weergegeven. Eén extrapolatie is lineair en veronderstelt weinig remmende (plafond)werking van bijvoorbeeld de beschikbaarheid van menselijk kapitaal. De tweede extrapolatie is logaritmisch en veronderstelt wel enige 'verzadiging' en remmende werking, maar wordt nog wel gekenmerkt door een lichte groei die verband houdt met onder andere een toenemende vraag en het productiever kunnen inrichten van het werk (onder meer door slimme inzet van AI).



6.3 Hoofdvraag 3: wat kan de overheid doen om bovengenoemd economisch potentieel te realiseren?

3. Wat kan de overheid doen om bovengenoemd economisch potentieel te realiseren?
- **a. Welke middelen kan de overheid gebruiken om – wanneer nodig - te interveniëren?**
- **b. Welk effect kunnen we verwachten door de inzet van deze middelen?**
- **c. Relateer aan de ontwikkelingen zoals omschreven bij vraag 2.**

De cybersecuritysector, economische kansen en de rol van de overheid zijn grote thema's. Het is dan ook niet mogelijk in een onderzoekstraject als dit om het onderwerp in de volledige breedte te belichten. Om die reden is het zinvol om *binnen* het onderwerp te prioriteren waar logische aanknopingspunten voor beleid zitten. Deze prioritering is aangebracht door de voornaamste kansen en bedreigingen voor de Nederlandse cybersecuritysector te identificeren, en deze te relateren aan bestaande sterktes en zwaktes van de sector. Hier zijn vier thema's uit gekomen, namelijk [1] de inzet van AI voor het vergroten van de productiviteit, [2] de beschikbaarheid van kwantitatief en kwalitatief voldoende cyberprofessionals, [3] de overnames van (succesvolle) cybersecuritybedrijven door externe partijen en [4] het bewustzijn van gebruikers op het gebied van cybersecurity. Deze stap in dit onderzoek is dus gebruikt om te **signaleren** waar aanknopingspunten voor beleid zitten.

Gegeven deze aanknopingspunten voor beleid is het nog niet gezegd dat het ook legitiem is als overheid om te interveniëren. Hiervoor dient er namelijk een heldere rationale te zijn om te interveniëren. Deze **rationale** wordt vaak geanalyseerd in de vorm van drie perspectieven op falens c.q. redenen waarom de economie en maatschappij niet de gewenste ontwikkeling doorgaat als de overheid niet ingrijpt; dit zijn de perspectieven van marktfalen, systeemfalen en transformatiefalen. Voor de vier aanknopingspunten is naar de legitimering voor overheidsbeleid gekeken, en voor ieder aanknopingspunt is er minimaal één reden waarom overheidsingrijpen wenselijk is.

De vervolgvraag is wat voor beleid dan **ontwikkeld** en **uitgevoerd** dient te worden. Vooropgesteld constateren we dat er al enorm veel beleid is ontwikkeld en wordt uitgevoerd. Deels is dit landelijk geïnitieerd beleid, maar er gebeurt ook veel op regionaal en lokaal niveau. Er is zodanig veel bestaand beleid dat het gevaar van versnippering en suboptimale coördinatie reëel is; een gevaar dat op zijn minst in de perceptie van menig geïnterviewde bestaat en als zodanig ervaren wordt. Onder meer vanwege deze reden is de NLCS ontwikkeld, welke met vier pijlers en meer dan 200 (gezamenlijke) acties aan de weg timmert. Een belangrijke conclusie uit dit onderzoek is dan ook om vooral door te gaan en verder in te zetten op het stroomlijnen van alle initiatieven en activiteiten die al ontplooid worden, en een kritische houding te nemen ten aanzien van nóg meer beleid en initiatieven.

Het bovenstaande in acht nemende, zijn er in dit onderzoek voor de vier aanknopingspunten suggesties aangedragen voor eventueel aanvullend beleid. Voor [1] **de inzet van AI** heeft dit met name betrekking op het (nog verder) faciliteren van kruisbestuiving tussen de twee disciplines, bijvoorbeeld in de vorm van meer verwevenheid in allerhande innovatieprogramma's en voorstellen of gerichte agendering via de inkoopfunctie van de overheid (bijv. met een SBIR).

Voor [2] **het zorgen voor kwantitatief en kwalitatief voldoende cyberprofessionals** adviseren we met name om de discussie rondom arbeidsmarkttekorten breder te trekken dan enkel de cybersecuritysector, omdat het probleem ook speelt voor de ICT in generieke zin en zelfs sectoren buiten de ICT (denk bijv. aan het onderwijs of de zorg). Het onderliggende fundamentele probleem gaat over hoe we ons schaarse menselijk kapitaal in Nederland willen inzetten, hoe we dat (willen) prioriteren, en hoe we als overheid daar een positie in kiezen. Het onderling concurreren tussen sectoren en beroepen in Nederland gaat dit fundamentele probleem niet oplossen, leidt wel tot hoge(re) kosten voor 'iedere concurrerende sector', dus een cybersector-overstijgende visie op het onderwerp is wat ons betreft waardevol. Hier is ook al aandacht voor, onder meer in de HCA ICT, maar we vermoeden dat het onderwerp in brede zin meer besproken mag worden.

Voor [3] **het voorkomen van onwenselijke overnames** kan er gekeken worden naar (strengere) wet- en regelgeving die de mogelijkheden voor overnames beperkt, of er kan via financiële routes getracht worden ongewenste overnames te ontmoedigen of andere ontwikkelpaden van betreffende bedrijven te stimuleren. Dit kan bijvoorbeeld door het nemen van aandelen of door het stimuleren van beschikbaar kapitaal voor deze partijen. Ook hier geldt dat dit een meer generiek vraagstuk in Nederland is, en ook hier adviseren we om dit op een cybersecuritysector-overstijgend niveau aan te pakken om onnodig specifiek sectorbeleid te voorkomen. Wel kan beargumenteerd worden dat deze sector 'anders' is vanwege haar directe relatie met publieke waarden als (nationale) veiligheid en strategische autonomie.

Voor [4] **het vergroten van het bewustzijn van gebruikers** adviseren we primair om de bestaande inspanningen nog beter te coördineren en in te zetten. Er gebeurt ook hier immers veel op landelijk, regionaal en lokaal niveau. Het onderwerp cybersecurity is daarbij ook sterk verweven binnen mkb-dienstverlening op het gebied van digitalisering in brede zin.

Deze constatering wordt onderbouwd door de recent uitgevoerde 'Regioscan Digitalisering MKB': een scan waarin samen met EZK, PTvT en alle twaalf provincies in kaart is gebracht welk publiek en publiek-privaat ondersteuningsaanbod er is voor het mkb op het gebied van digitalisering. Lokale en regionale netwerken zijn sterke routes/mechanismen om bedrijven en medewerkers te bereiken, en landelijke samenwerking kan vanwege schaalvoordelen juist weer helpen om bijvoorbeeld effectieve informatieproducten te creëren en te distribueren. Voor specifieke sectoren en/of niches waar nog weinig aanbod beschikbaar is, kunnen uiteraard additionele inspanningen opgezet worden, maar we adviseren om hier uiterst voorzichtig mee om te gaan. Het introduceren van (nog) meer initiatieven en beleid introduceert immers ook nog meer complexiteit in het systeem, waardoor het bereik en de effectiviteit van beleidsinspanningen onder druk kan komen te staan.

Het effect van de benoemde eventuele (aanvullende) beleidsmaatregelen kunnen we binnen dit onderzoek niet aantonen. Het beleid moet daar allereerst nog een stuk concreter voor uitgewerkt worden. Vervolgens is idealiter een ex-ante evaluatie benodigd om verwachte effecten in kaart te brengen. Desalniettemin hopen de auteurs van deze publicatie dat de gepresenteerde analyse bijdraagt aan de volgende fase.

Bijlage 1. Onderzoeksaanpak

Stap 1: Verkennende literatuurstudie

Het voorspellen van trends in cybersecurity is geen sinecure. Cybersecurity is zeer dynamisch veld en leunt sterk op de ontwikkelingen in de cybercriminaliteit. Op deze ontwikkelingen is weinig zicht, we lopen dus altijd achter de feiten aan. Om vooraf een zo compleet mogelijk beeld te krijgen van de relevante trends, hebben we de ontwikkelingen vanuit vier perspectieven bekeken, te weten:

1. Trends in dreigingen. Hoe ontwikkelt cybercriminaliteit zich en welke dreigingen komen er op ons af?
2. Trends in de activiteiten en samenstelling van de industrie. Hoe ontwikkelt het aanbod van activiteiten zich in Nederland?
3. Trends in de arbeidsmarkt. Welke cybersecurity functies worden gevraagd?
4. Trends in het investeringsklimaat. Welke ontwikkelingen spelen op het gebied van instituties, infrastructuur, macro-economie en fiscaliteit, gezondheid en kwaliteit van leven, onderwijs- en kennisinfrastructuur, marktwerking en handel, arbeidsmarkt, financiële markt, bedrijfsdynamiek, innovatie, duurzaamheid en digitalisering?

Het bovenstaande literatuuronderzoek is uitgevoerd voordat we met de andere onderzoeksstappen zijn begonnen. Dit gaf ons voldoende context om een goede invulling te geven aan deze stappen.

Stap 2: Vacatureonderzoek

Om de cybersecurityarbeidsmarkt in kaart te brengen is een beknopt vacatureonderzoek uitgevoerd. Jobdigger beheert een database waarin de vacatureteksten van alle vacatures die in Nederland online komen worden bijgehouden. Deze database is doorzocht door middel van zoektermen, vergelijkbaar met het identificeren van cybersecuritybedrijven via Innovatiespotter. Specifiek is gekeken of één van de volgende woorden voorkomt in de vacaturetitel: 'cyber', 'security', 'beveiliging' of 'hacker'. De resulterende vacatures zijn vervolgens opgewerkt om een overzicht te krijgen van relevante functies en gevraagde vaardigheden en de ontwikkeling hiervan per jaar in de periode 2015-2021. We zijn ons ervan bewust dat in veel gevallen vacatures ook worden vervuld via informele kanalen en er geen formele vacaturetekst wordt uitgezet. Dat geldt echter voor de arbeidsmarkt als geheel. Niettemin zijn de aantallen vacatures, aard van de functies en gevraagde vaardigheden vacatureteksten een aardige proxy voor de ontwikkeling van de cybersecurityarbeidsmarkt. De uitkomsten van deze analyse zijn te vinden in Bijlage 6.

Stap 3: Interviews

Tijdens de interviews zijn de volgende onderwerpen besproken:

- Eventuele aanvullingen op de eerder gedefinieerde **trends** uit de literatuurstudie.
- Waar de **economische kansen** van de cybersecuritysector liggen.
- Eventueel **overheidsingrijpen** om het potentieel van de cybersecuritysector te realiseren.

In totaal hebben we zestien interviews afgenomen met verschillende typen actoren; cybersecurityexperts, marktpartijen en een expert in economie. De interviews zijn ingestoken als een open gesprek waarin wij gesprekspartners vroegen naar hun mening over de

bovenstaande aspecten. Een overzicht van de gesprekspartners en het interview protocol is bijgevoegd in Bijlage 5.

Stap 4: Innovatiespotter, verkrijgen van het onderzoeksample

Uitgangspunten

In onze visie is de tekst op de website van een bedrijf leidend bij het bepalen of zij activiteiten ontplooien op het gebied van cybersecurity. Met andere woorden: Alleen als een bedrijf op zijn website aangeeft actief te zijn in dit domein, dan voert het bedrijf cybersecurity activiteiten uit. We doen de aanname dat elk relevant cybersecuritybedrijf in Nederland een website heeft met passende informatie. Dat zal niet in alle gevallen kloppen: (1) kleine bedrijven hebben mogelijk geen website en zullen dan niet worden meegenomen, (2) sommige kleine bedrijven geven op hun website mogelijk niet (goed) aan dat ze cybersecurity activiteiten ontplooien en (3) sommige bedrijven zullen om specifieke redenen *onder de radar willen blijven* en hun activiteiten niet openbaar willen maken. We erkennen deze drie zwaktes, maar zijn van mening dat deze aanpak gegeven de mogelijkheden de beste optie is.

Om de cybersecuritysector in kaart te brengen is o.a. gebruik gemaakt van Innovatiespotter. De database van het bedrijf Innovatiespotter biedt een database aan met alle tekst van de websites van alle Nederlandse bedrijven. Innovatiespotter heeft met behulp van een webscraper een database opgezet waarin de website teksten van alle primaire[192] websites van Nederlandse bedrijven zijn opgeslagen. Door middel van een online tool kan deze database worden bevraagd aan de hand van zoektermen, ook wel een query genoemd. De tool gaat na of de zoektermen, of een combinatie van zoektermen, voorkomen op de website van een bedrijf. Als dat zo is wordt het bedrijf toegevoegd aan het resultaat. Doordat de database van Innovatiespotter de inhoud van de websites van alle Nederlandse bedrijven doorzoekt is het op deze manier mogelijk om bedrijven met cybersecurity activiteiten in Nederland te identificeren.

Deze database van Innovatiespotter bevat enkel gegevens over bedrijven. Slechts enkele bedrijven in Nederland zullen R&D uitvoeren specifiek toegespitst op cybersecurity als technologie. Daarnaast wordt educatie op het gebied van cybersecurity voornamelijk aangeboden door onderwijsinstellingen. Het vinden van deze bedrijven en onderwijsinstellingen aan de hand van tekst op de website zal leiden tot veel ruis, gegeven dat hier voornamelijk generiek termen als "educatie", "training", "opleiding" en "research and development" kunnen worden toegepast. Om de hoeveelheid ruis in de data te verminderen is er daarom voor gekozen om deze categorie buiten beschouwing te laten. Hiermee vinden we dus slechts bedrijven die cybersecurityproducten en -diensten produceren en integreren.

Definitie van filters

Een tweede stap die we vervolgens moeten zetten is het definiëren van de filters of "*sleutels*". Welke tekst moet op een website van een bedrijf staan om als cybersecuritybedrijf aangemerkt te worden? Hier ligt uiteraard een grote uitdaging. Als we als term "cyber" kiezen, dan vinden we ook allerlei bedrijven die niet tot de populatie horen.[193] Als we alleen als term "pentesting" kiezen, dan missen wel allerlei bedrijven. Daarom hebben we aansluiting

---

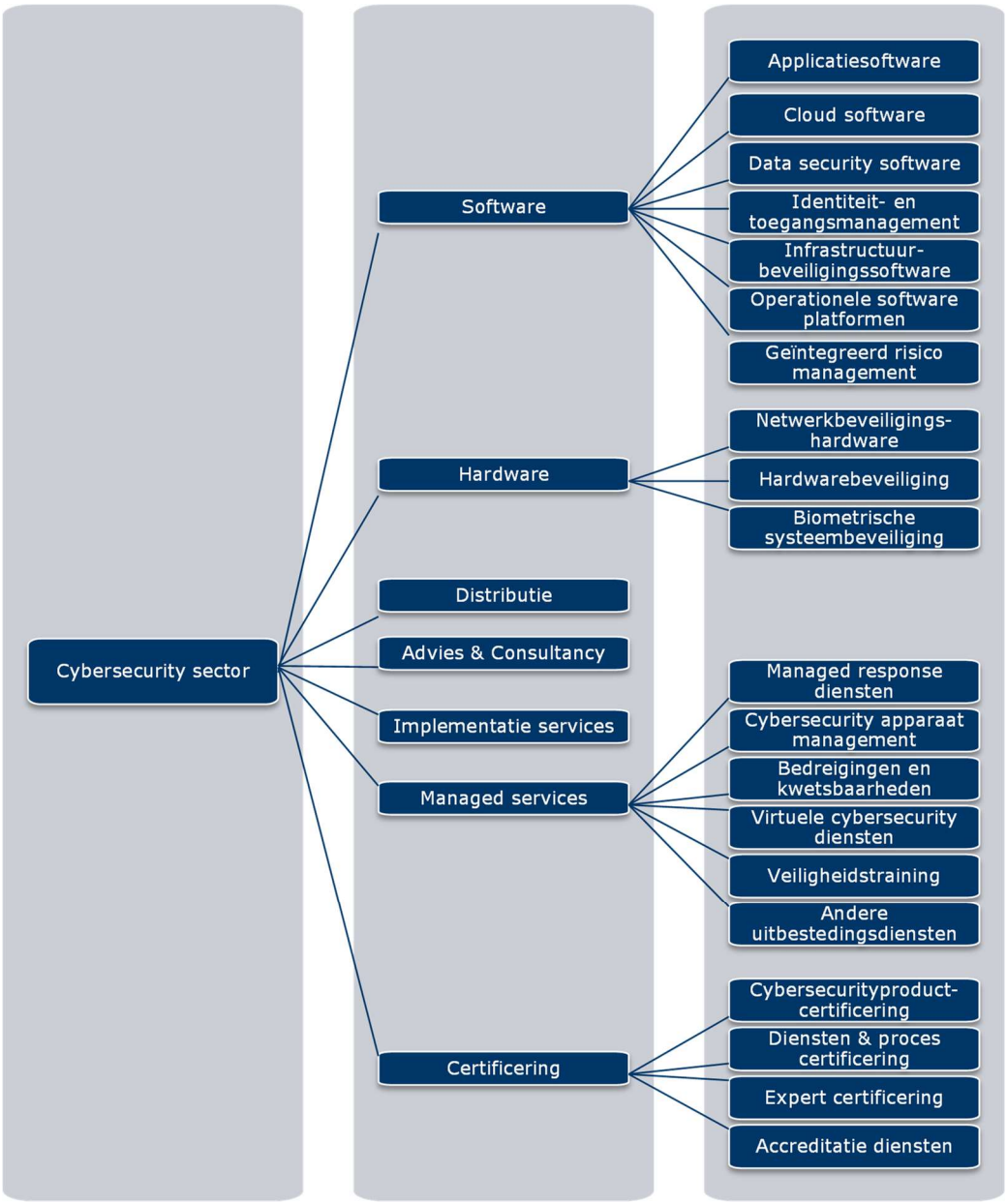
[192] Een bedrijf kan uiteraard meerdere websites hebben, bijvoorbeeld voor verschillende producten, diensten of merken. We hanteren de website die ze zelf hebben opgegeven bij de KvK.

[193] Op de website van Albert Heijn staat bijvoorbeeld een recept voor Chocolate fridge cake met pecannoten met als bron: *cyber kitchen.* Dat AH niet tot de cybersecuritysector behoort is evident, maar als we als filter alleen *cyber* zouden gebruiken dan worden zij wel geïdentificeerd als bedrijf in de cybersecuritysector.

gezocht bij de marktanalyse die ENISA van de cybersecuritymarkt uitvoerde in 2022.[194] Zij hanteren een taxonomie met hierin allerlei verschillende soorten activiteiten en onderverdelingen. Dit laat zich goed vertalen in sleutels en zorgt direct voor een logische marktindeling. Maar hoe we de termen ook selecteren, ook hier zullen we fouten maken. Wanneer de termen te breed zijn zullen we sommige bedrijven ten onterechte aanmerken als cybersecuritybedrijf. Wanneer de termen te smal zijn zullen we sommige bedrijven niet aanmerken als cybersecuritybedrijf terwijl ze het in werkelijkheid wel zijn. Voor beide aspecten kunnen we deels corrigeren, daar gaan we later op in.

De onderstaande afbeelding toont de taxonomie die ENISA heeft ontwikkeld. Bij de toelichting hiervan, worden verschillende meer specifieke **zoektermen** gegeven die passen bij de (sub)categorieën. Per subcategorie is een **zoekquery** opgesteld met deze zoektermen in zowel het Nederlands als Engels. Zo hebben we filters gegenereerd die we over de database kunnen leggen. Merk op dat in Figuur 1 de ENISA categorie R&D en educatie ontbreekt.

194 https://www.enisa.europa.eu/publications/enisa-cybersecurity-market-analysis-framework-ecsmaf/@@download/fullReport



Figuur 1 Overzicht van de ENISA (sub)categorieën

De initiële queries zijn op verschillende manieren verfijnd. Hieronder wordt dit beschreven.

- **Exclusie van termen**. De zoekqueries zijn verfijnd door middel van exclusie van termen. Zo resulteerde het gebruik van de zoekterm *'user authentication'* in bedrijven die in een pop-up benoemen dat zij cookies gebruiken op hun website. Maar dit zijn uiteraard niet allemaal cybersecuritybedrijven. Deze zoekterm is daarom verfijnd naar *'User authentication' NOT 'cookies for user authentication'*. Dit betekent dat alle websites die *'user authentication'* noemen buiten de context *'cookies for user authentication'* als relevant worden aangemerkt. De zoekqueries voor elke subcategorie in de taxonomie zijn aan de hand hiervan verfijnd om zo de hoeveelheid Type I-fouten (*false positives*) te verminderen.
- **Triangulatie**. De resulterende set bedrijven is gevalideerd door middel van triangulatie met lijsten van bedrijven die evident binnen de Nederlandse cybersecuritysector vallen. Dit komt deels uit eigen kennis en netwerken van Dialogic, en deels van de

ledenlijst van de brancheorganisatie Cyberveilig Nederland. Door middel van deze triangulatie kan een inschatting worden gedaan over de mate waarin er sprake is van Type II-fouten (*false negatives*). Vinden we de bedrijven die we logischerwijs moeten vinden? Dat was niet altijd het geval. Op basis van deze analyse zijn de zoektermen verder verfijnd. We vonden verschillende fouten:

- Sommige bedrijven missen omdat hun output te specifiek is om gevangen te worden in de termen van ENISA. We hebben deze output specifiek toegevoegd in de queries. Een voorbeeld hiervan is Technolution dat specificeert in het maken van lijnvercijferaars[195].
- Sommige bedrijven missen omdat hun output in de Nederlandse context wordt geplaatst en ENISA Engelse termen hanteert. In de eerste iteratie is over het hoofd gezien om de Nederlandse vertaling van enkele afkortingen toe te voegen in de queries. Een goed voorbeeld zijn activiteiten met betrekking tot de Baseline Informatiebeveiliging Overheid (BIO). We hebben deze output specifiek toegevoegd in de queries.
- Sommige bedrijven zijn wel lid van Cyberveilig Nederland, maar hebben geen Nederlands KvK-nummer. WithSecure is bijvoorbeeld een Fins bedrijf dat lid is van Cyberveilig Nederland. In onze benadering vallen bedrijven zonder KvK-nummer buiten de Nederlandse cybersecuritysector. Hiervoor is dus niet gecorrigeerd.
- Sommige bedrijven zijn wel lid van Cyberveilig Nederland, maar voeren activiteiten uit die te ver af staan van cybersecurity, zoals advocatenkantoren. In onze benadering vallen deze buiten de Nederlandse cybersecuritysector en hiervoor is niet gecorrigeerd.

De output van de bovenstaande analyse is handmatig bekeken en geanalyseerd. Op basis hiervan zijn we tot de conclusie gekomen dat er relatief veel *false positives* (type 1 fouten) werden gevonden. Met andere woorden: er werden bedrijven gevonden die volgens ons evident geen cybersecurity activiteiten uitvoeren, maar wel op de lijst stonden. Hiervoor hebben we een aantal additionele filters ingevoegd:

- **Websites**. Sommige bedrijven geven een evident foute website door bij de KvK, zoals de website van hun internet serviceprovider, de hoster van hun website of LinkedIn. In alle drie de gevallen is het evident deze websites informatie over cybersecurity maatregelen bevat. We hebben alle bedrijven met dit soort websites verwijderd.
- **SBI**. Er is gefilterd op de **hoofdactiviteit** van een bedrijf aan de hand van SBI-codes. Wanneer een SBI-categorie mogelijk relevante cybersecuritybedrijven kan bevatten is de categorie behouden in het filter. Dat wil zeggen dat een categorie alleen is verwijderd wanneer het evident was dat bedrijven in deze categorie *geen* cybersecurity activiteiten ontplooien. Enkele voorbeelden hiervan zijn *Bemiddeling bij handel, huur of verhuur van onroerend goed*, *Overige paramedische praktijken* en *alternatieve genezers en Apotheken*.
- **KvK-nummers.** De dataset uit Innovatiespotter bevat meerdere bedrijven die onder hetzelfde KvK-nummer zijn ingeschreven. Dit zijn bijvoorbeeld verschillende vestigingen of aftakkingen binnen hetzelfde bedrijf. In een vervolgstap worden bedrijven op basis van KvK-nummers gekoppeld aan administratieve bedrijfsinformatie in de CBS-microdata omgeving. Omdat deze gegevens beschikbaar zijn per KvK-nummer is het van belang om de huidige dataset op KvK-nummer te ontdubbelen.

[195] https://www.technolution.com/prime/nl/lijnvercijfering/

Uit de analyse is een verzameling aan bedrijven tot stand gekomen die in dit onderzoek zijn aangehouden als bedrijven met cybersecurity activiteiten.

Op basis van de bovenstaande analyse is een database ontstaan met hierin 5.436 unieke KvK-nummers. Het analyseren van deze bedrijven biedt ons de gelegenheid om te controleren of de uitkomsten aannemelijk zijn. In Bijlage 1 worden deze uitkomsten weergegeven. Duidelijk is dat de verdeling van locatie van KvK-inschrijvingen over de provincies aannemelijk is. Noord-Holland, Zuid-Holland, Utrecht en Noord-Brabant voeren de lijst aan. Ook als we naar de steden waar deze KvK-inschrijvingen gevestigd zijn kijken ontstaat een aannemelijk beeld. De volgorde is Amsterdam, Utrecht, Rotterdam, Den Haag, Haarlemmermeer, Eindhoven, et cetera. Verder geven de SBI-codes ook vertrouwen. De grootste SBI branches zijn *J: Informatie en communicatie*, *M: Advisering, onderzoek en overige specialistische zakelijke dienstverlening* en *Financiële instellingen*. Ook de andere velden (rechtsvorm, gebouwfunctie, oprichtingsjaar, aantal werknemers) geven geen reden tot zorg.

Stap 5: Administratieve data (CBS)

De resultaten uit Innovatiespotter zijn gekoppeld aan administratieve bedrijfsgegevens in de CBS microdata-omgeving. De administratieve bedrijfsgegevens zijn echter niet beschikbaar op KvK-nummer niveau, maar op een hoger niveau. Tijdens het opwerken van de KvK-nummers naar het juiste niveau kunnen drie situaties voorkomen:

1. Het KvK-nummer is één-op-één te vertalen naar het bedrijfsniveau.
2. Het KvK-nummer is niet te koppelen naar het bedrijfsniveau.
3. Meerdere KvK-nummers behoren tot hetzelfde ID op het bedrijfsniveau.

Wanneer een KvK-nummer niet te koppelen is naar een hoger bedrijfsniveau (situatie 2) valt dit bedrijf weg. Wanneer meerdere KvK-nummers tot hetzelfde ID op bedrijfsniveau behoren (situatie 3) is slechts één van deze bedrijven in de dataset behouden om dubbelingen te voorkomen. Het aantal bedrijven is daarmee van 5.436 afgenomen tot 5.006. Voor deze bedrijven zijn vervolgens het aantal werknemers, de omzet, de toegevoegde waarde en de uitgaven aan R&D-activiteiten gekoppeld. Vervolgens zijn de bedrijven uitgesplitst naar de volgende verdelingen: ENISA categorie, grootteklasse, SBI en regio (noord, midden-noord, midden-zuid en zuid) in Nederland, en zijn de gegevens geplot voor de jaren 2017-2021. Gegevens over R&D-uitgaven zijn beschikbaar voor de periode 2017-2020. Daarnaast is informatie over R&D-uitgaven beschikbaar op basis van steekproef waarbij bedrijven met minder dan 10 werknemers worden uitgesloten. Door de beperkte beschikbaarheid van deze gegevens is deze data enkel uitgesplitst naar ENISA categorie en grootteklasse, welke wij als meest informatief beoordelen. De uitkomsten van deze analyse zijn te vinden in Bijlage 4.

Stap 6: Enquêtedata

Om verdieping aan te brengen in de kwantitatieve analyse is een enquête uitgezet onder bedrijven in de cybersecuritysector. De enquête is gehost via de interne dashboard omgeving van Dialogic, DiaDashboard. De bedrijven uit Innovatiespotter (n=5.436) waarvoor een mailadres bekend was zijn benaderd om de enquête in te vullen. Dit betreft circa 2400 unieke emailadressen. Hiervan bleken 370 emailadressen niet meer actief of niet correct. Daarmee hebben 2030 bedrijven de survey ontvangen, waarvan 127 bedrijven hebben geantwoord. Daarmee is een response van 6,3% behaald. Bedrijven zijn gevraagd om aan te geven onder welke categorieën uit het conceptuele model zij hun bedrijf scharen; categorie A (cyber R&D-ers), B (Producenten van cyberproducten en - diensten) en/of C (cyber integrators). Hierna volgden categorie-specifieke vragen, gevolgd door algemene afsluitende vragen over bedrijfsinformatie. De gehele enquête en uitkomsten zijn beschreven in Bijlage 3.

Stap 7: Verdiepende literatuurstudie

Tijdens de afronding van het onderzoek hebben wij een verdiepend literatuuronderzoek uitgevoerd om de uitkomsten van de SWOT-analyse nader te duiden.

Stap 8: Validatiesessie

De informatie over toekomstige trends en mogelijke overheidsingrijpen die zijn opgehaald uit de eerdere onderzoekstappen zijn getoetst en verrijkt in een validatiesessie met cybersecurityexperts. Daarnaast zijn de sterktes, zwaktes, kansen en bedreigingen van de Nederlandse cybersecuritysector, en hun samenhang, besproken en bediscussieerd tijdens deze validatiesessie. Een eerste opzet van de SWOT-analyse is gepresenteerd en mogelijke beleidsopties zijn besproken.

Bijlage 2. Uitkomsten KvK data

In deze bijlage presenteren we de uitkomsten van de KvK data die afkomstig is uit de gefilterde database van Innovatiespotter. Omdat CBS microdata meer mogelijkheden biedt met betrekking tot sensitieve data, zoals de omzet en toegevoegde waarde van bedrijven, gebruiken we dat als primaire bron voor onze analyses. We presenteren deze data om aan te tonen dat er sprake is van een goede filtering aangezien er aannemelijke resultaten uitkomen. De provincies waar we de meeste activiteiten verwachten (Randstad en Noord-Brabant) scoren inderdaad het hoogte. Hetzelfde geldt voor de steden: Amsterdam, Utrecht, Rotterdam en Den Haag scoren hoog. De verdeling over de SBI-codes is ook aannemelijk. Veel *J: Informatie en communicatie* en veel *M: advisering*. Opvallend is de hoge score van *K: financiële instellingen*. We hebben dit nader onderzocht. Het bleek dat in deze set veel organisaties die als "holding" zijn beschreven voorkwamen. De activiteiten die zij, of de bedrijf waar ze aandelen van hadden, ontplooiden waar wel degelijk gericht op cybersecurity. Bij de CBS-microdata wordt op het niveau van bedrijfseenheden een analyse uitgevoerd waardoor holdings worden samengevoegd met de aan hen verbonden partijen.

Tabel 6. Verdeling over provincies

Provincie	Aantal bedrijven
Noord-Holland	1368
Zuid-Holland	1210
Utrecht	723
Noord-Brabant	706
Gelderland	546
Overijssel	259
Limburg	185
Flevoland	129
Groningen	115
Drenthe	93
Friesland	75
Zeeland	27
Totaal	5436

Tabel 7. Verdeling over steden (top 20)

	Aantal bedrijven
Amsterdam	626
Utrecht	269
Rotterdam	246
's-Gravenhage	180
Haarlemmermeer	166
Eindhoven	142
Amersfoort	97
Groningen	87
's-Hertogenbosch	83
Almere	76
Breda	75
Haarlem	71
Arnhem	69
Delft	68
Rijswijk	65
Veenendaal	56
Apeldoorn	56
Amstelveen	55
Nijmegen	54
Enschede	53
Overig	2842
Eindtotaal	5436

Tabel 8. Verdeling over SBI-codes

	Aantal bedrijven
J: Informatie en communicatie	2243
M: Advisering, onderzoek en overige specialistische zakelijke dienstverlening	1335
K: Financiële instellingen	905
G: Groot- en detailhandel; reparatie van auto's[196]	371
N: Verhuur van roerende goederen en overige zakelijke dienstverlening	273
P: Onderwijs	133
C: Industrie	68
F: Bouwnijverheid	60
S: Overige dienstverlening	38
D: Productie en distributie van en handel in elektriciteit, aardgas, stoom en gekoelde lucht	7
Q: Gezondheids- en welzijnszorg	2
O: Openbaar bestuur, overheidsdiensten en verplichte sociale verzekeringen[197]	1
Eindtotaal	5436

Tabel 9. Verdeling over rechtsvorm

	Aantal bedrijven
B.V.	4041
Eenmanszaak	1098
V.O.F.	122
Buitenlandse vennootschap	104
N.V.	30
Coöperatie	20
Maatschap	10
C.V.	10
Europese N.V.	1
Eindtotaal	5436

[196] In deze categorie valt zowel (45) Handel in en reparatie van auto's, motorfietsen en aanhangers, als (46) Groothandel en handelsbemiddeling (niet in auto's en motorfietsen) en (47) Detailhandel (niet in auto's).

[197] Zoals in de tekst aangegeven: de SBI-codes worden meer dan eens slecht ingevuld. De organisatie met de SBI-code valt in de categorie *Openbaar bestuur, overheidsdiensten en verplichte sociale verzekeringen*. Wij zouden deze eerder scharen onder *J: Informatie en communicatie*.

Tabel 10. Verdeling naar oprichtingsjaar

	Aantal bedrijven
1820-1899	4
1900-1909	0
1910-1919	3
1920-1929	11
1930-1939	6
1940-1949	12
1950-1959	10
1960-1969	30
1970-1979	65
1980-1989	175
1990-1999	786
2000-2009	1483
2010-2019	2384
2020-2022	467
Eindtotaal	5436

Bijlage 3. Enquête en generieke uitkomsten

Enquête

Startpagina

Survey economische kansen Nederlandse cybersecurity sector

Emailadres*

Voor het Ministerie van EZK voeren wij (Dialogic) een onderzoek uit naar de economische kansen van de cybersecuritysector. We kijken daarbij onder andere naar trends op het gebied van cybersecurity en mogelijke effecten daarvan op de cybersecuritymarkt en het Nederlandse verdienvermogen. Om inzicht te krijgen in de economische kansen van de Nederlandse cybersecuritysector spreken we met cybersecurityexperts en experts op het gebied van cybercriminaliteit, economen en beleidsexperts. Daarnaast zetten we een survey uit onder Nederlandse cybersecurity bedrijven. Het gaat hierbij zowel om bedrijven die zich richten op cybersecurity als bedrijven die cybersecurity verwerken in hun diensten of producten. U bent werkzaam bij een van deze bedrijven. We zouden u dan ook willen vragen om deze survey in te vullen. Het invullen van de survey zal ongeveer **5-10 minuten** duren.

Indien u vragen heeft over deze survey kunt u contact opnemen met Sonja Kleter (kleter@dialogic.nl)

Categorie indeling conceptueel model

Startpagina

Voert uw organisatie R&D op het gebied van cybersecurity uit?*

- Ja
- Nee
- Weet ik niet zeker

Levert uw organisatie cybersecurity producten en/of diensten? *

- Ja
- Nee
- Weet ik niet zeker

Levert uw organisatie niet-cybersecurity eindproducten of diensten waar cybersecurity wel een belangrijk onderdeel van uitmaakt?*

Bijvoorbeeld: auto's, medische apparatuur of online betaaldiensten. Dit zijn niet-cybersecurity producten/diensten waar cybersecurity wel een belangrijk onderdeel van uitmaakt (medische apparaten moeten immers niet gehackt kunnen worden).

- Ja
- Nee
- Weet ik niet zeker

Groei van de cybersecuritysector

Groei van de cybersecurity sector

Categorie	Voorbeelden van producten en diensten
Training	Cybersecurity training.
Software	Software voor applicatiebeveliging, cloudbeveiliging, databeveiliging, identiteits- en toegangsmanagement, en risicomanagement.
Hardware	Hardware voor cybersecurity zoals biometrische cybersecurity systemen, en beveiliging voor hardware.
Verkoop/Levering	Verkoop/levering van cybersecurity software en hardware aan de eindgebruiker.
Advies & Consulting	Het ontwikkelen van en adviseren over cyberbeveilings- en risicostrategieën, pentesten/red teaming
Implementatie	Het ontwikkelen en implementeren van cybersecurityoplossingen.
Managed Services (beheer)	Het beheer, onderhoud en testen van cybersecurityproducten (o.a. incident response, cybersecurity as a service)

Bij welke van de onderstaande cybersecuritydiensten en -producten verwacht u de komende 3 jaar de meeste groei?

- ○ Onderzoek & Ontwikkeling
- ○ Training
- ○ Software
- ○ Hardware
- ○ Verkoop/Levering
- ○ Advies & Consulting
- ○ Implementatie
- ○ Managed Services (beheer)
- ○ Certificering

Zijn er andere specifieke trends op het gebied van cybersecurity activiteiten?

Het gaat om activiteiten die niet in bovenstaande vraag staan benoemd

In welke mate beperken de volgende factoren de groei van de cybersecurity sector?

	Niet	Enige mate	Sterke mate
Tekort aan hardware	○	○	○
De (semi) monopolistische status van leveranciers	○	○	○
Tekort aan generiek kapitaal	○	○	○
Tekort aan durfkapitaal voor start-ups	○	○	○
Concurrentie van buitenlandse partijen	○	○	○
Tekort aan gekwalificeerd personeel (o.a. door onvoldoende inbedding van cybersecurity in onderwijs)	○	○	○
Tekort aan investeringen in omscholingstrajecten om cyberexpertise van werknemers te verhogen	○	○	○
Gebrek aan bewustzijn van de risico's van cybercriminaliteit	○	○	○
Gebrek aan beleid rondom cybersecurity	○	○	○

Zijn er andere factoren die de groei van de cybersecurity (gaan) remmen?

Het gaat om factoren die niet in bovenstaande vraag staan benoemd

Cyber R&D

R&D

Op welke cybersecurity onderwerpen richt de R&D van uw organisatie zich?

Wat zijn belangrijke opkomende onderwerpen op het gebied van cybersecurity R&D? Zijn er nieuwe 'hot topics'?

Welk deel van de omzet van uw organisatie wordt besteed aan cybersecurity R&D activiteiten?

- ○ 0-10%
- ○ 10-20%
- ○ 20-30%
- ○ 30-40%
- ○ 40-50%
- ○ 50-60%
- ○ 60-70%
- ○ 70-80%
- ○ 80-90%
- ○ 90-100%
- ○ Weet ik niet

Hoe heeft het aandeel van de omzet dat uw organisatie investeert in R&D zich ontwikkeld?

- ○ Het aandeel is afgenomen
- ○ Het aandeel is gelijk gebleven
- ○ Het aandeel is toegenomen
- ○ Weet ik niet

Op welk TRL-niveau richt de R&D van uw organisatie zich?

Er zijn meerdere antwoorden mogelijk

Om de specifieke fase aan te duiden waarop R&D gericht is worden vaak de Technology Readiness Levels (TRL) gebruikt.

Verkennen (Discovery phase): TRL 1, 2 en 3

- Level 1: Fundamenteel onderzoek. U doet onderzoek naar uw innovatieve idee en de basisprincipes van de innovatie. U bent hierbij bezig met fundamenteel onderzoek en deskresearch.
- Level 2: Toegepast onderzoek. U gaat nu bezig met de formulering van het technologisch concept en de praktische toepassingen. In deze fase bent u vooral bezig met experimenteel en/of analytisch onderzoek.
- Level 3: Toetsing (Proof of principle / Proof of concept). U onderzoekt de toepasbaarheid van het concept op experimentele basis (experimenteel proof of concept). U toetst en valideert hypotheses over verschillende componenten van het concept.

Ontwikkelen (Development phase): TRL 4, 5 en 6

- Level 4: Implementatie en test prototype. U gaat de Proof-of-concept van uw innovatie op labschaal testen. Een prototype dat u in deze fase ontwikkelt, kost relatief weinig geld en tijd om te ontwikkelen en is daarmee nog ver verwijderd van een definitief product, proces of dienst.
- Level 5: Validatie prototype. U onderzoekt de werking van het technologisch concept in een relevante omgeving. Dit is de 1e stap in de demonstratie van de technologie. Een prototype dat u in deze fase ontwikkelt, kost relatief veel tijd en geld en is niet ver verwijderd van het uiteindelijke product of systeem.
- Level 6: Demonstratie prototype in testomgeving. U gaat het concept uitgebreid testen en demonstreren in een relevante testomgeving. Het testen vindt plaats na de technische validatie in een relevante (pilot) omgeving, zoals een proeftuin. Het concept geeft inzicht in de werking van alle componenten tezamen.

Demonstreren (Demonstration phase): TRL 7 en 8

- Level 7: Demonstratie prototype in operationele omgeving. U gaat het concept testen en demonstreren in een gebruikersomgeving om werking in een operationele omgeving te bewijzen. De demonstratie van het concept in een praktijkomgeving levert nieuwe inzichten op voor de definitieve markttoepassing van uw innovatie.
- Level 8: Product/dienst is compleet en operationeel. In deze fase krijgt uw innovatie zijn definitieve vorm. U hebt de technologische werking getest en het is bewezen dat het voldoet aan gestelde verwachtingen, kwalificaties en normen (certificering). Daarnaast bepaalt u de financiële kaders voor (massa)productie en lancering en bent u klaar voor de volgende stap.

- [ ] 1-3
- [ ] 4-6
- [ ] 7-8
- [ ] Weet ik niet

Producenten van cybersecurityproducten en -diensten

Cybersecurity activiteiten

Categorie	Voorbeelden van producten en diensten
Training	Cybersecurity training.
Software	Software voor applicatiebeveliging, cloudbeveiliging, databeveiliging, identiteits- en toegangsmanagement, en risicomanagement.
Hardware	Hardware voor cybersecurity zoals biometrische cybersecurity systemen, en beveiliging voor hardware.
Verkoop/Levering	Verkoop/levering van cybersecurity software en hardware aan de eindgebruiker.
Advies & Consulting	Het ontwikkelen van en adviseren over cyberbeveilings- en risicostrategieën, pentesten/red teaming
Implementatie	Het ontwikkelen en implementeren van cybersecurityoplossingen.
Managed Services (beheer)	Het beheer, onderhoud en testen van cybersecurityproducten (o.a. incident response, cybersecurity as a service)
Certificering	Certificering en accreditatie van cybersecurityproducten.

Welke cybersecuritydiensten en -producten levert uw organisatie?

- [ ] Training
- [ ] Software
- [ ] Hardware
- [ ] Verkoop/Levering
- [ ] Advies & Consulting
- [ ] Implementatie
- [ ] Managed Services (beheer)
- [ ] Certificering
- [ ] Anders, namelijk

Welk deel van de omzet van uw organisatie komt uit bovenstaande activiteiten?

Geef hierbij een schatting op basis van de meest recente gegevens

- ○ 0-10%
- ○ 10-20%
- ○ 20-30%
- ○ 30-40%
- ○ 40-50%
- ○ 50-60%
- ○ 60-70%
- ○ 70-80%
- ○ 80-90%
- ○ 90-100%

Hoe was de omzetontwikkeling van deze activiteiten de afgelopen 5 jaar?

Negatieve getallen geven aan dat de omzet is gekrompen.

- ○ meer dan 100% krimp per jaar
- ○ 75-100% krimp per jaar
- ○ 50-75% krimp per jaar
- ○ 25-50% krimp per jaar
- ○ 0-25% krimp per jaar
- ○ De omzet is ongeveer gelijk gebleven
- ○ 0-25% groei per jaar
- ○ 25-50% groei per jaar
- ○ 50-75% groei per jaar
- ○ 75-100% groei per jaar
- ○ meer dan 100% groei per jaar

Hoe zal de omzet van deze activiteiten zich de komende 5 jaar naar verwachting ontwikkelen?

Negatieve getallen geven aan dat de omzet is gekrompen.

- ○ meer dan 100% krimp per jaar
- ○ 75-100% krimp per jaar
- ○ 50-75% krimp per jaar
- ○ 25-50% krimp per jaar
- ○ 0-25% krimp per jaar
- ○ De omzet is ongeveer gelijk gebleven
- ○ 0-25% groei per jaar
- ○ 25-50% groei per jaar
- ○ 50-75% groei per jaar
- ○ 75-100% groei per jaar
- ○ meer dan 100% groei per jaar

Integrators

Integrators

Wat zijn de belangrijkste producten of diensten die u verkoopt/aanbiedt?

Het gaat om diensten/producten waar cybersecurity wel onderdeel van uitmaakt. U kunt meerdere producten of diensten invullen (maximaal 5)

- [ ] 1
- [ ] 2
- [ ] 3
- [ ] 4
- [ ] 5

In welke mate geeft de cyberveiligheid van uw dienst/product u een competitief voordeel ten opzichte van concurrenten?

- ○ In zeer beperkte mate
- ○ In beperkte mate
- ○ Enigszins
- ○ In sterke mate
- ○ In zeer sterke mate

Waarom besteedt u aandacht aan de cyberveiligheid van uw product of dienst?

- [ ] Competitief voordeel ten opzichte van concurrenten
- [ ] Verplicht vanuit wet- en regelgeving
- [ ] Anders, namelijk

Welk deel van uw kosten (inkoop, eigen personeel) is direct gerelateerd aan cybersecurity?

- ○ 0-10%
- ○ 10-20%
- ○ 20-30%
- ○ 30-40%
- ○ 40-50%
- ○ 50-60%
- ○ 60-70%
- ○ 70-80%
- ○ 80-90%
- ○ 90-100%
- ○ Weet ik niet

Hoe heeft het aandeel van uw kosten dat gericht is op cyberveiligheid in de afgelopen 5 jaar ontwikkeld?

- ○ Het aandeel is afgenomen
- ○ Het aandeel is gelijk gebleven
- ○ Het aandeel is toegenomen
- ○ Weet ik niet

Bedrijfsinformatie

Bedrijfsinformatie

Hoeveel personeelsleden, uitgedrukt in voltijdsbanen (FTE), zijn actief in de Nederlandse vestiging(en) van uw organisatie (indicatief)?*

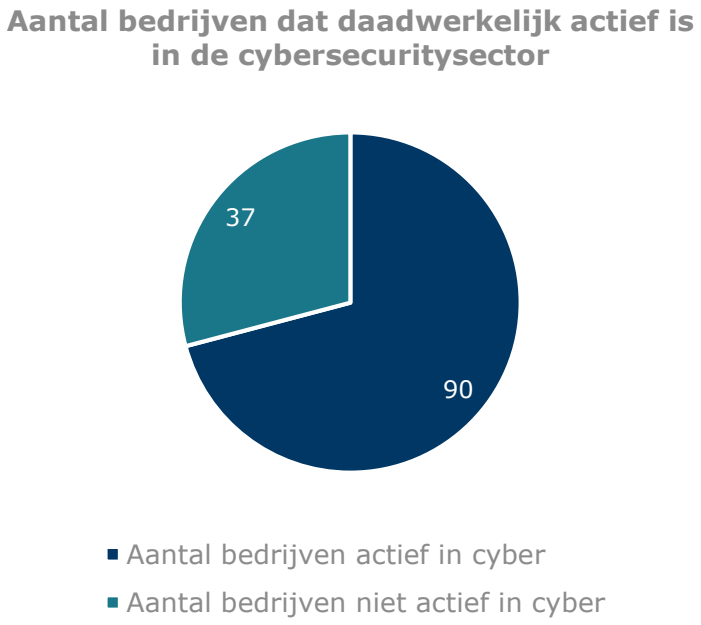
Wij zouden graag de meest recente gegevens ontvangen. Het zou fijn zijn als u het jaar van de gegevens kunt vermelden in uw antwoord.

Wat was de omzet, uitgedrukt in miljoenen euro, van de Nederlandse vestiging(en) van uw organisatie (indicatief)?*

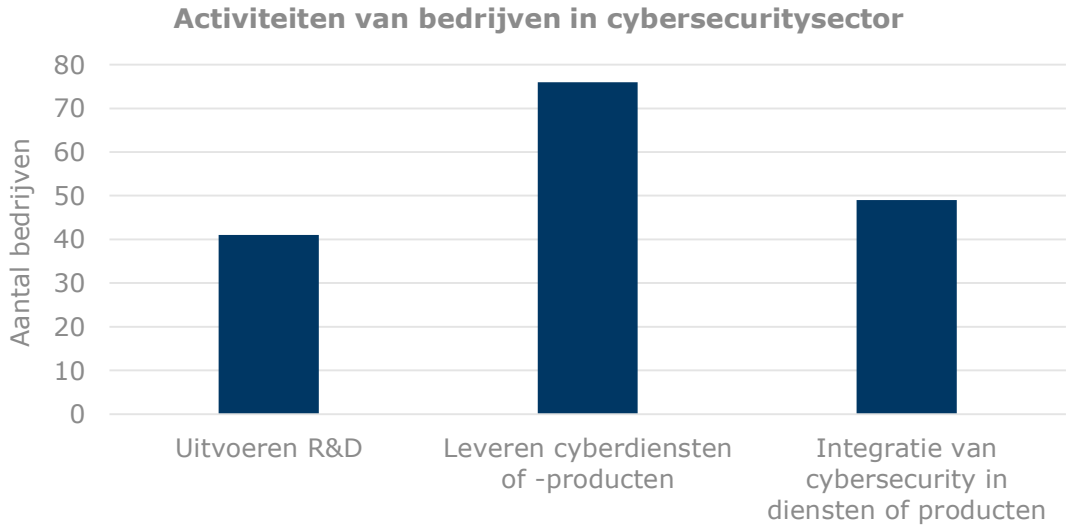
Wij zouden graag de meest recente gegevens ontvangen. Het zou fijn zijn als u het jaar van de gegevens kunt vermelden in uw antwoord.

Uitkomsten

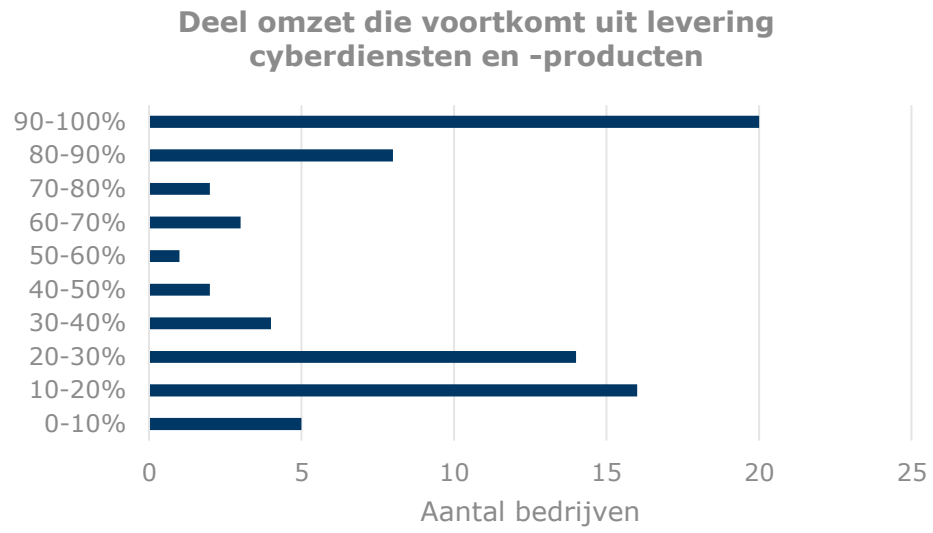
Generieke uitkomsten (alle enquête respondenten, n= 127)



Figuur 14. Bedrijven die wel en niet actief zijn in de cybersecuritysector

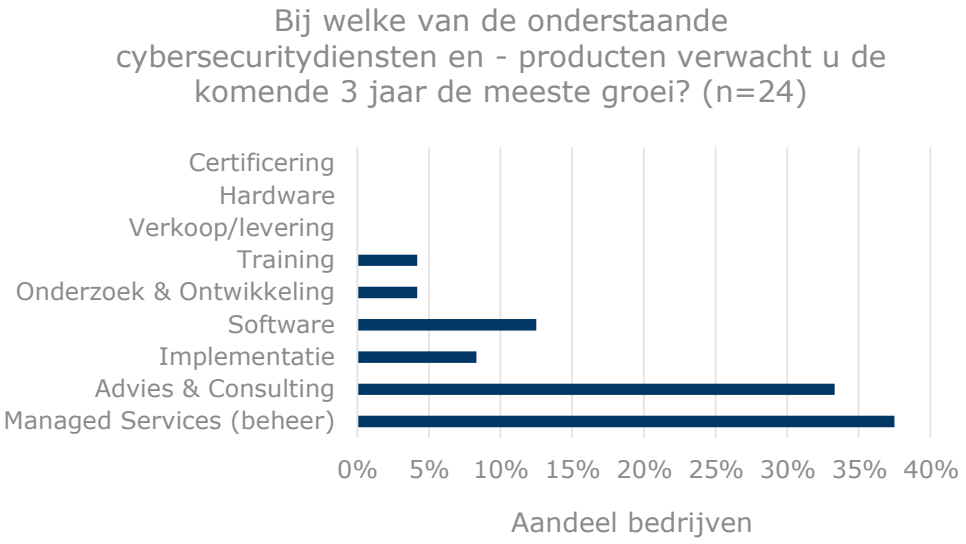


Figuur 15. Soort activiteiten van bedrijven in de cybersecuritysector

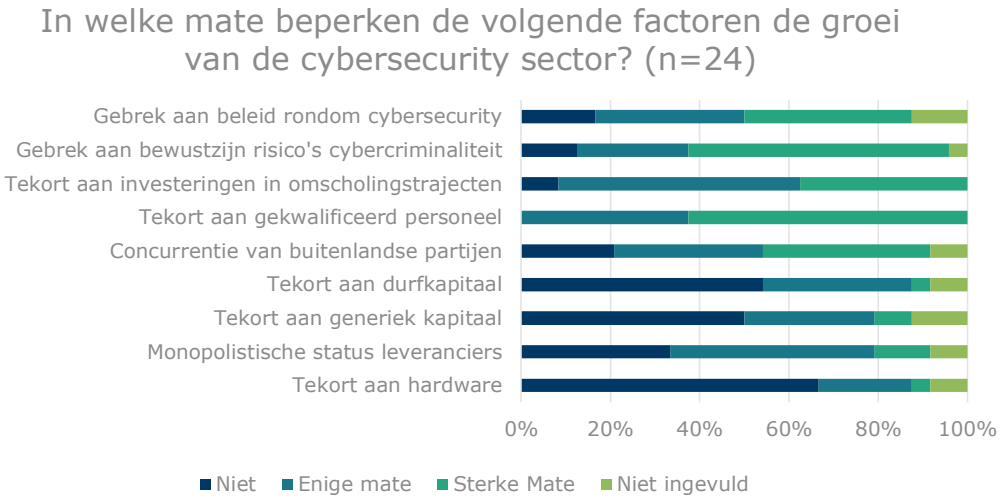


Figuur 16. Omzet uit levering van cyberdiensten en -producten

Groei van de sector (respondenten die actief zijn in R&D, levering van producten & diensten en integratie)

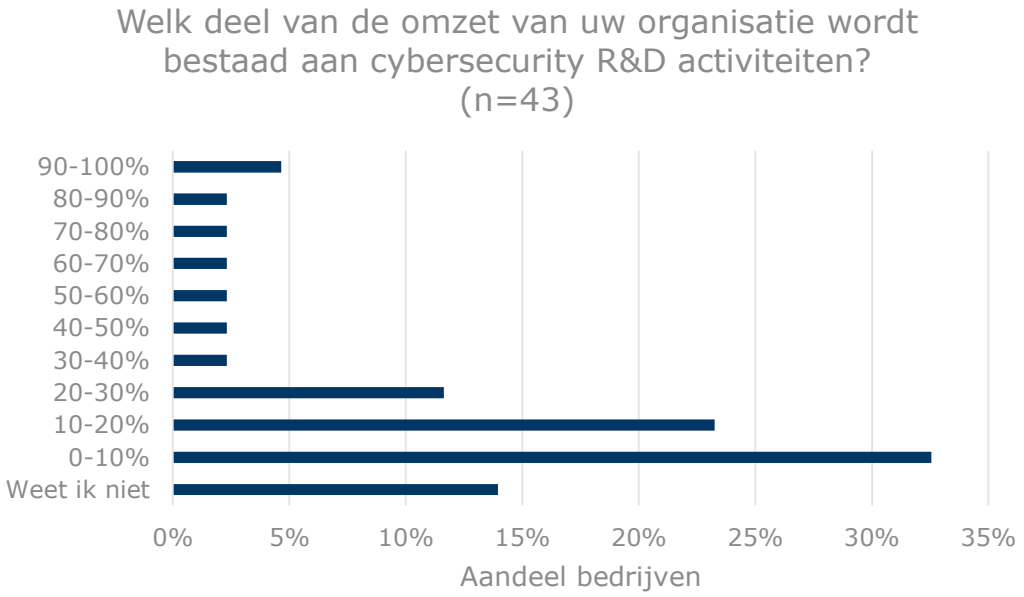


Figuur 17. Verwachte groei naar categorie

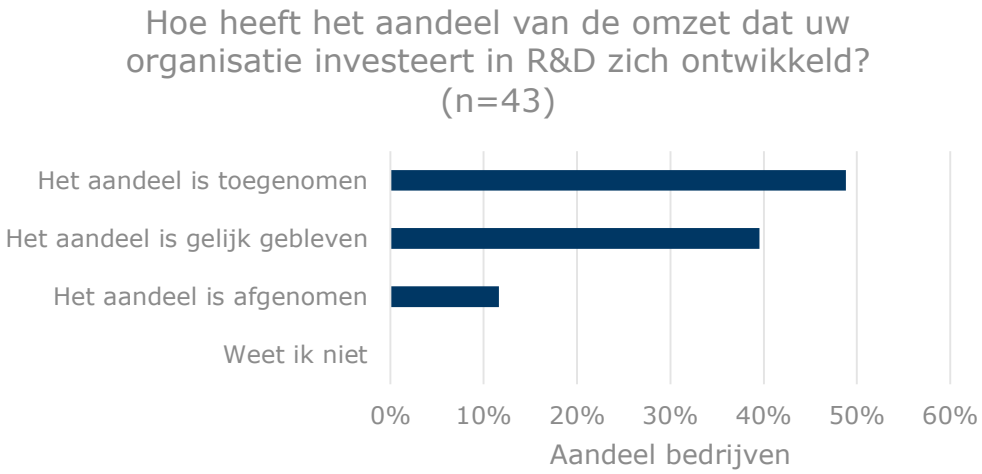


Figuur 18. Redenen voor beperkingen aan groei

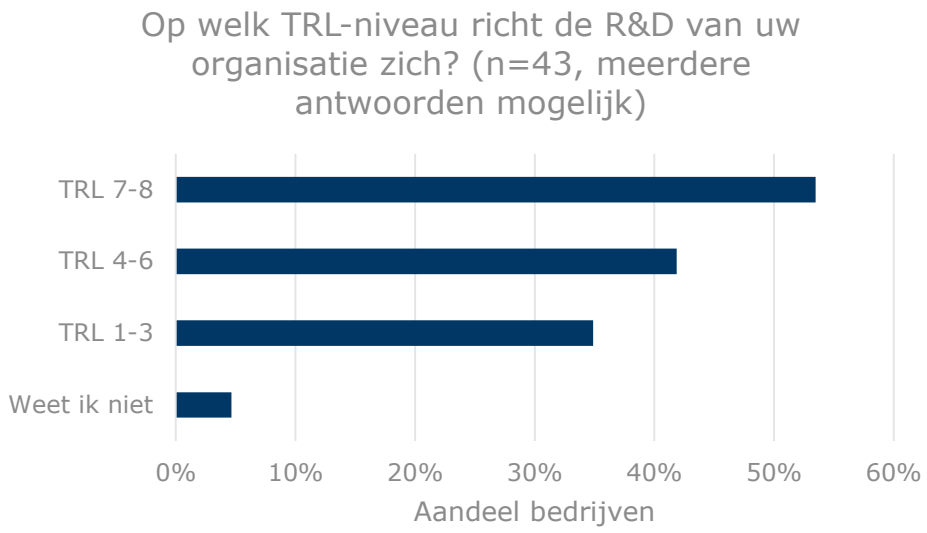
Cyber R&D – respondenten die actief zijn binnen R&D



Figuur 19. Deel van de omzet besteed aan R&D



Figuur 20. Ontwikkeling uitgaven aan R&D



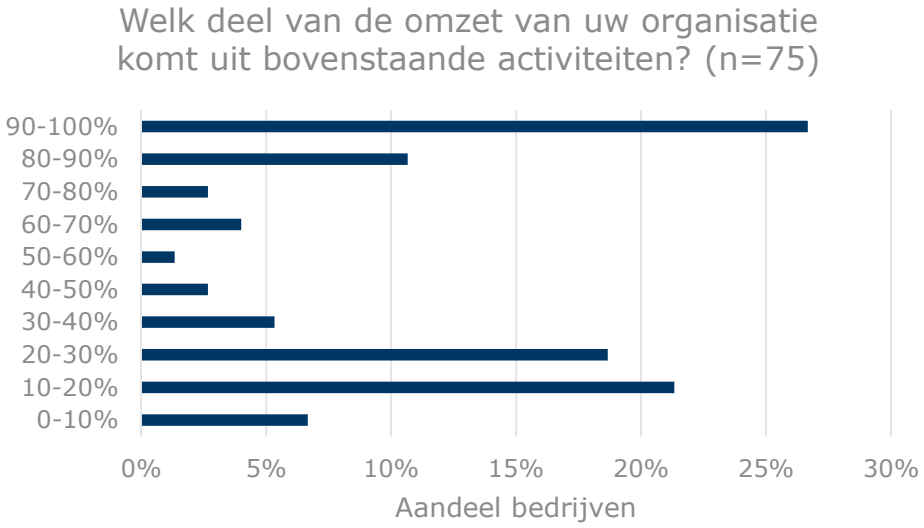
Figuur 21. TRL niveau van R&D

TRL staat voor Technology Readiness Level en geeft de mate van ontwikkeling van een technologie aan (TRL 1 staat aan het begin van de ontwikkeling en TRL 9 is technologie die technisch en commercieel gereed is).[198] Hierbij is TRL 1, 2 en 3 *verkennen*, met hierin fundamenteel onderzoek, toegepast onderzoek en toetsing. TRL 4, 5 en 6 draait om *ontwikkelen* waarin prototypes centraal staan. TRL 7 en 8 draaien om *demonstraties*. Het is duidelijk dat respondenten vooral aangeven gericht te zijn op demonstraties, aangezien meer dan de helft zich richt op TRL 7 en 8.

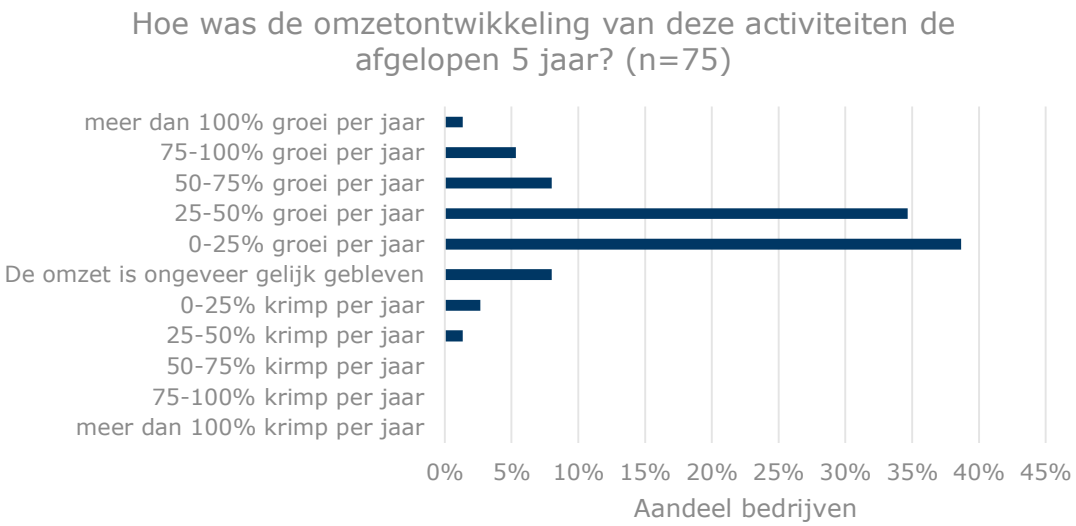
[198] https://www.rvo.nl/onderwerpen/trl

Levering van cybersecurityproducten en diensten - respondenten die actief zijn met levering van cybersecurityproducten en diensten

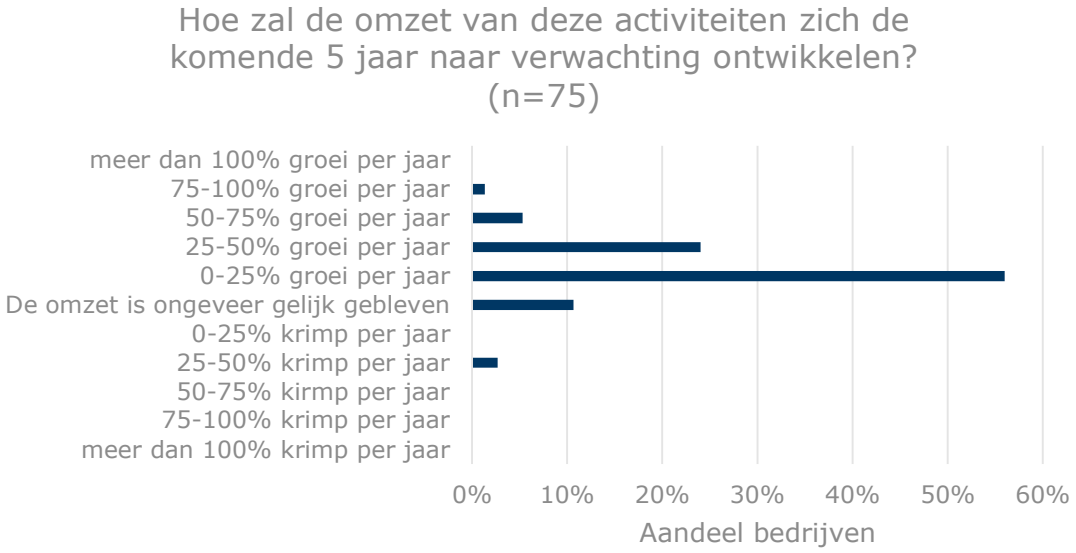
Figuur 22. Type diensten en -producten die geleverd worden



Figuur 23. Deel van de omzet uit cybersecurityproducten en -diensten

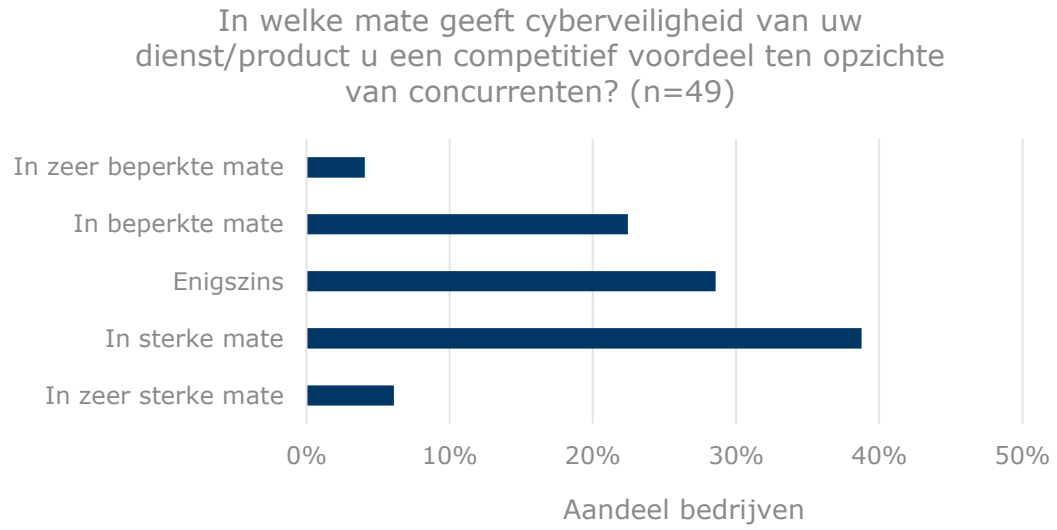


Figuur 24. Omzetontwikkeling van cybersecurityproducenten



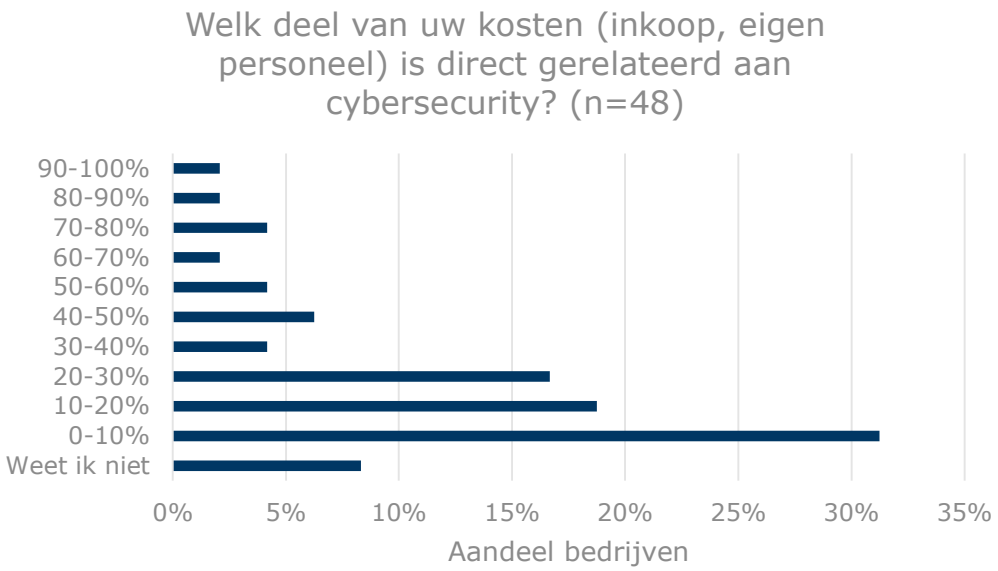
Figuur 25. Verwachte ontwikkeling van de omzet

Integrators – respondenten die actief zijn als integrator



Figuur 26. Mate van competitief voordeel van integratie cyberveiligheid

Figuur 27. Motivatie van integratie cyberveiligheid



Figuur 28. Aandeel van de kosten gerelateerd aan cybersecurity

Figuur 29. Ontwikkeling van kosten voor cyberveiligheid

Bijlage 4. Uitkomsten CBS-Microdata

In deze bijlage presenteren we alle uitkomsten van de analyse van CBS-microdata. De tabellen waarin de ENISA categorieën zijn gebruikt als verdeling bevatten geen eindtotaal. Dit is omdat een bedrijf in meerdere ENISA categorieën kan opereren. Het optellen van de categorieën per jaar geeft daarmee een vertekend beeld. Verder moet worden opgemerkt dat de cijfers waarschijnlijk een bovenkant van de schatting zijn. Dat komt omdat (1) een deel van de bedrijven ten onrechte in de sample zit en (2) de bedrijven die terecht in de sample zitten ook activiteiten uitvoeren die geen betrekking hebben op cybersecurity. Wij presenteren daarom na de analyse van de CBS-microdata de gecorrigeerde uitkomsten. Het aantal bedrijven is niet gecorrigeerd.

De natuur van de gebruikte methode om bedrijven met cybersecurity activiteiten te identificeren staat toe om slechts huidig actieve bedrijven te identificeren. De KvK-nummers van deze bedrijven zijn per jaar gekoppeld aan de CBS-microdata. Gegeven dat cybersecurity een dynamische sector is, is het aannemelijk dat een deel van deze bedrijven na 2015 zijn opgericht. Bedrijven zijn daarom niet meegenomen in jaren voor hun oprichting. Dit is terug te zien in het groeiende aantal bedrijven over de jaren. Daarnaast is het niet mogelijk in de geschiedenis te kijken wat betreft websites van cybersecuritybedrijven omdat deze simpelweg niet meer online staan. Het is daarom mogelijk dat wij voor eerdere jaren een onderschatting van de omvang van de sector maken.

Op basis van enquêteresultaten is de correctiefactor als volgt bepaald: bedrijven met minder dan 10 werknemers halen ~50% van hun omzet uit cybersecurity-activiteiten, bedrijven met 10-99 werknemers halen ~40% van hun omzet uit cybersecurity-activiteiten en bedrijven met 100 werknemers of meer halen ~25% van hun omzet uit cybersecurity-activiteiten. Dit komt overeen met een gewogen gemiddelde van ~29%. Indien de uitsplitsingen naar grootteklasse in tabellen aanwezig zijn, hebben we de drie separate percentages gehanteerd. In de andere tabellen hebben we het gewogen gemiddelde van 29% gebruikt.

Uitkomsten van de CBS-microdata analyse

Aantal bedrijven

Tabel 11. Het aantal bedrijven per categorie. Eén bedrijf kan in meer dan één categorie vallen en cijfers zijn niet op te tellen.

Categorie	2015	2016	2017	2018	2019	2020	2021
Advies	988	1046	1091	1185	1222	1271	1299
Certificering	363	388	425	451	469	485	493
Distributie	229	246	265	292	308	329	332
Hardware	440	463	473	505	525	541	560
Implementatie	303	333	342	367	387	404	427
Managed services	931	1011	1063	1151	1209	1285	1342
Software	947	1010	1087	1170	1226	1290	1342

Tabel 12. Aantal bedrijven per grootteklasse

Grootteklasse	2015	2016	2017	2018	2019	2020	2021
0	405	471	509	585	582	624	630
1	907	972	1036	1128	1219	1242	1310
2	236	221	236	236	252	298	290
3-4	214	225	224	237	244	257	274
5-9	297	328	327	330	360	371	386
10-19	311	305	338	344	321	328	327
20-49	262	289	303	332	348	374	393
50-99	144	141	148	162	176	175	175
100-149	53	60	66	78	81	69	73
150-199	32	37	34	37	34	50	49
200-249	15	18	25	23	26	29	31
250-499	40	47	45	47	55	64	68
500-999	27	25	26	29	32	30	26
1000 of meer	32	37	40	36	38	37	42
Eindtotaal	2975	3176	3357	3604	3768	3948	4074

Tabel 13. Het aantal bedrijven per regio

Regio	2015	2016	2017	2018	2019	2020	2021
Noord Nederland (Friesland, Groningen, Drenthe)	161	175	187	195	219	226	236
Noord-midden Nederland (Noord-Holland, Flevoland, Overijssel)	905	977	1027	1100	1172	1215	1254
Zuid-midden Nederland (Zuid-Holland, Utrecht, Gelderland)	1383	1467	1543	1650	1712	1809	1858
Zuid Nederland (Zeeland, Noord-Brabant, Limburg)	526	557	600	659	665	698	726
Nederland	2975	3176	3357	3604	3768	3948	4074

Tabel 14. Het aantal bedrijven per SBI-code

SBI-code	2015	2016	2017	2018	2019	2020	2021
C: Industrie	52	51	51	52	55	55	54
F: Bouwnijverheid	44	44	45	44	49	52	52
G: Groot- en detailhandel; reparatie van auto's	269	268	281	286	295	300	311
J: Informatie en communicatie	1202	1292	1373	1499	1600	1701	1750
K: Financiële instellingen	402	423	442	481	475	484	495
M: Advisering, onderzoek en overige specialistische zakelijke dienstverlening	781	848	896	951	992	1036	1078
N: Verhuur van roerende goederen en overige zakelijke dienstverlening	127	146	162	173	183	185	194
Overig	98	104	107	118	119	135	140
Eindtotaal	2975	3176	3357	3604	3768	3948	4074

Aantal werknemers

Tabel 15. Het aantal werknemers bij bedrijven per categorie. Eén bedrijf kan in meer dan één categorie vallen en cijfers zijn niet op te tellen.

Categorie	2015	2016	2017	2018	2019	2020	2021
Advies	81620	80528	83204	84091	89039	87222	88582
Certificering	10011	10499	11501	12630	12921	13682	13900
Distributie	18880	19191	20165	21253	20966	21725	21840
Implementatie	29954	34264	33602	35082	34331	31198	35226
Overig (Managed services, Software en Hardware)	613073	858990	722728	689861	733854	660836	727346

Tabel 16. Het aantal werknemers van bedrijven per regio

Regio	2015	2016	2017	2018	2019	2020	2021
Noord Nederland (Friesland, Groningen, Drenthe)	18002	19592	11454	8669	12049	9409	9330
Noord-midden Nederland (Noord-Holland, Flevoland, Overijssel)	129839	212923	151110	156096	153191	130718	149924
Zuid-midden Nederland (Zuid-Holland, Utrecht, Gelderland)	69341	70704	93511	89625	91317	112260	119929
Zuid Nederland (Zeeland, Noord-Brabant, Limburg)	67577	71962	65002	43919	66888	45365	47122
Nederland	284759	375181	321077	298309	323445	297752	326305

Tabel 17. Het aantal werknemers van bedrijven per SBI-code

SBI-code	2015	2016	2017	2018	2019	2020	2021
C: Industrie	7541	7682	7623	8002	8042	7738	7658
F: Bouwnijverheid	2537	2463	2414	2455	2738	2776	2849
G: Groot- en detailhandel; reparatie van auto's	17700	16370	16064	16135	16223	16852	18341
J: Informatie en communicatie	58150	61767	61031	58241	60821	83758	88806
K: Financiële instellingen	81933	89087	67691	64572	86172	55909	64533
M: Advisering, onderzoek en overige specialistische zakelijke dienstverlening	107667	185967	151783	143739	138952	115874	129820
N: Verhuur van roerende goederen en overige zakelijke dienstverlening	11187	12283	12582	13247	13396	12783	12198
Overig	1544	1862	1889	1918	2051	2062	2100
Eindtotaal	288259	377481	321077	308309	328395	297752	326305

De tabel met het aantal werknemers per grootteklasse van bedrijven ontbreekt om logische redenen.

Omzet

Tabel 18. De omzet van bedrijven per categorie in miljarden euro's. Eén bedrijf kan in meer dan één categorie vallen en cijfers zijn niet op te tellen.

Categorie	2015	2016	2017	2018	2019	2020	2021
Advies	11,8	14,4	17,7	16,9	19,1	19,8	17
Certificering	2,3	2,5	3	3,3	3,7	3,9	4,1
Distributie	5,2	6,2	6,1	7,8	7,1	11,7	10,2
Hardware	7,4	8,6	8,2	9	9,4	12,3	11,6
Implementatie	4,4	4,9	4,9	5,1	5,4	7,9	7,4
Managed services	11	12,2	11,9	14,6	17,1	21,4	20,6
Software	9,7	10,8	12	13,2	14,5	18,4	18,7

Tabel 19. De omzet van bedrijven per grootteklasse in miljarden euro's

Grootteklasse	2015	2016	2017	2018	2019	2020	2021
1	0,18	0,19	0,27	0,28	0,27	0,27	0,25
2	0,12	0,16	0,18	0,15	0,20	0,18	0,17
3-4	0,20	0,21	0,21	0,25	0,32	0,24	0,37
5-9	0,77	0,77	0,74	0,92	1,21	1,12	1,05
10-19	1,63	2,15	1,55	1,62	1,15	1,41	1,84
20-49	2,31	2,27	3,33	3,05	2,80	3,41	3,95
50-99	2,59	2,42	2,76	3,94	4,45	4,94	4,65
100-149	3,25	3,71	3,23	3,73	5,06	3,82	3,69
150-249	4,03	5,26	5,09	6,83	6,51	10,22	7,51
250-499	5,53	5,92	7,14	5,99	6,98	9,81	11,06
500-999	2,80	2,79	2,47	3,52	4,80	3,39	3,65
0 of meer dan 999	9,00	12,59	15,49	16,77	18,10	19,23	17,83
Eindtotaal	32,43	38,44	42,45	47,05	51,85	58,03	56,03

Tabel 20. De omzet van bedrijven per regio in miljarden euro's

Regio	2015	2016	2017	2018	2019	2020	2021
Noord Nederland (Friesland, Groningen, Drenthe)	0,66	0,66	0,72	0,77	0,92	1,01	1,01
Noord-midden Nederland (Noord-Holland, Flevoland, Overijssel)	11,54	15,10	17,49	16,87	19,42	21,69	22,22
Zuid-midden Nederland (Zuid-Holland, Utrecht, Gelderland)	14,46	16,52	16,17	20,12	20,69	23,16	22,55
Zuid Nederland (Zeeland, Noord-Brabant, Limburg)	5,77	6,15	8,07	9,28	10,83	12,18	10,25
Nederland	32,43	38,44	42,45	47,05	51,85	58,03	56,03

Tabel 21. De omzet van bedrijven per SBI-code in miljarden euro's

SBI-code	2015	2016	2017	2018	2019	2020	2021
C: Industrie	1,86	1,88	1,90	1,72	1,97	1,88	2,13
F: Bouwnijverheid	0,43	0,46	0,44	0,46	0,48	0,66	0,85
G: Groot- en detailhandel; reparatie van auto's	8,37	9,68	10,04	11,16	11,29	11,33	11,96
J: Informatie en communicatie	11,11	12,06	11,60	15,13	16,56	21,90	20,40
K: Financiële instellingen	3,85	4,63	6,96	8,44	10,07	11,43	8,27
M: Advisering, onderzoek en overige specialistische zakelijke dienstverlening	5,23	7,78	9,54	6,94	7,75	7,20	9,03
N: Verhuur van roerende goederen en overige zakelijke dienstverlening	1,34	1,70	1,73	2,97	3,41	3,33	3,06
Overig	0,24	0,26	0,23	0,23	0,31	0,30	0,33
Eindtotaal	32,43	38,44	42,45	47,05	51,85	58,03	56,03

R&D-uitgaven

Tabel 22. De R&D-uitgaven van bedrijven per categorie in miljoenen euro's. Vanwege beperkingen in de data zijn verschillende categorieën samengevoegd. Eén bedrijf kan in meer dan één categorie vallen en cijfers zijn niet op te tellen.

Categorie	2015	2016	2017	2018	2019	2020
Hardware	56,9	44,9	37,0	64,1	62,5	52,2
implementatie	14,8	20,6	21,0	21,9	28,2	38,2
Overig	1237,5	1346,5	2194,4	2139,2	2734,6	2410,5

Tabel 23. De R&D-uitgaven van bedrijven per grootteklasse in miljoenen euro's. Vanwege beperkingen in de data zijn verschillende grootteklasse samengevoegd.

Grootteklasse	2015	2016	2017	2018	2019	2020
10 - 49	5,1	9,1	11,2	8,0	12,0	9,8
50 - 149	48,3	56,1	59,6	62,3	51,1	28,3
150 - 249	19,1	11,4	13,4	19,5	47,4	81,8
250 - 999	93,6	92,8	86,8	112,7	128,9	209,4
1000 of meer	992,3	1114,0	1545,1	1451,4	1883,4	1629,7
Eindtotaal	1158,4	1283,5	1716,1	1653,9	2122,8	1959,1

Tabel 24. De R&D-uitgaven van bedrijven per grootteklasse als deel van de omzet

Grootteklasse	2015	2016	2017	2018	2019	2020
10 - 49	0,13%	0,21%	0,23%	0,17%	0,30%	0,20%
50 - 149	0,83%	0,91%	1,00%	0,81%	0,54%	0,32%
150 - 249	0,47%	0,22%	0,26%	0,29%	0,73%	0,80%
250 - 999	1,12%	1,07%	0,90%	1,18%	1,09%	1,59%
1000 of meer	11,02%	8,85%	9,98%	8,66%	10,41%	8,48%
Eindtotaal	3,57%	3,34%	4,04%	3,52%	4,09%	3,38%

Toegevoegde waarde

Tabel 25. De toegevoegde waarde van bedrijven per categorie in miljarden euro's. Eén bedrijf kan in meer dan één categorie vallen en cijfers zijn niet op te tellen.

Categorie	2015	2016	2017	2018	2019	2020
Advies	6,6	6,5	9,5	10,1	10,6	10,6
Certificering	0,7	0,8	0,8	1,0	1,0	1,1
Distributie	1,8	2,1	2,1	2,4	2,6	2,4
Hardware	2,7	3,1	3,1	3,5	3,5	3,6
Implementatie	2,1	2,5	2,4	2,7	3,0	2,6
Managed services	10,4	11,8	11,4	11,2	12,3	12,2
Software	7,8	8,6	11,9	12,9	13,4	12,6

Tabel 26. De toegevoegde waarde van bedrijven per grootteklasse in miljarden euro's. Vanwege beperkingen in de data zijn verschillende grootteklasse samengevoegd.

Grootteklasse	2015	2016	2017	2018	2019	2020
1	0,06	0,06	0,06	0,07	0,07	0,08
2	0,03	0,03	0,03	0,03	0,03	0,04
3-4	0,05	0,05	0,05	0,05	0,05	0,06
5-9	0,15	0,17	0,17	0,17	0,19	0,21
10-19	0,50	0,44	0,43	0,42	0,38	0,41
20-49	0,69	0,76	0,91	1,10	1,05	1,10
50-99	0,87	0,97	0,98	1,07	1,29	1,22
100-149	0,63	0,70	0,90	1,05	1,23	0,79
150-199	0,60	0,69	0,63	0,76	0,58	0,91
200-249	0,29	0,44	0,54	0,45	0,54	0,82
250-499	1,50	1,55	1,57	1,72	2,15	2,27
500-999	2,10	2,43	2,43	2,77	3,01	2,99
1000 of meer	13,20	14,14	16,52	16,54	17,30	17,06
Eindtotaal	20,67	22,43	25,23	26,18	27,87	27,95

Tabel 27. De toegevoegde waarde van bedrijven per regio in miljarden euro's

Regio	2015	2016	2017	2018	2019	2020
Noord Nederland (Friesland, Groningen, Drenthe)	0,96	1,04	0,88	0,87	1,13	0,86
Noord-midden Nederland (Noord-Holland, Flevoland, Overijssel)	10,70	11,94	9,19	10,29	10,55	9,95
Zuid-midden Nederland (Zuid-Holland, Utrecht, Gelderland)	6,04	6,11	11,34	11,29	11,80	12,60
Zuid Nederland (Zeeland, Noord-Brabant, Limburg)	2,97	3,34	3,81	3,73	4,40	4,54
Nederland	20,67	22,43	25,23	26,18	27,87	27,95

Tabel 28. Toegevoegde waarde van bedrijven per SBI-code in miljarden euro's

SBI-code	2015	2016	2017	2018	2019	2020
C: Industrie	0,71	0,70	0,68	0,72	0,75	0,75
F: Bouwnijverheid	0,15	0,19	0,17	0,19	0,31	0,30
G: Groot- en detailhandel; reparatie van auto's	2,30	2,25	2,43	2,66	2,74	2,43
J: Informatie en communicatie	7,56	7,77	7,01	6,88	7,48	8,35
K: Financiële instellingen	3,45	4,06	7,34	7,30	7,91	7,77
M: Advisering, onderzoek en overige specialistische zakelijke dienstverlening	5,71	6,53	6,59	7,35	7,52	7,29
N: Verhuur van roerende goederen en overige zakelijke dienstverlening	0,66	0,78	0,85	0,94	1,00	0,89
P: Onderwijs	0,12	0,15	0,16	0,14	0,17	0,17
Eindtotaal	20,67	22,43	25,23	26,18	27,87	27,95

Gecorrigeerde uitkomsten

Aantal werknemers cybersecurity activiteiten

Tabel 29. Het aantal werknemers bij bedrijven per categorie. Eén bedrijf kan in meer dan één categorie vallen en cijfers zijn niet op te tellen.

Categorie	2015	2016	2017	2018	2019	2020	2021
Advies	23670	23353	24129	24386	25821	25294	25689
Certificering	2903	3045	3335	3663	3747	3968	4031
Distributie	5475	5565	5848	6163	6080	6300	6334
Implementatie	8687	9937	9745	10174	9956	9047	10216
Overig (Managed services, Software en Hardware)	177791	249107	209591	200060	212818	191642	210930

Tabel 30. Het aantal werknemers van bedrijven per regio

Regio	2015	2016	2017	2018	2019	2020	2021
Noord Nederland (Friesland, Groningen, Drenthe)	5221	5682	3322	2514	3494	2729	2706
Noord-midden Nederland (Noord-Holland, Flevoland, Overijssel)	37653	61748	43822	45268	44425	37908	43478
Zuid-midden Nederland (Zuid-Holland, Utrecht, Gelderland)	20109	20504	27118	25991	26482	32555	34779
Zuid Nederland (Zeeland, Noord-Brabant, Limburg)	19597	20869	18851	12737	19398	13156	13665
Nederland	82580	108803	93113	86510	93799	86348	94628

Tabel 31. Het aantal werknemers van bedrijven per SBI-code

SBI-code	2015	2016	2017	2018	2019	2020	2021
C: Industrie	2187	2228	2211	2321	2332	2244	2221
F: Bouwnijverheid	736	714	700	712	794	805	826
G: Groot- en detailhandel; reparatie van auto's	5133	4747	4659	4679	4705	4887	5319
J: Informatie en communi-catie	16864	17912	17699	16890	17638	24290	25754
K: Financiële instellingen	23761	25835	19630	18726	24990	16214	18715
M: Advisering, onderzoek en overige specialistische zake-lijke dienstverlening	31223	53930	44017	41684	40296	33603	37648
N: Verhuur van roerende goederen en overige zake-lijke dienstverlening	3244	3562	3649	3842	3885	3707	3537
Overig	448	540	548	556	595	598	609
Eindtotaal	83596	109468	93113	89410	95235	86348	94629

De tabel met het aantal werknemers per grootteklasse van bedrijven ontbreekt om logische redenen.

Omzet cybersecurity activiteiten

Tabel 32. De omzet van bedrijven per categorie in miljarden euro's. Eén bedrijf kan in meer dan één categorie vallen en cijfers zijn niet op te tellen.

Categorie	2015	2016	2017	2018	2019	2020	2021
Advies	3,4	4,2	5,1	4,9	5,5	5,7	4,9
Certificering	0,7	0,7	0,9	1,0	1,1	1,1	1,2
Distributie	1,5	1,8	1,8	2,3	2,1	3,4	3,0
Hardware	2,1	2,5	2,4	2,6	2,7	3,6	3,4
Implementatie	1,3	1,4	1,4	1,5	1,6	2,3	2,1
Managed services	3,2	3,5	3,5	4,2	5,0	6,2	6,0
Software	2,8	3,1	3,5	3,8	4,2	5,3	5,4

Tabel 33. De omzet van bedrijven per grootteklasse in miljarden euro's

Grootteklasse	2015	2016	2017	2018	2019	2020	2021
1	0,1	0,1	0,1	0,1	0,1	0,1	0,1
2	0,1	0,1	0,1	0,1	0,1	0,1	0,1
3-4	0,1	0,1	0,1	0,1	0,2	0,1	0,2
5-9	0,4	0,4	0,4	0,5	0,6	0,6	0,5
10-19	0,7	0,9	0,6	0,6	0,5	0,6	0,7
20-49	0,9	0,9	1,3	1,2	1,1	1,4	1,6
50-99	1,0	1,0	1,1	1,6	1,8	2,0	1,9
100-149	0,8	0,9	0,8	0,9	1,3	1,0	0,9
150-249	1,0	1,3	1,3	1,7	1,6	2,6	1,9
250-499	1,4	1,5	1,8	1,5	1,7	2,5	2,8
500-999	0,7	0,7	0,6	0,9	1,2	0,8	0,9
0 of meer dan 999	2,3	3,1	3,9	4,2	4,5	4,8	4,5
Eindtotaal	9,4	11,0	12,1	13,5	14,7	16,4	16,0

Tabel 34. De omzet van bedrijven per regio in miljarden euro's

Regio	2015	2016	2017	2018	2019	2020	2021
Noord Nederland (Friesland, Groningen, Drenthe)	0,2	0,2	0,2	0,2	0,3	0,3	0,3
Noord-midden Nederland (Noord-Holland, Flevoland, Overijssel)	3,3	4,3	5,0	4,8	5,5	6,1	6,4
Zuid-midden Nederland (Zuid-Holland, Utrecht, Gelderland)	4,2	4,7	4,6	5,8	5,9	6,6	6,5
Zuid Nederland (Zeeland, Noord-Brabant, Limburg)	1,7	1,8	2,3	2,7	3,1	3,4	2,9
Nederland	9,4	11,0	12,1	13,5	14,7	16,4	16,0

Tabel 35. De omzet van bedrijven per SBI-code in miljarden euro's

SBI-code	2015	2016	2017	2018	2019	2020	2021
C: Industrie	0,5	0,5	0,5	0,5	0,6	0,5	0,6
F: Bouwnijverheid	0,1	0,1	0,1	0,1	0,1	0,2	0,2
G: Groot- en detailhandel; reparatie van auto's	2,4	2,8	2,9	3,2	3,2	3,2	3,4
J: Informatie en communicatie	3,2	3,4	3,3	4,3	4,7	6,2	5,8
K: Financiële instellingen	1,1	1,3	2,0	2,4	2,9	3,2	2,4
M: Advisering, onderzoek en overige specialistische zakelijke dienstverlening	1,5	2,2	2,7	2,0	2,2	2,0	2,6
N: Verhuur van roerende goederen en overige zakelijke dienstverlening	0,4	0,5	0,5	0,8	1,0	0,9	0,9
Overig	0,1	0,1	0,1	0,1	0,1	0,1	0,1
Eindtotaal	9,4	11,0	12,1	13,5	14,7	16,4	16,0

R&D-uitgaven cybersecurity activiteiten

Tabel 36. De R&D-uitgaven van bedrijven per categorie in miljoenen euro's. Vanwege beperkingen in de data zijn verschillende categorieën samengevoegd. Eén bedrijf kan in meer dan één categorie vallen en cijfers zijn niet op te tellen.

Categorie	2015	2016	2017	2018	2019	2020
Hardware	16,5	13,0	10,7	18,6	18,1	15,1
implementatie	4,3	6,0	6,1	6,4	8,2	11,1
Overig	358,9	390,5	636,4	620,4	793,0	699,0

Tabel 37. De R&D-uitgaven van bedrijven per grootteklasse in miljoenen euro's. Vanwege beperkingen in de data zijn verschillende grootteklasse samengevoegd.

Grootteklasse	2015	2016	2017	2018	2019	2020
10 - 49	2,0	3,7	4,5	3,2	4,8	3,9
50 - 149	24,2	28,1	29,8	31,2	25,5	14,2
150 - 249	9,5	5,7	6,7	9,8	23,7	40,9
250 - 999	46,8	46,4	43,4	56,3	64,4	104,7
1000 of meer	496,1	557,0	772,5	725,7	941,7	814,9
Eindtotaal	578,7	640,8	856,9	826,2	1060,2	978,6

Tabel 38. De R&D-uitgaven van bedrijven per grootteklasse als deel van de omzet

Grootteklasse	2015	2016	2017	2018	2019	2020
10 - 49	0,1%	0,2%	0,2%	0,2%	0,3%	0,2%
50 - 149	0,8%	0,9%	1,0%	0,8%	0,5%	0,3%
150 - 249	0,5%	0,2%	0,3%	0,3%	0,7%	0,8%
250 - 999	1,1%	1,1%	0,9%	1,2%	1,1%	1,6%
1000 of meer	11,0%	8,9%	10,0%	8,7%	10,4%	8,5%
Eindtotaal	3,8%	3,5%	4,3%	3,7%	4,3%	3,5%

Toegevoegde waarde cybersecurity activiteiten

Tabel 39. De toegevoegde waarde van bedrijven per categorie in miljarden euro's. Eén bedrijf kan in meer dan één categorie vallen en cijfers zijn niet op te tellen.

Categorie	2015	2016	2017	2018	2019	2020
Advies	1,9	1,9	2,8	2,9	3,1	3,1
Certificering	0,2	0,2	0,2	0,3	0,3	0,3
Distributie	0,5	0,6	0,6	0,7	0,7	0,7
Hardware	0,8	0,9	0,9	1,0	1,0	1,0
Implementatie	0,6	0,7	0,7	0,8	0,9	0,8
Managed services	3,0	3,4	3,3	3,2	3,6	3,5
Software	2,3	2,5	3,4	3,7	3,9	3,6

Tabel 40. De toegevoegde waarde van bedrijven per grootteklasse in miljarden euro's. Vanwege beperkingen in de data zijn verschillende grootteklasse samengevoegd.

Grootteklasse	2015	2016	2017	2018	2019	2020
1	0,0	0,0	0,0	0,0	0,0	0,0
2	0,0	0,0	0,0	0,0	0,0	0,0
3-4	0,0	0,0	0,0	0,0	0,0	0,0
5-9	0,1	0,1	0,1	0,1	0,1	0,1
10-19	0,2	0,2	0,2	0,2	0,2	0,2
20-49	0,3	0,3	0,4	0,4	0,4	0,4
50-99	0,3	0,4	0,4	0,4	0,5	0,5
100-149	0,2	0,2	0,2	0,3	0,3	0,2
150-199	0,2	0,2	0,2	0,2	0,1	0,2
200-249	0,1	0,1	0,1	0,1	0,1	0,2
250-499	0,4	0,4	0,4	0,4	0,5	0,6
500-999	0,5	0,6	0,6	0,7	0,8	0,7
1000 of meer	3,3	3,5	4,1	4,1	4,3	4,3
Eindtotaal	5,5	6,0	6,7	7,0	7,5	7,5

Tabel 41. De toegevoegde waarde van bedrijven per regio in miljarden euro's

Regio	2015	2016	2017	2018	2019	2020
Noord Nederland (Friesland, Groningen, Drenthe)	0,3	0,3	0,2	0,2	0,3	0,2
Noord-midden Nederland (Noord-Holland, Flevoland, Overijssel)	2,9	3,2	2,5	2,8	2,8	2,7
Zuid-midden Nederland (Zuid-Holland, Utrecht, Gelderland)	1,6	1,6	3,0	3,0	3,2	3,4
Zuid Nederland (Zeeland, Noord-Brabant, Limburg)	0,8	0,9	1,0	1,0	1,2	1,2
Nederland	5,5	6,0	6,7	7,0	7,5	7,5

Tabel 42. Toegevoegde waarde van bedrijven per SBI-code in miljarden euro's

SBI-code	2015	2016	2017	2018	2019	2020
C: Industrie	0,2	0,2	0,2	0,2	0,2	0,2
F: Bouwnijverheid	0,0	0,1	0,0	0,1	0,1	0,1
G: Groot- en detailhandel; reparatie van auto's	0,6	0,6	0,6	0,7	0,7	0,7
J: Informatie en communicatie	2,0	2,1	1,9	1,8	2,0	2,2
K: Financiële instellingen	0,9	1,1	2,0	2,0	2,1	2,1
M: Advisering, onderzoek en overige specialistische zakelijke dienstverlening	1,5	1,7	1,8	2,0	2,0	2,0
N: Verhuur van roerende goederen en overige zakelijke dienstverlening	0,2	0,2	0,2	0,3	0,3	0,2
P: Onderwijs	0,0	0,0	0,0	0,0	0,0	0,0
Eindtotaal	5,5	6,0	6,7	7,0	7,5	7,5

Uitgebreide analyse R&D activiteiten

Aantal bedrijven

Tabel 43. Aantal bedrijven in de R&D personeel, inkomsten door voordeel WSBO en R&D uitgaven analyses

	2015	2016	2017	2018	2019	2020
CS	190	213	224	225	244	244
NL	7281	7451	7503	7629	7773	7852

Personeel

Tabel 44. R&D personeel in termen van aantal medewerkers en opgetelde FTE voor de cybersecuritybedrijven vergeleken met alle bedrijven

		2015	2016	2017	2018	2019	2020
CS	R&D Medewerkers	8750	11993	14355	14606	18332	18240
	R&D FTE	6353,5	9304,87	11789,2	11896,13	15124,32	15010,66
NL	R&D Medewerkers	96065	102086	104075	111512	117551	119162
	R&D FTE	70974,99	76305,55	79854,04	85898,24	90483,43	92274,19

Inkomsten (voordeel door WSBO)

Tabel 45. Inkomsten gemeten als het voordeel door WSBO voor de cybersecuritybedrijven vergeleken met alle bedrijven. Bedragen zijn in miljoenen euro's weergegeven.

	2015	2016	2017	2018	2019	2020
CS	29,68	48,06	50,32	41,31	54,07	56,16
NL	307,84	653,18	643,35	594,50	660,53	661,67

Uitgaven aan R&D

Tabel 46. Uitgaven aan interne en externe R&D voor de cybersecuritybedrijven vergeleken met alle bedrijven. Bedragen zijn in miljoenen euro's weergegeven.

		2015	2016	2017	2018	2019	2020
CS	Interne R&D	820,78	897,86	1373,68	1337,03	1707,6	1601,83
	Externe R&D	337,64	386,7	342,43	317,99	415,2	357,27
	Totale uitgaven	1158,42	1283,46	1716,11	1653,93	2122,8	1959,1
NL	Interne R&D	9413,31	9914,06	10231,55	10922,69	12053,21	12708,37
	Externe R&D	3396,94	4088,46	3937,1	4103,56	4158,1	4058,52
	Totale uitgaven	12810,26	14002,52	14168,65	15026,26	16211,32	16766,89

Aantal bedrijven dat aan onderzoek doet

Tabel 47. Het aantal bedrijven dat aangeeft aan R&D onderzoek te doen.

	2015	2016	2017	2018	2019	2020
CS	104	115	123	123	145	141
NL	2882	2949	2873	2962	3073	3135

Percentage uitgaven aan typen onderzoek

Tabel 48. Percentuele verdeling van uitgaven aan verschillende typen R&D onderzoek.

		2015	2016	2017	2018	2019	2020
CS	Fundamenteel	9,46%	10,24%	9,58%	9,00%	10,58%	9,58%
	Toegepast	40,14%	42,02%	41,54%	37,53%	41,30%	43,68%
	Experimenteel	50,39%	47,74%	48,87%	53,47%	48,13%	46,74%
NL	Fundamenteel	10,44%	10,91%	11,09%	11,61%	10,93%	10,89%
	Toegepast	39,08%	39,19%	37,62%	37,34%	39,54%	42,15%
	Experimenteel	50,49%	49,91%	51,30%	51,04%	49,53%	46,96%

Verdeling van uitgaven aan interne R&D activiteiten

Tabel 49. Percentuele verdeling van uitgaven aan verschillende interne kostenposten.

		2015	2016	2017	2018	2019	2020
CS	Aantal bedrijven	96	110	118	118	142	137
	Bruto lonen	87,32%	87,86%	88,47%	87,74%	87,31%	87,06%
	Overige uitgaven	8,95%	9,30%	9,08%	9,88%	8,85%	10,44%
	R&D investeringen	1,08%	1,02%	0,65%	0,70%	0,79%	0,58%
	Overige R&D investeringen	2,65%	1,82%	1,80%	1,68%	3,06%	1,91%
NL	Aantal bedrijven	2676	2747%	2696	2777	2875	2937
	Bruto lonen	83,25%	82,97%	82,98%	82,68%	82,14%	82,49%
	Overige uitgaven	12,14%	12,62%	12,58%	12,86%	13,56%	13,52%
	R&D investeringen	1,41%	1,28%	1,32%	1,29%	1,07%	1,06%
	Overige R&D investeringen	3,19%	3,12%	3,12%	3,17%	3,23%	2,93%

Verdeling van uitgaven aan externe R&D activiteiten in Nederland

Tabel 50. Percentuele verdeling van uitgaven aan verschillende externe kostenposten in Nederland.

		2015	2016	2017	2018	2019	2020
CS	Aantal bedrijven	36	30	27	34	43	40
	Uitgaven aan overige bedrijven binnen het concern	7,71%	7,83%	25,76%	16,22%	7,66%	11,78%
	Uitgaven aan overige bedrijven buiten het concern	86,53%	82,63%	65,24%	73,04%	79,12%	73,35%

		2015	2016	2017	2018	2019	2020
	Uitgaven aan researchinstellingen en universiteiten	5,76%	9,53%	8,99%	10,74%	13,23%	14,86%
NL	Aantal bedrijven	1490	1271	1138	1175	1177	1218
	Uitgaven aan overige bedrijven binnen het concern	11,66%	13,12%	13,25%	14,77%	14,57%	16,32%
	Uitgaven aan overige bedrijven buiten het concern	74,37%	72,88%	72,81%	70,78%	70,3%	67,37%
	Uitgaven aan researchinstellingen en universiteiten	13,97%	14%	13,94%	14,46%	15,14%	16,31%

Verdeling van uitgaven aan externe R&D activiteiten in het buitenland

Tabel 51. Percentuele verdeling van uitgaven aan verschillende externe kostenposten in het buitenland.

		2015	2016	2017	2018	2019	2020
CS	Aantal bedrijven	28	25	25	20	27	26
	Uitgaven aan overige bedrijven binnen het concern	60,11%	51,61%	58,06%	58,87%	53,82%	47,28%
	Uitgaven aan overige bedrijven buiten het concern	31,64%	46,23%	41,36%	39,37%	44,11%	46,73%
	Uitgaven aan researchinstellingen en universiteiten	8,25%	2,16%	0,58%	1,76%	2,06%	5,99%
NL	Aantal bedrijven	760	688	693	677	725	745
	Uitgaven aan overige bedrijven binnen het concern	36,44%	34,93%	38,48%	38,93%	43,16%	40,72%
	Uitgaven aan overige bedrijven buiten het concern	50,45%	52,63%	51,06%	49,77%	47,48%	48,77%
	Uitgaven aan researchinstellingen en universiteiten	13,11%	12,44%	10,46%	11,3%	9,35%	10,52%

CIS data

Octrooiaanvragen

Tabel 52. Aantal bedrijven dat octrooiaanvragen heeft gedaan in de periode 2018-2020.

	Octrooi_aangevraagd	Percentage
CS (n = 329)	20	6,1%
NL (n = 7425)	621	8,4%

Omzetverdeling voor productinnovaties

Tabel 53. Percentuele verdeling van omzet gegenereerd uit verschillende typen producten.

	CS (n = 152)	NL (n = 2465)
Nieuw voor de markt	13,96%	14,02%

	CS (n = 152)	NL (n = 2465)
Nieuw voor bedrijf	13,68%	13,50%
Onveranderd	72,36%	72,48%
Totaal	100,0%	100,0%

Ontwikkeling productinnovaties – Goederen

Tabel 54. Het aantal bedrijven dat goederen heeft geïntroduceerd die nieuw zijn voor het bedrijf, verdeeld naar type ontwikkelsamenwerking

	Ontwikkelpartij	Absoluut	Percentage
CS (n = 58)	Eigen bedrijf	43	74,1%
	In samenwerking met ander bedrijf of instelling	22	37,9%
	Eigen bedrijf door aanpassing op goederen van derden	8	13,8%
	Uitsluitend andere bedrijven	8	13,8%
NL (n = 1742)	Eigen bedrijf	1354	78,5%
	In samenwerking met ander bedrijf of instelling	856	49,7%
	Eigen bedrijf door aanpassing op goederen van derden	292	16,9%
	Uitsluitend andere bedrijven	167	9,7%

Ontwikkeling productinnovaties – Diensten

Tabel 55. Het aantal bedrijven dat diensten heeft geïntroduceerd die nieuw zijn voor het bedrijf, verdeeld naar type ontwikkelsamenwerking.

	Ontwikkelpartij	Absoluut	Percentage
CS (n = 132)	Eigen bedrijf	112	84,8%
	In samenwerking met ander bedrijf of instelling	52	39,4%
	Eigen bedrijf door aanpassing op goederen van derden	21	15,9%
	Uitsluitend andere bedrijven	10	7,6%
NL (n = 1415)	Eigen bedrijf	1052	74,3%
	In samenwerking met ander bedrijf of instelling	623	44,0%
	Eigen bedrijf door aanpassing op goederen van derden	290	20,5%
	Uitsluitend andere bedrijven	157	11,1%

Bijlage 5. Overzicht interviewrespondenten & interview protocol

Tabel 56. Overzicht interview respondenten

Naam	Organisatie/affiliatie
Liesbeth Holterman	Cyberveilig Nederland
Melvin Koelewijn	SURFcert
Lokke Moerel	Hoogleraar
Bibi van de Berg	Hoogleraar Cybersecurity Governance
Michel Verhagen	Digital Trust Center
Michiel Steltman	DINL
Eddy Boot	Dcypher
Patrick de Graaf	TNO
Pim Takkenberg	Northwave
Lodi Hensen	Tesorion
Inge Bryan	Fox-IT
Ronald Prins	Hunt & Hackett, voorheen Fox-IT
Nort van Schayik	Compumatica
Tim de Wolf	Technolution
Marcel van Asperdt	Eye Security
Ronald Verbeek	Cio platform

Interviewprotocol

Doelstelling onderzoek:
Op verzoek van het Ministerie van Economische Zaken en Klimaat, Directoraat-generaal Economie en Digitalisering, Directie Digitale Economie voert Dialogic een onderzoek uit naar de economische kansen van de cybersecuritysector. Het doel van dit onderzoek is om 1) na te gaan wat het economische verdienvermogen van Nederland is op het gebied van cybersecurity; 2) het potentieel van de sector en toekomstige trends in kaart te brengen alsmede hun verwachte effect op het verdienvermogen; en 3) na te gaan wat de overheid kan doen om dit economisch potentieel te realiseren.

Aanpak:
We spreken met cybersecurityexperts en experts op het gebied van cybercriminaliteit, economen en marktpartijen. Daarnaast voeren we een uitgebreide kwantitatieve analyse uit (gebruikmakend van CBS-microdata). Ook zetten we literatuurstudie in en organiseren we een validatiesessie met experts.

Procedure:
Er wordt een verslag gemaakt dat later wordt voorgelegd aan de respondent ter goedkeuring. Dit verslag wordt verder niet gedeeld met derden, alleen gebruikt voor dit onderzoek en er worden in het eindrapport geen direct herleidbare quotes opgenomen. In het eindrapport nemen wij op met welke personen en organisaties wij gesproken hebben (mits daar toestemming voor wordt gegeven). We vragen of de respondent akkoord gaat met deze voorwaarden.

Algemene introductie

1. Kunt u uzelf kort introduceren?

Trends in cybersecurity

Op basis van literatuuronderzoek hebben wij een aantal trends in cybersecurity geïdentificeerd [interviewer presenteert de belangrijkste resultaten].

1. In hoeverre klopt dit beeld? Wat zijn volgens u relevante trends op het gebied van cybersecurity(dreigingen)? Heeft u aanvullingen?
2. Wat zijn relevante trends binnen de sector cybersecurity? Heeft u aanvullingen op onze bevindingen?
3. Wat voor invloed gaan deze trends hebben op de cybersecuritysector? En op organisaties buiten deze sector?
4. Wat voor functies zijn hiervoor nodig? In hoeverre veranderen de benodigde competenties de komende periode?
5. Welke andere randvoorwaarden zijn bepalend? [factoren investeringsklimaat noemen]

Verdienvermogen

1. Wat is uw beeld van het huidige economische verdienvermogen van Nederland op het gebied van cybersecurity?
   a. Zijn er voldoende bedrijven en werknemers actief in deze sector?

b. In hoeverre hebben factoren van het investeringsklimaat/vestigingsklimaat hier mee te maken? [voorbeelden investeringsklimaat: tekort aan kapitaal/cybersecurity professionals/moeilijk om idee om te zetten in vermarktbaar product)

Overheidsingrijpen

2. In hoeverre is het gewenst dat de overheid 'iets doet' om de sector te ondersteunen (zodat het economisch potentieel voor Nederland gerealiseerd kan worden)?
3. Wat zou dit dan moeten zijn?/ Welke middelen zou de overheid hiervoor in moeten zetten?
4. Welk effect zouden zulke interventies van de overheid teweeg brengen?/Welk effect kunnen we verwachten door de inzet van deze middelen?
5. Hoe groot zou de rol van de overheid moeten zijn in dit domein? Is cybersecurity een (semi-)publiek goed? Kan je met zonder overheid voldoende innoveren? Functioneert de markt zelf voldoende om veiligheid te garanderen?

Tot slot

6. Zijn er nog andere zaken die u naar aanleiding van dit gesprek kwijt wilt?

Bijlage 6. Vacatureonderzoek

Tabel 57. Top 25 cybersecurityfuncties per jaar. Bron: Dialogic o.b.v. data Jobdigger[199]

Functie	2015	2016	2017	2018	2019	2020	2021	Eindtotaal
Cybersecurity Consultant/Adviseur Informatiebeveiliging	285	339	434	462	368	486	678	3052
(Information) Security Officer	130	242	311	376	456	483	743	2741
Security Specialist	172	202	247	258	310	324	475	1988
Security (Software/System) Engineer	203	170	223	233	225	268	457	1779
Security Manager	44	64	128	119	139	130	225	849
Security Analyst	37	73	88	82	75	119	205	679
Security Architect	53	50	71	85	93	104	211	667
Ethical Hacker	84	76	116	89	87	115	93	660
Cyber Security Expert	12	25	30	60	27	55	74	283
Projectleider Cyber Security	10	24	26	37	32	33	59	221
Netwerkbeheerder/Systeembeheerder	14	21	23	17	35	32	59	201
Security (Pen)Tester	20	22	27	22	21	33	20	165
Traineeship Cyber Security	12	19	24	39	36	19	15	164
Cyber Security Developer	14	7	13	21	12	27	33	127
Security Coördinator/Coördinator Informatiebeveiliging	7	9	12	6	18	13	56	121
Cyber Security Professional	16	6	18	9	18	6	47	120
Medewerker Informatiebeveiliging/Security	10	15	20	10	17	16	23	111
Security Researcher/Scientist	2	1	6	10	10	7	68	104
Account Manager Security	20	9	14	9	12	10	22	96
IT Security Auditor	11	7	4	23	13	23	15	96
Privacy Officer	0	5	13	22	12	14	28	94
Applicatiebeheerder	1	5	14	3	6	26	11	66
IT/Cyber Security		4	28	21	6	3	1	63
Security Administrator	5	8	5	2	9	10	4	43
Security Operator	4	2	4	6	5	8	14	43

[199] Exclusief de vacatures van de bemiddelingsinstellingen. Van de vacatures die via bemiddelingsinstellingen (onder andere uitzendbureaus) worden uitgezet kan, door een beperkte omschrijving van de vacature, niet goed worden bepaald of hij al eerder is uitgezet. Om te voorkomen dat er vacatures dubbel worden meegenomen, is daarom besloten om de vacatures die worden uitgezet door bemiddelingsinstellingen niet mee te nemen. Specifiek is gekeken of één van de volgende woorden voorkomt: 'cyber', 'security', 'beveiliging' of 'hacker'

Tabel 58. Top 25 meest gevraagd cybersecurityvaardigheden Bron: Dialogic o.b.v. data Jobdigger

Vaardigheid	Aantal vacatures (2015)	Aantal vacatures (2021)
Informatiebeveiliging	1355	4214
Certified Information Systems Security Professional	580	1596
Certified Information Security Manager	287	1109
Certified Information Systems Auditor	354	787
Pro-active Security Strategy	209	693
Splunk	109	609
Risicoanalyses	264	538
SIEM	296	510
Penetration Testing	144	474
Data protection	85	413
Netwerkbeveiliging	386	394
incident response	145	371
Security architecture	117	350
Department of Justice Systems Development Life Cycle	97	322
Open Web Application Security Project	145	291
Certified Ethical Hacker	241	287
Intrusion Detection Systems	195	286
GRC	134	285
Risicomanagement	98	274
Ethical Hacker	286	270
Security monitoring	113	263
Certified Cloud Security Professional	10	255
Certified Information Privacy Professional	18	251
Intrusion Prevention Systems	186	248
Control Objectives for Information	202	244
Totaal	**6056**	**15334**

Contact:
Dialogic innovatie & interactie
Hooghiemstraplein 33-36
3514 AX Utrecht
Tel. +31 (0)30 215 05 80
www.dialogic.nl