# “Innovatie is het onderscheid tussen een leider en een volger”

## Analyse vraag naar kennisbehoefte vanuit de cybersecuritysector

Auteurs:

Petra Oldengarm
Liesbeth Holterman

Datum: 21 juni 2019

# Inhoud

Management samenvatting ..... 3
Inleiding ..... 4
Aanleiding van het onderzoek: vraag vanuit EZK ..... 4
Aanpak van het onderzoek ..... 4
Deel 1. De cybersecuritysector in Nederland ..... 6
Digitalisering zorgt voor noodzaak cybersecurity ..... 6
De cybersecurity sector in Nederland ..... 6
Cybersecuritydiensten in Nederland ..... 7
Deel 2. Kennis- en innovatiebehoeften van de cybersecuritysector ..... 9
Techniek ..... 10
Organisatie ..... 11
Mens ..... 11
Deel 3. Oplossingsrichtingen ten behoeve van de mismatch ..... 12
Deel 4. Versterken groeibehoefte cybersecurity sector ..... 15
Tekort aan cybersecurity specialisten ..... 15
Bredere aandacht voor cybersecurity in het onderwijs ..... 15
De overheid als launching customer ..... 16
Belang van vergroten cybersecurity voor (MKB-)ondernemers ..... 16
Bewustwording van cybersecurity op C-level loopt achter ..... 16
Afdwingen van standaarden en normeringen ..... 16
Rol van toezichthouders ..... 16
Meer kennisopbouw vanuit de vraagkant ..... 16
Fiscale prikkels ..... 17
Meer aandacht en oplossingen voor insiders threat ..... 17
Deel 5. Conclusies ..... 18

# Management samenvatting

"Innovatie is het onderscheid tussen een leider en een volger" (innovation distinguishes between a leader and a follower), aldus Steve Jobs. Deze uitspraak is zeker van toepassing op de Nederlandse cybersecuritysector. Het is een jonge sector die snel verandert. De complexiteit van de problematiek en het publiek-private karakter van cybersecurity maakt van de cybersecuritysector in Nederland een groeisector (leiderschap) wanneer de juiste maatregelen worden genomen.

De Nederlandse regering heeft de ambitie om Nederland tot de kopgroep te laten behoren van de Global Cybersecurity Index. Deze is gebaseerd op 25 indicatoren die de mate van commitment van elk land meet op het gebied van juridische maatregelen, technische maatregelen, organisatorische maatregelen, capaciteitsopbouw en samenwerking.

Om de positie van Nederland te versterken is het noodzakelijk dat de innovatieketen op het terrein van cybersecurity wordt verbeterd. Vanwege de rol van de Nederlandse cybersecuritysector, als potentiële accelerator voor innovatievraagstukken, is Cyberveilig Nederland gevraagd een inventarisatie te doen onder haar leden die een eerste aanzet moet geven in de beantwoording van de vraag waar de behoefte van de sector ligt. Uitkomst van deze inventarisatie is dat er vanuit de Nederlandse cybersecuritysector verschillende innovatievraagstukken leven waarbij onderzoeksinstellingen een belangrijke rol kunnen spelen. Hierbij is het wel essentieel dat er één centraal punt komt waar het overzicht aanwezig is van alle cybersecurity onderzoeksvelden (gamma, alfa en bèta) zodat er vraag- en aanbod gestuurd onderzoek kan plaatsvinden. Een andere belangrijke conclusie op basis van de inventarisatie is dat de Nederlandse cybersecuritysector een MKB-sector is. Onderzoeks- en innovatie instrumenten lijken niet altijd goed te passen op de behoeften en investeringsmogelijkheden van MKB-cybersecuritybedrijven. Zeker in het licht dat er grote tekorten zijn aan cybersecurityspecialisten. Hierdoor is de ruimte om medewerkers en financiële middelen vrij te maken voor (lange termijn) innovatievraagstukken ten opzichte van korte termijn klantbehoeften er één die in het voordeel van de korte termijn werkt. Innovatie van de sector kan daarmee (in Nederland) op de lange termijn nadelig worden beïnvloed.

# Inleiding

## Aanleiding van het onderzoek: vraag vanuit EZK

Sinds de uitvoering van het Regeerakkoord Rutte 3 wordt gewerkt aan de versterking van kennis en innovatie op het gebied van cybersecurity. Er is inmiddels een aantal beleidskaders beschreven door de departementen van Defensie, J&V en EZK. Het gaat specifiek om:

- Defensie Cyber Strategie
- Nationale Cyber Security Agenda
- Nederlandse Digitaliseringsstrategie

Binnen de missie gedreven aanpak topsectoren (thema 'Veiligheid'), wordt gewerkt aan een Kennis en Innovatie Agenda Cybersecurity met daaraan gekoppeld Kennis en Innovatie Contracten (KIC's). Ter ondersteuning van dit proces heeft het ministerie van Economische Zaken en Klimaat Cyberveilig Nederland benaderd een behoefte inventarisatie te doen naar cybersecurity kennis en –innovatie bij de leden van Cyberveilig Nederland.

## Aanpak van het onderzoek

Voor het uitvoeren van de inventarisatie zijn de volgende fasen onderkend:

- Fase 1 – literatuuronderzoek
- Fase 2 – schriftelijke inputronde
- Fase 3 – diepte-interviews
- Fase 4 – afstemming met relevante stakeholders
- Fase 5 – Analyse en rapportage

De input die in de fasen 1 tot en met 3 is verzameld heeft zich met name op de volgende vraagstelling gericht:

1. Wat zijn de belangrijkste innovatie opgaven op het gebied van cybersecurity waar Nederlandse cyberbedrijven zich aan willen committeren?
2. Ten opzichte van welke specifieke kennisinhoudelijke vraagstukken ligt hun kennis en innovatie behoefte (dit kunnen alfa, bèta of gamma kennis thema's zijn)?
3. Op welke maatschappelijke/economische toepassingsgebieden willen bedrijven zich verder ontwikkelen?
4. Wat zijn de meest gewaardeerde samenwerkingsvormen voor het Nederlandse Cybersecurity bedrijfsleven op het gebied van publiek-private samenwerking?
5. Zien deze bedrijven concrete mogelijkheden voor samenwerking met kennisinstellingen en of de overheid bij hun ambities?
6. Welke randvoorwaarden zijn van belang voor bedrijven bij eventuele samenwerking met kennisinstellingen en of overheden?

Met een aantal leden zijn diepte-interviews gehouden. Daarnaast heeft TNO een sessie georganiseerd in het kader van de Kennis en Innovatieagenda Cyber, waarbij ook enkele leden van Cyberveilig Nederland input hebben geleverd. Tenslotte heeft Cyberveilig Nederland samen met dcypher een bijeenkomst gehouden met als titel 'cybersecuritysector meets science' om beter zicht te krijgen waar

de kennisbehoeften en -mogelijkheden liggen voor wederzijdse samenwerking en waar nog een gat overbrugd moet worden. Al deze input is gebruik voor deze inventarisatie.

# Deel 1. De cybersecuritysector in Nederland

Met een inventarisatie van de kennis- en innovatiebehoefte van de Nederlandse cybersecuritysector willen we een beter beeld krijgen van de doorstroming van kennis vanuit kennisinstellingen richting cybersecuritysector. Omdat de behoefte naar kennis- en innovatie sterk samenhangt met de groeimogelijkheden van de sector in Nederland is het document in een aantal delen onderverdeeld. Het eerste deel schetst een algemeen beeld van de Nederlandse omvang van de cybersecuritysector, in het tweede deel wordt ingegaan op de kennis- en innovatiebehoeften en wordt een mismatch geïdentificeerd. In het derde deel worden enkele oplossingsrichtingen met betrekking tot die mismatch besproken. Het vierde deel geeft weer waar de groeibehoefte zit en het document sluit in het vijfde deel af met conclusies en aanbevelingen.

## Digitalisering zorgt voor noodzaak cybersecurity

Nederland is een digitale koploper in de wereld en één van de '*most connected countries in the world*'. Rond de 97 procent van de Nederlandse bevolking heeft toegang tot internet. Nederland behoort daarmee tot de digitale voorhoede binnen Europa. Deze digitalisering brengt economische kansen met zich mee én vraagt om het verhogen van de weerbaarheid tegen cyberdreigingen. Door digitalisering zijn steeds meer bedrijven, burgers en overheden in toenemende mate afhankelijk van informatie- en communicatietechnologie. Discontinuïteit door onder andere cybercriminaliteit en diefstal van (intellectuele) eigendommen wordt steeds reëler. Desinformatie ('fake news') en de ondermijning van de democratische rechtsorde is een zorgelijke ontwikkeling. Aandacht voor cybersecurity is daarom geen luxe, maar noodzaak. Het verkleinen van de digitale kwetsbaarheid van Nederland is een gemeenschappelijke uitdaging waar de overheid, kennisinstellingen en het cybersecurity bedrijfsleven tezamen een belangrijke rol spelen.

## De cybersecuritysector in Nederland

De verwachting is dat de toename van de mondiale cybersecuritymarkt groeit naar ongeveer 250 miljard dollar in 2023.[1] Onduidelijk is hoe groot de markt van cybersecurity dienstverleners is in Nederland. In 2016 is op verzoek van het ministerie van Economische Zaken en Klimaat een onderzoek uitgevoerd naar de economische kansen van de cybersecuritysector in Nederland. Hieruit bleek dat ongeveer 10% van de omzet van ICT-dienstverleners gekoppeld is aan cybersecuritydienstverlening met een omzet van tussen de € 6,9 en € 7,5 miljard in 2014.2 Hoewel Cyberveilig Nederland niets af doet aan dit onderzoek dient wel te worden opgemerkt dat maar een gedeelte van de cybersecuritymarkt zichzelf in een ICT-dienstverlener kan herkennen. Het vakgebied van cybersecurity is breder dan dat van techniek alleen en richt zich op mens, techniek en organisatie: van secure softwareontwikkelaars, tot auditors tot gedragswetenschappers. De inschatting is dat er rond de 250 bedrijven in Nederland dienstverlening bieden binnen het vakgebied van cybersecurity. Het betreft dan zowel bedrijven die zich 100% op cybersecurity richten als bedrijven die cybersecurityproducten en -diensten als onderdeel leveren van een breder portfolio. Dit is bovendien exclusief de (grote) groep van zelfstandig ondernemers. Wanneer je kijkt naar het ledenbestand van Cyberveilig Nederland (per 1 juli 2019 bestaande uit bijna 50 leden) dan kun je de volgende voorzichtige conclusie trekken over de cybersecuritysector in Nederland:

- Cybersecurity dienstverleners in Nederland bestaan uit (kleine) MKB-bedrijven;

[1] https://www.statista.com/statistics/595182/worldwide-security-as-a-service-market-size/
[2] https://www.rijksoverheid.nl/documenten/rapporten/2016/05/17/economische-kansen-nederlandse-cybersecurity-sector

- Cybersecuritydienstverlening is vaak een aparte business binnen een andere bedrijfstak. Denk hierbij aan KPN Security binnen KPN of de Cybersecurity Unit binnen Hoffmann.
- Er is een breed aanbod van cybersecuritydiensten, gericht op oplossingen rond mens, techniek en organisatie.

Onderverdeling leden Cyberveilig Nederland per 1 juni 2019 naar bedrijfsomvang (uitgedrukt in aantal medewerkers)[3]:

| Aantal medewerkers | Aantal cybersecurity dienstverleners |
|---|---|
| 2-10 | 26 |
| 11-20 | 3 |
| 21-50 | 10 |
| 51-100 | 3 |
| 101-250 | 2 |
| 250-400 | 2 |
| 400+ | 0 |

Tenslotte mag niet onvermeld blijven dat de laatste jaren verschillende (toonaangevende) Nederlandse cybersecuritybedrijven zijn overgenomen door buitenlandse partijen. Voorbeelden hiervan zijn Fox-IT (Britse NCC-Group), Security Matters (Amerikaanse ForeScout), Redsocks (Roemeense Bitdefender) en recent SecureLink (Franse Orange). Redenen voor deze overnames zijn onder andere de behoefte aan het vergroten van de slagkracht en de wens van expansie van deze bedrijven naar buitenlandse markten.

## Cybersecuritydiensten in Nederland

De cybersecuritysector creëert toegevoegde waarde door het aanbieden van producten en diensten die de cyberrisico's proberen te verminderen en schade efficiënt herstellen. Op basis van de Cybersecurity Monitor van het CBS en geredeneerd vanuit de afnemers van cybersecuritydiensten kan worden gezegd dat in 2016 50 % van de bedrijven met 10 of meer werkzame personen een ICT-veiligheidsincident heeft gehad, waarvan de helft ook kosten moest maken. Voor de bedrijven met 2 tot 10 werkzame personen was dit 26%, waarvan 44 % kosten moest maken.[4] Waar een aantal jaren geleden cybersecurity nog werd gezien als een ICT-vraagstuk wordt het inmiddels steeds vaker onderkend als een business vraagstuk, waar ICT een belangrijk onderdeel van is. Dat zie je terug in de cybersecuritysector in Nederland. Deze bestaat naast de 'traditionele' managed service securityproviders, of gespecialiseerde cybersecurity bedrijven, ook steeds meer uit bedrijven die vanuit een ander vakgebied zijn toegetreden tot de cybersecuritymarkt. Het leveren van technische oplossingen blijft belangrijk binnen de Nederlandse cybersecuritysector, maar er komt ook steeds meer dienstverlening beschikbaar voor de organisatorische en menselijke aspecten van cybersecurity.

[3] Cyberveilig Nederland kent leden die 100% cybersecurity dienstverlener zijn en leden waarvan een deel van de dienstverlening op cybersecurity is gericht. Van de laatste worden alleen de FTE geteld van de medewerkers die deel uit maken van de desbetreffende cybersecurity directie, afdeling of unit.

[4] https://www.cbs.nl/nl-nl/publicatie/2018/38/cybersecuritymonitor-2018

Cybersecuritydienstverlening wordt vaak onderverdeeld in een vijftal domeinen: Identificatie, Protectie, Detectie, Reactie en Herstel.[5] Wanneer we deze plotten op de soorten dienstverlening van de leden van Cyberveilig Nederland dan komen we tot de volgende soorten dienstverlening (niet uitputtend, puur ter verduidelijking):

| Identify (Identificatie) | Protect (Bescherming) | Detect (Detectie) | Response (Reactie) | Recover (Herstel) |
|---|---|---|---|---|
| 1. Asset Management<br>2. Business Environment<br>3. Governance<br>4. Risk Assessment<br>5. Risk Management Strategy | 1. Access Control<br>2. Awareness and Training<br>3. Data Security<br>4. Information Protection Processes and Procedures<br>5. Maintenance<br>6. Protective Technology | 1. Anomalies and Events<br>2. Security Continuous Monitoring<br>3. Detection Processes | 1. Response Planning<br>2. Communications<br>3. Analysis<br>4. Mitigation<br>5. Improvements | 1. Recovery Planning<br>2. Improvements<br>3. Communications |

[5] Gebaseerd op het NIST-framework. Zie: https://www.nist.gov/cyberframework

## Deel 2. Kennis- en innovatiebehoeften van de cybersecuritysector

Een deel van de Nederlandse cybersecuritysector is door een groot tekort aan cybersecurityspecialisten en een toenemende vraag uit de markt voornamelijk bezig met groei-ambities en minder met innovatie-vraagstukken. Er is een grote vraag naar talent, maar te weinig aanbod. Ook bestaat de sector uit een groeiend aantal (startup) bedrijven dat zich bezighoudt met innovatieve producten en diensten, maar een lange aanlooptijd (en investeringen) nodig heeft om hier een goed winstmodel uit te halen. Zeker wanneer technische oplossingen als dienst wordt aangeboden moet er flink geïnvesteerd worden. Het beginnen van bijvoorbeeld een SOC-dienst kost zeer veel tijd en investeringen:

Het starten van een SOC[6]

Faciliteiten: Meubels, computerapparatuur, speciale badges eisen, macht, HVAC, telefonie
Arbeid: SOC analisten, shift leads, SOC managers
Ondersteuning arbeid: Netwerk ondersteuning, system support, database-ondersteuning, telefonie ondersteuning, security device management (wanneer niet door de SOC)
Onderwijs en Training: trainingen, conferenties, HBO/WO medewerkers
Threat intell abonnementen: Up-to-the-minute informatie over de nieuwste bedreigingen
Monitoring technologie: Hardware, software, opslag en implementatie
Aanvullende technologieën: Probleem en change management, e-mail, architectuurontwerp, het delen van kennis

Er zijn voldoende bedrijven binnen het cybersecurity werkveld te noemen die zijn ontstaan, of een nauwe samenwerking hebben met wetenschappelijke instellingen in Nederland.[7] Sommigen worden tijdens het scale-up proces overgenomen door andere cybersecurity bedrijven, de meeste blijven op dit moment nog relatief klein (tussen de 5 en 20 medewerkers).

Wanneer je het innovatie-vermogen van de Nederlandse cybersecurity sector puur bekijkt vanuit de afdelingen R&D dan kun je constateren dat maar een klein aantal van de Nederlandse cybersecurity bedrijven een *dedicated* team heeft dat zich hiermee bezighoudt. Dat is ook niet zo gek als je de gemiddelde omvang van deze cybersecurityondernemingen in ogenschouw neemt. Opvallend is dat deze R&D-teams niet veel samenwerken met de universitaire wereld. Bij bedrijven die geen specifieke R&D-afdelingen hebben wordt wel aan het ontwikkelen aan nieuwe (innovatieve) producten en diensten gedaan, maar veel meer vanuit de dagelijkse werkzaamheden ("onderzoek wordt naast de dagelijkse werkzaamheden gedaan. Dat is goed voor de ontwikkeling van onze medewerkers en veel van hen vinden het leuk om te doen") en gericht op het ontwikkelen van nieuwe producten en diensten die op korte termijn aan het portfolio kunnen worden toegevoegd.

Opvallend is dat er weinig interactie plaatsvindt tussen de Nederlandse universitaire wereld en het cybersecuritybedrijfsleven, terwijl personeel wel over en weer wordt geworven op (HBO- en) WO-niveau. Ook wordt er bij cybersecurity dienstverleners in Nederland amper gebruik gemaakt van PhD-posities en onderzoeksmogelijkheden. Van alle geïnterviewden gaat één bedrijf binnenkort een PhD

[6] https://www.2staff.nl/succesvolsecurityoperationscenterSOC en https://www.ncsc.nl/actueel/factsheets/factsheet-soc-inrichten-begin-klein.html

[7] Denk bijvoorbeeld aan Bitsensor, ontstaan door studenten aan de TU Eindhoven. Ook Security Matters (inmiddels overgenomen door Forescout) is ontstaan vanuit de TU Twente (dankzij een valorisatie grant van STW/ICTRegie) en later ook in samenwerking met de TU Eindhoven. Fox-IT heeft mede door de nabijheid van de TU Delft kunnen uitgroeien tot een groot toonaangevend cybersecurity bedrijf.

student aannemen voor een onderzoek. Als redenen worden gegeven dat de ontwikkelingen binnen het cyberdomein snel gaan en dat een PhD-traject daarvoor te lang duurt. Ook de extra kennisopbouw wordt niet als voordeel gezien: "studenten met een minor of een bachelor zijn meer dan geschikt voor de werkzaamheden die ze moeten uitvoeren. De klant vraagt er ook niet om."

Waar eerst met name de focus lag op het bieden van technische oplossingen, komt nu meer oog voor het belang van een goede samenhang tussen techniek, organisatie en mens om de cyberweerbaarheid te vergroten. Innovaties die een betere balans brengen tussen dit drietal is wenselijk. Denk dan bijvoorbeeld aan het meten of gedragsinterventies effectief zijn door middel van het toepassen van analyse-algoritmes binnen een SOC-omgeving.

Bovenstaande laat zien er dat kansen zijn voor een betere samenwerking tussen de cybersecuritysector en de wetenschap. Voor het gemak worden deze kansen, of beter gezegd kennis- en innovatiebehoeften onderverdeeld in drie categorieën: techniek, organisatie en mens.

## Techniek

De basis van veel cybersecurityoplossingen is techniek. Nieuwe technieken maken zorgen bijvoorbeeld voor snellere detectie, maar kunnen ook menselijke fouten helpen verminderen.

Op gebied van techniek ziet de sector de volgende innovatievraagstukken:

1. Automatiseren van werkzaamheden
    a. Manieren om geautomatiseerd kwetsbaarheden te signaleren in broncode;[8]
    b. Het automatiseren van veel voorkomende stappen in het pentest-proces (en het leren van het gedrag van de pentester om deze sneller/efficiënter te maken);
    c. Automatisch patchen op applicatie-level;[9]
    d. Manieren om automatisch te detecteren of een organisatie wel/niet compliant is (met wetgeving, standaarden en/of eigen beleid).
2. Uitdagingen op gebied van post-kwantum ontwikkelingen
    a. Robuustheid van crypto-algoritmen in een post-kwantum tijdperk kunnen testen;
    b. Post-kwantum communicatiemethoden;
    c. Post-kwantum encryptie.
3. Artificial intelligence / machine learning
    a. Integreren machine learning en kunstmatige intelligentie in detectie en response oplossingen: lange termijn (volledig vervangen) en minder lange termijn (werkproces minder tijdrovend maken);[10]
    b. Kunstmatige detectie van botnets;
    c. Machine learning in software vulnerabilities.
4. OT Security
    a. (Automatische) detectie binnen een industriële omgeving.
5. Cyberweerbaarheid koppeling van techniek met mens en organisatie

[8] Amerikaanse en Israëlische bedrijven zijn hier mee bezig. De Defensie Cyber Strategie schenk hier ook aandacht aan: https://www.defensie.nl/downloads/publicaties/2018/11/12/defensie-cyber-strategie-2018
[9] Kaspersky heeft hier al een oplossing voor.
[10] Verschillende geïnterviewden zijn kritisch of de inzet van kunstmatige intelligentie en machine learning daadwerkelijk een verbetering kan opleveren. Zij stellen dat het werk in bijvoorbeeld een SOC nog altijd veel creativiteit van medewerkers vraagt, hetgeen niet snel door een algoritme ondervangen kan worden.

a. Wat is de correlatie tussen je cyberweerbaarheid en de mate waarin je (technische) cybersecuritymaatregelen hebt genomen?
b. Ontwikkelen technologie die security fouten op basis van menselijk gedrag ondervangt.

## Organisatie

Behalve techniek is een belangrijk onderdeel van cybersecurity het inrichten van beheersbare processen. Ook op dit gebied zijn innovaties nodig, bijvoorbeeld:

1. Governance
    a. Wat is de intrinsieke motivatie van een bestuurder om informatiebeveiliging naar een hoger niveau te brengen?
2. Riskmanagement
    a. Hoe kunnen we de effectiviteit van genomen cybersecuritymaatregelen meten? Wat is de correlatie tussen je cyberweerbaarheid en de mate waarin je (organisatorische) cybersecuritymaatregelen hebt genomen?
    b. Meetbare en voorspellende risk-analyses in plaats van statische 'momentopnames'. Hoe kun je risk-analyses dynamisch maken? Hoe kunnen onder andere meer data en betere risico-indicatoren helpen?
    c. Methodiek om securityaanpak door middel van data te evalueren op effectiviteit rondom oplossingen mens, organisatie en techniek en de relatie tussen deze.
3. Identity management
    a. Hoe kun je het identity landschap vereenvoudigen zodat je niet verschillende rollen/stellels/identiteiten moet beheren (inloggen met Facebook, eHerkenning, DigiD, etc);
    b. Wat zijn goede identity-oplossingen binnen het IoT-domein. Veel IoT hebben (nog) geen 'identity'-component (middellange termijn).

## Mens

Op gebied van menselijke interventies is het belangrijk om de verschuiving te maken van awareness (begrip) naar gedrag (handelen). De volgende thema's spelen op gebied van innovatie:

1. Welke gedragsinterventies zijn van belang in het cyberweerbaar krijgen van medewerkers? Welke bewezen gedragsinterventies binnen andere sectoren kunnen ook toegepast worden binnen het cybersecurity werkveld?
2. (Meetbare) gedragsinterventies rondom (de genomen) cybersecuritymaatregelen: technische data gebruiken voor het menselijke aspect;
3. Hoe krijgen we beter zicht op de werkwijzen van cybercriminelen zodat we betere beschermingsmethoden kunnen maken?

Opgemerkt dient te worden dat cybersecurity een nog relatief nieuw onderzoek- en toepassingsdomein is. Dit uit zich onder andere in het gebrek aan kwalitatieve en kwantitatieve data over cyberweerbaarheid, cybercrime, correlatie inzet van middelen en mate van weerbaarheid, etc. Hier kan de wetenschap een belangrijke rol in spelen, niet alleen in het ontwikkelen van kwalitatief goede en representatieve datasets, maar ook bij het ontwikkelen van goede meet- en analysemodellen. Wetenschap kan evenzeer een rol spelen in het analyseren van datasets waarover publieke- en private organisaties beschikken.

## Deel 3. Oplossingsrichtingen ten behoeve van de mismatch

In het vorige hoofdstuk is vastgesteld dat er sprake is van een mismatch tussen het cybersecurity bedrijfsleven en de wetenschap. Dit hoofdstuk gaat in op een aantal oplossingsrichtingen ten behoeve van deze mismatch:

1. Onvoldoende overzicht. Het is onduidelijk welke onderzoeken waar gebeuren en wat de relevantie kan zijn voor het cybersecurity bedrijfsleven. Eén aanspreekpunt vanuit de wetenschap waar alle onderzoeksvragen vanuit de sector neergelegd kunnen worden en waar overzicht is wie wat waar doet is een essentiële eerste stap zijn. Hierbij is kennis van zowel de cybersecurity sector, de vraagzijde van cybersecurity ontwikkelingen en kennis van het onderzoek domein essentieel. Eén loket waar alle onderzoeksvragen en -behoeften terecht komen;
2. Betere aansluiting van (HBO- en) WO-opleidingen bij de behoefte van de cybersecurity bedrijven. Alle van de geïnterviewden zagen onvoldoende aansluiting tussen het aangeboden curriculum en de werkzaamheden die bij een cybersecurity dienstverlener worden uitgevoerd: "geen enkele studie op HBO of WO-niveau sluit aan op de werkzaamheden, we leiden dus zelf op. Hierdoor duurt het enkele maanden voordat nieuwe medewerkers effectief in te zetten zijn." Door één van de geïnterviewden werd opgemerkt dat er sprake is van een grote omloopsnelheid en tekorten van docenten aan een aantal Hogescholen. Docenten met de juiste kennis trekken weg vanwege het tekort aan specialisten en de (hogere) salarissen die binnen het bedrijfsleven worden geboden. Dit zorgt voor een neerwaartse spiraal waar bedrijven zelf ook hun verantwoordelijkheid in moeten nemen. Bedrijven kunnen bijvoorbeeld een heel blok van een vak voor hun rekening nemen inclusief workshops.

   Door de mismatch tussen opleidingen en het cybersecurity bedrijfsleven zijn eigen opleidingstrajecten ontstaan. Vele cybersecurity bedrijven hebben eigen opleidingscentra waar niet alleen eigen (nieuw) personeel de juiste kennis en kunde wordt bijgebracht, maar ook andere geïnteresseerde klanten (onder andere Computest, Fox-IT, Motiv, Northwave en Tesorion hebben een 'Academie');
3. Te lange weg tussen R&D en resultaat voor de markt. Het is een lange weg voordat een onderzoek(svraag) tot concrete dienstverlening leidt: formuleren onderzoeksvraag → uitwerken vraag → met uitkomsten aan de slag (R&D) → nieuwe dienstverlening uitzetten bij de (potentiële) klant;
4. Samenhang. Er is weinig samenhang tussen de vragers van cybersecuritydiensten, de cybersecuritysector en de wetenschap. Door deze samenhang wel te creëren krijg je een duidelijke vraag-allocatie ("waar ben ik mogelijk kwetsbaar voor?") hetgeen tot onderzoeksvragen kan leiden en van waaruit nieuwe producten en diensten kunnen worden ontwikkeld. Dit vraagt een versterking van het cyber-ecosysteem;
5. Andere financieringsmanieren om de sector en de wetenschap beter samen te laten werken. Momenteel is de meest geëigende manier om samen te werken het starten van een PhD-traject. Een aantal van de geïnterviewde bedrijven ziet een meerwaarde in het starten van consortia waar met verschillende bedrijven en onderzoeksinstituten wordt samengewerkt aan de oplossingen van een probleem of het creëren van nieuwe producten en diensten;
6. Verminderen van de tekorten aan cybersecurityspecialisten. Deze tekorten hebben een rechtstreeks gevolg voor de R&D-capaciteiten: ga je schaars personeel inzetten om geld te verdienen of om lange termijn producten en diensten te ontwikkelen?

7. Meer aandacht voor cybersecurity binnen andere wetenschapsdomeinen. Cybersecurity is een combinatie van mens, organisatie en techniek. Deze moeten meer met elkaar in balans worden gebracht. Hiervoor is het van belang om andere academische domeinen te integreren ("holistische benadering") binnen het cybersecurity domein. Denk hierbij aan gedrag, recht, data-analyse, kunstmatige intelligentie, machine learning, maar ook bij technische studies ten behoeve van bijvoorbeeld OT-security;
8. Ontbreken van vakliteratuur. Zoals gezegd is cybersecurity een relatief nieuw vakgebied. Het vakgebied is ontstaan vanuit de computerwetenschap. De laatste tijd komt er meer aandacht aan andere domeinen die van belang zijn voor digitale weerbaarheid te maken. Onder andere binnen de gammawetenschappen. Veel cybersecurityoplossingen zijn gericht op het creëren van awareness, die zeer effectief zijn om mensen bewust te maken van de digitale risico's die zij lopen. Het ontbreekt aan van voldoende vakliteratuur over gedragswetenschap in relatie tot cybersecurity.
9. OT-security als groei- en innovatiekans. De complexiteit en automatiseringsgraad van technische installaties neemt steeds verder toe in Nederland. Bedrijven worden steeds afhankelijker van systemen en het Internet of Things groeit exponentieel. Cybersecurity in het ICS/SCADA en Industrial Automation & Control Systems domein wordt nog onderbelicht in het aantal diensten en producten dat hierin voor handen is. Aangezien Nederland veel technische kennis heeft en technische universiteiten hoog staan aangeschreven ligt op dit terrein een duidelijke innovatiekans.

Naast het gebrek aan een goede wisselwerking tussen het cybersecurity bedrijfsleven en de wetenschap zijn er ook nog andere aandachtspunten te vermelden die het de innovatie van het Nederlandse cybersecurity bedrijfsleven in de weg staan:

1. Belang van informatiedeling vanuit de overheid. Het delen van informatie over cybersecurity-incidenten moet de norm worden. Door diverse meldplichten en de Algemene Verordening Gegevensbescherming (AVG) heeft de overheid unieke informatie over de oorzaken en effecten van incidenten. Deze beschikbare informatie binnen onder andere het Nationaal Cyber Security Centrum (NCSC), de Autoriteit Persoonsgegevens (AP), en andere toezichthouders zou omgezet moeten worden in kwalitatief hoogwaardige informatie die gebruikt kan worden om innovatieve producten en diensten te ontwikkelingen die aansluiten bij de behoeften vanuit de markt. Uiteraard mag de overheid duidelijke voorwaarden stellen waaronder gedeeld mag worden met belanghebbenden. Het delen van (dreigings)informatie zorgt ook voor betere kwaliteit van de (dreigings) informatie waardoor het algehele niveau van cybersecurity binnen Nederland omhooggaat.[11]
2. Aandacht voor scale-ups en investeringen/extern kapitaal. In Nederland komt steeds meer aandacht voor het startup-klimaat. Denk hierbij aan het succes van Startup Delta. Echter waar startups zich kenmerken tot innovatie en productontwikkeling is aandacht voor het opschalen ook belangrijk. Hiervoor is onder andere toegang tot kapitaal belangrijk omdat (met name) technische oplossingen veel startkapitaal vragen. Een aantal van de geïnterviewden heeft ervaring met het aantrekken van

[11] Opgemerkt dient te worden dat er vanuit de overheid al verschillende initiatieven worden ontplooid om deze informatiedeling op gang te brengen. Zo is Cyberveilig Nederland in gesprek met het NCSC in het kader van het OKTT-traject en over aansluiting van SOC-dienstverleners aan het Nationaal Detectie Netwerk (NDN). Ook het DTC-programma, waar het niet vitale deel van het Nederlandse bedrijfsleven cyberweerbaar wordt gemaakt brengt informatiedeling op gang die een positieve uitwerking kan hebben op de behoefte naar nieuwe producten en diensten.

extern kapitaal. Hierbij werd aangegeven dat de toegang tot Amerikaans kapitaal makkelijker is dan het aantrekken van kapitaal vanuit Europa. Een aantal van de respondenten gaf aan dat er weinig kennis over cybersecurity is bij investeerders. Hierdoor dreigen irreële verwachtingen over groeikansen en omzet het te winnen van de kwaliteit van de dienstverlening. Een aantal van de geïnterviewden gaf aan dat de toegang tot private financieringen ook lastig was, terwijl andere respondenten juist aangaven dat het relatief gemakkelijk is om private funding aan te trekken.

3. Versimpeling (innovatie) subsidies t.b.v. MKB-bedrijfsleven. Een aantal van de geïnterviewden stelde dat het voor hen, als MKB-bedrijf, zeer moeilijk is om zicht te krijgen op de verschillende subsidiepotjes die voor innovatie beschikbaar zijn. Dit geldt zowel op provinciaal, nationaal (o.a. DTC/TVO en WBSO), als Europees (Horizon2020) niveau: "Zicht krijgen op welke subsidies interessant zijn en waar wij aanspraak op zouden kunnen maken is dusdanig ingewikkeld en tijdrovend dat wij hiervoor een gespecialiseerd subsidiebureau voor moeten inhuren, hetgeen wij dus maar niet doen." Ook de vorm waarin de regelingen zich manifesteren nodigt weinig uit tot deelname. Bij veel regelingen moeten bedrijven naast tijd ook financiële middelen in samenwerkingsprojecten steken. Gezien de omvang van de marktpartijen, zijn deze nagenoeg niet aanwezig. Innovatieve regelingen die beter aansluiten op deze sector zijn daarom nodig.
4. De overheid als accelerator van innovatie. Ongeveer 85% van de digitale capaciteiten wordt door Nederland geïmporteerd, waarvan het merendeel van buiten de EU. Dit maakt Nederland digitaal kwetsbaarder terwijl steeds meer organisaties, waaronder de overheid, juist sterk afhankelijk zijn van digitale capaciteiten. Met name voor de Nederlandse inlichtingendiensten, het NCSC, Rijkswaterstaat en het ministerie van Defensie liggen, vanwege de aard van hun werkzaamheden, mogelijkheden wanneer zij een groter belang hechten aan nationale cyberproducten.
5. Vaststellen essentiële cybersecurity key-capaciteiten door stimuleren Europese markt. Voor veel van de technische oplossingen, bijvoorbeeld binnen een SOC, zijn cybersecurity dienstverleners grotendeels afhankelijk van Amerikaanse producten (zoals Fortinet, Palo Alto, etc). Meerdere geïnterviewden gaven aan dat Europese alternatieven wenselijk zouden zijn vanwege de internationale politieke spanningen en het autonomie/afhankelijkheids-vraagstuk. Om dit te stimuleren moet wel een duidelijke vraag komen vanuit de (Europese) overheid. Het is een politiek en ambtelijk vraagstuk welke cybersecuritydiensten en producten essentieel zijn om een zelfstandige positie in op te bouwen. Wanneer deze vraag helder is kan hier innovatie uit gestimuleerd worden.

Wat als een positief punt wordt gezien zijn de verschillende wet- en regelgevingen die op het gebied van cybersecurity en privacy zijn ontstaan vanuit Europa. Europese wetten en regelgevingen als de AVG (GDPR), WBNI (NIS-directive) en de Cybersecurity Act dragen bij aan een betere integratie en mogelijkheden van de Europese markt en dus van de Nederlandse cybersecuritysector. Ook wordt het hierdoor makkelijker om business uit te breiden naar het buitenland. Meerdere geïnterviewden hebben interesse of zijn bezig met het versterken van hun positie in het buitenland. Met name Duitsland, het Verenigd Koninkrijk, Benelux en 'de Nordics' worden genoemd als potentiele regio's om de business uit te breiden.

In relatie tot bovenstaande gaf een aantal van de geïnterviewde bedrijven aan dat zij bewust alle diensten vanuit Nederland leveren en alleen Nederlandse kapitaal gebruiken, omdat het 'BV-Nederland signatuur' als een positief *selling-point* door klanten wordt gezien.

# Deel 4. Versterken groeibehoefte cybersecurity sector

## Tekort aan cybersecurityspecialisten

Nieuwe medewerkers worden met name geworven op HBO en WO-niveau. Cybersecurity betreft een relatief nieuw vakgebied. Hierdoor zijn er weinig opleidingen die aansluiten op de werkzaamheden die in het (cybersecurity) bedrijfsleven worden gevraagd. 'Kennis en vaardigheden sluiten niet aan bij de gevraagde werkzaamheden. Ook wordt geconstateerd dat cybersecuritytalenten worden 'weggekocht' door grote tech-bedrijven uit, met name, de Verenigde Staten. Eén van de geïnterviewden heeft het hoofdkantoor verplaatst vanuit een provincie naar Amsterdam, om op deze manier ook internationaal personeel aan te trekken.

*Alle geïnterviewden gaven aan dat het tekort aan specialisten een negatieve impact heeft op de groeimogelijkheden en ambities voor hun bedrijf. Ook staat hierdoor de kwaliteit van de geleverde dienstverlening onder druk.*

Ook wordt er veel effort gestoken in bijvoorbeeld summerschools en hackatons om schaars talent binnen te halen. Deze schaarste betreft voornamelijk technisch specialisten (zoals bijvoorbeeld ethische hacker/pentesters, SOC-analisten). Echter ook voor andere specialismen binnen het werkveld wordt affiniteit en/of kennis van cybersecurity gevraagd, hetgeen te beperkt aanwezig is. De geïnterviewden zouden willen zien dat cybersecurity wordt aangeboden binnen het lagere en middelbare onderwijs. Ook zou het goed zijn als personeel uit aanpalende vakgebieden wordt omgeschoold.

Ondanks dat technische ontwikkelingen als machine learning en kunstmatige intelligentie een belangrijke rol kunnen spelen binnen het cybersecurity domein blijft het belang van 'de mens' essentieel. Veel van de werkzaamheden vragen creativiteit (denk aan pentesten) en/of oordeelsvorming (SOC-analisten). Het tekort aan specialisten laat zich dus niet snel door technische vernieuwingen vangen.

NB. Het tekort aan specialisten heeft ook nog een onbedoeld neveneffect: de salarissen van technisch specialisten lopen snel op. Met enkele jaren werkervaring kan al snel enkele malen boven modaal worden verdiend. De loonkosten kunnen hierdoor een negatief effect hebben op de kosten van cybersecuritydienstverlening hetgeen de toegang tot cybersecurity diensten voor MKB-bedrijven moeilijker maakt.

## Bredere aandacht voor cybersecurity in het onderwijs

Digitale vaardigheden zijn noodzakelijk om de ambitie van het kabinet rondom digitalisering waar te maken. Omdat cybersecurity van belang is binnen alle facetten van de digitalisering van de Nederlandse samenleving is het belangrijk dat er meer aandacht komt voor cybersecurity. In verschillende opleidingen ontbreekt het aanleren van securityvaardigheden. Een voorbeeld is de opleiding softwareontwikkeling. Binnen de opleidingen is er amper plaats voor security. Laat programmeurs standaard ook security in de software ontwikkelen. Maar ook binnen andere domein (alfa, beta en gamma) geldt dit. "Gevoel voor techniek is belangrijk. Psychologen weten wel veel van de mens af en hoe zij zich gedragen. Binnen het werkveld van cybersecurity is het toch wel belangrijk dat er kennis is van hoe techniek doorwerkt binnen het gedrag."

### De overheid als launching customer

De Rijksoverheid zou het goede voorbeeld moeten geven in het nemen van beveiligingsmaatregelen tegen cyberdreigingen. Het ministerie van Binnenlandse Zaken en Koninkrijkrelaties zou dit actief moeten stimuleren en, indien nodig, randvoorwaardelijke kaders voor de verschillende ministeries op moeten stellen. Ook het afnemen van Pentesten zou integraal onderdeel uit moeten maken van de cybersecuritymaatregelen bij de vitale infrastructuur. Dit zou de overheid kunnen afdwingen. Daarnaast kan de overheid innovaties binnen cybersecurity stimuleren door zelf actief vraag gestuurd te werken.

### Belang van vergroten cybersecurity voor (MKB-)ondernemers

Bijna alle geïnterviewden maken zich zorgen over het cyber-bewustzijn van, met name, MKB-ondernemers. Het nemen van een aantal basale stappen (goed wachtwoord-beleid, tijdig patchen, etc) wordt hierbij al gezien als een enorme stap om de algemene weerbaarheid van het Nederlandse bedrijfsleven snel te vergroten. Alle geïnterviewden herkennen het beeld dat het onderwerp cybersecurity als onvoldoende belangrijk wordt gezien omdat er de (onterechte) aanname is dat MKB-ondernemers niet vatbaar zijn voor cyber-incidenten. Een aantal van de geïnterviewden ziet hier een belangrijke rol voor belangenorganisaties, waarbij VNO-NCW en MKB-Nederland het voortouw zouden moeten nemen om dit onderwerp nadrukkelijk bij hun leden op de kaart te zetten. Ook gaf één van de geïnterviewden aan dat wanneer er wel wordt geïnvesteerd in cybersecuritymaatregelen, dit vooral voortkomt uit de AVG en het nemen van maatregelen om te voorkomen dat je boetes krijgt dan dat de digitale weerbaarheid van de organisatie een 'incentive' is.

### Bewustwording van cybersecurity op C-level loopt achter

Het onderwerp is voor veel bestuurders nog steeds een IT-vraagstuk in plaats van een business-vraagstuk, zo stellen de meeste geïnterviewden. Hierdoor ontstaat onvoldoende commitment vanuit de directie van een organisatie, waardoor niet altijd de juiste investering plaatsvindt. Eén van de geïnterviewden stelde voor om het onderwerp cybersecurity op te nemen in MBA-opleidingen.

### Afdwingen van standaarden en normeringen

Standaardisatie helpt bedrijven om het 'cybersecurity'-wiel niet opnieuw uit te vinden en draagt bij aan een voldoende basisniveau van te nemen maatregelen. Voorbeelden hierbij zijn de ISO270xx (met 27001 als de bekendste) en de IEC 62443 ('OT-equivalent van de 27001'). Het is van belang dat dit soort standaarden worden getoetst aan concrete casussen en de norm worden op minimaal Europees niveau.

### Rol van toezichthouders

Door verschillende wetten en meldplichten wordt het belang van toezichthouders op het gebied van cybersecurity steeds groter. Aandachtspunt hierbij is de kennis van cybersecurity binnen de toezichthouders. Het TIBER-project van de Nederlandse Bank wordt door verschillende geïnterviewden genoemd als een goed voorbeeld om de mate van veiligheid naar een hoger plan te brengen, wat een aanstuwende werking heeft op de vraag naar cybersecuritydiensten (in dit geval red- en blueteaming), maar ook op de kwaliteit van de dienstverlening.[12]

### Meer kennisopbouw vanuit de vraagkant

Het tekort aan cybersecurityspecialisten wreekt zich over de gehele linie: niet alleen vanuit de cybersecurity dienstverleners, maar ook vanuit de vragers van cybersecuritydiensten. Omdat de

[12] https://www.dnb.nl/binaries/TIBER-NL%20Guide%20Second%20Test%20Round%20final_tcm46-365455.pdf?2019062015

kwaliteit van de vraagstelling tekortschiet wordt er onvoldoende gemeten op de kwaliteit van de cybersecurity dienstverleners. Ook worden niet altijd de juiste oplossingen gevraagd voor het ontstane probleem. Meer hoogwaardige kennis vanuit de vraagkant stuwt de kwaliteit van cybersecuritydienstverlening omhoog.

### Fiscale prikkels

Een aantal geïnterviewden gaf aan dat positieve fiscale prikkels kunnen helpen in het vergroten van toepassing van cybersecuritymaatregelen. Bedrijven die 'security' toepassen en integreren om daarmee hun producten en dienstverlening beter te beveiligen zouden hiervoor fiscaal beloond kunnen worden. De overheid zou het financieel aantrekkelijker kunnen maken voor bedrijven om te investeren in een hogere mate van cyberweerbaarheid. Te denken valt aan het versneld kunnen afschrijven van investeringen die de digitale weerbaarheid vergroten, fiscale stimuleringen voor bedrijven die hun hard- en software veilig ontwikkelen en het stimuleren van cybersecurity innovaties middels de WBSO of SBIR-regelingen. De kennisbehoefte is pas compleet als ook de vraagkant daarbij betrokken wordt. Dat is ook de beleidslijn die CVNL samen met dcypher wil volgen: de brug slaan van onderzoek naar consument.

### Meer aandacht en oplossingen voor insiders threat

De meeste cybersecuritymaatregelen die worden genomen richten zich op buiten-binnen en omgekeerd. Omdat de afhankelijkheid van ICT in de meeste organisaties dusdanig groot is, wordt het belang van dreigingen die van eigen medewerkers komt ook groter. Hier is nog onvoldoende aandacht voor. In dat kader werd ook door één van de geïnterviewden genoemd dat er meer aandacht zou moeten komen voor het screenen van cybersecuritypersoneel. Omdat de vraag naar cybersecuritydiensten groeit, komen steeds meer en vaker medewerkers van cybersecuritybedrijven in aanraking met gevoelige systeeminformatie van bijvoorbeeld vitale objecten of intellectuele eigendommen. Af te vragen is of een VOG afdoende is voor deze medewerkers.

## Deel 5. Conclusies

Op basis van de interviews de overige input kunnen de volgende voorzichtige conclusies worden getrokken:

1. Behoefte aan overzicht en coördinatie binnen het onderzoeks- en kennisdomein in Nederland. Momenteel is er vanuit de sector geen overzicht welke onderzoeken er lopen en welke kansen er liggen voor (potentiële) samenwerkingen op het gebied van onderzoek en innovatie. Er is wel degelijk behoefte aan innovatie binnen de cybersecuritysector in Nederland. Echter, op dit moment is er geen 'plek' waar vraag en aanbod samenkomen. Oftewel, er is geen volwassen ecosysteem op het gebied van cybersecurity innovatie.
2. De cybersecuritysector in Nederland is een groeisector, waarbij grote tekorten zijn aan cybersecuritytalent. Hierdoor kan het zijn dat er meer aandacht wordt besteed aan groei dan aan innovatie;
3. De cybersecuritysector is een MKB-sector. Weinig cybersecuritybedrijven hebben een eigen R&D-afdeling. Hierdoor zijn nauwelijks (grote) budgetten beschikbaar voor onderzoeksgelden. Het (later) kunnen toepassen van onderzoek(sresultaten) is een belangrijke vereiste voor de bedrijven. Hier is nog een groot gat tussen de wetenschap en de cybersecuritysector;
4. De laatste jaren zijn verschillende cybersecuritybedrijven overgenomen door buitenlandse bedrijven. Mede vanuit de groei- en innovatiebehoefte zijn de meeste van deze overnames tot stand gekomen. Het is een politiek vraagstuk of deze ontwikkelingen een negatieve impact (kunnen) hebben op het 'autonomie' en 'made in Nederland/Europa'-vraagstuk zoals dat nu wordt gevoerd naar aanleiding van Kaspersky en Huawei (5G).