TNO innovation for life

Hoofdrapport

Onderzoek naar de impact van R&D&I in het cybersecurity domein

TNO Vector
www.tno.nl
+31 88 866 00 00
info@tno.nl

TNO 2023 R11836 - Onderzoek naar de impact van R&D&I in het cybersecurity – 1 oktober 2023

Onderzoek naar de impact van R&D&I in het cybersecurity domein

Hoofdrapport

Auteurs	Marcel de Heide Gabriela Bodea Reg Brennenraedts (Dialogic) Erik Brouwer (SEO) Sonja Kleter (Dialogic) Elene Lenders (SEO) Anastasia Yagafarova

Rubricering rapport	TNO Public
Titel	TNO Public
Rapporttekst	TNO Public
Aantal pagina's	49 (iexclusief voor- en achterblad
Aantal bijlagen	0
Opdrachtgever	Ministerie van Economische Zaken en Klimaat
Projectnaam	SUP - EZK-ECON. PERSP. CYBERSEC. 2021
Projectnummer	060.49187

Samenvatting

Dit rapport beschrijft de resultaten van een onderzoek naar de impact van R&D&I in het cybersecurity domein. In de context van dit onderzoek zijn vier onderzoeksvragen beantwoord. Deze samenvatting en het rapport zelf zijn gestructureerd volgens deze vragen. De antwoorden zijn tot stand gekomen op basis van statistieken die in de context van dit onderzoek zijn samengesteld, en een serie van interviews.

1. **Hoe leidt cybersecurity R&D&I tot maatschappelijke en economische waarde? Wat is het 'onderliggende' proces?**

De geïnterviewden maken onderscheid tussen twee vormen van effecten van R&D&I.

- Met directe effecten refereren ze aan de impact op organisaties die de resulterende kennis toepassen in hun producten of diensten. De impact beperkt zich in deze context tot 'de aanbieder' hier van.
- Met indirecte effecten wordt gerefereerd aan de brede impact van het gebruik van cybersecurityproducten en -diensten die het resultaat zijn van R&D&I. Niet (alleen) de aanbieders profiteren van deze effecten, maar ook (bovenal) de gebruikers van cybersecurity oplossingen. Het meest genoemde voorbeeld is de bijdrage van cybersecurity toepassingen (en de onderliggende R&D&I) aan onze economische én nationale veiligheid (in de context van opsporing en wetshandhaving, en in het defensiedomein - defensief én offensief).

De geïnterviewden stellen dat directe economische effecten van R&D&I in het cybersecurity domein zijn relatief beperkt - de impact van indirecte effecten is veel groter.

2. **Hoe staat NL er nu voor / wat is de huidige status - van input naar impact?**

Input: R&D uitgaven en -ontwikkeling; R&D personeel

- Op basis van bewerkingen van bestaande statistieken kan geconcludeerd worden dat bedrijven in het cybersecurity domein (*pure* zowel als *partial players*) gemiddeld veel kennisintensiever zijn dan die van de gehele populatie in Nederland: zij geven per onderneming ongeveer 10 maal meer uit aan R&D (2020 als referentiejaar).
- De uitgaven aan R&D van deze bedrijven groeide in de periode 2015-2020 met 95% - veel meer dan de totale private groei van 30% in dezelfde periode.
- Ook de omvang van het R&D personeelsbestand van deze bedrijven groeide sterk. In de periode 2015-2020 werd deze 2,3 maal zo groot - tegenover een groei van 13% gemiddeld bij alle Nederlandse bedrijven.
- De vraag naar (R&D&I) cybersecurity personeel kent een opwaartse ontwikkeling in de onderzochte periode van begin 2014 tot eind 2021, met een duidelijke versnelling na 2020. Vanaf begin 2022 is juist weer een daling in uitgezette vacatures waarneembaar.

Activiteiten: omvang en karakteristieken onderzoek

- In de periode 2015-2020 is het aandeel van de bedrijven in het cybersecurity domein dat zelf aan onderzoek doet licht gestegen: van 54,7% naar 57,8%. Dit onderzoek is voornamelijk van het type 'experimenteel' en 'toegepast', en in veel mindere mate 'fundamenteel'.
- Meerdere partijen geven aan (in de interviews en de survey) dat zij geen eigen onderzoeks- en innovatiecapaciteit hebben op het gebied van cybersecurity. Zij participeren in publieke gefinancierde onderzoekstrajecten. In de periode 2020-2022 is er door RVO ongeveer €35 miljoen aan dit soort onderzoek gefinancierd, in 91 projecten.

Nederlandse partners hebben in dezelfde periode in 53 EU-projecten geparticipeerd, met een totale omvang van €206 miljoen.

Output: patenten

- In de periode 2016-2018 heeft 8,4% van de totale populatie van bedrijven in Nederland een octrooi aangevraagd, tegen 6,1% in het cybersecurity domein.

Outcome: effecten van R&D&I op omzet

- Nederlandse bedrijven die cybersecurity R&D&I uitvoeren doen minder aan productinnovaties (17,6% van de bedrijven in de populatie) dan alle bedrijven in Nederland (23,2%), maar meer aan procesinnovaties (40,1% tegen 19,1%).
- R&D&I is voor deze bedrijven net zo belangrijk voor hun omzet als voor alle innovatieve bedrijven in Nederland.
- Producten / diensten 'nieuw voor de markt' genereren in het domein gemiddeld 13,96% van de omzet - tegenover 14,02% voor de gehele populatie van innoverende bedrijven. 'Nieuw voor het bedrijf' bepaalt 13,68% van de omzet - tegenover 13,50% voor alle ondernemingen.

Impact: ontwikkelingen in toegevoegde waarde

- De groei in toegevoegde waarde van Nederlandse bedrijven met cybersecurity activiteiten over de periode 2015-2020 bedraagt 35%. Merk hierbij wel op dat de ontwikkeling van de toegevoegde waarde niet het resultaat hoeft te zijn van onderzoek en innovatie in het cybersecurity domein alleen.

3. Wat is de invloed van beleid op de huidige situatie?

Veel van de gesprekspartners stellen dat de rol die de Nederlandse overheid speelt in (het sturen van) het cybersecurity domein te beperkt is - bijvoorbeeld met regelgeving van de markt, maar ook als actor in de markt (aan de vraag- en aanbodzijde). Cybersecurity is in de praktijk belegd is bij verschillende ministeries, elk met hun eigen doelstellingen. De rol van R&D&I in de context van die verschillende doelstellingen ook nog eens verschillend, en niet (altijd) heel prominent.

Met name de kleinere bedrijven benoemen beperkingen van het huidige instrumentarium waar vergelijkbare organisaties in andere sectoren ook mee worstelen. De perceptie is dat het huidige innovatie-instrumentarium niet past bij de praktijk van deze (voornamelijk dienstverlenende) cyberbedrijven. De focus op de lange termijn bijvoorbeeld van instrumenten als de PPS toeslag sluit niet aan bij de korte-termijn focus van de innovatiebehoefte.

4. Hoe moet de toekomstige beleidsmix worden vormgegeven?

Veel van de gesprekspartners benoemen dat de vraag naar cybersecurity oplossingen achter lijkt te blijven bij de relevantie die het in hun ogen heeft voor het goed functioneren van de economie en de samenleving. Als geconcludeerd wordt dat dit wordt veroorzaakt door het feit dat cybersecurity een (semi)publiek goed is (en een beslissing over de exacte invulling in die context is evenzeer een politieke afweging), dan leidt dat ook tot een aantal conclusies:

- R&D&I in het cybersecurity domein wordt niet alleen gehinderd door 'traditionele' vormen van marktfalen die worden geassocieerd met het doen van onderzoek en innovatie (zoals het optreden van *spillover* effecten, coördinatiefalen, etc.).
- De 'traditionele' instrumenten (zoals de MIT en de PPS toeslag) zijn dientengevolge niet afdoende om R&D&I in het domein aan te jagen.
- Er is een duidelijke rationale en legitimatie voor een andere rol van de overheid (in de markt, aan de vraagzijde als ook aan de aanbodzijde).

De geïnterviewden stellen dat wat betreft kennis die we 'in huis' zouden moeten hebben dat de overheid moet nadenken wat zij kan 'overlaten aan de (Nederlandse) markt', en wat zij zelf zou moeten (laten) uitvoeren omdat 'die markt niet tot de juiste oplossingen komt'. Dit refereert specifiek aan de rol van de overheid in de aanbodzijde van de markt.

Inhoudsopgave

1 Inleiding

1.1 Aanleiding onderzoek

Onderzoek en innovatie op het gebied van cybersecurity zijn essentieel om ook toekomstige uitdagingen voor het functioneren van de digitale infrastructuur in Nederland te kunnen adresseren. De overheid probeert daarom de richting en de omvang van *research, development en innovation* (hierna: R&D&I) beter te begrijpen, om het (indien noodzakelijk en waar mogelijk) beter te kunnen sturen in het domein.

Nederland behoort tot de meest gedigitaliseerde landen in Europa en in de wereld. In de meest recente survey van de Europese Commissie die de digitale 'status en vooruitgang' van de 27 lidstaten monitort en meet (zie (DESI 2022)), scoort Nederland een derde plaats. Deze positie reflecteert het relatief hoge niveau van digitale connectiviteit dat Nederland bereikt heeft; van het relatief hoge en steeds groeiende niveau van adoptie en integratie van digitale technologieën in de Nederlandse samenleving en in de economie; en tegelijkertijd van een mogelijke structurele afhankelijkheid van digitale technologieën en netwerken, nationaal en internationaal. Het belang van het duurzaam, weerbaar en toekomstbestendig veiligstellen van het digitale stelsel wordt hierdoor sterk benadrukt.

De Nederlandse overheid probeert deze 'digitale status' van Nederland nader te versterken en te beschermen, met specifiek beleid en bijbehorende interventies. Een voorbeeld in deze context is de nieuwe integrale cybersecuritystrategie (NLCS, (NCTV 2022)). Onderzoek en innovatie worden prominent benoemd in deze strategie.

Kader 1: De Nederlandse 'digitale status'.

Om dit thematisch onderzoeks- en innovatiebeleid zo effectief (in het bereiken van de specifieke beleidsdoelen) en efficiënt (wat betreft het gebruik van publieke middelen) mogelijk vorm te kunnen geven is inzicht nodig in (de verschillende vormen van) impact van R&D&I. Een eerste uitgebreide initiële analyse in de context van dit brede onderzoek (TNO 2022a) heeft bevestigd dat juist dat inzicht ontbreekt - door een gebrek aan relevante statistieken en een (breed gedragen) methodologisch kader om de effecten van onderzoek en innovatie te vangen. Dit rapport beschrijft de resultaten van een onderzoek naar de impact van R&D&I in het cybersecurity domein.

1.2 Onderzoeksvragen

Om nader inzicht te krijgen in de impact van cybersecurity R&D&I is TNO in 2021 een onderzoekstraject gestart.[1] In dit traject zijn (achteraf gezien) verschillende opeenvolgende 'fasen' te onderscheiden, die nader beschreven worden in Paragraaf 1.3. Op basis van deze eerdere fasen zijn een viertal onderzoeksvragen geformuleerd (zie Kader 2). Het onderzoek dat in dit rapport wordt beschreven draagt bij aan de beantwoording van deze vragen.

[1] Dit onderzoek is opgezet middels additionele programmafinanciering door het Ministerie van Economische Zaken en Klimaat, met bijbehorende karakteristieken / randvoorwaarden.

Doel van het vervolgonderzoek is (kortweg) om bij te dragen aan effectief en efficiënt onderzoeks- en innovatiebeleid in het cybersecurity domein. Dit resulteert in de volgende onderzoeksvragen:

1. Hoe leidt cybersecurity R&D&I tot maatschappelijke en economische waarde? Wat is het 'onderliggende' proces?
2. Hoe staat NL er nu voor / wat is de huidige status - van input naar impact?
3. Wat is de invloed van beleid op de huidige situatie?
4. Hoe moet de toekomstige beleidsmix worden vormgegeven?

Daarnaast moet dit onderzoek ook leiden tot (een aanzet voor) de ontwikkeling van een aanpak / methodiek voor een structurele evaluatie van de impact van cybersecurity R&D&I.

Kader 2: Onderzoeksvragen.

1.3 Brede onderzoeksopzet: bestaande basis en voorafgaande resultaten

1.3.1 Basis onderzoek: vervolg op resultaten eerdere trajecten

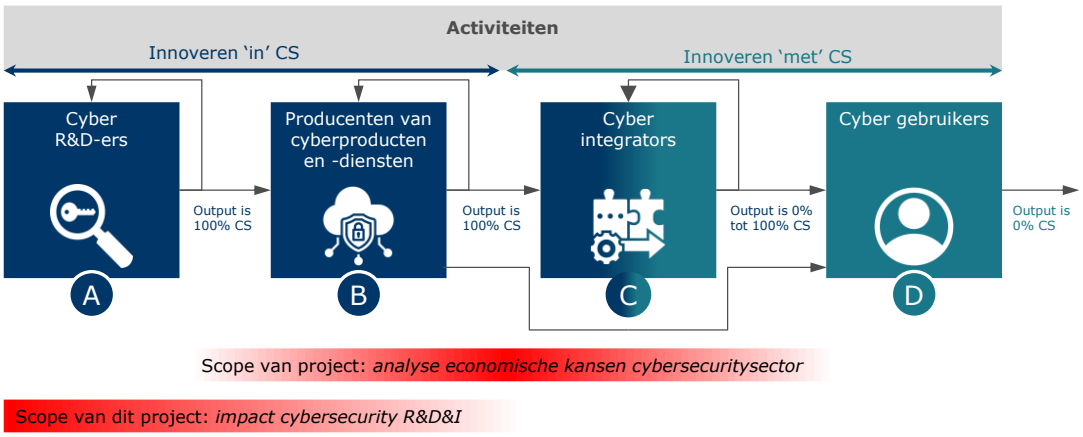
Voor beantwoording van bovengenoemde onderzoeksvragen bouwt het in 2021 opgestarte onderzoekstraject voort op meerdere eerdere onderzoeken (met bijbehorende aannames, methodieken, resultaten en conclusies). Meest relevant in deze context zijn:

- Een inventarisatie uit 2016 naar de omvang van de cybersecurity sector in Nederland, gemaakt als aanzet om inzicht te krijgen in de economische kansen van de sector (SEO 2016).
- Een onderzoek uit 2019 naar hoe de innovatieketen op het terrein van cybersecurity kan worden versterkt. Het bijbehorende rapport (TNO 2019) beschrijft de actoren in de cybersecurity innovatieketen, en de verschillende vormen van samenwerking in de context van verschillende vormen van innovatie in het domein.
- Een vervolg (update) van bovengenoemde inventarisatie uit 2016, uitgezet in de periode 2022 - 2023 door het ministerie van EZK (zie (Dialogic 2023)). De fase van het onderzoekstraject dat in dit rapport wordt beschreven is in parallel uitgevoerd aan deze opdracht. Enkele van de gebruikte methodieken (om actoren te identificeren, en informatie over en met hen te verzamelen, zie Hoofdstuk 2) zijn dusdanig vormgegeven dat ze in beide trajecten input hebben geleverd. De beide onderzoeken moeten wel beschouwd worden als 'losstaand'.

In Figuur 1.1 is de scope van de inventarisatie en die van dit onderzoekstraject weergegeven, uitgezet tegen de verschillende activiteiten (en bijbehorende actoren) in het cybersecurity domein.

De sample van cybersecurity actoren die is samengesteld in de context van (Dialogic 2023) voor de analyse van de economische kansen van de cybersecurity sector is ook gebruikt voor dit onderzoekstraject - specifiek om op om op basis van CBS microdata R&D statistieken te aggregeren. Op deze manier hebben de indicatoren die productie en (een deel van het) R&D&I gedrag adresseren dezelfde basis.

Kader 3: Relatie inventarisatie economische kansen cybersecurity sector, en onderzoek naar de impact van cybersecurity R&D&I.



Figuur 1.1: Scope onderzoekstrajecten, uitgezet naar activiteiten in het cybersecurity domein.

1.3.2 Basis onderzoek: vervolg op eerdere resultaten huidige onderzoekstraject

Behalve bovengenoemde onderzoeken bouwt dit rapport, bij de beantwoording van de onderzoeksvragen van Kader 2, ook op eerdere fasen uit dit onderliggende onderzoekstraject. Deze eerdere fasen moeten gezien worden als een basis waarop de richting van dit onderzoek na afronding iedere keer verder is uitgewerkt. Het onderzoekstraject wordt hier onder nader beschreven / geïllustreerd aan de hand van verschillende eerdere resultaten.

1.3.2.1 Raamwerk voor overheidsinterventie

Als basis voor een gemeenschappelijke visie op de rol van de overheid in het aanjagen van R&D&I is een sessie georganiseerd door TNO voor het ministerie van EZK, waarbij (onder andere) de volgende issues zijn geadresseerd: i) de investeringsbeslissing van bedrijven wat betreft onderzoek en innovatie; ii) 'traditionele' vormen van marktfalen die leiden tot private onderinvestering in R&D; en iii) de effectiviteit en efficiency van verschillende modaliteiten van publieke interventie.

1.3.2.2 Analyse R&D&I indicatoren in het cybersecurity domein

In een volgende fase van het onderzoekstraject is een inventarisatie gemaakt van bestaande indicatoren die (de effecten van) R&D&I in het cybersecurity domein beschrijven. De resultaten zijn beschreven in (TNO 2022a). Op basis van deze inventarisatie kan geconcludeerd worden dat deze set onvoldoende inzicht geeft om een basis te vormen voor beleidsformulering:

- De bestaande set van indicatoren is beperkt in omvang, en adresseert cybersecurity op een hoog (geaggregeerd) niveau.
- Informatie over specifieke technologieën en toepassingen in het domein is niet beschikbaar.
- Veel van de indicatoren proberen vormen van Outcome van het doen van onderzoek en innovatie te vangen, en veel minder van Input, Output en Impact (zie Figuur 4.1).
- Veel van de indicatoren adresseren vooral traditionele vormen van innovatie en samenwerking, en niet bijvoorbeeld open source innovatie.

(TNO 2022a) concludeert daarnaast ook dat het bewerken van bestaande indicatoren die R&D&I 'in den brede' adresseren (zoals 'totale uitgaven aan R&D') zodat nieuwe indicatoren

worden gecreëerd die specifiek het cybersecurity domein beschrijven (en waarvoor nieuwe bijbehorende statistieken zouden moeten worden gecreëerd) complex is, met een duidelijke relatie tussen kwaliteit en benodigde inzet. Hetzelfde geldt voor het creëren van geheel nieuwe indicatoren (met bijbehorende nieuwe statistieken, al dan niet gebouwd op nieuwe microdata).

1.3.2.3 Opzet klankbordgroep

In een volgende fase van het onderzoekstraject is vervolgens een klankbordgroep (met vertegenwoordigers van EZK I&K en NGF, CBS, CPB, Dialogic, SEO en WODC) opgezet, die de verdere aanpak en (voorlopige) resultaten heeft getoetst.

1.3.2.4 Scoping

De laatste stap voor de implementatie van het onderzoek dat de basis vormt voor dit rapport was de uitvoering van een zogenaamde 'scopingfase', waarin noodzakelijke 'kaders' voor de richting van het vervolgonderzoek zijn bepaald. De resultaten van deze fase zijn beschreven in (TNO 2022b). Elementen die zijn benoemd in deze context zijn:

- Definitie van 'cybersecurity'.
- (Werk)definitie van (het doen van) R&D&I met cybersecurity, en in het cybersecurity domein.
- Kader voor het beschrijven van de actoren in het cybersecurity domein: ecosysteem / waardeketen / innovatieketen.
- Kader voor het beschrijven van de effecten van R&D&I: Impact, Activiteiten, Output, Outcome, Impact (gebaseerd op de *'Theory of Change'* - gebruikt voor het beschrijven van impact van de NGF voorstellen).

Vanaf deze scopingfase zijn Dialogic en SEO betrokken bij de uitvoering van het onderzoekstraject.

1.4 Opzet rapport

Dit rapport gaat in het volgende hoofdstuk verder met een korte beschrijving van de aanpak van het onderzoek, voordat in de daarop volgende hoofdstukken de bijbehorende resultaten worden beschreven. Er is gekozen voor deze opzet omdat juist deze aanpak bepalend is voor de 'kwaliteit' van de informatie waarop de conclusies (de antwoorden op de onderzoeksvragen) zijn gebaseerd (zie Kader 4). Zo is het mogelijk (voor de lezer) om de resultaten van het onderzoek te 'duiden', en in een zeker perspectief te zetten.

De aanpak (met bijbehorende methodieken) is verder beschreven in een eigen document getiteld "Onderzoek naar de impact van R&D&I in het cybersecurity domein - Bijlagen". Deze vormt een basis voor een potentiële toekomstige structurele evaluatie van de impact van R&D&I in het domein - een deliverable van dit onderzoek.

Als aanvulling op deze huidige aanpak worden ook aanbevelingen gedaan, in dit hoofdrapport en het rapport met de bijlagen, voor 'eenvoudige' verbeteringen voor en aanvullingen op de gebruikte methodieken - op basis van de ervaringen opgedaan met hun toepassing in de context van dit onderzoek. Deze aanbevelingen worden gepresenteerd in grijs gearceerde kaders.

Dit rapport vervolgt na de korte beschrijving van de aanpak met de beantwoording van de onderzoeksvragen (zie Kader 2). Deze zijn gebruikt als basis voor de verdere structuur van dit

rapport: elke vraag is ‘beantwoord’ in een eigen hoofdstuk. Opgemerkt dient te worden dat per onderzoeksvraag één of meerdere methodieken zijn gebruikt, elk met hun eigen ‘*pros and cons’*. Hierdoor kan het lijken alsof niet alle hoofdstukken even ‘uitgewerkt’ zijn (niet alle onderzoeksvragen in dezelfde mate zijn beantwoord), en er een zekere ‘onbalans’ is in het rapport.

2 Aanpak onderzoek: basis voor conclusies

Dit (deel van het) onderzoek is uitgevoerd in drie opeenvolgende fasen: i) identificeren van relevante actoren; ii) informatie verzamelen met en over deze actoren; en iii) het formuleren van conclusies over de impact van R&D&I in het cybersecurity domein. Dit hoofdstuk beschrijft kort de aanpak en resultaten van fase (i) en (ii), om zo de 'kwaliteit' van deze 'basis' voor de conclusies van fase (iii) - de antwoorden op de onderzoeksvragen die verder in dit rapport zijn beschreven - te kunnen 'duiden', en in een zeker perspectief te zetten.

De 'kwaliteit' van dit onderzoek wordt met name bepaald door de 'kwaliteit' van de sample(s) van relevante actoren waarmee en waarover informatie wordt verzameld. Om de 'kwaliteit' van deze samples te duiden wordt een inschatting gemaakt van hoe de resulterende selecties zich verhouden tot de werkelijke populatie van actoren die aan R&D&I in het cybersecurity domein doen. Daarvoor wordt van elk van de samples de samenstelling beschreven, en een inschatting gemaakt van 'selectiefouten' die zijn gemaakt bij het identificeren van actoren, volgens het 'kader' beschreven in Tabel 2.2.

Het duiden van de kwaliteit van de sample kent wel een beperking: aspecten als de omvang en samenstelling van de 'werkelijke' populatie zijn niet bekend, omdat actoren op geen enkele manier in bestaande statistieken als zodanig zijn 'gelabeld'. Dit is onder andere ingegeven door het feit dat een duidelijke afbakening van (de onderliggende technologieën) van cybersecurity ontbreekt; en door de complexiteit van de R&D&I processen (zie (TNO 2022)).

Kader 4: Kwaliteit van de verschillende samples van actoren in het cybersecurity domein.

2.1 Identificeren actoren

Er zijn in de context van dit vervolgonderzoek drie verschillende bronnen gebruikt om samples van actoren in het cybersecurity domein (die aan R&D&I doen) samen te stellen: Innovatiespotter, Jobdigger, en data over R&D&I subsidieprojecten van RVO en de Europese Commissie.

De samples zijn in vier verschillende 'generieke' stappen samengesteld: i) samenstelling van een lijst van zoektermen; ii) identificatie van organisaties (in geval van Innovatiespotter), vacatures (in geval van Jobdigger), of R&D&I subsidieprojecten, op basis van deze zoektermen in de respectievelijke bron; iii) een 'validatieslag' om zo veel als mogelijk 'ruis' uit de resulterende set te verwijderen; en iv) samenstellen van een (bijbehorende) selectie van relevante actoren.

2.1.1 Selectie op basis van Innovatiespotter

Met behulp van een sample van 'Innovatiespotter' is in het kader van de inventarisatie van de economische kansen van de cybersecurity sector in Nederland (Dialogic, 2023) een

sample gemaakt van organisaties (bedrijven) die actief zijn in het cybersecurity domein.[2] Deze sample is ook gebruikt in de context van deze studie. Een belangrijk voordeel (behalve dat dit efficiënt is) is dat een groot deel van de resultaten van beide studies (en dan met name de gemaakte statistieken) dezelfde basis hebben, waardoor consistente conclusies over bijvoorbeeld productiegedrag in relatie tot R&D&I gedrag getrokken kunnen worden.[3]

Innovatiespotter beheert een database waarin de teksten op de websites van Nederlandse organisaties met een KvK-inschrijving (circa 2,8 miljoen organisaties) zijn opgeslagen. Van al deze organisaties is door middel van *webscraping* de inhoud van hun webpagina uitgelezen en opgeslagen in een database. De database koppelt per organisatie de basisgegevens uit de KvK-inschrijving (zoals adres, naam, contactgegevens, etc.) met de tekst die zij op hun website weergeven.

Uit het bestand van Innovatiespotter is een sample van 5.436 organisaties geïdentificeerd die actief zijn in het cybersecurity domein. Om een zeker inzicht te geven in de samenstelling van de selectie wordt deze in Tabel 2.1 beschreven, uitgesplitst naar de gebruikte categorieën van de ENISA taxonomie (ENISA 2022b) die gebruikt is als basis voor de zoektermen (zie Bijlage A.1).[4] Op basis van deze uitsplitsing kan geconcludeerd worden dat de sample vooral organisaties bevat in de categorieën *'managed services'*, *'software'* en *'advies & consultancy'*.

Tabel 2.1: Aantal met behulp van Innovatiespotter geïdentificeerde actoren in het cybersecurity domein, uitgesplitst naar ENISA categorie.[5]

ENISA categorie	Aantal organisaties (bedrijven)
Software	2278
Hardware	781
Distributie	507
Advies & Consultancy	1952
Implementatie services	703
Managed services	2506
Certificering	699
Totaal	5436

Het is aannemelijk dat lang niet al deze actoren aan R&D&I doen - de sample is veel meer een afspiegeling van de totale cyber populatie. Dit is ingegeven door het feit dat deze is vormgegeven in de context van de analyse zoals beschreven in (Dialogic 2023), dat als doel had de economische kansen van de sector als geheel te analyseren. Bij het informatie verzamelen over de actoren (de tweede fase van dit onderzoek) is hier rekening mee gehouden (zie Paragraaf 2.2.1).

[2] Zie: www.innovatiespotter.nl.
[3] Merk daarbij wel op dat dit niet een specifiek doel is van dit onderzoek, en dat ook niet alle mogelijke conclusies in deze context in dit rapport zullen worden geadresseerd.
[4] Omdat sommige organisaties in meer dan één categorie vallen telt het totaal van de individuele categorieën op tot meer dan 8.727.
[5] Merk op dat het totaal van de geïdentificeerde organisaties (bedrijven) hoger is dan de som van de aantallen voor de verschillende categorieën. Dit is ingegeven door het feit dat sommige organisaties (bedrijven) in meerdere categorieën vallen.

Onderzoek en innovatie in cybersecurity is anders dan in de meer traditionele sectoren van de economie (TNO 2019). Dit is onder andere ingegeven door het feit dat het (nog steeds) een relatief nieuw en breed containerbegrip is waar verschillende sub-sectoren onder kunnen worden verenigd; en omdat de toepassingen een weg vinden naar vele andere sectoren. Op basis van eerder onderzoek onderscheiden we verschillende soorten van actoren en vormen van onderzoek en innovatie, volgens de volgende dimensies:

Pure players - partial players (op basis van (TNO 2019))
In Nederland zijn relatief veel organisaties actief op het gebied van ICT en digitale beveiliging. Dit betreft zogenaamde '*pure players*' - organisaties die alleen cybersecurity gerelateerde activiteiten uitvoeren (zoals Hunt & Hacket uit de lijst van geïnterviewden voor dit onderzoek (zie Tabel 2.7)) - als ook '*partial players*' - actoren voor wie cybersecurity niet tot de '*core*' van hun activiteiten behoort (zoals NXP uit de lijst).

Innoveren *in* het domein, en *met* cybersecurity (op basis van (TNO 2022b))
Voor sommige actoren in het domein zijn cybersecurity oplossingen een doel van R&D&I. Dit wordt in het rapport verder aangeduid als innoveren in het cybersecurity domein. Voor anderen zijn cybersecurity oplossingen een basis voor verdere innovatie in andere domeinen. Dit wordt verder aangeduid als innoveren met cybersecurity (zoals bijvoorbeeld in de financiële sector gebeurt).

Open, gesloten en traditioneel innovatiemodel (op basis van (TNO 2019))
in het cybersecurity domein speelt kennis op veel verschillende manieren een belangrijke rol: om onderscheidend te zijn, om dreigingen het hoofd te kunnen bieden, etc. Bij het creëren van kennis in het R&D&I proces gaan actoren verschillend om met het delen van kennis, en daarmee met het samenwerken in innovatietrajecten, en hoe ze vervolgens met elkaar 'verbonden zijn' in het innovatie ecosysteem. In dit rapport wordt onderscheid gemaakt tussen drie verschillende innovatiemodellen. Deze indeling is gebaseerd op de praktijk van R&D&I in de sector, waarin een breed spectrum van vormen van innovatie is te vinden. Als 'extreem' is het volledig open model te herkennen (bijvoorbeeld de ontwikkeling van open-source softwareontwikkeling), waarbij kennis vrij toegankelijk is, en niet kan worden geclaimd. Aan de andere kant van dit spectrum is er het volledig gesloten model, waarbij bedrijven met '*trade secrets*' werken, en kennis afschermen van de buitenwereld. In dat spectrum ligt ook nog een derde (stabiele) vorm van samenwerking die is te benoemen / beschrijven als een meer traditioneel model, waarbij partijen hun kennis vastleggen (claimen) in patenten en literatuur, en waarbij deze door anderen kan worden gebruikt onder bepaalde voorwaarden.

Kader 5: Dimensies voor het beschrijven van de samenstelling van de sample.

Op basis van de gebruikte zoektermen is het waarschijnlijk dat vooral actoren zijn geïdentificeerd in de groep 'producenten van cybersecurity producten en diensten', en in mindere mate 'cyber integrators' (zie Figuur 1.1). Om de hoeveelheid ruis in de sample te beperken is de classificatie categorie R&D en educatie van de ENISA classificatie niet meegenomen in de zoektermen (zie Bijlage A.1). Het is mogelijk dat actoren daardoor onterecht niet zijn opgenomen, en de groep 'cyber R&D-ers' daardoor relatief ondervertegenwoordigd is – zogenaamde type II fouten (zie Tabel 2.2).

Tabel 2.2: Soorten fouten in de sample van actoren.

	Actor actief in het cybersecurity domein	Actor niet actief in het cybersecurity domein
Actor opgenomen in de sample	Echt positief: actor terecht opgenomen	Foutpositief: actor onterecht opgenomen in de sample *Type I fout*
Actor niet opgenomen in de sample	Foutnegatief: actor onterecht niet opgenomen *Type II fout*	Echte negatieven: actor terecht niet opgenomen

De sample bevat zowel *pure* als *partial players*; en actoren die innoveren in het cybersecurity domein, als ook met cybersecurity oplossingen (zie Kader 5). Het is niet waarschijnlijk dat veel actoren zijn geïdentificeerd die bijdragen aan open innovatie – dat vereist een analyse van *open source* platformen zoals uitgevoerd in de context van (TNO 2019).

Er is veel werk gestopt in het 'verbeteren' van de zoektermen, waardoor veel foutpositieven uit de sample zijn gehaald, en ook foutnegatieven minder voorkomen (zie Bijlage A.1). Hierdoor is de sample steeds verder geoptimaliseerd. Door het toepassen van verschillende 'generieke' filters is de set met actoren verder opgeschoond. Het valt echter niet uit te sluiten dat er nog steeds verschillende type I fouten in de sample zitten, omdat de gehele sample van geïdentificeerde actoren nooit één voor één is gecheckt – iets wat in de context van het onderliggende analyse van (Dialogic 2023) ook niet mogelijk was.

2.1.2 Selectie op basis van Jobdigger

Met behulp van gegevens van 'Jobdigger' is nog een sample gemaakt van actoren die actief zijn in het cybersecurity domein - en dan specifiek op het gebied van R&D&I. Jobdigger heeft met behulp van *webscraping* (en *spidering*) een database opgezet met vacaturedata en arbeidsmarktinformatie (op landelijk, provinciaal en COROP niveau (arbeidsmarktregio) tot aan gemeenten en standplaats), met 2014 als startjaar.[6] De vacatures zijn in de database gelabeld volgens specifieke classificaties,[7] gelinkt aan bijbehorende organisaties, en vervolgens aangevuld met gegevens van het KvK-register.

Uit het bestand van Jobdigger is een sample van 2.406 unieke organisaties geïdentificeerd die actief zijn in het cybersecurity domein (vanaf 2014). Om een zeker inzicht te geven in de samenstelling van de selectie wordt deze in Tabel 2.3 beschreven.[8] In dit geval zijn de actoren uitgesplitst naar beroepsklassen die door het projectteam zijn gedefinieerd op basis van (ENISA 2022a) - een taxonomie met functieprofielen die gebruikt is als basis voor de zoektermen (zie Bijlage A.2). Elke beroepsklasse heeft een eigen verwachte mate van betrokkenheid bij het doen van R&D&I, gebaseerd op een inschatting van het bijbehorende takenpakket van de bijbehorende functies:

- Kernberoepen zoals *'security consultants'* met cybersecurity als kernactiviteit, en R&D&I (zeer waarschijnlijk) als onderdeel van het takenpakket.

[6] Zie: www.jobdigger.nl.
[7] De gegevens (vacatures) worden door Jobdigger geclassificeerd volgens de International Standard Classification of Occupations (ISCO-classificatie), alsmede de eigen Jobdigger Classification of Occupation (JDCO-classificaties). De JDCO-classificatie richt zich alleen op Nederlandse en actuele beroepen en niet alleen op beroepsklassen zoals in het ISCO-model. Dat betekent dat de JDCO-classificatie wordt geüpdatet aan de hand van nieuw ontstane beroepen.
[8] Omdat sommige organisaties vacatures hebben uitgezet in verschillende beroepsklassen telt de som voor de individuele profielen op tot meer dan 2.406.

- Substitutieberoepen zoals *'data engineers'* en *'cloud engineers'*, met een bredere taakopdracht waar cybersecurity en het uitvoeren van R&D&I op het gebied van cybersecurity een nevenactiviteit kan zijn.
- *Educators* (docenten en instructeurs) bevat beroepsklassen die ook R&D&I op het gebied van cybersecurity zouden kunnen uitvoeren.
- Overige brede groep die niet behoren tot bovengenoemde beroepsklassen, maar waarvan mag worden aangenomen dat er een kans is (hoewel kleiner dan voor kern- en substitutieberoepen en *educators*) dat ze betrokken zijn bij cybersecurity R&D&I.

Tabel 2.3: Aantal met Jobdigger geïdentificeerde actoren betrokken bij R&D&I in het cybersecurity domein.[9]

Organisaties die op zoek waren naar de volgenge beroepsklassen	Aantal unieke organisaties
Kernberoepen	939 (39%)
Substitutieberoepen	856 (36%)
Educators (docenten en instructeurs)	119 (5%)
Bredere groep	1639 (68%)
Totaal	2406

Op basis van de gebruikte zoektermen is het waarschijnlijk dat de actoren die zijn geïdentificeerd in de database van Jobdigger vallen in de groepen 'cyber R&D-ers', 'producenten van cybersecurity producten en diensten', als ook 'cyber integrators' (zie Figuur 1.1). Het is ook waarschijnlijk dat vooral veel R&D intensieve organisaties zijn geïdentificeerd (als ook organisaties die R&D&I dienstverlening aanbieden). Alleen dit soort actoren zetten specifieke vacatures uit voor kernberoepen (en in mindere mate voor de overige categorieën), omdat zij deze R&D&I capaciteit kunnen 'onderhouden' voor hun structurele onderzoeks- en innovatieactiviteiten.[10]

Ook deze sample bevat zowel *pure* als *partial players*; actoren die innoveren in het cybersecurity domein, als ook met cybersecurity oplossingen; en organisaties die voornamelijk het traditionele of het gesloten innovatiemodel hanteren (zie Kader 5).

De zoektermen toegepast voor het samenstellen van de sample met kernberoepen is dusdanig 'gericht' dat de kans dat foutpositieven zijn opgenomen gering is. Bij iedere uitbereiding van de zoektermen neemt de kans daarop toe. Maar duidelijk is dat lang niet alle R&D&I actoren van de gehele populatie geïdentificeerd zijn, omdat de database van Jobdigger niet 'compleet' is: lang niet alle instellingen zullen hun vacaturen online uitzetten; en Jobdigger heeft beperkingen wat betreft toegang tot bepaalde vacaturewebsites (zie Bijlage A.2).

Veel werk is ook in dit geval gestopt in het 'verbeteren' van de zoektermen om foutpositieven uit de sample te halen, en foutnegatieven te voorkomen (zie bijlage A.2), en is de sample steeds verder geoptimaliseerd. Maar ook in deze context valt het niet uit te sluiten dat er nog steeds verschillende type I fouten in de sample zitten, omdat de gehele sample van geïdentificeerde actoren nooit één voor één is gecheckt.

[9] Merk op dat het totaal van de geïdentificeerde organisaties hoger is dan de som van de aantallen voor de verschillende categorieën. Dit is ingegeven door het feit dat sommige organisaties vacatures hebben uitgezet in verschillende beroepsklassen.

[10] Daarbij is er dan van uit gegaan dat de vacatures refereren aan langdurige dienstverbanden, niet aan posities voor incidentele en daarmee kortlopende / eindige onderzoekstrajecten. Dit is aannemelijk omdat er kosten zijn verbonden aan wervingstrajecten.

2.1.3 Selectie op basis van data van R&D&I subsidieprojecten

Met behulp van gegevens van R&D&I subsidieprojecten is nog een selectie gemaakt van actoren die actief zijn in het cybersecurity domein - en nogmaals specifiek op het gebied van onderzoek en innovatie. RVO (als uitvoeringsorganisatie van het Ministerie van Economische Zaken), en de Europese Commissie (EC), hebben elk een eigen database met (informatie over) publiek gefinancierde onderzoeksprojecten (waarin publieke en private organisaties samenwerken). In geval van RVO gaat het over projecten die gefinancierd worden middels de mkb-innovatiestimulering Regio en Topsectoren (MIT) over de periode 2015-2020, en de PPS-toeslag Onderzoek en Innovatie over de periode 2016-2020. Deze database kan doorzocht worden met 'Volg Innovatie'. In geval van de EC gaat het over de projecten gefinancierd in het kader van het Horizon 2020-kaderprogramma (Horizon 2020) voor onderzoek en innovatie over de periode 2014–2020. **Deze database kan doorzocht worden met** *Community Research and Development Information Service* (CORDIS). De gebruikte set van zoektermen is daarbij samengesteld op basis van (ENISA 2022b), en aangevuld en gevalideerd met (CBS 2020), (CWTS 2019), (RVO 2023), (Bree et. al 2023).

Op basis van de bovenbeschreven methodiek zijn 274 actoren geïdentificeerd die deelgenomen hebben aan innovatieve gesubsidieerde projecten door de Nederlandse overheid (zie Tabel 2.4).[11] Daarnaast is er een lijst samengesteld op basis van de deelname aan het Horizon2020 programma, met 238 unieke actoren.[12] In totaal zijn er met R&D&I subsidieprojectdata 499 unieke actoren op het gebied van cybersecurity geïdentificeerd. [13]

Tabel 2.4: Aantal met subsidieprojectdata geïdentificeerde actoren betrokken bij R&D&I in het cybersecurity domein.

	Gesubsidieerd door NL overheid	H2020	Totaal
Aantal organisaties	274	238	499

De bron, maar ook de zoektermen leiden tot een sample met actoren uit de 'producenten van cybersecurity producten en diensten', als ook 'cyber integrators' (zie Figuur 1.1).

Ook in dit geval is duidelijk dat lang niet alle R&D&I actoren van de gehele populatie geïdentificeerd zijn, omdat deze niet allemaal deelnemen aan publiek gefinancierde onderzoeksprojecten - bijvoorbeeld omdat ze uitsluitend een open of gesloten innovatiemodel hanteren (zie Kader 5). Sterker, het is waarschijnlijk dat de sample wordt gedomineerd door actoren die het traditionele innovatiemodel omarmen.

Verder bevat ook deze sample bevat zowel *pure* als *partial players*; en actoren die innoveren in het cybersecurity domein als ook met cybersecurity oplossingen.

[11] De informatie over de actoren is niet met een unieke identificatie nummer vermeld. Op basis van de gelijkheid van de naam zijn aannames gemaakt dat het een organisatie is. Bijvoorbeeld, is het aangenomen dat 'Nederlandse organisatie TNO' en 'TNO' een organisatie is. Het kan zijn dat er minder unieke organisaties zijn.
[12] In tegenstelling tot de RVO data, zijn de organisaties vermeld met een identificatie nummer in Cordis databestanden. Dat is dus een aantal van unieke organisaties die deelgenomen hebben aan de cybersecurity projecten.
[13] Omdat sommige organisaties participeren in verschillende programma's telt de som voor de individuele financieringsbronnen op tot meer dan 499.

Veel werk is ook in dit geval gestopt in het 'verbeteren' van de zoektermen om foutpositieven uit de sample te halen, en foutnegatieven te voorkomen (zie bijlage B.3). Maar ook in deze context valt het niet uit te sluiten dat er nog steeds verschillende type I fouten in de sample zitten, omdat de gehele sample van geïdentificeerde actoren nooit één voor één is gecheckt. In de database met R&D&I subsidieprojecten bijvoorbeeld zitten naast organisaties die onderzoek en innovatie uitvoeren ook andere actoren, die bijvoorbeeld projecten coördineren, of diensten leveren voor de disseminatie van de onderzoeksresultaten. Het is mogelijk dat een aantal van deze organisaties toch is opgenomen in de sample.

2.1.4 Vergelijking Innovatiespotter - Jobdigger - R&D&I subsidieprojecten

De samples van geïdentificeerde actoren op basis van Innovatiespotter, vacatureteksten en het deelnamen aan het innovatieve subsidieprojecten zijn met elkaar vergeleken (op basis van KvK nummer en naam). Tabel 2.5 geeft inzicht in de overlap tussen de samples. In totaal zijn er 19 organisaties die onderdeel zijn van alle drie de selecties.

De overlap lijkt relatief beperkt. Dat kan als oorzaak hebben dat de samples, omdat ze gebaseerd zijn op verschillende bronnen, in de praktijk elk een ander deel van de totale populatie vangen van actoren die aan R&D&I in het cyberdomein doen. De analogie toegepast in de context van (TNO 2019) beschrijft dit als volgt: het cybersecurity domein is als een donkere kamer die wordt beschenen met verschillende 'lichtbronnen' - de methodieken toegepast om actoren te identificeren; en in de praktijk 'belichten' deze elk een bijna afzonderlijk deel van die ruimte.

Tabel 2.5: Aantal gemeenschappelijke cybersecurity R&D&I actoren per bron.

	R&D&I subsidieprojecten	Jobdigger totaal	Jobdigger kernberoepen	Innovatiespotter
R&D&I subsidieprojecten	499	51	36	50
Jobdigger totaal		2.406	939	159
Jobdigger kernberoepen			939	97
Innovatiespotter				5.436

In de praktijk is het moeilijk om in de samples onderscheid te maken tussen *pure* en *partial players*; tussen innoveren in het domein, en met cybersecurity; en tussen traditioneel, gesloten en open innoveren. In de samples zijn actoren die zich alleen bezig houden met gesloten en open innovatie ondervertegenwoordigd. Waarschijnlijk is er ook een zekere oververtegenwoordiging van private actoren (bedrijven) in de samples van Innovatiespotter en Jobdigger (o.a. doordat KvK nummer een basis vormen voor het structureren en labelen van actoren in de respectievelijke databases - zie ook Kader 6).

De aanname is de verschillende samples een goede basis vormen het beschrijven van het R&D&I gedrag van de gehele populatie in het cybersecurity domein. Daarmee vormen de selecties een basis voor verdere informatieverzameling om de impact van R&D&I te beschrijven - ook voor indicatoren en bijbehorende statistieken. Deze aanname is gebaseerd op het feit dat een reeks van (zorgvuldig uitgevoerde) methodieken is toegepast om op basis

van verschillende bronnen samples samen te stellen. Het is in de praktijk onmogelijk om te toetsen hoe representatief de samples zijn, omdat er geen inzicht is in de samenstelling van de 'werkelijke' populatie (zie Kader 5).

Aanbeveling 1

De samples die zijn samengesteld in de context van dit (vervolg)onderzoek zijn de (voor nu) best beschikbare basis voorhanden voor verdere informatieverzameling met en over de actoren in het cybersecurity domein betrokken bij R&D&I. In een eventueel vervolgonderzoek (als onderdeel van een structurele evaluatie van de impact in het domein) zou verder optimaliseren van de selectie een belangrijke prioriteit moeten zijn, gebaseerd op de ervaringen opgedaan in de context van deze analyse. Actoren die een open innovatiemodel omarmen bijvoorbeeld zijn zeer waarschijnlijk ondervertegenwoordigd in de uiteindelijke samples van organisaties die betrokken zijn bij R&D&I. Op basis van (TNO 2019) kan geconcludeerd worden dat er in deze groep veel individuen zijn, die in de context van hun 'open source' activiteiten niet verbonden zijn aan meer 'traditionele' organisaties. Om ook deze belangrijke actoren te vangen wordt aanbevolen in een volgend onderzoek een analyse te maken van platformen waarop deze actoren actief zijn, om ook de impact van dit soort innovatie te kunnen vangen.

2.2 Informatie met en over actoren verzamelen

In de volgende fase van het onderzoek is met als basis de verschillende samples informatie verzameld met en over de geïdentificeerde actoren: over hun onderzoeks- en innovatiegedrag, en over de effecten van hun activiteiten in deze context - van input tot impact. De informatie is verzameld door het maken van statistieken, interviews en een survey.

2.2.1 Statistieken

In de context van dit onderzoek zijn de organisaties (bedrijven) geïdentificeerd in de database van Innovatiespotter gekoppeld aan de corresponderende microdata van het CBS, om zo te komen tot enkele R&D en productiestatistieken (toegevoegde waarde) die de impact van onderzoek in de sector reflecteren.[14] Hiervoor zijn de ongeveer 5.500 KvK nummers omgezet naar het bedrijfsniveau zoals het CBS dat definieert, waardoor het aantal 'entiteiten' gedaald is naar ongeveer 4.000.[15]

[14] Het CBS verzamelt middels questionnaires die het uitzet informatie over bijvoorbeeld omvang personeelsbestand of uitgaven aan R&D bij bedrijven. Deze microdata worden gekoppeld aan een unieke code voor dat bedrijf. De organisaties uit de sample op basis van Jobdigger zijn gelinkt aan hun unieke code (op basis van het KvK nummer), zodat de corresponderende microdata voor alle actoren beschikbaar is, als basis voor het maken van statistieken.

[15] Tijdens het opwerken van de KvK-nummers naar het juiste niveau kunnen drie situaties voorkomen: i) het KvK-nummer is één-op-één te vertalen naar het bedrijfsniveau; ii) het KvK-nummer is niet te koppelen naar het bedrijfsniveau; en iii) 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.

Op basis van een inventarisatie van de geïdentificeerde actoren is de aanname gedaan dat de sample van Innovatiespotter vooral bedrijven bevat - in lijn met wat Innovatiespotter zelf claimt over de samenstelling van hun database. De statistieken gecreëerd op basis van de sample van Innovatiespotter worden daarom vergeleken met die van gehele populatie van bedrijven in Nederland.

In de praktijk blijken er ook organisaties als TNO opgenomen in de uiteindelijke selectie. In het geval van TNO is dat geen probleem omdat deze organisatie in de praktijk ook door het CBS wordt beschouwd als 'privaat' - bijvoorbeeld in de context van de Nationale rekening, en volgens de interpretatie van de *Frascati manual* (voor R&D statistieken).

Kader 6: Aanname bij de sample op basis van Innovatiespotter.

Voor deze 'entiteiten' zijn de toegevoegde waarde, R&D indicatoren en gegevens uit de Community Innovation Survey (CIS) geaggregeerd. Tabel 2.6 toont een overzicht van het aantal organisaties uit de sample gebaseerd op Innovatiespotter waarvoor er relevante microdata gegevens zijn.

- Gegevens over de toegevoegde waarde zijn gelijk aan de statistieken genoemd in de context van het onderzoek naar de economische kansen van de cybersecuritysector uitgevoerd in opdracht van het Ministerie Economische Zaken & Klimaat, en zijn beschikbaar voor de periode 2017-2021 (Dialogic 2023). Input voor de productiestatistieken (o.a. toegevoegde waarde) worden wel bevraagd bij de gehele populatie.
- De gegevens over R&D worden jaarlijks opgehaald door het CBS middels een steekproef, waarbij bedrijven met minder dan 10 werknemers zijn uitgesloten. De uitvraag omvat gegevens over de personele en financiële investering in R&D en welk typen onderzoek (fundamenteel, toegepast of experimenteel) een bedrijf uitvoert. Deze gegevens zijn beschikbaar voor de periode 2017-2020.
- Gegevens over innovatie komen uit de CIS enquête. De CIS enquête wordt tweejaarlijks uitgevraagd onder bedrijven met meer dan 10 werknemers op basis van steekproef. Deze enquête focust op product- en procesinnovaties en vraagt onder andere naar uitgevoerde innovatie activiteiten, omzetontwikkeling en samenwerking bij innovatie. Het meest recent gepubliceerde CIS bestand omvat de jaren 2016-2018.

Tabel 2.6: Overzicht van het aantal respondenten binnen de cybersecurity sector voor de verschillende indicatoren in het laatste jaar waarvoor de gegevens beschikbaar zijn.

Indicator	Aantal respondenten	Herkomstjaar sample
Toegevoegde waarde	3948	2020
R&D gegevens	244	2020
CIS enquête	329	2018

Opgemerkt dient te worden dat de sample gebaseerd op Innovatiespotter waarvoor (waarmee) de totale omvang van de toegevoegde waarde is bepaald, ook actoren bevat die niet (zelf) aan R&D&I doen.

Het feit dat bedrijven met minder dan 10 werknemers niet worden bevraagd in de context van de R&D en CIS enquête impliceert bovendien dat het innovatiegedrag van een belangrijk segment van de populatie van cybersecurity bedrijven niet wordt gevangen in de resulterende statistieken. En op basis van de resultaten van de interviews (zie paragraaf 2.2.2) kan geconcludeerd worden dat zij in de context van het cybersecurity domein een

omvangrijke en relevante groep vormen. Om dit te illustreren: in de totale sample van actoren geïdentificeerd op basis van Innovatiespotter vertegenwoordigen zij ongeveer 70% van de totale populatie. Op basis van die interviews kan echter ook geconcludeerd worden dat zij maar beperkt aan R&D&I doen (zie paragraaf 5.1). De aanname is daarom dat de resulterende statistieken toch een goed beeld geven van het R&D&I gedrag van de populatie.

Daarnaast dient opgemerkt te worden dat de resulterende statistieken gebaseerd op Innovatiespotter nu alle (productie en R&D&I) activiteiten van de organisaties in de sample beschrijven, niet die specifiek op het gebied van cybersecurity. De sample (en in de praktijk ook de gehele populatie) bestaat echter niet alleen uit *pure players*, maar ook uit *partial players*. Om een schatting te maken van de effecten van R&D&I in het cybersecurity domein zijn de statistieken daarom ook nog 'gecorrigeerd'. Voor deze studie zijn dezelfde correctiefactoren gebruikt als voor (Dialogic 2023). Deze zijn bepaald door het aantal werknemers 'actief in het cybersecurity domein' te schalen op het totaal aantal werknemers van een organisatie, en deze dan te middelen over de bijbehorende totale populatie in een bepaalde grootteklasse.

- Voor organisaties met minder dan 10 werknemers is dan de aanname dat het 'cybersecurity gerelateerde deel' gelijk is aan 0,5 maal de totale waarde van de respectievelijke indicator.
- Voor organisaties met 10-99 werknemers: 0,4 'cybersecurity gerelateerd' .
- Voor organisaties met 100 werknemers of meer halen: 0,25 'cybersecurity gerelateerd'.
- Indien de statistieken niet per grootklasse zijn gespecificeerd wordt een correctiefactor van 0,27 gehanteerd. Dit impliceert dan dus dat aangenomen is dat 'het cybersecurity gerelateerde deel' gelijk is aan 0,27 maal de totale waarde van de respectievelijke indicator.

Doel was om op basis van een eigen survey, uitgevoerd in de context van dit onderzoek, een correctiefactor te bepalen. Maar door de lage response op deze survey (zie Paragraaf 2.2.3) is besloten gebruik te maken van de resultaten van (Dialogic 2023). Opgemerkt dient te worden dat met het gebruik van deze correctiefactoren de accuraatheid (en daarmee de kwaliteit) van de resulterende statistieken waarschijnlijk minder wordt.

Kader 7: Dimensies voor het beschrijven van de samenstelling van de sample.

Op basis van de samples samengesteld met behulp van Jobdigger en R&D&I subsidieprojecten zijn daarnaast additionele statistieken gecreëerd die o.a. ontwikkelingen in de vraag naar cybersecurity (onderzoeks)personeel weergeven, als ook samenwerking in onderzoeks- en innovatietrajecten.

Aanbeveling 2

De statistieken gemaakt op basis van CBS microdata zijn samengesteld met de sample van Innovatiespotter (met een duidelijk reden, zie Paragraaf 2.1.1). Zeker de R&D en innovatie indicatoren zijn daarbij gebaseerd op een beperkte set van organisaties. Door het combineren van meer samples, verkregen op basis van verschillende bronnen en methodieken, zou de totale sample voor het koppelen met CBS microdata kunnen worden verbreed, waardoor de accuraatheid (en daarmee de kwaliteit) van de resulterende statistieken verbeterd zou kunnen worden.

2.2.2 Interviews

Om de statistieken zoals hierboven te kunnen duiden, en om de onderzoeksvragen te kunnen adresseren is een serie van interviews gehouden met representanten uit het

Nederlandse cybersecurity domein. De gesprekspartners zijn weergegeven in Tabel 2.7. De questionnaire gebruikt in de context van het onderzoek is weergegeven in Bijlage B.

Tabel 2.7: Overzicht geïnterviewden.

Organisatie	Vertegenwoordiging
Hunt & Hacket	Jurjen Harskamp (CEO en Co-founder)
TNO	Berry Vetjens (Managing Director (ai)) - TNO ICT, Strategy & Policy)
TNO	Thomas Attema (Senior Scientist - Applied Cryptography & Quantum Algorithms)
Cyberveilig Nederland	Liesbeth Holterman (Strategisch Adviseur)
InvestNL	Michiel Jonkman (Investment manager)
SGS Brightsight	Olaf Tettero (CTO)
TenneT	Ron Wibbelink (Team Manager Corporate Security & deputy C(I)SO)
Chubb Verzekeringen en Verbond van Verzekeraars	Wouter Wissink (Senior Principle Risk Engineer & Technology Industry Practioner Europe) Marko van Leeuwen (Beleidsadviseur zakelijke schadeverzekeringen)
Dcypher	Eddy Boot (Programmadirecteur, Directeur)
Tesorion	Lodi Hensen (Head of Incident Response & Threat Intelligence)
Morrison & Foerster	Lokke Moerel (Senior of Council)
Ministerie EZK	Michel Verhagen (Manager Digital Trust Center)
Compumatica	Nort van Schayik (Co-owner & Business development)
Northwave	Pim Takkenberg (General Manager)
Check Point Software Technologies	Zahier Madhar (Security Engineer, Check Point Evangelist, Office of the CTO)
Innovation Quarter	Martijn van Hoogenhuijze (Teamlead Team Smart & Secure / Senior Account Manager Safety & Security)
NXP	Joppe Bos (Researcher)
NEN	Inge Piek (Secretaris van de normcommissie Cybersecurity & Privacy)

2.2.3 Survey

Als aanvulling op de interviews is ook een survey uitgezet, met als specifiek doel om de inzichten verkregen in de voorgaande stappen van informatieverzameling te valideren en aan te vullen. De vragen in de survey refereren specifiek aan de onderzoeksvragen over huidige cybersecurity beleid, en de maatschappelijke en economische waarde van R&D in cybersecurity (zie Bijlage C).

De enquête heeft opengestaan tussen 4 April 2023 en 10 mei 2023. In de tussentijd zijn twee herinneringsmails verstuurd - op 19 April 2023 en 1 mei 2023.

In totaal zijn 2.391 cybersecurityorganisaties via mail benaderd met het verzoek deel te nemen aan de survey. De mailadressen zijn door Dialogic opgehaald in de database van Innovatiespotter. De mail voor de vragenlijst is naar het 'algemene' emailadres van het bedrijf gestuurd – dus niet 'persoonlijk', gericht op een specifieke vertegenwoordigers binnen de organisatie. In totaal bleken er 288 onbestelbare mails. Enkele respondenten waren daarnaast niet aanwezig of hebben duidelijk aangegeven geen interesse te hebben. Deze laatste groep bestaat uit 11 personen. In de twee herinneringsmails, die later gestuurd werden, werden deze personen niet meer meegenomen.

Met twee 'selectievragen' is getracht alleen die organisaties te bevragen die daadwerkelijk aan R&D&I in het cybersecurity domein doen. In totaal zijn op deze manier 93 respondenten uit de verdere survey gefilterd.

Kader 8: Organisaties benaderd voor de survey.

Uiteindelijk hebben 14 respondenten de enquête tot aan het einde uitgevuld - een *response rate* van 0,6% die veel lager is dan het gemiddelde van 5-10% dat mag worden verwacht bij een survey als deze. Het is moeilijk in te schatten wat de oorzaak is, maar een reden kan zijn dat, omdat de respondenten ook zijn benaderd in de context van (Dialogic 2023), er een zekere 'survey-moeheid' is ontstaan. Ook de lengte en het detailniveau van de vragen kan ervaren zijn als 'onoverkomelijk'.

Bijlage D geeft wat beschrijvende statistiek van de gegeven antwoorden, maar deze is vanwege de geringe omvang van de response niet representatief voor het onderzoeks- en innovatiegedrag in het cybersecurity domein. De individuele responses zijn wel verwerkt in de overige hoofdstukken.

De ervaringen opgedaan met het doorlopen van deze fase van informatieverzameling vormen de basis voor aanbevelingen voor een aanpak voor potentiële toekomstige structurele evaluatie van de impact van R&D&I in het domein.

Aanbeveling 3

(Enkele) vragen uit survey zoals als beschreven in Bijlage C zouden kunnen worden 'meegenomen' in een bredere enquête door het CBS, om de *response rate* te verhogen, om zo een beter beeld van het onderzoeks- en innovatiegedrag en resulterende effecten te verkrijgen. De 'correctiefactor' zoals beschreven in Paragraaf 2.2.1 zou in dat geval ook verder kunnen worden geoptimaliseerd, om zo een betere schatting voor de statistieken van een aantal van de indicatoren te kunnen doen.

3 Impact R&D&I: maatschappelijke en economische waarde

Dit hoofdstuk adresseert de eerste onderzoeksvraag: hoe de waarde van het doen van R&D&I in het cybersecurity domein kan worden beschreven en gemeten. Hiermee levert het input op voor de tweede onderzoeksvraag het volgende hoofdstuk, over de status van het NL cybersecurity innovatie-ecosysteem. De conclusies zijn gebaseerd op een analyse van de interviewresultaten, en reflecteren daarmee vooral de perceptie van belangrijke stakeholders in het domein.

De gesprekspartners zijn opvallend eensluidend in hun beschrijving van de effecten van onderzoek en innovatie, en ook gelijkgestemd als het gaat over het benoemen van de problemen om alle vormen van waarde te ‘vangen’ in bijvoorbeeld indicatoren. In de praktijk maken de geïnterviewden onderscheid tussen wat zij noemen ‘directe effecten’ van R&D&I, en ‘indirecte effecten’.

Met **directe** effecten wordt bedoeld de impact van onderzoek en innovatie op organisaties die de resulterende kennis toepassen in hun producten of diensten – zowel in het geval van innoveren in het cybersecurity domein als ook innoveren met cybersecurity oplossingen. De impact beperkt zich in deze context tot ‘de aanbieder’ van deze producten of diensten. Dit refereert aan een meer traditioneel perspectief op de impact van R&D&I, ‘op de sector zelf’. De perceptie is dat deze effecten relatief eenvoudig kunnen worden waargenomen (gemonitord) in de ‘economische prestaties’ van organisaties, en beschreven met (traditionele) indicatoren als toegevoegde waarde en werkgelegenheid (en arbeidsproductiviteit). Een eerste aanzet daartoe is beschreven in paragraaf 4.5.

Met **indirecte** effecten wordt gerefereerd aan de brede impact van het gebruik van cybersecurityproducten en -diensten die het resultaat zijn van R&D&I. Niet (alleen) de aanbieders profiteren van deze effecten, maar ook (bovenal) de gebruikers van cybersecurity oplossingen. Waarde wordt in deze context op veel verschillende manieren gecreëerd, en slaat op (even zoveel) verschillende manieren neer in de economie en in de samenleving. Het meest genoemde voorbeeld van brede impact is de bijdrage van cybersecurity toepassingen (en de onderliggende R&D&I) aan onze economische én nationale veiligheid (in de context van opsporing en wetshandhaving, en in het defensiedomein - defensief én offensief). Het is daarmee de basis voor vertrouwen dat onze samenleving en onze economie ‘op de huidige manier’ kan (blijven) functioneren. En dat draagt dan weer bij het aan bijvoorbeeld de aantrekkelijkheid van Nederland als vestigingsplaats voor overige economische activiteiten, en daar mee aan onze concurrentiepositie.

Cybersecurityoplossingen spelen daarnaast bijvoorbeeld ook een essentiële rol bij de verdere ‘digitalisering’ van de economie en de samenleving. Digitalisering speelt een essentiële rol bij

de transities waar de Nederlandse samenleving en economie voor staan - op het gebied van energie, gezondheidszorg, etc.

Deze (voorbeelden van) indirecte effecten zijn moeilijk te vangen in indicatoren, en (daarmee) moeilijk te monitoren of evalueren. Een proxy voor impact als 'totale schade die is voorkomen', of 'economische terugval bij afwezigheid van enig niveau van cyberveiligheid' refereert aan een situatie die simpelweg niet 'voorstelbaar' (meer) is, en daarmee ook niet te kwantificeren.

Eén van de mogelijkheden om een beeld te schetsen van de indirecte effecten van (R&D&I in) het cybersecurity domein is door een schatting te maken van de totale schade die is voorkomen met cybersecurity toepassingen. In de praktijk is het (om veel verschillende redenen) onmogelijk om dit exact in te voorspellen. Maar de omvang van de cyberverzekeringsmarkt kan wel een zeker inzicht geven in de verwachtingen die (een deel van) de samenleving heeft van de mogelijke impact van cybercrime.

De resultaten van dit onderzoek lijken te suggereren dat de markt voor cybersecurityverzekeringen nog onvoldoende ontwikkeld is: vraag en aanbod zijn nog onvoldoende 'op elkaar afgestemd'. De perceptie van verzekeraars bijvoorbeeld is dat risico's moeilijk zijn in te schatten (incidenten kunnen zich herhaaldelijk voordoen, en zijn moeilijk te voorspellen), en dat het cumulatierisico hoog is. Dit maakt het een lastige markt voor verzekeraars - het beeld is dan ook dat er in Nederland te weinig te verzekeraars zijn om alle risico's af te dekken. Aan de vraagzijde groeit het bewustzijn over de rol en relevantie van cybersecurity, en verandert het denken over het verzekeren van risico's van cyberaanvallen (zie een recent rapport van het WEF).

De bruto premieomzet van cyberverzekeringen in Nederland bedraagt ongeveer 65 miljoen euro (op een bruto premieomvang van de totale Nederlandse schadeverzekeringsmarkt van 15,5 miljard euro - cijfers over 2022).[16] Daar staat dan een zekere omvang van het schaderisico tegenover die verzekeraars met deze premie proberen 'af te dekken'. In de toekomst zou de bruto premieomvang (en het 'bijbehorende' schaderisico) gebruikt kunnen worden als een basis voor een schatting van de totale schade die is voorkomen met cybersecurity toepassingen.

Kader 9: Verzekeringen tegen cyberschade.

De gesprekspartners gaven aan dat 'impact van cybersecurity R&D&I' bovenal het gevolg is van cybersecurity toepassingen: niet de impact van cybersecurity soft- en hardware zelf, maar de toepassing daarvan in 'bredere' producten en diensten. De directe economische effecten van R&D&I in het cybersecurity domein zijn relatief beperkt.

De perceptie van de geïnterviewden is verder dat de effecten van innoveren met cybersecurity vele malen groter zijn dan innoveren in het cybersecurity domein (zie Kader 5).

[16] Zie: Cyber (verzekeraars.nl).

4 Het Nederlandse cybersecurity innovatie-ecosysteem

Doel van dit hoofdstuk is om (zo veel als mogelijk) de effecten van R&D&I in het cybersecurity domein te beschrijven, met behulp van het Input - Impact framework (zie Figuur 4.1). De resultaten kunnen gezien worden als (een aanzet tot) een nulmeting: een referentiepunt voor een verdere analyse van de impact in de tijd van R&D&I in het cybersecurity domein, en van de effecten van overheidsbeleid.

Aanbeveling 4

De analyse richt zich op de effecten van onderzoek en innovatie van de actoren in het Nederlandse cybersecurity domein.[17] Een internationale vergelijking van hun 'innovatieprestaties' wordt bemoeilijkt door een gebrek aan internationale statistieken (zie TNO 2022a). In een volgend onderzoek zou juist die internationale context één van de onderwerpen van analyse kunnen zijn, bijvoorbeeld op basis van de Global Cybersecurity Index (ITU Publications) of de Global Cybersecurity Index van het EC Composite Indicators & Scoreboard Explorer initiatief.

Figuur 4.1: Input – Impact framework om effecten R&D&I te structureren.

4.1 Input

Het input – impact framework refereert expliciet aan input om de doelmatigheid (efficiëntie) van de middelen die ingezet worden om R&D&I uit te voeren, en de effecten die dat heeft te kunnen duiden. Input van middelen in het Nederlandse cybersecurity innovatie-ecosysteem wordt in deze paragraaf beschreven aan de hand van R&D uitgaven en R&D personeel.

[17] Voor een overzicht van de verschillende actoren in het Nederlandse innovatie-ecosysteem, zie: (TNO 2019).

4.1.1 R&D-uitgaven en -ontwikkelingen

Eén van de belangrijkste indicatoren om input te duiden is de uitgaven die organisaties doen aan R&D (zie (TNO 2022b) voor de definitie). Tabel 4.1 toont de resultaten van dit onderzoek (op basis van de sample verkregen met Innovatiespotter) om de omvang hiervan te bepalen:

- Rij één geeft de totale R&D-uitgaven van Nederlandse organisaties actief in het cybersecurity domein weer (uit de sample, die de R&D questionnaire van het CBS hebben ingevuld. Merk op dat niet al deze uitgaven hoeven te refereren aan cybersecurity – deze kunnen ook betrekking hebben op andere activiteiten (omdat niet alle actoren *pure players* zijn).
- Rij twee geeft een schatting van hun aan cybersecurity gerelateerde R&D uitgaven (op basis van een zogenaamde correctiefactor, zie Paragraaf 2.2.1).
- Rij drie geeft de totale uitgaven aan R&D door Nederlandse bedrijven (die de R&D questionnaire van het CBS hebben ingevuld), om de overige cijfers in een zeker perspectief te kunnen zetten.

Omdat de aanname is dat de sample van actoren geïdentificeerd op basis van Innovatiespotter vooral bedrijven zijn worden de onderzoeksresultaten (van rij één en twee) vergeleken met de uitgaven aan R&D van alle bedrijven in Nederland (weergegeven in rij drie). Op basis van de resultaten kan geconcludeerd worden dat bedrijven (organisaties) in het cybersecurity domein gemiddeld veel kennisintensiever zijn dan de gehele populatie van Nederlandse bedrijven: zijn zij geven gemiddeld ongeveer 10 maal meer uit aan R&D.[18]

Tabel 4.1: Overzicht van uitgaven aan R&D [MEURO]. Bron: Dialogic op basis van CBS (R&D 2017 - 2020), gebaseerd op een sample van Innovatiespotter; en StatLine - Research en development; kerncijfers per sector van uitvoering (cbs.nl).

	2015	2016	2017	2018	2019	2020
R&D uitgaven van Nederlandse bedrijven (organisaties) met cybersecurity-activiteiten	0,82	0,90	1,37	1,34	1,71	1,60
aantal bedrijven	190	213	224	225	244	244
Aan cybersecurity gerelateerde R&D uitgaven van Nederlandse bedrijven (organisaties) met cybersecurity-activiteiten	0,22	0,24	0,37	0,36	0,46	0,43
aantal bedrijven	190	213	224	225	244	244
R&D uitgaven van alle Nederlandse bedrijven	9,52	10,00	10,67	11,00	11,85	12,31
aantal bedrijven	19.798	20.159	19.484	19.031	19.548	19.227

Op basis van de resultaten kan ook geconcludeerd worden dat in zijn algemeenheid de uitgaven aan R&D door bedrijven in de onderzochte periode zijn gestegen, maar dat die in het cybersecurity domein veel meer zijn gegroeid. In de periode over de periode 2015 - 2020 stegen de globale uitgaven met ongeveer 30%, en die in het cybersecurity domein met 95%.

Statistieken om de uitgaven aan R&D te vergelijken in een internationale context zijn er niet (zie (TNO 2022a)). De perceptie van veel van de geïnterviewden is dat landen “waar het

[18] Met 2020 als referentiejaar: gemiddelde uitgaven alle bedrijven in Nederland € 642.325; gemiddelde uitgaven organisaties met cybersecurity activiteiten € 6.557.377.

'veiligheidsdenken' verder is ontwikkeld" (zoals Israël), of "waar een grotere thuismarkt is" (zoals de VS), de intensiteit van de uitgaven hoger is.

Op basis van de sample van Innovatiespotter is het ook gelukt om statistieken te maken over de mate waarin onderzoek in het cybersecurity domein intern of extern wordt uitgevoerd.[19] Tabel 4.2 laat zien dat in de periode 2015 - 2020 het aandeel interne R&D uitgaven van Nederlandse organisaties met cybersecurity activiteiten sterk is gestegen. Dit suggereert dat in die periode deze bedrijven veel eigen onderzoekscapaciteit hebben gecreëerd. Dit is mogelijk ingegeven door het feit dat deze organisaties hun onderzoek niet willen delen (ook niet in de uitvoering) met anderen, bijvoorbeeld omdat ze een gesloten innovatiemodel hebben omarmd.

Tabel 4.2: Ontwikkeling van interne R&D uitgaven [MEURO]. Bron: Dialogic op basis van CBS (R&D 2017 - 2020), gebaseerd op een sample van Innovatiespotter.

	2015	2016	2017	2018	2019	2020
Aandeel interne R&D uitgaven van Nederlandse bedrijven (organisaties) met cybersecurity-activiteiten	70,9%	70,3%	79,7%	81,2%	80,7%	81,6%
aantal bedrijven	190	213	224	225	244	244

4.1.2 R&D personeel: bestaand en vraag

Een andere relevante indicator om input te duiden is de omvang van R&D personeel die organisaties in huis hebben (en daarmee moeten 'onderhouden') voor het doen van onderzoek. Tabel 4.3 toont de resultaten van dit onderzoek (op basis van de sample verkregen met Innovatiespotter) naar de omvang van deze groep van werknemers in het cybersecurity domein:

- Rij één geeft de totale omvang van het eigen R&D personeel van Nederlandse organisaties actief in het cybersecurity domein. Ook hier geldt weer dat niet al deze onderzoekers zich zullen bezighouden met cybersecurity.
- Rij twee geeft een schatting van de omvang van het aantal onderzoekers van deze organisaties die zich specifiek bezighouden met cybersecurity R&D&I.
- Rij drie geeft de totale omvang van eigen R&D personeel van alle Nederlandse bedrijven (eerste rij), om de overige cijfers in een zeker perspectief te kunnen zetten.

Op basis van de resultaten wordt bevestigd dat bedrijven (organisaties) in het cybersecurity domein gemiddeld veel kennisintensiever zijn dan de gehele Nederlandse populatie aan bedrijven: zij hebben ongeveer 7 maal meer R&D personeel in dienst.[20]

[19] Dit wordt door CBS als volgt gedefinieerd:
Intern: Uitgaven aan R&D activiteiten verricht met eigen of ingeleende R&D medewerkers.
Extern Uitgaven aan R&D activiteiten uitgevoerd door derden.
[20] Met 2020 als basisjaar: gemiddeld aantal R&D personeel alle bedrijven in Nederland 8,93 FTE; gemiddelde voor organisaties met cybersecurity activiteiten 61,5 FTE.

Tabel 4.3: Overzicht van inzet van R&D personeel [FTE]. Bron: Dialogic op basis van CBS (R&D 2017 - 2020), gebaseerd op een sample van Innovatiespotter; en StatLine - Research en development; kerncijfers per sector van uitvoering (cbs.nl).

	2015	2016	2017	2018	2019	2020
Inzet van R&D personeel van Nederlandse bedrijven (organisaties) met cybersecurity-activiteiten	6.354	9.305	11.789	11.896	15.124	15.011
aantal bedrijven	190	213	224	225	244	244
Inzet van cybersecurity gerelateerd R&D personeel van Nederlandse bedrijven (organisaties) met cybersecurity-activiteiten	1.716	2.512	3.183	3.212	4.083	4.053
aantal bedrijven	190	213	224	225	244	244
Inzet van R&D personeel van alle Nederlandse bedrijven	151.358	157.018	157.844	164.144	171.143	171.680
aantal bedrijven	19.798	20.159	19.484	19.031	19.548	19.227

Op basis van de resultaten kan ook geconcludeerd worden dat in zijn algemeenheid de omvang van R&D personeel bij bedrijven in Nederland is gegroeid - met ongeveer 13% in de periode 2015 - 2020; maar dat die omvang in het cybersecurity domein zich veel meer heeft ontwikkeld - 2,3 keer zo groot.

Het onderzoek heeft ook inzicht gegeven in de vraag naar cybersecurity personeel[21]. Tabel 4.4 toont de resultaten (op basis van de sample verkregen met Jobdigger) naar de omvang van de uitgezette vacatures in het cybersecurity domein. Kolom drie beschrijft het totaal aantal cybersecurity gerelateerde vacatures die refereren aan de verschillende profielen zoals beschreven in kolom twee. Kolom vier beschrijft voor deze profielen specifiek die vacatures die refereren aan (het doen van) R&D&I. Kolom vier beschrijft dus het aantal vacatures waarvan het zeker is dat het gaat over R&D&I personeel. In kolom drie wordt het totaal van de cybersecurity gerelateerde vacatures beschreven, waarvan een deel (groter dan beschreven in kolom vier) ook betrekking kan hebben op onderzoek en innovatie. Van rij één naar rij vier neemt die waarschijnlijkheid af.

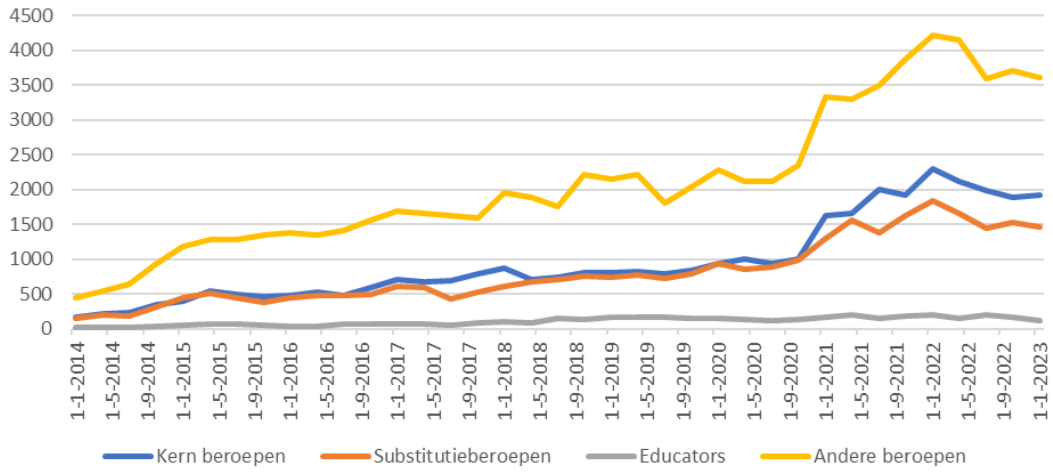
Tabel 4.4: Aantal nieuwe vacatures 2014 - Q1 2023. Bron: TNO, gebaseerd op een sample van Jobdigger.

Profiel	Cybersecurity vacatures	Cybersecurity en R&D&I vacatures
Kernberoepen	24.589	3.977
Substitutieberoepen	20.479	3.214
Educators of docenten	2.660	1.505
Bredere groep van overige relevante beroepsklassen	50.357	7.905
Totaal	98.085	16.601

[21] *'IT-auditor', 'auditor'* en *'quality specialist'* zijn buitgesloten van de selectie van deze personeelsgroep.

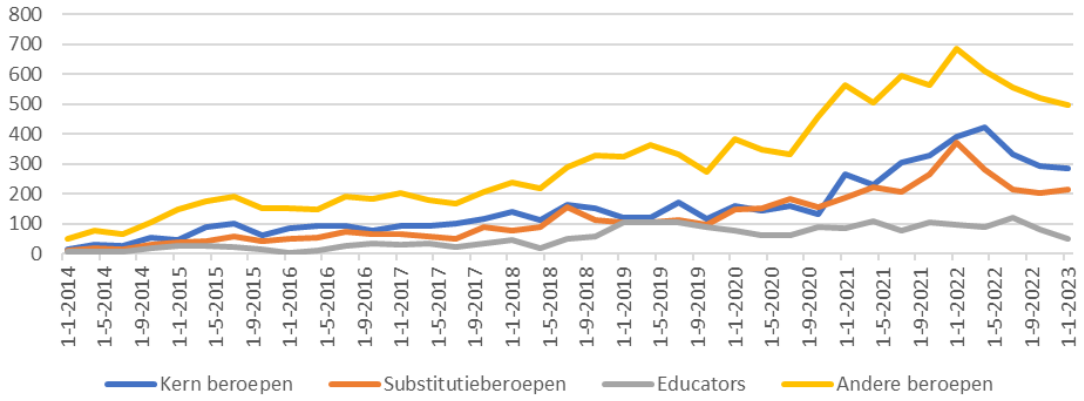
Figuur 4.2 geeft de ontwikkeling in omvang van het aantal vacatures voor cybersecurity specialisten voor de periode januari 2014 tot en met maart 2023 - in lijn met kolom twee van Tabel 4.4.

Figuur 4.3 geeft de ontwikkeling voor vacatures zoals kolom drie van Tabel 4.4. De vacatureontwikkeling voor cybersecurity specialisten waarbij expliciet wordt gerefereerd aan R&D&I volgt hetzelfde patroon als die voor de vacatureontwikkeling voor de 'generieke' cybersecurity specialisten. Er is in beide figuren een duidelijke verdere versnelling in de vraag waar te nemen na het derde kwartaal van 2020.[22] Het eerste kwartaal van 2022 luidt een afname in de vraag in voor bijna alle profielen ('breed' zowel als gericht op R&D&I). Deze ontwikkeling lijkt in lijn met de recente aankondigingen van 'techbedrijven' om personeel wereldwijd te ontslaan.[23] Wat hoe dan ook opvalt in beide figuren, voor alle profielen, is de (opwaartse) volatiliteit.



Figuur 4.2: Vacatureontwikkeling voor cybersecurity medewerkers. Bron: TNO, op basis van een sample van Jobdigger.

[22] Er is geen nader onderzoek gedaan naar de sterke stijging van na 2021, maar het is zeer waarschijnlijk dat deze is veroorzaakt door de effecten van de Covid-19 pandemie.
[23] Zie bijvoorbeeld: Tech Layoffs: US Companies With Job Cuts In 2022 and 2023. (crunchbase.com). Deze terugval zou veroorzaakte kunnen zijn door een ontwikkeling naar *back-to-normal* na de pandemie. Het zou ook zo kunnen zijn dat deze wordt veroorzaakt door het feit dat, omdat vacatures moeilijk zijn op te vullen, deze ook niet meer massaal worden uitgezet.



Figuur 4.3: Vacatureontwikkeling voor cybersecurity medewerkers specifiek refererend aan R&D&I. Bron: TNO, op basis van een sample van Jobdigger.

Aanbeveling 5

Het onderzoek naar input in R&D&I heeft zich beperkt tot uitgaven aan R&D, en omvang R&D personeel (inclusief ontwikkelingen in de vraag). In een volgend onderzoek zou ook geanalyseerd kunnen worden wat nu precies de kennis en vaardigheden zijn die huidige werknemers (inclusief onderzoekers) meebrengen, en zouden moeten hebben om aan de toekomstige vraag in het domein te voldoen. Dit omdat uit de interviews naar voren komt dat het gebrek aan goed gekwalificeerd personeel een belemmering vormt voor innovatie en verdere ontwikkeling van de sector. Het werk van de OECD, ENISA (ENISA 2022a) of CVD en HSD zou hierbij een basis kunnen vormen.

4.2 Activiteiten

Middelen zoals beschreven in Paragraaf 4.1 worden ingezet door organisaties voor innovatietrajecten. In deze paragraaf wordt de omvang en andere karakteristieken van deze activiteiten beschreven.

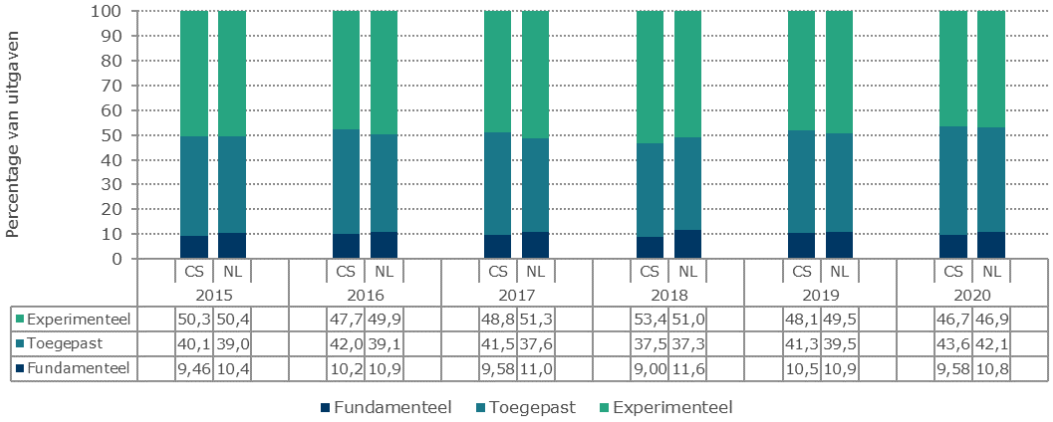
Tabel 4.5 toont (op basis van de selectie samengesteld met Innovatiespotter) dat in de periode 2015 - 2020 het aandeel van de organisaties in het cybersecurity domein dat aan onderzoek doet licht is gestegen.

Tabel 4.5: Overzicht van het aandeel bedrijven dat R&D onderzoek uitvoert. Bron: Dialogic op basis ban CBS (R&D 2017 - 2020), gebaseerd op een sample van Innovatiespotter.

	2015	2016	2017	2018	2019	2020
Aandeel Nederlandse bedrijven (organisaties) in het cybersecurity domein dat R&D uitvoert	54,7%	54,0%	54,9%	54,7%	59,4%	57,8%
aantal bedrijven	190	213	224	225	244	244

Op basis van deze sample is het ook mogelijk inzicht te verwerven in het soort onderzoek dat wordt verricht in het cybersecurity domein, en hoe dit zich verhoudt tot dat wat de gehele Nederlandse populatie aan bedrijven doet. De resultaten in Figuur 4.4 laten zien dat er weinig verschil zit in beide groepen: over de hele linie doen bedrijven gemiddeld het meest

aan experimenteel onderzoek, gevolgd door toegepast onderzoek; en in lijn der verwachting is slechts een klein deel van het uitgevoerde onderzoek fundamenteel.



Figuur 4.4: Verdeling van het typen onderzoek door bedrijven in de cybersecurity sector en alle bedrijven in Nederland. Bron: Dialogic op basis ban CBS (CIS 2016 - 2018), gebaseerd op een sample van Innovatiespotter.

Meerdere partijen geven aan (in de interviews en de survey) dat zij geen eigen onderzoeks- en innovatiecapaciteit hebben op het gebied van cybersecurity. Zij participeren in publieke gefinancierde onderzoekstrajecten (PPS projecten - open innovatiemodel, waarbij de gecreëerde kennis wel (deels) beschermd kan worden) die voor hen (mogelijk) relevante resultaten opleveren. Deze PPS projecten zijn vaak niet volledig toegespitst op cybersecurity, maar door de randvoorwaardelijkheid van cybersecurity is het automatisch een onderdeel van deze projecten.

Tabel 4.6: Aantal cyber R&D&I actoren en aantal cybersecurity innovatieve publiek gefinancierde PPS projecten (2020 - 2022). Bron: TNO, op basis van gegevens van RVO en CORDIS.

Kenmerken	RVO	CORDIS	Totaal
Aantal organisaties	274	238	499
Aantal projecten	91 (63%)	53 (47%)	144
Gemiddeld aantal projecten	1	3	2
Totaal subsidie voor alle cybersecurity projecten [€]	35.115.306	205.999.804	241.115.110

In de context van dit onderzoek is ook de relevantie van publieke gefinancierde onderzoekstrajecten geanalyseerd (op basis van data over subsidieprojecten). Op basis van de resultaten kan geconcludeerd worden dat in de periode 2010 - 2022 in totaal 144 innovatieve cybersecurity projecten zijn uitgevoerd, gefinancierd met nationale programma's als ook EU subsidie. In totaal zijn er 499 organisaties geïdentificeerd als actoren die deelgenomen hebben aan deze projecten (zie Tabel 4.6). De totale publieke financiering bedroeg € 241 miljoen euro in deze periode. 85% van deze middelen werd gealloceerd middels het EU H2020 programma.

Tabel 4.7: Aantal organisaties met 1, 2-5 en meer dan 5 cybersecurity innovatieve publiek gefinancierde PPS projecten (2010 - 2022). Bron: TNO, op basis van gegevens van RVO en CORDIS.

Aantal organisaties	RVO	CORDIS	Totaal
1 project	255 (93%)	167 (70%)	422 (85%)
2-5 projecten	19 (7%)	71 (30%)	90 (18%)
>5 projecten	1 (0%)	16 (7%)	17 (3%)
Totaal organisaties	274	238	499
Totaal aantal projecten	91	53	144

Een groot aandeel organisaties (85%) heeft deelgenomen aan slechts één subsidieproject. (zie Tabel 4.7). Meer organisaties hebben deelgenomen aan meerdere cybersecurity innovatieve projecten in het kader van H2020 dan via de middelen van het ministerie van EZK: 37% tegen 7%. De meeste projecten zijn uitgevoerd door 1 of 2 partners (53%) (zie Tabel 4.8).

Tabel 4.8: Aantal partners met 1-2, 3-9 en meer dan 10 cybersecurity innovatieve publiek gefinancierde PPS projecten (2020 - 2022). Bron: TNO, op basis van gegevens van RVO en CORDIS.

Aantal partners	RVO	CORDIS	Totaal
1-2 partners	51 (56%)	26 (49%)	77 (53%)
3-9 partners	37 (41%)	9 (17%)	46 (32%)
10 of meer partners	3 (3%)	18 (34%)	21 (15%)
totaal aantal projecten	91 (100%)	53 (100%)	144 (100%)

Op basis van de interviews kan geconcludeerd worden dat enerzijds vooral kennisinstellingen een prominente rol spelen in het bepalen van de richting van R&D&I in Nederland - de gesprekspartners benoemen dit als een “bottom up proces”. Anderzijds zijn er een beperkt aantal organisaties (zoals grote industriële actoren, maar ook verschillende publieke instanties en overheden) die een belangrijke rol spelen in die context. Voor hen is cyberveiligheid een topprioriteit (aan het worden), omdat bijvoorbeeld een geslaagde cyberaanval (niet alleen voor henzelf) grote maatschappelijk en economische gevolgen kan hebben. Hun ‘innovatiegedrag’ wordt nader verklaard in Hoofdstuk 5).

De geïnterviewden geven verder aan dat ‘afstemming’ (van vraag en aanbod) plaatsvindt in de context van bijvoorbeeld dcypher, maar ook clusters en brancheorganisaties als The Hague Security Delta, Cyberveilig Nederland, en ACCSS (Academic Cyber Security Society) spelen hierbij een rol.

Aanbeveling 6

De resultaten van dit (deel van het) onderzoek, naar R&D&I activiteiten, zijn niet gespecificeerd naar specifieke onderwerpen in onderzoek. In een volgend onderzoek zou bijvoorbeeld in de bestanden van CORDIS gezocht kunnen worden naar trends in technologievelden.

4.3 Output

De activiteiten zoals beschreven in paragraaf 4.2 leiden tot nieuwe kennis, die neerslaat in bijvoorbeeld patenten en publicaties. Op basis van de sample samengesteld met behulp van Innovatiespotter is het mogelijk inzicht te verwerven in het patentgedrag van organisaties in het cybersecurity domein. Door koppeling van de sample aan CBS microdata (CIS database)

is een inschatting te maken van het aandeel bedrijven dat een octrooi aanvraagt. In de periode 2016-2018 heeft 8,4% van de totale populatie van bedrijven in Nederland een octrooi aangevraagd. In het cybersecurity domein is dat 6,1%. Het is niet direct duidelijk wat de reden van deze lage score is. Mogelijk wordt dit veroorzaakt doordat het (in Europa) lastiger is om octrooien op software te verkrijgen; of omdat de dynamiek in deze sector het verkrijgen van IPR minder relevant maakt. In zijn algemeenheid geldt dat 'octrooigedrag' sectorspecifiek is, en dat vergelijken over sectoren heen weinig waardevolle inzichten oplevert.

De perceptie van de geïnterviewden is dat "[...] het kennisniveau [de kenniskapitaalvoorraad] en het academisch niveau in het cybersecurity domein in Nederland goed is [in een internationale context]." Uit de interviews komt verder naar voren dat Nederland met name goed is in academisch/ fundamenteel onderzoek, specifiek op het gebied van cryptografie en quantumtechnologie. Daarnaast heeft Nederland een sterke positie in IT-*auditing* en netwerkmonitoring.

Aanbeveling 7

In zijn algemeenheid is output van R&D&I (eenvoudig) te vangen met analyses van patenten en publicaties. In de context van het onderzoek zoals beschreven in (TNO 2018) is zo'n analyse uitgevoerd. Deze zou in een eventueel vervolgonderzoek herhaald kunnen worden, om zo inzicht te verkrijgen in relatieve sterktes in specifieke deelgebieden van het cybersecurity domein. Een internationale vergelijking is (tot op zekere hoogte) mogelijk op basis van het EU *Advanced Technologies for Industry* (ATI) initiatief. Opgemerkt dient wel te worden dat een analyse naar deze vormen van output alleen inzicht geven voor het traditionele innovatiemodel.

4.4 Outcome

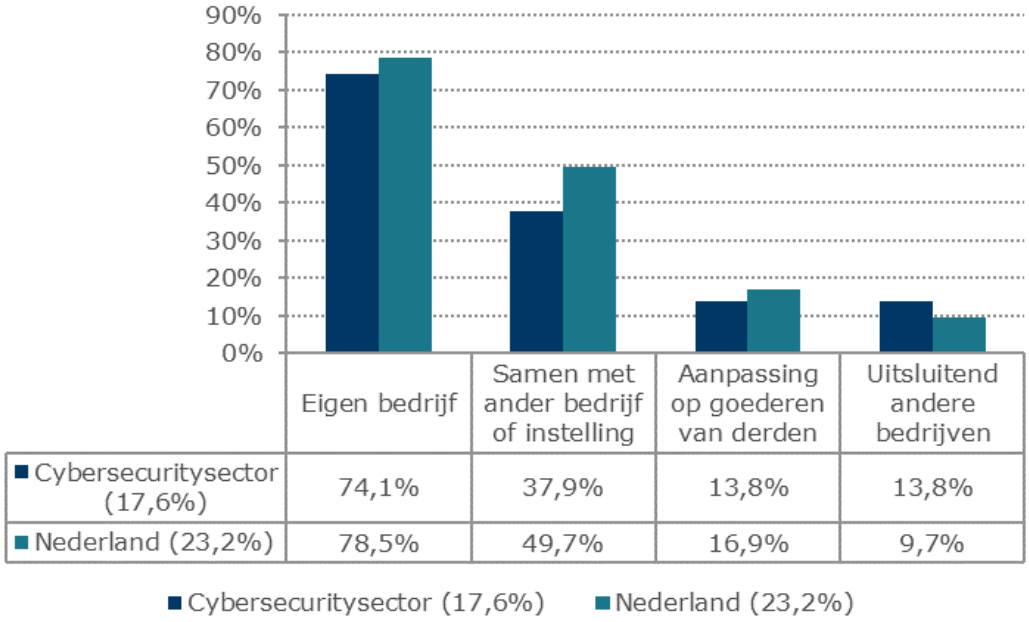
De kennis die het resultaat is van de activiteiten zoals beschreven in de voorgaande paragrafen wordt door bedrijven toegepast in hun productieproces. In deze paragraaf worden de effecten hiervan beschreven aan de hand van verschillende indicatoren.

Op basis van de sample samengesteld met behulp van Innovatiespotter is het ook mogelijk om inzicht te krijgen in de effecten die het doen van onderzoek en innovatie heeft op de omzet van organisaties die actief zijn in het cybersecurity domein, en dit te vergelijken met de *outcome* voor de hele populatie aan bedrijven in Nederland. Op basis van de resultaten van dat onderzoek kan geconcludeerd worden dat de omzetverdeling voor bedrijven in de cybersecuritysector vrijwel gelijk is als voor alle bedrijven in Nederland (zie Tabel 4.9). Als vanzelfsprekend is het grootste deel van de omzet afkomstig uit producten en diensten die nauwelijks of niet zijn veranderd. De omzet uit producten en diensten die nieuw zijn voor de markt is gelijk aan de omzet uit producten en diensten die slechts nieuw zijn voor het bedrijf.

Tabel 4.9: Overzicht van de omzetverdeling voor innovatieve bedrijven in de cybersecurity sector en alle bedrijven in Nederland. Bron: Dialogic op basis ban CBS (CIS 2016 - 2018), gebaseerd op een sample van Innovatiespotter.

	CS (aantal bedrijven =152)	NL (aantal bedrijven =2465)
Nieuw voor de markt	13,96%	14,02%
Nieuw voor bedrijf	13,68%	13,50%
Onveranderd of licht veranderd	72,36%	72,48%
Totaal	100,0%	100,0%

Op basis van de sample samengesteld met behulp van Innovatiespotter is het verder ook mogelijk inzicht te krijgen in: i) het soort productinnovaties dat bedrijven in het cybersecurity domein uitvoeren (producten of diensten); ii) hoe organisaties samenwerken in het bijbehorende innovatietraject; iii) om dit te vergeleken met de gehele Nederlandse populatie van bedrijven.



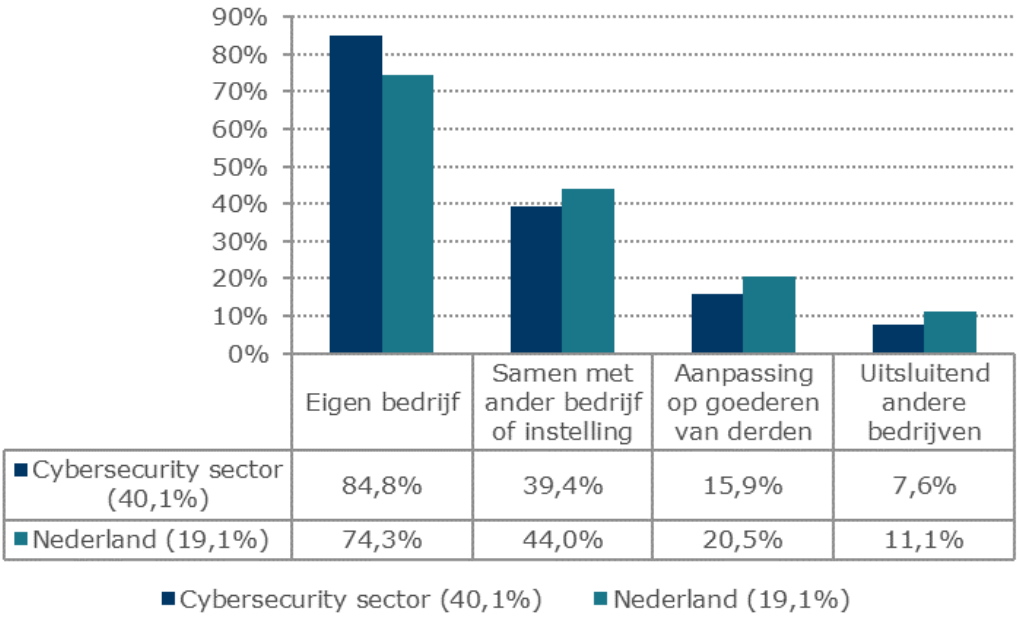
	Eigen bedrijf	Samen met ander bedrijf of instelling	Aanpassing op goederen van derden	Uitsluitend andere bedrijven
Cybersecuritysector (17,6%)	74,1%	37,9%	13,8%	13,8%
Nederland (23,2%)	78,5%	49,7%	16,9%	9,7%

Figuur 4.5: Samenwerkingspartners voor de ontwikkeling van nieuwe goederen door cybersecurity bedrijven en alle bedrijven in Nederland. Bron: Dialogic op basis ban CBS (CIS 2016 - 2018), gebaseerd op een sample van Innovatiespotter.

In Figuur 4.5 is het percentage van bedrijven dat aangeeft productinnovaties uit te voeren uitgesplitst naar de samenwerkingsvorm voor de ontwikkeling van deze productinnovatie weergegeven. Een eerste conclusie van dit onderzoek is dat organisaties in de cybersecuritysector minder aan productinnovaties doen (17,6%) dan bedrijven gemiddeld in Nederland (23,2%). Van de cybersecuritybedrijvenorganisaties die aan productinnovaties doet geeft 74,1% aan dit binnen het eigen bedrijf te doen en slechts 37,9% geeft aan dit ook met andere bedrijven of instellingen te doen. Beide percentages liggen lager ten opzichte van de sample van alle bedrijven in Nederland, waar bijna de helft aangeeft productinnovaties te ontwikkelen in samenwerking met andere bedrijven of instellingen. Daarnaast geeft 13,8% van de bedrijven (organisaties) in de cybersecuritysector aan productinnovaties te doen door aanpassingen door te voeren op de goederen van derden. Hetzelfde aandeel van de bedrijven geeft aan omzet te hebben vergaard uit productinnovaties die uitsluitend door andere partijen is ontwikkeld.

Figuur 4.6 toont het percentage van bedrijven dat aangeeft dienstinnovaties uit te voeren uitgesplitst naar de samenwerkingsvorm voor de ontwikkeling van deze dienstinnovatie. Cybersecuritybedrijven voeren gemiddeld meer dienstinnovaties uit (40,1%) vergeleken met alle bedrijven in Nederland (19,1%). De verdeling naar samenwerkingsvorm toont dat het grootste deel van de bedrijven intern dienstinnovaties ontwikkelt. Een kleiner aandeel van de bedrijven geeft aan dit ook in samenwerking met andere bedrijven of instellingen te doen. Slechts een klein deel van de bedrijven geeft aan dienstinnovaties te doen door

aanpassingen te doen aan innovaties van derden of uitsluitend gebruik te maken van de dienstinnovaties van derden, zonder enige aanpassing.



Figuur 4.6: Samenwerkingspartners voor de ontwikkeling van nieuwe diensten door cybersecurity bedrijven en alle bedrijven in Nederland. Bron: Dialogic op basis ban CBS (CIS 2016 - 2018), gebaseerd op een sample van Innovatiespotter.

Aanbeveling 8

Het meten (vangen) van de effecten van onderzoek en innovatie (met behulp van indicatoren) wordt steeds moeilijker van output naar impact. Een veelgebruikte indicator van *outcome* is 'aantal *startups* in een *hightech* domein' (omdat eventuele issues met het toewijzen van effecten van het doen van R&D&I in deze context acceptabel lijken). Voor een eventueel vervolgonderzoek zou Techleap gebruikt kunnen worden als basis voor zo'n analyse. Het is ook relevant om de verdere groei van economische activiteit van dit soort *startups* te volgen, bijvoorbeeld door een analyse van *mergers & acquisitions (M&A).*

4.5 Impact

De effecten van het toepassen van cybersecurity gerelateerde kennis in het productieproces van organisaties leidt tot impact op de economie, en op de samenleving. De resultaten van dit onderzoek suggereren dat alleen directe economische impact te schatten zijn (zie Hoofdstuk 3).

In de praktijk is alleen de ontwikkeling van de toegevoegde waarde gecreëerd door bedrijven betrokken bij cybersecurity R&D&I (op basis van de selectie gemaakt met de database van Innovatiespotter), als een proxy voor de directe economische impact (zie Tabel 4.10), ingegeven door de beperkingen van dit onderzoek (zie Aanbeveling 9). De groei in toegevoegde waarde van Nederlandse bedrijven met cybersecurity activiteiten over de periode 2015 - 2020 bedraagt 35%. Merk hierbij op dat de ontwikkeling van de toegevoegde waarde niet het resultaat hoeft te zijn van onderzoek en innovatie in het cybersecurity domein alleen.

Tabel 4.10: Overzicht van toegevoegde waarde van cybersecurity organisaties (bedrijven) [MEURO]. Bron: Dialogic op basis van CBS, gebaseerd op een sample van Innovatiespotter.

	2015	2016	2017	2018	2019	2020
Toegevoegde waarde van Nederlandse bedrijven (organisaties) met cybersecurity activiteiten	20,67	22,43	25,23	26,18	27,87	27,95
aantal bedrijven	2975	3176	3357	3604	3768	3948
Toegevoegde waarde van cybersecurity gerelateerde activiteiten van Nederlandse bedrijven (organisaties) met cybersecurity activiteiten	5,55	6,01	6,73	7,01	7,46	7,49
aantal bedrijven	2975	3176	3357	3604	3768	3948

Aanbeveling 9

In de context van dit onderzoek zijn een aantal indicatoren samengesteld met behulp van (gegevens van) het CBS, op basis van de selectie van actoren die is voortgekomen uit de database van innovatiespotter. De set van indicatoren is beperkt, ingegeven doordat deze reeds voor dit onderzoek, in de context van (Dialogic 2023) bepaald moest worden. De set zou in een toekomstige structurele evaluatie van de impact van R&D&I in het domein kunnen worden verbeterd of uitgebreid, zoals beschreven in (TNO 2022a). Denk hierbij bijvoorbeeld aan intensiteit van R&D uitgaven (uitgaven als een percentage van toegevoegde waarde, om input te beschrijven), of arbeidsproductiviteit als proxy voor economische impact.

5 Innovatiegedrag en de impact van de huidige beleidsmix

Doel van dit hoofdstuk is het beschrijven van de impact van de huidige beleidsmix op het innovatiegedrag van bedrijven in het cybersecurity domein. De conclusies zijn gebaseerd op de informatie verzameld tijdens de interviews en de survey, en geven daarmee de mening van de gesprekspartners en respondenten weer. Dit onderdeel van het onderzoek moet niet gezien worden als een ex-post analyse van huidig beleid en bijbehorende instrumenten.

Voor het beschrijven van de impact van de beleidsmix wordt eerst de '*businesscase*' van bedrijven in het cybersecurity domein geanalyseerd, en de rol die R&D&I daar in speelt. Dit geeft inzicht in het innovatiegedrag van bedrijven in de bijbehorende sectoren. Vervolgens zijn de '*drivers & barriers*' voor het doen van R&D&I benoemd. Als laatste wordt de impact van de huidige beleidsmix op het innovatiegedrag beschreven en geanalyseerd, gegeven deze '*drivers & barriers*'.

5.1 De '*businesscase*' van cybersecurity bedrijven, en de rol van R&D&I

In de praktijk bepaalt de vraag naar cybersecurity oplossingen de '*businesscase*' van bedrijven in het domein, en daarmee (de richting van) de bijbehorende R&D&I. Daarbij lijken er twee 'extremen' in een breder spectrum te bestaan die de vraag naar cybersecurity oplossingen bepalen: '*tick-in-the-box* dienstverlening' tegenover 'cyberveiligheid als topprioriteit'. In de praktijk refereert dit aan (bewerkingen van) *commercial off-the-shelf (COTS)* cybersecurity oplossingen tegenover (volledig) *custom made* oplossingen. Deze twee perspectieven worden hier onder nader uitgewerkt.

5.1.1 *Value-added resellers* voor COTS cybersecurity oplossingen

Er is een groep van organisaties (aan de ene kant van bovengenoemd spectrum) die cybersecurity diensten beschouwen als één van de randvoorwaarden om (economische) activiteiten te kunnen ontplooien. Om een zeker niveau van cyberveiligheid te verkrijgen huren ze externe cybersecurity bedrijven in voor wat ook wel (en misschien wat oneerbiedig) wordt aangeduid als '*tick-in-the-box*' dienstverlening.

De cybersecurity bedrijven die deze (vraag naar) diensten leveren worden beschreven als '*value-added resellers*'. Zij bouwen enerzijds op (licenties voor) soft- en hardware van met name grote buitenlandse bedrijven (vooral Amerikaanse) met een breed portfolio van geïntegreerde ICT producten en (*cloud*)diensten. Deze buitenlandse bedrijven zijn (wel) in

staat om middelen te steken in de R&D (ontwikkeling) van hun cybersecurity oplossingen, omdat zij in staat (bereid) zijn de risico's kosten en ontwikkelingstijd te dragen, en omdat zij hun producten en diensten aanbieden in een "pakket over de hele breedte", en (daarmee) hun potentiële markt breed is. Daarnaast zijn er in deze context ook aanbieders uit landen waar het 'veiligheidsdenken' verder ontwikkeld is, bijvoorbeeld omdat zij een constante cyberdreiging ervaren - vaak wordt in deze context verwezen naar Israël als voorbeeld. Cybersecurity bedrijven worden daar meer getriggerd (ook door de overheid) om nieuwe en radicale (en daarmee risicovolle) oplossingen te ontwikkelen.

Deze '*value-added resellers*' (voornamelijk *pure players,* behorend tot het mkb) zijn onderdeel van een hele keten die deze producten en diensten implementeert, onderhoudt, cursussen erover geeft, etc. Ze domineren de Nederlandse cybersecurity markt. Deze actoren doen zelf relatief weinig aan R&D: ontwikkeling wordt gefocust "op de randen van het onderzoeksveld, daar waar problemen zijn [...] Je repareert alleen als er iets stuk gaat, en alleen dat wat stuk gaat wordt gerepareerd." Ontwikkelingen / innovatietrajecten zijn vooral gericht 'op de korte termijn'. In de praktijk refereert het aan het samenvoegen van bestaande oplossingen voor "toepassingen in unieke situaties": incrementele innovatie in het cybersecurity domein.

paloalto NETWORKS	• Opgericht: 2005 • Hoofdkantoor: Santa Clara, Verenigde Staten • Beurgenoteerde onderneming, een van de bedrijven van de Nasdaq-100 Index
Marktwaarde	Ruim US $ 50.5 miljard (Q1 2023) (ruim US $ 65 miljard op 01.06.2023)
Omzet(groei)	US $ 5.5 miljard (2022) - 29% groei t.o.v. 2021 (US $4,3 miljard)
Klanten	• B2B: Bedrijven, organisaties, dienstenaanbieders, de publieke sector • Klanten in 180 landen • Voornamelijk indirecte distributie (via distributeurs en resellers/wederverkopers)
Producten & diensten	Producten (hardware & software, 24,8% van omzet) en diensten (abonnementen & support, 75,2% van omzet)
Marktsegmenten	• *Network security* • Full *end-to-end secure access service edge* (SASE) *platforms* & diensten • *Cloud security* • *Security operations* • *Threat intelligence*
Innovatie prioriteiten/ drijfveren/aanjagers	• *Next-generation* cybersecurity • *Zero-trust security* architecturen • *Platformisation* diepgaande integratie van producten en diensten • (Eigen) producten en diensten • Interoperabiliteit van eigen producten en diensten met producten en diensten van derden (testen, certificering)[24] • Toepassing van kunstmatige intelligentie (AI, inclusief generative AI en *Large Language Models*) & automatisering • Ontwikkeling van zowel hardware als software van kritiek belang voor het verbeteren van bestande producten en voor (abonnement) diensten • Korte termijn prioriteiten: samenwerking met eindgebruikers om huidige en toekomstige behoeftes te identificeren; nieuwe producten en functionaliteiten ontwikkelen door tijdig in te spelen op vraag eindgebruikers • Combineren met lange termijn strategische doelen (de concurrentiepositie verbeteren door bijv. overnames) • Additionele focus op onderzoek naar applicaties en dreigingen om snel te kunnen reageren op ontwikkelingen in de markt en snel veranderde dreigingslandschap • Gebruik van gelicentieerde technologie en producten van derden, ter aanvulling en ondersteuning van eigen R&D&I activiteiten
Organische innovatie, d.w.z. innovatie die in-house ontwikkeld is	• 49 nieuwe hoofdcategorieën producten (2022) • Investeringen: ruim US $1,4 miljard in 2022, vergeleken met ruim US $1,1 miljard in 2021 en ruim US $768 miljoen in 2020 • Bovengemiddelde R&D investeringen (tussen de 2 tot 5 keer meer dan andere cybersecurity *pure players*)
Anorganische innovatie: • Door *mergers & acquisitions* (M&A) d.w.z. door concentraties en overnames; en/of • Door gebruik van gelicentieerde producten van derden.	• Investeringen M&A: bijna US $800 miljoen (bruto) in 2022 vergeleken met bijna US $790 miljoen (bruto) in 2021 • Voor incrementele innovatie, m.n. voor de lange termijn strategie

R&D Personeel	• 3.268 R&D (2022) (vergeleken met 2.595 in 2021) van in totaal ruim 12.500 (2022) • 471 miljoen (2022) vergeleken met 429 miljoen (2021) en 275 miljoen (2020) • Op aandelen gebaseerde additionele beloning als incentives om R&D personeel/talent te verwen en te behouden
Samenwerkingen en kennisoverdracht	Onderwijs en training,[25] conferenties (bijv. Ignite[26] & Ignite Public Sector,[27] partnerschappen (bijv. met de Worldconomic Forum), bootcamps[28]

Tabel 5.1: Palo Alto Networks Inc., als voorbeeld van een succesvolle buitenlandse *pure player* die innoveert in het cybersecurity domein.

5.1.2 Sturing door eindgebruiker met cyberveiligheid als topprioriteit

Daarnaast zijn er organisaties voor wie cyberveiligheid een topprioriteit (aan het worden) is, omdat bijvoorbeeld een geslaagde cyberaanval (niet alleen voor henzelf) grote maatschappelijk en economische gevolgen kan hebben - denk hierbij aan de overheid (onder andere op het gebied van justitie en defensie), de financiële en telecom sector, en bedrijven en kennisinstellingen die unieke en strategische kennis (IP) hebben opgebouwd.[29]

Deze organisaties willen meer dan 'standaard', '*tick-in-the-box*' dienstverlening: zij willen als 'eindgebruiker' hun cyberveiligheid 'zelf in de hand hebben'. Voor de noodzakelijke R&D / ontwikkeling bouwen ze op eigen onderzoekscapaciteit, maar ook op die van externe kennispartners (zoals de TU's, Hogescholen en TNO). Cybersecurity bedrijven staan hier vaak 'buitenspel', omdat de eindgebruiker "de richting van de cybersecurity oplossing al zelf heeft bepaald of graag wil bepalen." De prikkel om kennis mee te ontwikkelen wordt verder beperkt omdat deze niet altijd breed toegepast kan (en mag) worden in hun eigen portfolio van producten en diensten.

De perceptie van de gesprekspartners is dat het overgrote deel van de startups in het cybersecurity domein zich bezig houdt met '*tick-in-the-box*' dienstverlening – weinig R&D intensief, en gebaseerd op '*mature*' technologie. R&D en innovatie door (overige) nieuwe cybersecurity bedrijven focust zich vooral op enkele niches. Veel geïnterviewden geven aan dat zij het idee hebben dat zodra deze bedrijven succesvol worden, ze worden verkocht aan grote buitenlandse partijen.[30] Een nadere analyse is noodzakelijk om dit beeld te kunnen bevestigen voor Nederland (zie Aanbeveling 8). Een voorbeeld in deze context uit de Cyber Threat Intelligence (CTI) markt is het Nederlandse EclictiqIQ.

Kader 10: Startups in het cybersecurity domein.

[24] Zie: https://www.paloaltonetworks.com/legal-notices/trust-center/tech-certs.
[25] Zie: https://www.paloaltonetworks.com/services/education.
[26] Zie: https://reg.paloaltonetworks.com/flow/paloaltonetworks/ignite22/faq/page/main.
[27] Zie: https://reg.publicsectorignite.paloaltonetworks.com/flow/paloaltonetworks/psignite23/mainevent/page/event-website?ref=infosec-conferences.com.
[28] Zie: https://register.paloaltonetworks.com/apac20230118sd1461?ref=infosec-conferences.com.
[29] Dit refereert aan sectoren die gedefinieerd worden als 'vitaal' volgens NIS2 (zie Kader 15).
[30] Dat beeld lijkt voor Frankrijk als een voorbeeld de situatie in de EU bevestigd te worden in een recent rapport van Wavestone.

5.2 De impact van overheidsbeleid op het R&D&I gedrag van bedrijven

5.2.1 Huidig beleid en instrumentarium

Cyberveiligheid voor EU burgers en bedrijven is een belangrijke prioriteit voor de EC. Dat heeft geleid tot onder andere een specifieke cybersecurity strategie en (plannen voor nieuwe) wet- en regelgeving. De Nederlandse overheid 'volgt' dit (juridische) kader, en heeft daarnaast recentelijk bijvoorbeeld ook zelf haar (internationale) cybersecurity strategie geformuleerd.[31] Deze complete set van beleidsinitiatieven vormen als het ware het kader waarbinnen cybersecurity R&D&I wordt uitgevoerd. Deze initiatieven worden (mede) ondersteund door specifieke (thematische) en generieke subsidie instrumenten die onderzoek en innovatie in het domein adresseren (zie Kader 11).

In de context van dit onderzoek is geanalyseerd wat de effecten van (enkele van deze) instrumenten zijn op (onder andere de omvang van) *collaborative research* in het Nederlandse cybersecurity domein. In geval van de EC gaat het over de projecten gefinancierd in het kader van het Horizon 2020-kaderprogramma (Horizon 2020) voor onderzoek en innovatie. In geval van de Nederlandse overheid gaat het over projecten die gefinancierd worden middels de mkb-innovatiestimulering Regio en Topsectoren (MIT), en de PPS-toeslag Onderzoek en Innovatie.

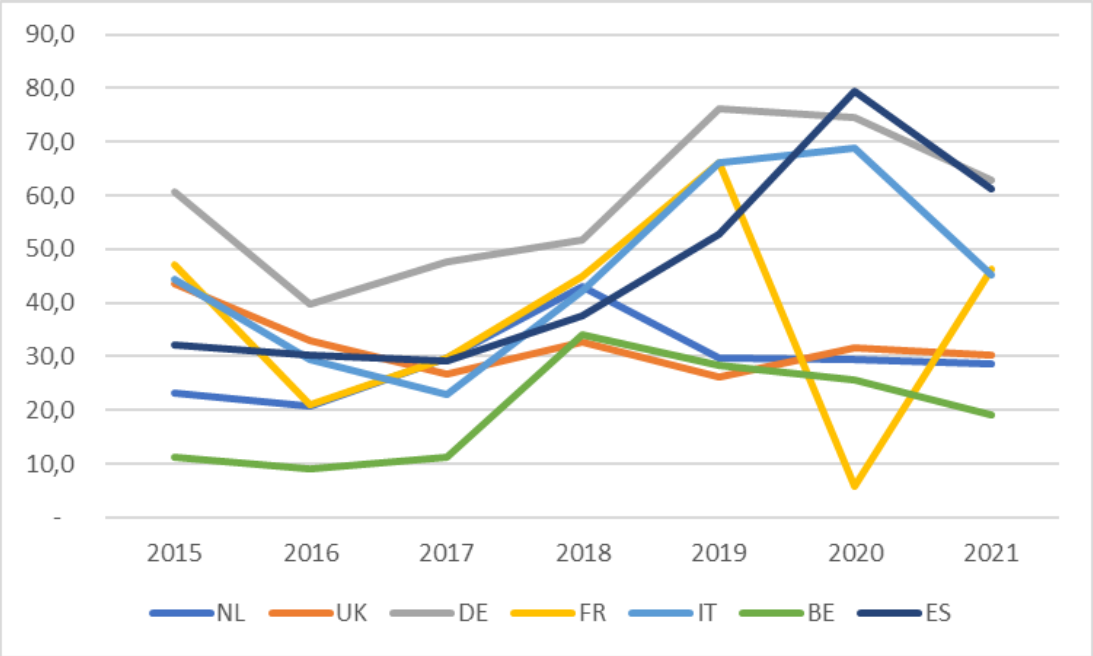
De totale uitgaven van deze drie programma's aan innovatieve cybersecurity projecten bedroegen ongeveer €152 mln. in de periode 2016 - 2020 - minder dan 0,5% van het totaal aan subsidies in deze context (zie Tabel 5.2).

Tabel 5.2: Overzicht van de subsidie voor de uitgevoerde cybersecurity innovatieve projecten [EURO] in de periode 2016 - 2020 van projecten gefinancierd door RVO (MIT en PPS-toeslag) en de EU (H2020). Bron: TNO.

Jaar van start project	Cybersecurity projecten	Alle projecten	Aandeel van de cybersecurity projecten
2016	22.146.082	9.860.136.055	0,225%
2017	31.370.383	10.511.288.416	0,298%
2018	52.441.950	7.126.176.733	0,736%
2019	32.451.836	8.551.385.145	0,379%
2020	35.289.599	8.424.382.851	0,419%
Totaal	151.553.768	34.613.233.145	**0,438%**

De subsidie uitgaven voor Nederlandse organisaties in innovatieve cybersecurity projecten in het kader van H2020 bedroegen gemiddeld €29,1 mln. per jaar - een sterke stijging sinds 2015, en met een piek in 2018 (zie Figuur 5.1). De uitgaven aan Duitse organisaties is in EU context het hoogst.

[31] Relevant in deze context is de Nederlandse Cybersecuritystrategie 2022-2028.



Figuur 5.1: Omvang subsidie voor innovatieve cybersecurity projecten in het kader van H2020 in de periode 2014 - voor organisaties uit Nederland, UK, Duitsland, Frankrijk, Italië, België, Spanje [mln. EURO].Bron: TNO.

De nieuwe EU cybersecurity strategie (2021) draagt bij aan een aantal specifieke doelstellingen voor de Unie, zoals technologische soevereiniteit en strategische autonomie, en vertaalt deze naar concrete 'prioriteiten' zoals: i) cybersecurity standaardisatie; ii) het bevorderen van sterke encryptie; iii) het bevorderen van een goed beveiligde (kritieke) infrastructuur; en iv) geïntensifieerde internationale samenwerking en informatie-uitwisseling.

Deze EU cybersecurity strategie 'bouwt' op (nieuwe voorstellen voor) wet- en regelgeving, alsmede specifieke R&D&I cybersecurity programma's:

Recente EU-wetgeving die op nationaal niveau al geïmplementeerd is of nog geïmplementeerd moet worden:

- Richtlijn betreffende maatregelen voor een hoog gezamenlijk niveau van **cyberbeveiliging in de Unie** (NIS2) (2022, *Directive on measures for high common level of cybersecurity across the Union*).
- Richtlijn betreffende de weerbaarheid van **kritieke entiteiten** (2022, *Directive on the resilience of critical entities*).
- De cyberbeveiligingsverordening - Verordening inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de **certificering** van de cyberbeveiliging van informatie- en communicatietechnologie (2019).
- Verordening 2022/2554 van 14 december 2022 betreffende digitale operationele weerbaarheid voor de **financiële sector**.
- Gedelegeerde handeling van Richtlijn 2014/53/EU betreffende de harmonisatie van de wetgevingen van de lidstaten inzake het op de markt aanbieden van radioapparatuur (*Radio Equipment Directive*); om de cyberveiligheid van ***IoT*** **en draadloze apparaten** op de Europese markt te verbeteren.

Voorstellen voor nieuwe EU wet- en regelgeving:

- Voorstel (2022) voor een Verordening betreffende horizontale cyberbeveiligingsvereisten voor **producten met digitale elementen**.
- Voorstel voor een verordening betreffende de Cybersolidariteitswet (april 2023) (*Proposed Regulation on the Cyber Solidarity Act*) voor de opsporing, voorbereiding en respons op **aanzienlijke en grootschalige cyberbeveiligingsdreigingen en -aanvallen**.
- Voorstel (2022) voor een Verordening betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de **instellingen, organen en instanties van de Unie**.
- Voorstel voor een verordening betreffende markten in cryptoactiva (2020) voor de **financiële sector**.

Andere initiatieven:

- De initiatief om EU-beleid inzake cyberdefensie (*Cyber Defence*) te ontwikkelen, met een technologie *roadmap* voor **security en defensie**.

EU cybersecurity R&D&I funding:

- Horizon Europe - bijna €400 mln. voor **onderzoek en innovatie** op het gebied van *Civil Security for Society*, 2023-2024; aangevuld in 2023 met een additionele €50 mln. voor een werkprogramma om civiel veiligheidsonderzoek te financieren.
- Digital Europe programma - €375 mln. euro voor de periode 2023-2024 om de **collectieve weerbaarheid** van de EU tegen cyberdreigingen te vergroten.
- Initiatieven rondom het ontwikkelen van cybersecurity **vaardigheden** (skills).

De Nederlandse cybersecurity beleidsmix is beschreven in (TNO 2018). Een recente en relevante aanvulling op het overzicht in dit rapport is de **Internationale Cyberstrategie voor een open, vrij en veilig digitaal domein** **met als s**trategische doelstellingen: i) tegengaan van cyberdreigingen van staten en criminelen; ii) versterken van democratische en mensenrechtelijke principes online; iii) behoud van een wereldwijd open, vrij en veilig internet. Een overzicht van alle relevante instrumenten die (publiek-)private R&D&I in het domein adresseren is te vinden op de site van RVO.

Kader 11: Beleidscontext: Nederland en de EU.

5.2.2 Perceptie van de impact van het beleid en bijbehorende instrumenten op R&D&I

De response van de interviews en survey op vragen over de huidige beleidsmix die R&D&I adresseert is zo divers als het cybersecurity domein zelf. Met name de kleinere bedrijven (in het cybersecurity domein vooral *value-added resellers*) benoemen 'beperkingen' van het huidige instrumentarium waar vergelijkbare organisaties in andere sectoren ook mee worstelen. De perceptie is dat "het huidige innovatie-instrumentarium niet past bij de praktijk van de dienstverlenende cyberbedrijven. De focus op de lange termijn [van de PPS toeslag] sluit niet aan bij de korte-termijn focus van de innovatiebehoefte. [...] De tijd die genomen wordt voor beoordeling van voorstellen is te lang." Vertegenwoordigers van de sector benoemen ook de problemen met het opbrengen van een bepaald niveau van 'cofinanciering' (en dan vooral 'direct' in plaats van '*in kind*'), en het overbruggen van '*the valley of death*'. Ook wordt het vestigingsklimaat voor start ups als "minder sterk" ervaren vergeleken met andere landen.

Veel van de geïnterviewden refereren ook aan een belangrijke barrière voor R&D&I, zoals benoemd in Paragraaf **Error! Reference source not found.**: de (in hun ogen) beperkte rol die de overheid speelt in het cybersecurity domein. De perceptie is dat cybersecurity in de praktijk belegd is bij verschillende ministeries, elk met hun eigen doelstellingen. De rol van R&D&I in de context van die verschillende doelstellingen ook nog eens verschillend, en niet (altijd) heel prominent. Het idee leeft dat er dientengevolge maar een beperkte regie is wat betreft die richting van (publiek gefinancierd) onderzoek en innovatie, dat de keten van kennisontwikkeling naar kennistoepassing nog steeds niet goed op elkaar is afgestemd, en dat dientengevolge de transitie van onderzoek naar toepassing niet optimaal verloopt. "Met dcypher is er een goede start gemaakt, maar verdere sturing is noodzakelijk."

6 Conclusies: suggesties voor aanpassingen in de beleidsmix

Doel van dit hoofdstuk is om suggesties te doen voor de vormgeving van de toekomstige beleidsmix. Dit hoofdstuk bouwt daarvoor op de beschrijving van enkele belangrijke aspecten van de *'as is'* situatie wat betreft R&D&I in het cybersecurity domein: de *drivers* en *barriers* van onderzoek en innovatie (Paragraaf **Error! Reference source not found.**); en de perceptie van de 'geschiktheid' van de huidige beleidsmix (zoals beschreven in paragraaf 0). Daarnaast worden de aanbevelingen gebaseerd op een korte beschrijving van de mogelijke *'will be'* (of *'should be'*) situatie: een beeld van de geïnterviewden en de respondenten van de survey van de gewenste impact van cybersecurity op de economie en de samenleving, en de richting van (R&D&I) die daarvoor nodig is.

De resultaten van dit het onderzoek, zoals beschreven in Hoofdstuk 4, suggereren dat in ieder geval de omvang van R&D&I in het cybersecurity domein (Input en Activiteiten) is toegenomen. Het doen van onderzoek en innovatie wordt echter gehinderd door specifieke vormen van marktfalen, die maken dat (private) actoren 'onderinvesteren' in R&D&I, en die verdere publieke interventie legitimeren.[32] Daarnaast lijkt de markt voor cybersecurity oplossingen verder gehinderd te worden door een achterblijvende vraag die een grotere rol van de overheid noodzakelijk lijkt te maken (zie Kader 11).

6.1 De toekomst van het cybersecurity domein

De gesprekspartners en respondenten van de survey zijn opvallend eensgezind als het gaat over de gewenste impact van cybersecurity. Zij refereren in deze context (in verschillende bewoordingen) aan de het bijdragen aan maatschappelijk en economische veiligheid - geformuleerd bijvoorbeeld als "het voorkomen van schade [en] het borgen van veiligheid in de gehele keten." Cybersecurity wordt daarbij in de praktijk gezien als een essentieel element voor de verdere 'digitalisering' van de economie en de samenleving, en daarmee voor de transities waar we voor staan - op het gebied van energie, gezondheidszorg, etc. Dit correspondeert (niet verrassend) met hun visie op de brede maatschappelijke en economische waarde van cybersecurityproducten en -diensten zoals beschreven in Hoofdstuk 3.

Merk hierbij op dat de omvang van de sample van geïnterviewden beperkt is, en dat dientengevolge het overzicht dat geschetst wordt niet 'compleet'.

[32] Zie: State aid rules for research, development & innovation (framework) (europa.eu).

6.2 Toekomstige beleidsmix

De perceptie van de *as is* en de *will be* situatie van de actoren in het cybersecurity domein resulteert in een aantal aanbevelingen voor de toekomstige overheidsinterventie. Opvallend is dat de respondenten niet zozeer refereren aan de vormgeving van instrumenten en hun *policy delivery*, maar (op een veel 'hoger' / abstracter niveau) aan de rol van de overheid in het domein zelf (door het voeren van regie), en in de samenleving (door het creëren van *awareness* over cyberveiligheid).

Veel van de gesprekspartners benoemen dat de vraag naar cybersecurity oplossingen achter lijkt te blijven bij de relevantie die het in hun ogen heeft voor het goed functioneren van de economie en de samenleving. Om een 'meer regie-voerende rol' van de overheid in deze context te duiden moet een belangrijke onderliggende vraag worden beantwoord: is cyberveiligheid een (semi-) publiek goed of niet (zie Kader 11)? Als geconcludeerd wordt dat het antwoord op die vraag "ja" is (en een beslissing over de exacte invulling in die context wordt niet alleen getrokken op basis van onderzoek, maar is evenzeer een politieke afweging), dan leidt dat ook tot een aantal conclusies (aannames):

- R&D&I in het cybersecurity domein wordt niet alleen gehinderd door 'traditionele' vormen van marktfalen die worden geassocieerd met het doen van onderzoek en innovatie (zoals het optreden van *spillover* effecten, coördinatiefalen, etc.).
- De 'traditionele' instrumenten (zoals de MIT en de PPS toeslag) zijn dientengevolge niet afdoende om R&D&I in het domein aan te jagen.
- Er is een duidelijke rationale en legitimatie voor een andere rol van de overheid (in de markt, aan de vraagzijde als ook aan de aanbodzijde) - gelijk bijvoorbeeld als in de context van defensie of onderwijs.

De geïnterviewden benoemen een aantal voorbeelden hoe de overheid een andere meer regie-voerende rol zou kunnen voeren. Daarbij dient opgemerkt te worden dat ze zeker geen complete invulling geven van de rol van de overheid indien cyberveiligheid wordt beschouwd als een publiek goed. Hun aanbevelingen zijn veel breder in deze context.

Veel gesprekspartners stellen dat er veel organisaties en ministeries actief zijn op het gebied van R&D&I in het cybersecurity domein. Maar "[dat] leidt ertoe dat veel partijen langs elkaar heen werken [...]. Er wordt veel onderzoek uitgevoerd, waar weinig actie uit blijkt te volgen. Een centraal loket zou dit probleem ook kunnen verminderen."

De geïnterviewden benoemen verder dat de Nederlandse overheid "zou moeten nadenken over de vraag welke basis we in huis zouden moeten hebben" (wat betreft kennis, maar ook productie in specifieke toepassingsgebieden als 'energie' en 'water') om nationale en economische veiligheid te waarborgen; "wat we kunnen 'afnemen' van partijen [uit landen] die we vertrouwen"; en "wat we bereid zijn af te nemen van overige partijen." Dit lijkt te refereren aan de vraag op welke technologievelden de overheid een zeker mate van (open strategische) autonomie wil hebben. In die context is het goed om te realiseren dat producten en diensten waarin veel cybersecurity oplossingen zitten, vaak uit landen komen die 'veiligheidsbelangen' hebben die niet gelijk zijn aan die van ons. Maar dit gaat ook over de vraag welke sectoren de Nederlandse overheid van strategisch belang acht, en die dientengevolge 'cyberveilig' moeten zijn – denk aan de Rotterdamse haven. Dit specifieke voorbeeld biedt volgens de gesprekspartners ook kansen voor verdere economische ontwikkeling van de cybersecurity oplossingen in deze context "[aansluiten] bij onze kracht en sterkte op het gebied van logistieke ketens."

De geïnterviewden stellen dat wat betreft kennis die we ‘in huis’ zouden moeten hebben dat de overheid moet nadenken wat zij kan ‘overlaten aan de (Nederlandse) markt’, en wat zij zelf zou moeten (laten) uitvoeren omdat ‘die markt niet tot de juiste oplossingen komt’. Dit refereert specifiek aan de rol van de overheid in de aanbodzijde van de markt. Maar de geïnterviewden hebben ook suggesties voor een meer regie-voerende rol aan de vraagkant. Zo merken zij op (als voorbeeld om dit te illustreren) dat “De Nederlandse overheid momenteel alleen voor het geclassificeerde segment eisen [heeft] gesteld waaraan de producten die de overheid gebruikt moeten voldoen. Wanneer de overheid een duidelijkere voorbeeldfunctie pakt door deze eisen te stellen voor alle producten binnen de overheid, kan dit een impuls vormen voor de markt. Ook hier speelt echter het probleem dat cybersecuritybeleid is versnipperd binnen de overheid: welk ministerie zou deze transitie tot voorbeeldfunctie op zich kunnen nemen?”

Bijna alle gesprekspartners noemen dat er in de beleidsmix meer aandacht moet zijn voor het creëren van ‘*awareness*’ van de noodzaak van het toepassen van cybersecurity producten en diensten. “Het ‘veiligheidsdenken’ is [in zijn algemeenheid] in Nederland beperkt ontwikkeld.” Het idee is dat hiermee de vraag naar Nederlandse cybersecurity producten en diensten kan worden vergroot, resulterend in een extra prikkel voor R&D&I. Maar veel van de geïnterviewden benoemen expliciet dat ook bedrijven in het cybersecurity domein verantwoordelijkheid dragen in deze context. “Regelgeving kan helpen om te sturen. De AVG bijvoorbeeld heeft het denken over cyberveiligheid beïnvloed. De nieuwe Europese Cybersecurity Act zal ook een impact hebben op het innovatiegedrag van bedrijven.”
De gesprekspartners refereren hier ook naar het belang van ‘sociale innovatie’: onderzoek naar hoe de ‘*uptake*’ van cybersecurity technologie in de maatschappij te versnellen.

Referenties

Bree, M.W. van, Gijsbers, G.W., Otto, D.P., Janssen, V., Winkels, E., Goes, M., Gielgens, L., van den Horst, T. (2023) Herijking sleuteltechnologieën 2023.

CBS (2020). *Cybersecuritybedrijven in Nederland - (cbs.nl)*.

CWTS (2019) *De wetenschappelijke en technologische rol van Nederland in het domein cybersecurity sinds 2005*.

Dialogic (2020). *Onderzoeks- en innovatie-ecosystemen in Nederland*.

Dialogic (2023). *De economische kansen van de cybersecuritysector* .

EC (2022). *Digital Economy and Society Index (DESI) 2022*.

ENISA (2022a). *European Cybersecurity Skills Framework (ECSF) - User Manual - ENISA (europa.eu)*.

ENISA (2022b). *ENISA Cybersecurity Market Analysis Framework (ECSMAF) — ENISA (europa.eu)*.

Jackson, D.J. (2011). *What is an Innovation Ecosystem? National Science Foundation*.

NCTV (2022). *Nederlandse Cybersecuritystrategie 2022-2028*.

RVO (2023). *Inzet op sleutel technologieën vanuit de WBSO*.

SEO (2016) *Economische kansen Nederlandse cybersecurity-sector*.

TNO (2019). *Onderzoek naar het versterken van de innovatieketen op het terrein van cybersecurity*. TNO-rapport 2019 R10769.

TNO (2022a). *SUP - EZK-ECON. PERSP. CYBERSEC. 2021 - R&D&I indicatoren in het cybersecurity domein*. TNO-rapport 2022 R10738.

TNO (2022b). *SUP - EZK-ECON. PERSP. CYBERSEC. 2021 - Scoping onderzoek naar de impact van R&D&I in het cybersecurity domein*. TNO-rapport 2022 R11751.

TNO (2022c). *Resultaten kwantitatieve analyse Cyber Workforce Development*. TNO-rapport 2022.

ICT, Strategy & Policy

Anna van Buerenplein 1
2595 DA Den Haag
www.tno.nl

TNO innovation for life