Samenvatting

Om onderzoeks- en innovatiebeleid gericht op het versterken van het cybersecurity domein 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.

Om bij te dragen aan de vormgeving van effectief en efficiënt onderzoeks- en innovatiebeleid in het cybersecurity domein zijn in de context van dit onderzoek de volgende vragen geadresseerd:[1]

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?

Het onderzoek is uitgevoerd een drietal opeenvolgende fasen. Als eerste is, op basis van databases Innovatiespotter, Jobdigger, en RVO en de Europese Commissie, een drietal samples van actoren in het cybersecurity domein samengesteld - elk met hun eigen karakteristieken. Het samenstellen van deze samples is uitgevoerd ineen aantal stappen, die als volgt zijn 'samen te vatten': i) samenstellen van een lijst van termen om in de databases te kunnen zoeken; ii) samenstellen van een eerste sample met relevante actoren; iii) verbeteren en valideren van deze selectie om te komen tot een uiteindelijke set van actoren.[2]

In de volgende fase is informatie met en over actoren verzamelen: i) door het maken van nieuwe beschrijvende statistieken van de geïdentificeerde samples (als basis voor conclusies voor het gehele cybersecurity domein); ii) door het maken van nieuwe statistieken voor bestaande actoren door het koppelen van actoren uit de samples aan CBS microdata over onderzoek, innovatie en productie; iii) door het afnemen van interviews met stakeholders; en iv) door het uitzetten van een survey.

Als laatste zijn conclusies geformuleerd over de impact van R&D&I in het cybersecurity domein. Deze conclusies zijn in het rapport, en in deze samenvatting, gestructureerd volgens de onderzoeksvragen.

Kader 1: Onderzoeksopzet.

Impact R&D&I: maatschappelijke en economische waarde

Om de eerste onderzoeksvraag te kunnen beantwoorden zijn stakeholders bevraagd over wat waarde is die wordt gecreëerd door (R&D&I) in het cybersecurity domein, hoe deze tot stand komt, en hoe deze 'gevangen' zou kunnen worden (in 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

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

[2] 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. 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 ((TNO 2019) en TNO 2022a)).

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. Een eerste aanzet voor het omschrijven van de omvang van deze effecten is gedaan met de beantwoording van de tweede onderzoeksvraag hier onder.
- 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 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. 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.

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.

Het Nederlandse cybersecurity innovatie-ecosysteem: van input tot impact

De effecten van R&D&I in het cybersecurity domein zijn beschreven met behulp van het input - impact framework, op basis van de statistieken die in het kader van dit onderzoek zijn ontwikkeld, en op basis van de resultaten van de interviews en de survey.

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

Bedrijven in het cybersecurity domein blijken gemiddeld veel kennisintensiever te 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 van deze bedrijven groeide in de periode 2015 - 2020 met 95% - veel meer dan de totale private groei van 30% in deze periode. Statistieken om de (groei in) uitgaven te vergelijken in een internationale context zijn er niet. De perceptie van veel van de geïnterviewden is echter dat landen "waar het 'veiligheidsdenken' verder is ontwikkeld" (zoals Israël), of "waar een grotere thuismarkt is" (zoals de VS), de intensiteit van de uitgaven hoger is.

Ook de omvang van het R&D personeelsbestand van bedrijven in het cybersecurity domein die aan onderzoek doen 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 2022, met een duidelijke versnelling na 2020. Na 2022 is juist weer een daling in uitgezette vacatures waarneembaar.

Merk op dat de onderzochte bedrijven in het cybersecurity domein niet allemaal *pure players* zijn, en dat dientengevolge de (groei in) uitgaven en inzet van R&D personeel niet alleen wordt besteed aan cybersecurity onderzoek.

Activiteiten: omvang en karakteristieken onderzoek

In de periode 2015 - 2020 is het aandeel van de bedrijven in het cybersecuritydomein (*pure* zowel als *partial*) dat zelf aan onderzoek doet licht gestegen: van 54,7% naar 57,8%. Dit onderzoek is voornamelijk experimenteel of 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. In het cybersecuritydomein (van *pure* en *partial players*) 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.

Outcome: effecten van R&D&I op omzet
Nederlandse bedrijven die cybersecurity R&D&I uitvoeren (als *pure* of *partial* player) 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
Dit onderzoek heeft alleen geleid tot nader inzicht in de omvang van directe impact van R&D&I op de economie. Op basis van het onderzoek kan geconcludeerd worden dat de groei in toegevoegde waarde van Nederlandse bedrijven met cybersecurity activiteiten over de periode 2015 - 2020 35% bedraagt. 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.

Een vervolgonderzoek zou juist de directe en indirecte impact nader moeten adresseren - ook om iets te zeggen over efficiënt het domein is in het omzetten van input en activiteiten in impact op de maatschappij en de samenleving.

Innovatiegedrag en de impact van de huidige beleidsmix

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.

- 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 die worden beschreven als 'value-added resellers'. Deze bouwen voor hun dienstverlening 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.
  De 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.

- 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.
  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. 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.

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). 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.

Voor het beantwoorden van de vraag wat nu precies de rol is van de overheid in het cybersecurity domein, zou eerst een andere belangrijke onderliggende vraag moeten worden geadresseerd, die al langer onbesproken en daarmee onbeantwoord is (zie (TNO 2018)): is cyberveiligheid een (semi-) publiek goed of niet? Een antwoord op de vraag is niet eenvoudig te geven - en ook geen onderwerp van deze studie. In de praktijk echter ligt in Nederland (en de EU) de verantwoordelijkheid voor cyberveiligheid (in ieder geval voor nu) voornamelijk bij (eind)gebruikers van digitale toepassingen (producten en diensten). Maar recent onderzoek door het WEF bijvoorbeeld laat zien dat in Europa gebruikers van internetdiensten de verantwoordelijkheid vooral leggen bij *network & internet service providers* en de overheid, en niet zozeer bij zichzelf. Als gevolg daarvan kan weer gesteld worden dat de vraag naar cybersecurity oplossingen (in de Nederlandse markt) onvoldoende ontwikkeld en gearticuleerd is, en daarmee remt het ook de omvang (en richting) van 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.” Met name sectorvertegenwoordigers 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 startups als “minder sterk” ervaren vergeleken met andere landen.

Conclusies: suggesties voor aanpassingen in de beleidsmix

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 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 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."

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.

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.