Anna van Buerenplein 1
2595 DA Den Haag
Postbus 96800
2509 JE Den Haag

www.tno.nl

T +31 88 866 00 00

TNO-rapport

TNO 2019 R10769

Onderzoek naar het versterken van de innovatieketen op het terrein van cybersecurity

"Als je doet wat je deed, krijg je wat je kreeg"

Datum	10 januari 2020
Auteur(s)	Gabriela Bodea (TNO) Hettie Boonman (TNO) Puck van den Brink (TNO) Marcel de Heide (TNO) Cor Ottens (TNO) Matthijs Veenendaal (TNO) Jos Winnink (CWTS) Annemarie Zielstra (TNO)
Exemplaarnummer	
Oplage	
Aantal pagina's	95
Aantal bijlagen	
Opdrachtgever	Ministerie van Economische Zaken en Klimaat
Projectnaam	
Projectnummer	060.38971

Management samenvatting

Inleiding

Nederland is één van de meest gedigitaliseerde samenlevingen ter wereld (ITU, 2017), (Europese Commissie, 2019) en één van de eerste OECD-landen die een cybersecurity-strategie opstelde (de Nationale Cyber Security Strategie 'Slagkracht door samenwerking' (NCTV, 2011)). Door de opkomst van nieuwe (digitale) technologieën, verdere ontwikkeling van bestaande technologieën en de impact die dat heeft op digitalisering, wordt cybersecurity en cybersecurity-innovatie steeds belangrijker voor een goed functionerende en concurrerende economie, en voor het algemeen vertrouwen in de digitale samenleving.

Vraag

Dit onderzoek is, in opdracht van het ministerie van Economische Zaken en Klimaat (EZK), uitgevoerd om inzicht te geven in de innovatieketen op het terrein van cybersecurity en om na te gaan of en hoe deze innovatieketen versterkt kan worden. Het onderzoek richtte zich op beantwoording van de volgende vragen: *Wie innoveert, op welk gebied, onder welk innovatiemodel, waar op de TRL-schaal, met wie en waarom (wat zijn de incentives voor bedrijven om te innoveren en wat beperkt hen daarin)?*

Dit onderzoek is een beschrijving en analyse van de cybersecurity-innovatieketen. Dit is de eerste keer dat er onderzoek is gedaan naar het functioneren van de Nederlandse cybersecurity-innovatieketen in zijn geheel.

Aanpak

Doordat het cybersecurity-domein relatief jong is, zijn er specifieke uitdagingen verbonden aan dit onderzoek ten aanzien van het vergaren van de noodzakelijke informatie en inzichten. Zo is er bijvoorbeeld nog geen eenduidig en algemeen gedragen definitie van wat cybersecurity nu precies is. Dit leidt ertoe dat, door het ontbreken van een duidelijke afbakening, er nauwelijks tot geen informatie te vinden is in bestaande bronnen en databases voor indicatoren zoals 'uitgaven aan R&D' door de actoren in de cybersecurity-keten.

Voor het verzamelen van de voor het onderzoek benodigde gegevens is daarom een methodiek ontwikkeld, bestaande uit kwalitatieve en kwantitatieve methoden om bestaande maar vooral nieuwe informatie en data bijeen te brengen, om zo deelaspecten van de keten te analyseren. Als uitgangspunt voor de gegevensverzameling is de definitie van het CBS van het concept 'cyber secure' omarmd en nader geïnterpreteerd om te komen tot een werkbare afbakening van cybersecurity. De op basis van de methodiek bij elkaar gebrachte kennis, levert inzichten op in het functioneren van de keten, maar roept tegelijkertijd ook nieuwe (onderzoeks)vragen op.

Gedurende het onderzoek heeft een klankbordgroep met de onderzoekers gediscussieerd over de aanpak en de bevindingen, deze waar mogelijk getoetst

aan de achterban en daarmee waardevolle input geleverd en de bevindingen verder aangescherpt. De klankbordgroep bestond uit de volgende organisaties: CBS, CPB, Cyberveilig Nederland, dcypher, Dialogic, ministerie van Defensie en ministerie van Justitie en Veiligheid.

Dit onderzoek heeft geresulteerd in een landschapsbeschrijving. Het is een eerste inventarisatie en bedoeld om de discussie op een hoger niveau te tillen. Als zodanig is dit onderzoek te beschouwen als een nulmeting.

Conclusies en aanbevelingen

Het onderzoek heeft veel nieuwe inzichten opgeleverd. Hieronder volgen de meest in het oog springende conclusies aan de hand van de verschillende onderzoeksvragen:

Wie innoveert?
Niet één ecosysteem
Het Nederlandse cybersecurity-innovatielandschap is heel divers en bestaat uit een grote verscheidenheid aan categorieën actoren, samenwerkingsverbanden en initiatieven die direct of indirect een bijdrage leveren aan cybersecurity-innovatie.[1] De cybersecurity-industrie bestaat zowel uit ‘pure players’ (bedrijven die alleen cybersecurity gerelateerde activiteiten uitvoeren) als ‘partial players’, bedrijven voor wie cybersecurity niet tot de kern van hun activiteiten behoort.

Bijzonder aan het cybersecurity-domein is ook dat individuen zich organiseren in samenwerkingsverbanden als open software ontwikkeling ‘communities’ of de ‘ethical hacker community’ om daarmee een belangrijke bijdrage te leveren aan de innovatieketen.

Op welk gebied?
Nederlandse actoren leveren een grote bijdrage aan het totale onderzoek op het gebied van cybersecurity
De in de context van dit onderzoek uitgevoerde bibliometrische analyse laat zien dat Nederland binnen de EU tot de koplopers behoort wat betreft het aantal wetenschappelijke publicaties, direct na het VK, Duitsland, Frankrijk en Spanje, maar duidelijk vóór de andere lidstaten. Wetenschappelijke publicaties op het gebied van cybersecurity vinden voornamelijk plaats in de wetenschapsvelden ‘computer science disciplines’ en ‘communicatie’. Relatief minder frequent zien we de onderzoeksgebieden ‘criminology & penology’ en ‘mathematics interdisciplinary applications’.

Ook wat betreft de omvang van het aantal uitvindingen behoort Nederland binnen de EU tot de meest prominente landen. De volgende technologiegebieden kennen de meeste octrooiaanvragen: (1) de transmissie van digitale informatie, (2) draadloze communicatie, o.a. Wi-Fi-netwerken, (3) het verwerken van digitale informatie en (4) beeldcommunicatie.

[1] De vraagzijde van onderzoek en innovatie, en dan met name die actoren die niet zelf aan onderzoek en innovatie doen, zijn niet expliciet geadresseerd in de context van dit onderzoek.

Op welke manier - onder welk innovatiemodel?

Innovatie vindt in een veelvoud van vormen plaats

Het onderzoek laat zien dat de innovatieketen een veelvoud van vormen van innovatie kent; van volledig open tot volledig gesloten. Binnen innovatietrajecten worden vaak verschillende innovatiemodellen gebruikt. Zo kan open-software in gesloten innovatie geïntegreerd worden of komt er uit gesloten innovatie een oplossing die uiteindelijk terecht komt in een open innovatietraject.

Nadruk ligt op 'sustaining innovation'

Innovatie-activiteiten door Nederlandse bedrijven zijn met name gericht op 'sustaining innovation': probleem-gedreven innovatie gericht op het vinden van een oplossing voor een concrete vraag uit de markt.
Wat onvoldoende uit de verf komt is 'disruptive innovation': innovatie die zich niet richt op symptoombestrijding maar op baanbrekende toepassingen die de structurele tekortkomingen in cybersecurity adresseren.

Waar op de TRL schaal?

Actoren uit het innovatiesysteem binnen de cybersecurity-innovatieketen opereren waar dat te verwachten is. Zo zijn universiteiten en NWO-instituten vooral terug te vinden in de lagere TRL-niveaus (TRL 0 - 3). De Technische Universiteiten innoveren voornamelijk tot en met TRL 4, maar verleggen ook meer en meer hun scope tot en met TRL 7. De Toegepast Onderzoek Organisaties (TO2) richten zich met name op TRL 4 tot TRL 7.

Bedrijven zijn nauwelijks direct betrokken bij fundamenteel onderzoek. Zij opereren meestal vanaf TRL 4. Het onderzoek laat verder zien dat er in Nederland nagenoeg geen bedrijven actief zijn die het hele innovatieproces van TRL 0 - 9 zelfstandig kunnen uitvoeren. Ook startups en MKB-bedrijven opereren vanaf TRL 4. Ze lijken echter in mindere mate actief zijn in de hoge TRL-niveaus 7 - 9, mogelijk doordat deze bedrijven moeilijk zelfstandig voorbij TRL-niveau 6 komen.

Met wie?

Per onderwerp ontstaan specifieke samenwerkingsverbanden

Er wordt op een veelheid van onderwerpen geïnnoveerd en per onderwerp ontstaan specifieke samenwerkingsverbanden. Zo ontstaan hubs rondom bedrijven en kennisinstellingen waar bepaalde innovatie wordt gepusht. Samenwerking tussen de verschillende partijen in de cybersecurity- innovatieketen is echter geen vanzelfsprekendheid.

Als samenwerking plaatsvindt, dan is deze bijna altijd gericht op technologieontwikkeling. Partijen vinden elkaar in die context op een specifiek onderwerp. Wanneer dat tot succes heeft geleid, wordt de samenwerking echter niet automatisch voortgezet.

Waarom?

Drivers

De belangrijkste driver voor innovatie is de grote vraag naar cybersecurity-oplossingen. De brede aandacht voor, onder andere, cybercrime en in het oog springende incidenten zorgen voor een sterk groeiende vraag naar cybersecurity-producten.

Uit het onderzoek komt naar voren dat de sector ervaart dat de beschikbare private financiering (in de vorm van 'debt- en equity-financiering') voldoende is. Dit impliceert echter niet dat er geen behoefte is aan additionele financiering in de vorm van bijvoorbeeld subsidies voor het adresseren van vormen van marktfalen die refereren aan het doen van onderzoek en innovatie.

Barriers

i) Gebrek aan visie en sturing over de keten

De resultaten van de interviews geven aan dat de overheid als geheel geen eenduidige visie heeft op de rol voor cybersecurity in de Nederlandse samenleving en economie en hoe die moet worden ingevuld.

Naast het gebrek aan een heldere visie vindt er weinig sturing over de keten heen plaats. De verschillende ecosystemen blijken nog weinig van elkaars kennis te profiteren.

ii) Huidige set van instrumenten is niet effectief

Publieke kennisinstellingen stellen dat de totale omvang van publieke uitgaven aan (fundamenteel en toepassingsgericht) cybersecurity gerelateerd onderzoek achterblijft bij andere landen in Europa.

Met name private actoren hebben moeite met de complexiteit van instrumenten voor onderzoek en innovatie. Zij ervaren deze als ingewikkeld, met complexe procedures en regelgeving. Daarnaast is de looptijd over het algemeen te lang voor MKB-bedrijven en startups, die binnen twee jaar rendement op hun investering moeten hebben. Verder komt naar voren dat het huidige instrumentarium vooral traditionele actoren ondersteunt, zoals grote bedrijven en kennisinstellingen. Als laatste constateren private partijen dat het instrumentarium niet is toegerust om startups de 'valley of death' (de stap van concept naar product) te laten overbruggen.

iii) Beperkt absorptievermogen

Hoewel de vraag naar cybersecurity-oplossingen groot is, laat het onderzoek zien dat gebruikers steeds meer moeite hebben om de laatste ontwikkelingen op dit gebied te implementeren. Het gaat hier om beperkingen in de absorptiecapaciteit van zowel bedrijven als overheid. Er is in brede zin een gebrek aan kennis (kwaliteit) en mensen (capaciteit en continuïteit) om de snelle veranderingen in het domein te kunnen volgen en nieuwe toepassingen te implementeren.

iv) Gebrek aan goed opgeleide mensen

De sectoren in de Nederlandse economie die worden gedreven door hoogwaardige technologie worden in zijn algemeenheid gehinderd door een gebrek aan goed opgeleide mensen. Dit geldt nog meer voor de onderliggende onderzoeks- en innovatietrajecten in deze sectoren.

Tot slot: aanbevelingen

Op verzoek van het ministerie van EZK bevat dit rapport een aantal aanbevelingen om de innovatiecapaciteit van de keten te versterken. Deze aanbevelingen zijn

geformuleerd door het onderzoeksteam, en vervolgens getoetst tijdens een bijeenkomst van de klankbordgroep, opdat zij een bredere verankering hebben in de innovatieketen.

Er is een meervoudige set van aanbevelingen geformuleerd. Een aantal adresseert de huidige situatie en hoe deze verder te optimaliseren middels aanpassingen in de huidige set van instrumenten die de keten ondersteunt. Uit het onderzoek komt verder duidelijk naar voren dat voor het werkelijk cyberveilig maken van Nederland veel meer nodig is. Daarom zijn een aantal additionele aanbevelingen gedaan, die refereren aan bijvoorbeeld een heroverweging van de relevantie van cybersecurity, en de mate van autonomie voor Nederland in het digitale domein.

De eerste set van aanbevelingen rust op het onderzoek en geeft suggesties voor verbetering van de huidige werking van de innovatieketen. Deze aanbevelingen refereren aan beperkte aanpassingen in de huidige beleidsmix, en zijn generiek van aard (ze lijken ook relevant en toepasbaar voor beleid dat andere sectoren adresseert):

1. De cybersecurity-innovatieketen is gebaat bij specifiek (thematisch) beleid dat structurele ondersteuning geeft aan alle actoren die een rol spelen in de bredere cybersecurity-innovatieketen.
2. De continuïteit van het instrumentarium moet worden gewaarborgd. Het instrumentarium moet meer zekerheden bieden door zowel de samenstelling, modaliteiten en regelgeving meerjarig vast te leggen. De instrumenten moeten tevens meerjarig voor inschrijving open blijven (d.w.z. geen ‘calls’ die een beperkte looptijd hebben, en op een specifiek moment sluiten).
3. De overheid zou haar rol als ‘launching customer’ in de innovatieketen moeten intensiveren.[2] De actoren vragen in deze context specifiek om voortzetting en intensivering van de SBIR-regeling voor het cybersecurity-domein.
4. Om de effectiviteit van publieke ondersteuning te vergroten zouden langjarige onderzoeksprogramma’s en bijbehorende projecten een grotere flexibiliteit moeten kennen in het aanvraagproces bij de uitvoering. Dit om de dynamiek in de keten beter te kunnen volgen. Dit impliceert het creëren van mogelijkheden tot kortlopende trajecten, en het tussentijds evalueren en aanpassen van trajecten. Het impliceert daarnaast ook een versimpeling in het proces van aanvragen van ondersteuning, en een verkorting van het proces van evaluatie van projectvoorstellen.
5. De overheid zou de effectiviteit van het instrumentarium kunnen verbeteren door de participatiegraad van met name kleinere ondernemingen, zoals startups, te verhogen. Dat kan bijvoorbeeld door procedures te vereenvoudigen, de bekendheid van ondersteuningsmogelijkheden te vergroten en één loket specifiek voor de cybersecurity-innovatieketen op te zetten.

Het onderzoek maakt verder duidelijk dat innovatie in het cybersecurity-domein wordt gehinderd door een gebrek aan coördinatie: tussen vraag naar en aanbod

[2] Zie (Dialogic, 2017) voor richtlijnen voor de invulling van de overheid als launching customer (www.dialogic.nl).

van kennis; op het gebied van samenwerking bij kennisontwikkeling en innovatie-activiteiten (van laag naar hoog TRL-niveau, en tussen de verschillende actoren in de keten); tussen verschillende micro-ecosystemen die de innovatieketen vormen. Voor een verbetering in de regie en sturing in de keten gelden de volgende aanbevelingen - waarbij alle actoren uit de keten, de overheid en de governance structuur, maar ook niet-traditionele actoren een rol hebben:

6. Voor regie en sturing is het noodzakelijk beter inzicht te hebben in het functioneren van de innovatieketen. Structurele monitoring en evaluatie is daarom vereist. De hier gepresenteerde analyse is een eerste stap in die richting, maar een follow-up is noodzakelijk, met medewerking van additionele actoren zoals het CBS, en additionele methoden om de keten op een objectieve manier te kunnen beschrijven en monitoren.
7. Om de uitwisseling van informatie en kennis binnen de veelzijdige cyberinnovatie-keten te versterken is het aan te bevelen een (virtuele) entiteit in het leven te roepen. Het lijkt het meest effectief om daarbij te bouwen op bestaande publieke en private initiatieven en organisaties en hun bijbehorende kennis, maar met inachtneming van de tekortkomingen van de huidige structuren. Het doel ervan is dat het bestaande initiatieven verbindt en eventuele witte vlekken invult, teneinde kennis, inzicht en overzicht over de gehele kennis- en innovatieketen te bundelen. Deze entiteit ontsluit kennis, helpt partijen bij het koppelen van vraag en aanbod en fungeert tevens als katalysator en aanjager, legt verbindingen tussen partijen en initiatieven en signaleert nieuwe ideeën. Actoren uit de keten - overheden, bedrijven, universiteiten, hogescholen en kennisinstellingen - zullen in een nader uit te denken governance structuur allemaal een rol moeten spelen.
8. Door het delen van dreigingsinformatie met de actoren in de keten kan de ontwikkeling van cybersecurity-innovatie worden gestuurd. Dit geeft richting aan samenwerking voor vormen van dreiging die actoren niet eenvoudig individueel kunnen oplossen. De coördinerende entiteit zoals hierboven benoemd zou hierbij een rol kunnen spelen als een mechanisme om deze informatie op een verantwoorde manier te delen.
9. De huidige beleidsmix moet worden uitgebreid om coördinatie in de innovatieketen te bevorderen. Ook niet-traditionele actoren in de keten zouden ondersteund moeten kunnen worden door de bestaande instrumenten.
10. Het instrumentarium moet daarnaast de toegang van private actoren tot de publieke kennisinfrastructuur verbeteren, ook op de hogere TRL-niveaus. Zo is publieke financiering voor één-op-één samenwerking tussen publieke en private partijen bij onderzoek en innovatie beperkt beschikbaar.

Uit het onderzoek, en dan met name uit de interviews, komt het beeld naar voren dat bovengenoemde aanbevelingen alleen niet voldoende zullen zijn om Nederland cyberveilig te maken. Een aantal meer structurele veranderingen in beleid en de bijbehorende doelstellingen zijn daarvoor noodzakelijk. Aanvullend zijn met de klankbordgroep nog twee aanvullende aanbevelingen geformuleerd die niet direct op het onderzoek rusten, maar op de expert opinion van de leden van de klankbordgroep.

De nu volgende aanbevelingen betreffen uitgangspunten en hebben te maken met (politieke) keuzes over de rol van cyberveiligheid in de Nederlandse samenleving én economie. Hiermee kan onderzoek en innovatie in de gehele keten beter worden gestuurd - iets dat nu ontbreekt volgens de geïnterviewden.

1. De overheid moet haar rol in het cyberveilig maken van de Nederlandse samenleving heroverwegen. De complexiteit van het domein en de daaraan verbonden cybersecurity-uitdagingen is zo groot dat de samenleving deze niet vanzelf kan adresseren. De aanbeveling is daarom, in lijn met onder andere de visie van het World Economic Forum (WEF), cybersecurity te beschouwen als een 'publiek goed'.
2. In het verlengde hiervan moet ook een discussie worden gevoerd over de mate van autonomie die voor Nederland in het digitale domein zeker moet worden gesteld.[3] In lijn met de conclusies van de Wetenschappelijke Raad voor Regeringsbeleid (WRR) is een discussie nodig over welke mate van 'strategische autonomie' wenselijk en haalbaar is (WRR, 2019).

Wanneer er gestreefd wordt naar een structurele verandering van de innovatieketen na dan heeft dat implicaties voor onder andere beleid en financiering. De invulling daarvan gaat voorbij aan deze opdracht.

[3] In deze context wordt ook wel gesproken van 'digitale soevereiniteit'.

Inhoudsopgave

1 Inleiding

Nederland is één van de meest gedigitaliseerde samenlevingen ter wereld (ITU, 2017), (Europese Commissie, 2019). Verdere digitalisering en de opkomst van nieuwe (digitale) technologieën onderstrepen het belang van cybersecurity en cybersecurity-innovatie voor een goed functionerende en een concurrerende economie en voor het vertrouwen in de digitale samenleving.

Nederland heeft het belang van cybersecurity in een vroeg stadium onderkend en was één van de eerste OESO-landen die een cybersecurity-strategie opstelde (de Nationale Cyber Security Strategie 'Slagkracht door samenwerking' (NCTV, 2011))

Het beeld van de omvang en de urgentie van de huidige cybersecurity-problematiek is echter incompleet, versnipperd en onvoldoende gekwantificeerd. Even incompleet is het beeld van de omvang en samenstelling van het Nederlandse cybersecurity-domein in zijn geheel. Aangezien dit een belemmering kan vormen bij het correct definiëren van de cybersecurity-uitdagingen en tot een minder goed presterende innovatieketen kan leiden, is dit aanleiding voor de verdere verkenning van het cybersecurity-innovatielandschap (vraag- en aanbodzijde) in de volgende hoofdstukken. Daarin wordt ingegaan op de verschillende categorieën relevante actoren, hun onderlinge verbanden en verhoudingen, hun belangen en incentives.

1.1 Aanleiding voor het onderzoek

In een brief aan de Tweede Kamer van juni 2018 over kennisontwikkeling schrijft de minister [Grapperhaus] van Justitie en Veiligheid (J&V): "Vanwege het huidige versnipperde landschap van organisaties die zich bezighouden met cybersecurity kennisontwikkeling, wordt vanuit het kabinet een verkenning gestart naar de mogelijkheden voor versterking van de kennis- en innovatieketen voor cybersecurity, de opzet van een Kennis en Innovatie Agenda (KIA) daartoe en hoe een langjarige samenwerking, tussen publieke en private partijen, over de hele kennis- en innovatieketen heen kan worden georganiseerd" (ministerie van J&V, 2018b).

De minister [Wiebes] en staatssecretaris [Keijzer] van Economische Zaken en Klimaat (EZK) schrijven in juli 2018 aan de Tweede Kamer over missiegedreven innovatiebeleid: "In Nederland en overal ter wereld staan we voor enorme maatschappelijke uitdagingen en veranderen zowel nieuwe technologieën als de digitale revolutie ons leven ingrijpend. Dit vergt een nieuwe aanpak die niet de technologie en de gevestigde orde van vandaag als vertrekpunt neemt, maar die nadrukkelijk ook vernieuwers en uitdagers betrekt. De grote baanbrekende innovaties komen vaak niet alleen van de gevestigde partijen; er zijn ook nieuwe partijen nodig die het bestaande ecosysteem versterken" (ministerie van EZK, 2018).

Om tot een nieuwe aanpak te komen, is eerst onderzoek nodig naar de werking van de innovatieketen. Het ministerie van EZK heeft TNO de opdracht gegeven om hier onderzoek naar te doen. Niet voor niets luidt de subtitel 'Als je doet wat je deed, krijg je wat je kreeg'.

1.2 Context van het onderzoek

In de afgelopen drie jaar is er door de departementen, NWO en TNO intensief samengewerkt rond de Maatschappelijke Uitdaging Veilige Samenleving (MU VS) op het thema cybersecurity en door het topteam ICT, NWO en TNO gewerkt aan een MJIP cybersecurity onder de sleuteltechnologieën. Tevens is in het kader van de vernieuwing topsectorenbeleid gestart met een missiegedreven aanpak onder andere op het thema veiligheid.

"Missies en nieuw missiegedreven beleid hebben de potentie om het vinden van oplossingen voor maatschappelijke uitdagingen te versnellen. Een goede invulling draagt bij aan het creëren van maatschappelijk draagvlak en aan het verder versterken van de Nederlandse economie. Zowel in eigen land, als in omringende landen en Brussel wordt gewerkt aan deze nieuwe aanpak. Dit biedt kansen om initiatieven en middelen op elkaar te laten aansluiten en zo synergie te creëren. Veel van de uitdagingen zijn immers grensoverschrijdend en vereisen samenwerking en coördinatie" (Goetheer, 2018). Missiegedreven onderzoeks- en innovatiebeleid draagt bij aan het proces van innoveren, aandacht vragen voor bepaalde maatschappelijke uitdagingen en hier massa voor creëren. Het is belangrijk om de volgende drie factoren helder te krijgen om een maatschappelijke uitdaging aan te gaan en hierop in te zetten: onzekerheid, complexiteit en overeenstemming.

Het stimuleren van 'sleuteltechnologieën' is een belangrijk doel van het topsectoren- en innovatiebeleid voor dit kabinet. Sleuteltechnologieën (key enabling technologies) zijn technologieën die essentieel zijn voor het oplossen van maatschappelijke uitdagingen – die in de missies uitgewerkt zijn - en ook voor het benutten van grote economische kansen. Sleuteltechnologieën zijn dus relevant voor onderzoek en wetenschap, maar óók voor mens en maatschappij, economie en nieuwe markten. Een belangrijk kenmerk van sleuteltechnologieën is hun grote impact en brede bereik: het gaat om technologie die kan worden toegepast in verschillende missies vanuit meerdere sectoren[4].

In 2017 startte een verkenning naar welke sleuteltechnologieën voor Nederland het meest kansrijk zijn. Dit heeft geleid tot een viertal technologieclusters:

- Fotonica en lichttechnologieën (zoals geïntegreerde fotonica)
- Nanotechnologieën (bijvoorbeeld nanomaterialen)
- Quantumtechnologieën (zoals quantum computing)
- Hightech, nader onderverdeeld in vijf categorieën: i) Digitale technologieën (zoals artificial intelligence en security); ii) Geavanceerde materialen (zoals dunne film en coatings); iii) Chemische technologieën (zoals katalytische technologie); iv) Life science-technologieën (zoals industriële biotechnologie); v) Engineering- en fabricagetechnologieën (zoals robotica)

Vanuit het missiegedreven beleid is er een thema veiligheid waarin ook cybersecurity een plek vindt. De KIA Veiligheid beschrijft de ambitie van de betrokken topsectoren om met samenhang een bijdrage te leveren aan essentiële innovaties en valorisatietrajecten voor de missies en daarmee bij te dragen aan het aanpakken van maatschappelijke opgaven op het gebied van Veiligheid als wel het verdienvermogen van Nederland. De kennis- en innovatieagenda is vastgelegd in de vorm van meerjarige missiegedreven innovatieprogramma's (MMIP's) en zijn de basis voor het kennis- en innovatiecontract (KIC) (Holland High Tech, "Samen organiseren, samen innoveren, één doel).[5]

Kader 1: Missies en nieuw missiegedreven beleid

[4] www.pnoconsultants.com
[5] www.hollandhightech.nl

De missiegedreven aanpak op het thema Veiligheid is vastgelegd in een gedragen publiek-private Kennis en Innovatie Agenda (KIA) Veiligheid met een missie Cyberveiligheid. Voor de KIA Veiligheid zijn vijf deelprogramma's voor Cyberveiligheid geïdentificeerd:

- Bestrijden cybercrime;
- Bevorderen ontwikkeling cybercompetenties;
- Defensieve cybertechnologie;
- Offensieve cybertechnologie;
- Ketenweerbaarheid en governance.

Het missiegedreven innovatiebeleid benadrukt de noodzaak tot het gezamenlijk beheren en afstemmen van de agenda's, ook die van de sleuteltechnologieën, zodat kennisontwikkeling en innovatie optimaal bijdraagt aan het oplossen van alle maatschappelijke uitdagingen (Energietransitie en Duurzaamheid, Landbouw, Water en Voedsel, Gezondheid en Zorg en Veiligheid), zoals vastgelegd in de missies.

Naast dit onderzoek loopt op dit moment tevens een aantal aanpalende initiatieven die ook input leveren voor het versterken van de innovatieketen; de kwalitatieve en kwantitatieve analyse van de kennispositie van Nederland door NWO-TNO en CWTS en het ophalen van de aanbodzijde op cybersecurity door Cyberveilig Nederland.

1.3 Doel van het onderzoek

Het ministerie van EZK wil de innovatieketen op het terrein van cybersecurity versterken. Daartoe is het nodig het inzicht te vergroten in de actoren in de keten, de relaties tussen de actoren, de beschikbare financieringsinstrumenten, het functioneren van die keten en de knelpunten waar deze actoren tegenaan lopen. Dit zal gedaan worden door literatuuronderzoek en gesprekken met stakeholders.

Dit onderzoek beschrijft en analyseert de innovatieketen op het terrein van cybersecurity. De bij elkaar gebrachte kennis levert een overzicht en roept tegelijkertijd nieuwe vragen op die om nadere uitwerking en verdieping vragen. In die zin vormt dit onderzoek een inventarisatie en het fundament om de discussie op een hoger niveau te tillen en is als zodanig te beschouwen als een 'nulmeting'.

Dit onderzoek en de vervolgstappen leggen het fundament voor het verder structureren, organiseren en professionaliseren van het cybersecurity-domein. Het uiteindelijke doel is het versterken van de innovatieketen en het organiseren van langjarige samenwerking tussen publieke en private partijen.

1.3.1 Duidelijkheid over cybersecurity

Cybersecurity is een parapluconcept dat meerdere wetenschaps- en technologie-gebieden bestrijkt. Een definitie die voldoende nauwkeurig het onderwerp afbakent is nodig om voor het onderzoek zoektermen te definiëren, relevante documenten te selecteren, data te verzamelen, de actoren in de keten te bepalen, alsmede de financieringsinstrumenten in kaart te brengen. Het komen tot een definitie is dan ook de eerste stap in dit onderzoek.

1.3.2 Afbakening cybersecurity-domein

Het cybersecurity-domein is complex en opgebouwd uit verschillende lagen. Een eenzijdige focus op innovatie op grond van enkele definitie doet geen recht aan de complexiteit van het domein. Door het domein in brede zin te beschrijven kan beter inzichtelijk worden gemaakt wat innovatie op het terrein van cybersecurity allemaal kan omvatten.

1.3.3 Moet de overheid ingrijpen?

Er zijn veel percepties in de buitenwereld over cybersecurity: het cybersecurity-domein is gefragmenteerd, het oude topsectorenbeleid leidt tot weinig (baanbrekende) innovaties, publiek-private samenwerking komt niet of nauwelijks van de grond, het stimuleringsinstrumentarium is onvolledig en kennis blijft op de plank liggen.

Of de overheid moet ingrijpen is de vraag. Eerst is onderzoek nodig naar de werking van de keten; naar het inzichtelijk maken van de knelpunten teneinde hierin verbetering aan te brengen.

1.3.4 Scope van het onderzoek

De scope van het onderzoek is het beschrijven en analyseren van de innovatieketen op het terrein van cybersecurity. Het onderzoek is geen evaluatie van bestaande beleidsinitiatieven. Met de beschrijving en analyse wordt het mogelijk om gericht beleid te ontwikkelen.

De innovatieketen voor cybersecurity wordt beschreven aan de hand van een aantal kernvragen:

- Wie innoveert?
- Op welk gebied?
- Onder welk innovatiemodel?
- Waar op de TRL-schaal?
- Met wie?
- Waarom?

Het gaat om de cybersecurity-innovatieketen van Nederland op dit moment en hoe deze zich in zekere zin verhoudt in haar internationale context.

1.3.5 Klankbordgroep

Gedurende het onderzoek heeft een klankbordgroep discussie gevoerd over de aanpak en de bevindingen, deze waar mogelijk getoetst met de achterban, waardevolle input geleverd en de bevindingen aangescherpt. De klankbordgroep bestond uit de volgende leden:
Jan Piet Barthel (dcypher), Reg Brennenraedts (Dialogic), Danny van Elswijk (CBS), Liesbeth Holterman (Cyberveilig Nederland), Matthijs van der Hulst (ministerie van Defensie), Bastiaan Overvest (CPB), Martin Pekárek en Raymond Doijen (ministerie van J&V).

De in hoofdstuk 10 en 11 beschreven ‘conclusies en aanbevelingen’ zijn door de klankbordgroep onderschreven. De eerste aanbevelingen rusten op het onderzoek en geven suggesties voor de verbetering van de huidige werking van de innovatieketen. Aanvullend zijn met de klankbordgroep aanbevelingen

geformuleerd die niet direct op het onderzoek rusten. Samen met de opdrachtgever zal worden besproken welke vervolgstappen n.a.v. het onderzoek zullen worden gezet.

1.3.6 Methodologie

Omdat dit - voor zover bekend - de eerste poging is geweest om tot een integrale beschrijving van de cybersecurity-innovatieketen te komen is het nodig vooraf een aantal opmerkingen bij de methodologie te maken. De op basis van de methodiek bij elkaar gebrachte kennis levert inzichten in het functioneren van de keten, maar roept ook nieuwe vragen op, die op hun beurt weer vragen om een nadere verdieping en uitwerking.

De analogie die het onderzoeksteam in deze hanteert is de volgende: De cybersecurity-innovatieketen is als een donkere kamer. Die belichten we met verschillende methoden. Er is niet één methode die de hele kamer kan belichten, en de gecombineerde methoden belichten ook niet de gehele kamer. De voor dit onderzoek gehanteerde methodologie is vastgelegd in een apart rapport (TNO, 2019a).

1.4 Leeswijzer

In hoofdstuk 2 wordt het onderzoeksdomein afgebakend door het vaststellen van een definitie, inzicht te verschaffen in het belang van het cybersecurity-domein en de uitdagingen waar Nederland voor staat. In hoofdstuk 3 worden de actoren in Nederland die innoveren op het terrein van cybersecurity beschreven en in hoofdstuk 4 wordt beschreven op welk gebied zij dit doen. In hoofdstuk 5 wordt beschreven welke innovatiemodellen worden gehanteerd. In hoofdstuk 6 wordt, op grond van de TRL-schaal, geanalyseerd waar de primaire actoren in het innovatieproces hun onderzoeks- en innovatieactiviteiten uitvoeren en in hoofdstuk 7 wordt de samenwerking tussen deze actoren beschreven. Hoofdstuk 8 beschrijft de incentives maar ook de barriers voor de primaire actoren in de keten voor het doen van onderzoek en in hoofdstuk 9 staan, op verzoek van het ministerie van EZK, de door de overheid gecreëerde beleidsincentives (beleidsinitiatieven en de bijbehorende set van instrumenten). Hoofdstuk 10 bevat de conclusies van het onderzoek zoals beschreven in de voorgaande hoofdstukken. Als zodanig is dit hoofdstuk te lezen als een uitgebreide samenvatting van het onderzoek. Hoofdstuk 11 bevat de aanbevelingen.

Bij dit rapport hoort ook een aantal ondersteunende documenten. De annexen zijn in een apart document verzameld. Een methodologierapport (TNO, 2019a), de bibliometrische analyse van CWTS (CWTS, 2019), en de GitHub analyse (TNO, 2019b) zijn apart beschikbaar.

2 Scope en context: cybersecurity en de relevantie voor de Nederlandse samenleving

2.1 Inleiding: het cybersecurity domein

Voor het onderzoek is het allereerst noodzakelijk te definiëren wat cybersecurity is. Voor het doen van kwalitatief onderzoek moet worden afgebakend waarnaar gezocht wordt. In dit hoofdstuk wordt daartoe de gehanteerde definitie beschreven. Daarnaast wordt het cybersecurity-domein in brede zin omschreven om de nodige context voor het onderzoek te schetsen.

In dit hoofdstuk wordt verder de context van het probleem geschetst door inzicht te verschaffen in het belang en de omvang van digitalisering in Nederland en de daar uit voortvloeiende relevantie van cybersecurity. Hiertoe wordt verder inzicht verschaft in de dreigingen in het digitale domein, de relevante actoren en hun rationale.

2.2 Definitie cybersecurity

Om de scope van het onderzoek te beschrijven en af te bakenen is het wenselijk een zo specifiek en eensluidende definitie als mogelijk te hanteren. Dit dient als basis voor het verzamelen van gegevens, zowel kwalitatief als kwantitatief.[6]

Voor dit onderzoek wordt voor cybersecurity de definitie gehanteerd van het Centraal Bureau voor de Statistiek (CBS) in de Cybersecuritymonitor van 2018 (CBS, 2018). Het CBS baseert zich op de definitie van het Nationaal Cyber Security Centrum (NCSC) uit 2016 en komt tot het volgende antwoord op de vraag wat cyber secure is:

Cyber secure is (CBS, 2018): *"Het vrij zijn van gevaar of schade veroorzaakt door verstoring of uitval van ICT of door misbruik van ICT. Het gevaar of de schade door misbruik, verstoring of uitval kan bestaan uit beperking van de beschikbaarheid en betrouwbaarheid van de ICT, schending van de vertrouwelijkheid van in ICT opgeslagen informatie of schade aan de integriteit van die informatie."*

"Cyber secure zoals hier gedefinieerd is in feite de ideale situatie. In de CBS Monitor wordt onder cybersecurity verstaan: het streven naar deze ideale situatie. Dit betekent dat cybersecurity alle maatregelen omvat die bijdragen aan het bereiken van de ideale situatie. Cybersecurity – of eigenlijk het ontbreken ervan – omvat echter ook het tekort- schieten van deze maatregelen of het ontbreken van maatregelen. Deze laatste twee situaties kunnen zich manifesteren in de vorm van incidenten."

Kader 2: Wat is cyber secure?

[6] Voor het beschrijven van iedere innovatieketen is het van belang om een goede begrippenlijst uit te werken. Deze taxonomie moet zo goed zijn, dat het de basis kan vormen voor vervolgonderzoeken. In het kader van dit onderzoek is een lijst met zoektermen gemaakt (zie het Methodologie rapport, TNO 2019 R11839), maar dat is nog geen algemeen aanvaarde taxonomie voor dit domein. Er zijn immers meer lijsten in omloop en die hangen heel erg af van de gebruikte definitie op cybersecurity. Cyberveilig Nederland heeft bijvoorbeeld ook een 'woordenlijst' opgesteld. Ook in de EU wordt gewerkt aan een taxonomie (zie (ENISA, 2017)).

Zoals ook het CBS concludeert in (CBS, 2018) is er echter geen eensluidende algemeen geaccepteerde definitie van cybersecurity en aanverwante begrippen. Het betreft hier niet meer dan een algemene definitie en is daardoor meer een containerbegrip dan een voor dit onderzoek werkbare afbakening.

2.3 Het cybersecurity-domein

Het cybersecurity-domein is complex en opgebouwd uit verschillende lagen. Een eenzijdige focus op innovatie op grond van de hierboven gehanteerde definitie doet geen recht aan de complexiteit van het domein, zeker aangezien er nog geen eensluidende definitie wordt gehanteerd. Door het domein in brede zin te beschrijven kan beter inzichtelijk worden gemaakt wat innovatie op het terrein van cybersecurity allemaal kan omvatten.

In de kern gaat het traditioneel vooral om informatiebeveiliging: het waarborgen van de confidentialiteit, integriteit en beschikbaarheid van data. Door het toegenomen belang van het digitale domein gaat cybersecurity echter over veel meer dan alleen de beschikbaarheid, integriteit en vertrouwelijkheid van informatie. Het gaat over de veiligheid van het digitale domein in zijn geheel en daarmee de veiligheid van aan alles wat daarvan afhankelijk is. Het gaat dan ook over sociale, -technologische en bestuurlijke aspecten, zoals maatschappelijke overwegingen en verantwoordelijkheden in ketens. Cybersecurity in brede zin dient daarmee een maatschappelijk belang. Voor de brede benadering van het thema cybersecurity wordt ook de term ‘cyber resilience’ (cyberweerbaarheid) gebruikt (Meulen, 2015).

In brede zin zijn er verschillende niveaus van cybersecurity te benoemen. Van specifieke technische toepassingen om data te beveiligen tot maatregelen die gericht zijn op het beschermen van de fundamentele rechten van burgers in het digitale domein. Globaal kunnen de volgende niveaus worden onderscheiden:

- Waarborgen vertrouwelijkheid, beschikbaarheid integriteit van netwerken en systemen;
- Waarborgen vertrouwelijkheid, beschikbaarheid integriteit van informatie;
- Waarborgen van vertrouwelijkheid, beschikbaarheid integriteit van diensten, producten en processen;
- Waarborgen economische en bestuurlijke processen;
- Waarborgen van veiligheid en integriteit van de samenleving;
- Waarborgen van waarden en grondrechten.

Deze gelaagdheid komt ook terug in het Nederlandse beleid. Het brede strategische doel is het veiliger maken van de digitale samenleving. In de Nederlandse Cybersecurity Agenda (NCSA), Nederland Digitaal Veilig (NCTV, 2018a) staat de definitie van cybersecurity zoals we die kennen van het NCSC, maar wordt ook geduid hoe breed die definitie moet worden geïnterpreteerd: “Nederland is een van de meest gedigitaliseerde landen ter wereld. We beschikken daarmee over uitstekende voorwaarden om internationaal koploper te zijn, in het veilig en in vrijheid snel nieuwe technologieën uitrollen en gebruiken. Die nieuwe technologieën spelen een steeds belangrijkere rol in ons dagelijks leven. Denk bijvoorbeeld aan *e-commerce*, maar ook aan digitale communicatie met de dokter, de school en de overheid. Verdergaande digitalisering in de zorg (*e-health*),

mobiliteit (*e-automotive*) en toename van gebruiksvoorwerpen met een internetverbinding (*Internet of Things*), zorgen er bovendien voor dat het cyberdomein en het fysieke domein meer met elkaar vervlochten raken. Deze ontwikkelingen brengen ook ethische kwesties aan het licht ten aanzien van privacy en omgang met data. Het beschermen van waarden en grondrechten in het digitale domein is eveneens een belangrijk onderdeel van cybersecurity. Burgers moeten erop kunnen rekenen dat hun grondrechten zowel online als offline gewaarborgd zijn en dat hun privacy ook in het digitale domein gegarandeerd is."

Het perspectief van de overheid is breed, omdat het de enige manier is om de ambitie waar te maken. Het ministerie van EZK stelt als ambitie dat (ministerie van EZK, 2019a): "Nederland in staat [is] om op een veilige wijze de economische en maatschappelijke kansen van digitalisering te verzilveren. Door in te zetten op het ontwikkelen van cybersecurity kennis en innovatie streeft Nederland ernaar om binnen vijf jaar in de top 10 van zowel de Global Cybersecurity Index (GCI) als de National Cyber Security Index (NCSI) te staan.

2.4 Context van het probleem

In deze paragraaf wordt kort uiteengezet wat het belang van cybersecurity is voor de samenleving, welke dreigingen er zijn en hoe deze wordt gepercipieerd. In het Cybersecurity Beeld Nederland van 2019 onderstreept de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) dat onze samenleving vrijwel volledig afhankelijk is geworden van gedigitaliseerde processen en systemen en dat de dreiging van criminelen en statelijke actoren in het digitale domein onverminderd groot blijft (NCTV, 2019). Dat maakt het versterken van de digitale veiligheid en weerbaarheid essentieel om maatschappelijke ontwrichting te voorkomen (NCTV, 2019). Dit wordt benadrukt door de perceptie van de burger over de dreiging die het digitale domein met zich meebrengt.

Het effectief kunnen waarborgen van de veiligheid, betrouwbaarheid en beschikbaarheid van digitale netwerken en systemen, hardware en software is daarom van groot belang. In deze paragraaf wordt als laatste kort ingegaan op de grootste uitdagingen van digitalisering voor de samenleving.

2.4.1 Omvang digitalisering in Nederland

Nederland is een van de koplopers op het gebied van digitale connectiviteit, internet gebruik, digitale publieke en commerciële dienstverlening en bedrijfsdigitalisering. In 2017 stond Nederland op de zevende plek in de Global ICT Development Index (2017) van de ITU (ITU, 2017), en in 2018 op de vierde plek in de Europese 'Digital Economy and Society Index (DESI)' (Europese Commissie, 2019). Het internet is daarmee onderdeel van het dagelijkse leven van 95% van alle Nederlanders.

Aan de digitalisering wordt circa 25% van de economische groei de afgelopen jaren in Nederland toegeschreven, net als een constante stijging van het aantal (nieuwe) ICT-banen en het creëren van nieuwe kansen en mogelijkheden voor (technologische) innovatie (Ministerie van EZK, 2019b). Naar verwachting zal de digitalisering van Nederland voortzetten door de opkomst van onder andere het

'Internet of Things' (IoT), de introductie van 5G en de groeiende adoptie van 'cloud computing' diensten (ENISA, 2018b).[7]

2.4.2 Dreigingen

De digitale dreiging is veelzijdig. In het CSBN van 2019 worden de volgende dreigingen onderkend (NCTV, 2019):

- Verstoring: het opzettelijk tijdelijk aantasten van de beschikbaarheid van informatie, informatiesystemen of -diensten.
- Sabotage: het opzettelijk en zeer langdurig aantasten van de beschikbaarheid van informatie, informatiesystemen of -diensten, mogelijk leidend tot vernietiging.
- Informatiemanipulatie: aantasting van de integriteit van informatie door het opzettelijk wijzigen van informatie.
- Informatiediefstal: aantasting van de vertrouwelijkheid van informatie door het kopiëren of wegnemen van informatie.
- Spionage: aantasting van de vertrouwelijkheid van informatie door het kopiëren of wegnemen van informatie door statelijke of aan staten gelieerde actoren.
- Systeemmanipulatie: aantasting van informatiesystemen of -diensten; gericht op de vertrouwelijkheid of integriteit van informatiesystemen of -diensten. Deze systemen of diensten worden daarna ingezet om andere aanvallen uit te voeren.
- Storing/uitval: aantasting van de integriteit of beschikbaarheid als gevolg van natuurlijk, technisch of menselijk falen.
- Lek: aantasting van de vertrouwelijkheid als gevolg van natuurlijk, technisch of menselijk falen.

De dreigingsmatrix in het CSBN geeft inzicht in de dreiging die uitgaat van diverse actoren tegen doelgroepen in de samenleving.

[7] Dit rapport schetst een toekomstscenario voor 2025 waarin er wereldwijd 80 miljard 'devices' - ruim 10 per persoon - via het internet met elkaar verbonden zullen zijn.

	Overheid	Vitaal	Privaat	Burgers
Staten/ staatsgelieerd	Spionage Informatiemanipulatie	Sabotage Verstoring Spionage	Spionage Systeemmanipulatie	Spionage
Criminelen	Verstoring Systeemmanipulatie Informatiediefstal	Verstoring Systeemmanipulatie	Verstoring Informatiemanipulatie Informatiediefstal Systeemmanipulatie	Verstoring Informatiemanipulatie Informatiediefstal Systeemmanipulatie
Terroristen	Sabotage	Sabotage		
Hacktivisten	Verstoring	Verstoring	Verstoring Informatiemanipulatie	
Cybervandalen en scriptkiddies	Verstoring	Verstoring	Verstoring	
Insiders	Informatiediefstal		Informatiediefstal	
Niet opzettelijk handelen	Storing/uitval Lek	Storing/uitval Lek	Storing/uitval Lek	Lek

De dreigingsmatrix geeft inzicht in de dreigingen die uitgaan van verschillende actoren tegen verschillende doelwitten. De tabel is niet uitputtend en bevat niet alle dreigingen die voorstelbaar zijn, maar beperkt zich tot de dreigingen waarvan ingeschat wordt dat actoren voldoende intentie en capaciteit hebben of tot actoren van wie eerder activiteiten zijn waargenomen.

Legenda:

Geel:	Er is intentie maar geen middelen/ kennis (capaciteit) OF er is activiteit waargenomen maar middelen/ kennis zijn beperkt OF er is activiteit waargenomen maar alleen intentie specifieke doelwitten te raken
Oranje:	Middelen/ kennis zijn aanwezig en intentie is sterk aanwezig OF intentie is sterk aanwezig en activiteiten zijn waargenomen
Rood:	Er zijn veel middelen/ kennis en intentie is zeer sterk aanwezig OF intentie is zeer sterk aanwezig, er is veel activiteit waargenomen en er zijn (veel) middelen/ kennis

Figuur 1. Dreigingsmatrix. Bron: CSBN 2019 (NCTV, 2019).

Voor het tegengaan van de dreigingen in het digitale domein is het ook noodzakelijk zicht te hebben op de verschillende actoren en hun motieven. De NCTV noemt in het CSBN 2019 een groot aantal daders. Hierbij wordt geconstateerd dat grootste dreiging uitgaat van staten en aan staten gelieerde actoren. Verder worden criminelen, terroristen, hacktivisten, cybervandalen, scriptkiddies en insiders genoemd. Tevens gaat er dreiging uit van het niet opzettelijk handelen door gebruikers van digitale systemen.

In het CSBN van 2018 wordt eerder geconstateerd dat (NCTV, 2018b): “[ongeacht] het motief - persoonlijk, economisch, ideologisch of geopolitiek - een cyberaanval al jaren een profijtelijk middel [is] voor de realisatie van uiteenlopende doelen van actoren. […] Vele soorten digitale aanvallen zijn laagdrempelig uit te voeren als gevolg van de hieronder beschreven fundamentele oorzaken. Daardoor hoeft een aanvaller zelf lang niet altijd over veel capaciteiten te beschikken voor een aanval. Zelfs actoren die daarover wel beschikken, kunnen vaak al volstaan met eenvoudige aanvalsvormen.”

2.4.3 Perceptie burger

Van groot belang is de vraag hoe individuele burgers veiligheid ervaren en hoe de opkomst van grootschalige digitalisering (technologie) dit beïnvloedt. Uit een Europese survey blijkt een hoog aantal Nederlandse burgers bezorgd te zijn over o.a. cybercrime (84%) en de veiligheid van hun gegevens (Europese Commissie, 2018).

Er is echter nog onvoldoende data beschikbaar om te kunnen vaststellen of deze perceptie van de Nederlandse burger gefundeerd is. De bereidheid van niet alleen burgers maar ook van bedrijven om melding te maken of aangifte te doen van verschillende vormen van cybercrime, computervredebreuk, datalekken blijft relatief laag (ruim een kwart, volgens de Cybersecuritymonitor 2018 van het CBS). Volgens het CBS kan de vrees voor imagoschade voor bedrijven hiervoor een belemmering zijn. En volgens een EU-survey weet 78% van de Nederlanders niet waar melding of aangifte van cybermisdrijven gedaan kan worden (Europese Commissie, 2018).

Uit de Cybersecuritymonitor blijkt tevens dat 8,5% van de Nederlandse internetgebruikers van 12 jaar of ouder (ruim 1,2 miljoen mensen) in de voorgaande twaalf maanden slachtoffer is geweest van digitale criminaliteit. De uitkomsten van de Eurobarometer survey onder de Nederlanders onderschrijven dit beeld (Europese Commissie, 2018).

Naast deze cijfers over cybercrime bevat ook de voortgangsrapportage over de NCSA-cijfers over deze problematiek. Uit dat rapport blijkt bijvoorbeeld dat in 2018 het NCSC 2400 incidenten afgehandeld had (geautomatiseerde meldingen niet inbegrepen) (Ministerie van J&V, 2018b).

2.4.4 Uitdagingen

De huidige literatuur en beleidsdocumenten wijst op een aantal al aanwezige uitdagingen die uit digitalisering voortvloeien en die een grote impact op alle (vitale en niet vitale) sectoren kunnen hebben. Deze uitdagingen zijn onder andere:

- De toenemende hoeveelheid aan én beschikbaarheid van data in digitale vorm en het gebruik daarvan;
- De uitdagingen die geassocieerd zijn met het opslaan en het verwerken van data in de cloud;
- De uitdagingen die voortvloeien uit de toenemende real-time en geautomatiseerde verwerking van data;
- De toenemende complexiteit en de grote wederzijdse afhankelijkheid van (digitale)systemen en actoren;
- De almaar groeiende wederzijdse afhankelijkheid tussen cyber- en fysieke systemen (bijvoorbeeld door de opkomst van het internet der dingen);
- De steeds grotere complexiteit van leveranciersketens;
- De uitdagingen die geassocieerd worden met het beveiligen van ‘legacy’ systemen;
- Het gebrek aan interoperabele cybersecurityoplossingen;
- De beperkte bereidheid van bedrijven om in hun (cyber)security te investeren;
- De steeds grote behoefte aan gekwalificeerde cybersecurity experts en beperkte uitstroom uit het onderwijs of bijscholings-mogelijkheden;
- Het relatief beperkte cyberbewustzijn en -kennis van burgers/consumenten;
- De bekende en onbekende gevolgen van opkomende (digitale) technologieën, zoals ‘quantum computing’;
- De toegenomen verwevenheid van de civiele en militaire digitale domeinen;
- Het spanningsveld dat kan ontstaan tussen verschillende fundamentele rechten en waarden (bijvoorbeeld tussen het recht op veiligheid en het recht op privacy);
- De complexiteit en multi-stakeholder benadering van governance in het cyberdomein;

- Het grensoverschrijdend karakter van cybersecurity die om samenwerking in EU- en breder internationaal verband vraagt;
- De aanwezigheid van systemische cybersecurity risico's.

3 Wie innoveert: actoren in het cybersecurity-domein

3.1 Inleiding

Dit hoofdstuk schetst een beeld van de verschillende actoren in Nederland die een rol hebben in de cybersecurity-innovatieketen. Daarbij wordt onderscheid gemaakt tussen 'primaire actoren' (actoren die onderzoek en innovatie uitvoeren) en 'secundaire actoren' (actoren die een rol hebben in de governance van de innovatieketen en het onderzoek en innovatie bijvoorbeeld sturen, ondersteunen of initiëren). Deze laatste groep van secundaire actoren is niet volledig beschreven in dit hoofdstuk: die actoren die een rol hebben in het ondersteunen van samenwerking tussen de primaire actoren worden beschreven in hoofdstuk 7 getiteld 'Met wie: samenwerking in de innovatieketen'.

De resultaten in dit hoofdstuk leunen sterk op de informatie verkregen uit de analyse van de bestaande literatuur en beschikbare rapporten die de keten beschrijven. Met behulp van de interviews, input van de klankbordgroep en verschillende meer kwantitatieve onderzoeksmethoden is getracht de relevantie van de actoren nader te duiden.

3.2 Primaire actoren

3.2.1 (Technische) Universiteiten en fundamentele onderzoeksinstellingen

Bijna alle academische instellingen in Nederland zijn op grotere of kleinere schaal betrokken bij onderzoek naar technische en (in mindere mate) sociaalwetenschappelijke (cyber)security onderwerpen. Dit onderzoek gebeurt soms binnen bestaande onderzoeksgroepen, en soms binnen speciaal opgerichte onderzoeksgroepen, kenniscentra, en samenwerkingsverbanden. Daaronder vallen, bijvoorbeeld, het Centrum Wiskunde & Informatica, de Technische Universiteit Eindhoven, de Technische Universiteit Delft, Universiteit van Amsterdam, Radboud Universiteit Nijmegen, Rijksuniversiteit Groningen, Tilburg University, Universiteit Leiden (de Cyber Security Academie), Universiteit Twente, de Vrije Universiteit, NSCR,[8] en de Erasmus Universiteit Rotterdam.[9]

De Nederlandse (technische) universiteiten en fundamentele onderzoeksinstellingen hebben een lange traditie op het gebied van (cyber)security-onderzoek. Internationaal behoort Nederland tot de landen met de grootste bijdrage aan het aantal wetenschappelijke publicaties op het gebied van cybersecurity (CWTS, 2019). Uit de citatieanalyse blijkt dat de technische

[8] Het Nederlands Studiecentrum Criminaliteit en Rechtshandhaving (NSCR) is het nationale instituut voor fundamenteel wetenschappelijk onderzoek naar criminaliteit en rechtshandhaving. Het NSCR is onderdeel van de institutenorganisatie van de Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO) en werkt samen met de Vrije Universiteit Amsterdam (VU) en het Amsterdam Law and Behavior Institute (A-LAB). Zie www.nscr.nl.

[9] Volgens een recente inventarisatie, i.o.v. dcypher, (zie verder) worden er in Nederland "twintig cybersecurity-opleidingen aangeboden door achttien onderwijsinstellingen. Vijftien hiervan zijn voltijd (vijf master, tien bachelor) en vijf deeltijd (drie master, twee bachelor). Drie van de vijf voltijd masteropleidingen zijn tweejarig (120 ECTS) en twee zijn éénjarig (60 ECTS). Bacheloropleidingen worden grotendeels door hogescholen aangeboden (11 van de 12). Bron: www.dcypher.nl.

universiteiten Delft, Eindhoven en Twente de meeste wetenschappelijke publicaties op hun naam hebben staan.

Uit een voorlopige en meer beperkte analyse van de Nederlandse deelname aan onderzoek binnen het EU-kaderprogramma tussen 2000 en 2019, komen dezelfde technische universiteiten vaker naar voren - Eindhoven, Delft en Twente - evenals de stichting VU en de Universiteit van Amsterdam.

Op basis van een aantal wetenschappelijke publicaties waaraan over de periode 2005–2017 door medewerkers van Nederlandse actoren is meegewerkt, komt Nederland direct na de grotere EU-landen (het Verenigd Koninkrijk, Duitsland, Frankrijk en Spanje) en duidelijk vóór de andere lidstaten. Het Verenigd Koninkrijk is het EU-land met de meeste publicaties op haar naam. Wanneer naar uitvindingen wordt gekeken zijn de verschillen tussen de EU-lidstaten kleiner en komt Nederland op een zesde positie na Frankrijk, Duitsland, het Verenigd Koninkrijk, Zweden en Finland. Wanneer naar het aantal artikelen in wetenschappelijke tijdschriften en in conferentiebijdragen uit de periode 2005–2017 wordt gekeken dan blijkt het aantal artikelen waaraan auteurs uit China hebben bijgedragen vergelijkbaar is met het aantal artikelen waaraan auteurs afkomstig uit de EU28 landen hebben bijgedragen. Het aantal artikelen in wetenschappelijke tijdschriften afkomstig uit China vertoont evenwel sinds 2008 een sterke groei,[10] terwijl de groei van de EU28 veel gematigder is. Het gevolg is dat het aandeel van China op jaarbasis inmiddels dat van de EU28 is gepasseerd.

Het aantal wetenschappelijke publicaties waarbij auteurs van Nederlandse actoren betrokken zijn vertoont een enigszins sterkere groei dan het wereldtotaal van wetenschappelijke publicaties. Tot 2013 was de groei van het aantal Nederlandse wetenschappelijke artikelen vergelijkbaar met die van de EU28, maar lijkt sinds 2014 af te remmen. Voor de VS geldt dat het aantal wetenschappelijke publicaties langzamer groeit dan dat van China en ook dan dat van de EU28. Het aandeel van de VS in het totale aantal wetenschappelijke publicaties op het gebied van de cybersecurity vertoont sinds 2005 een dalende tendens waardoor haar aandeel inmiddels achterblijft bij dat van zowel China als de EU28.

Kader 3: Omvang aantal wetenschappelijke publicaties van Nederlandse actoren. Bron: (CWTS, 2019).

3.2.2 Hogescholen

Innovatieve concurrentiekracht vraagt om investering in voortgezet onderwijs: van een betere aansluiting tussen mbo, hbo en universiteiten tot de bouw van testfaciliteiten tot investering in kansrijke kennisgebieden (OCW, 2019). Enkele hogescholen hebben cybersecurity onderzoeksgroepen en kenniscentra ingericht, zoals het Centre of Expertise Cyber Security aan The Hague University of Applied Sciences: de Cybersafety Research Group aan NHL Stenden University of Applied Sciences in Leeuwarden; Security Management aan Saxion University of Applied Science; het cybersecurity-lectoraat van Kokkeler van Avans; onderzoeksactiviteiten aan de Hogeschool Rotterdam, Fontys, Hogeschool Utrecht en Hogeschool van Amsterdam. Bij hogescholen ligt het accent meer op onderwijs, maar het praktijkgerichte onderzoek is in opkomst. Het onderzoek heeft geeft informatie opgeleverd die de rol en relevantie van onderzoek en innovatie door hogescholen nader kan duiden.

[10] Een mogelijke (gedeeltelijke) verklaring voor deze groei is dat Chinese onderzoekers meer in het Engelstalige tijdschriften, die de belangrijkste basis vormen van de gebruikte literatuur databases, zijn gaan publiceren.

3.2.3 *Instellingen voor toegepast onderzoek (TO2-instellingen)*

In het Nederlandse innovatielandschap instellingen spelen de instellingen voor toegepast onderzoek een belangrijke rol in de ontwikkeling, verspreiding en benutting van kennis. Daartoe werken zij samen met bedrijven, overheden en andere kennisinstellingen, onder meer via publiek-private samenwerking. Uit de kennisinstellingen voor toegepast onderzoek (verenigd in de TO2-federatie) is met name TNO actief op het gebied van cybersecurity, naast in een beperkte mate National Aerospace Laboratory (NLR).

Uit de patenten- en citatiesanalyse (CWTS, 2019) blijkt dat van de bovengenoemde publieke kennisinstellingen in Nederland, alleen TNO actief is op zowel het gebied van wetenschappelijk onderzoek (resulterend in publicaties in wetenschappelijke tijdschriften en conferentieartikelen) als op het gebied van innovatie en technologische ontwikkeling (resulterend in patentaanvragen). Ook uit de voorlopige analyse van de Nederlandse deelname aan onderzoek binnen het EU-kaderprogramma tussen 2000 en 2019 blijkt dat TNO bij relatief veel internationale projecten betrokken is. Daarnaast komt ook de Stichting IMEC Nederland relatief vaak voor.

3.2.4 *Industrie*

In Nederland zijn relatief veel bedrijven actief op het gebied van ICT en digitale beveiliging. Dit betreft zogenaamde ‘pure players’ - bedrijven die alleen cybersecurity gerelateerde activiteiten uitvoeren - als ook ‘partial players’ - actoren voor wie cybersecurity niet tot de ‘core’ van hun activiteiten behoort, zoals bijvoorbeeld banken.[11]

Een verkenning uitgevoerd door VKA en SEO Economisch Onderzoek (Hendriks et al, 2016) suggereert dat de omzet van de Nederlandse cybersecurity-sector in 2014 tussen de € 6,9 en € 7,5 miljard lag. De bijdrage van de sector aan het Nederlandse bbp bedroeg ongeveer 0,6%. De verwachte jaarlijkse groei van omzet uit cybersecurity-activiteiten werd geschat op ongeveer 7%. Omdat het onderzoek zicht beperkte tot cybersecurity-gerelateerde activiteiten binnen de ICT-sector zijn de cijfers volgens de auteurs een onderschatting van de werkelijke totale omvang. Desalniettemin concludeert het rapport dat de sector “een behoorlijke omvang heeft en bovendien snelgroeiend is.”

Data van StartupDelta geeft een indicatie voor het aantal kleine en middelgrote commerciële ‘pure players’ in de cybersecurity-domein (aanbieders van uitsluitend

[11] Voorbeelden van pure players als ook partial players waarvoor cybersecurity een essentieel element is van hun economische activiteiten zijn Nederlandse bedrijven zoals KPN en XS4ALL (nu onderdeel van KPN), maar ook andere bedrijven zoals NEDAP, Irdeto en Fox-it (nu onderdeel van de Britse NCC-groep). Daarnaast zijn een aantal grote internationale-bedrijven in Nederland gevestigd die cybersecurity-expertise aanbieden, zoals Thales, Siemens en Capgemini. Andere relevante bedrijven zijn ASML (halfgeleiders) en Prodrive Technologies (embedded computing systems), Neways (halfgeleiders, advanced electronic applications).
Relevant om te noemen in deze context zijn Individuele verzekeraars. In Nederland richten deze zich al sinds 2011 op de cybersecurity-markt. Deze is nog relatief kleinschalig. Individuele verzekeraars (zoals NN) en de branche doen zelf ook onderzoek naar cybersecurity en gerelateerde diensten. Het Centrum voor Verzekeringsstatistiek (CVS) schat dat het totale premievolume van cyberverzekeringen in 2015 slechts 10 miljoen euro bedroeg, tegen 2,3 miljard dollar in de Verenigde Staten (zie www.verzekeraars.nl).

cybersecurity-producten en -diensten). Het aantal startups en scale-ups in juli 2019 werd ingeschat op 140 - 220 ondernemingen in de subcategorieën public security, cloud & infrastructure, device security & antivirus, data protection; en identity & access. Tussen een derde en de helft van deze ondernemingen is in de afgelopen 5 jaar (sinds 2014) opgericht. StartupDelta identificeert daarnaast ook een 30-tal 'corporates'.[12] Tabel 1 geeft een overzicht van de geografische concentratie van de geïdentificeerde ondernemingen.

In een recent rapport van Cyberveilig Nederland (zie volgende paragraaf), worden vergelijkbare cijfers genoemd (Oldengarm & Holterman, 2019). De inschatting van Cyberveilig Nederland is dat de sector uit ongeveer 250 bedrijven bestaat. "Het betreft dan zowel bedrijven die zich 100% op cybersecurity richten als bedrijven die cybersecurity-producten en -diensten als onderdeel leveren van een breder portfolio". Volgens deze analyse bestaat de sector uit voornamelijk (kleine) MKB-bedrijven, met daarnaast relatief veel zelfstandig ondernemers.

De nadruk ligt voor de sector vooral op groei, en niet specifiek op innovatie.

	startups / scale-ups	corporates
Groningen	5	1
Friesland	1	
Drenthe	2	
Overijssel	9	
Gelderland	7	1
Utrecht	58	7
Flevoland	5	
Noord-Holland	64	16
Zuid-Holland	63	5
Zeeland		
Noord-Brabant	23	1
Limburg	3	

Tabel 1: Cyber security startups / scale-ups en corporates in Nederland. Bron: StartupDelta (juli 2019).[13]

De laatste jaren zijn verschillende cybersecurity-bedrijven overgenomen door buitenlandse bedrijven en dat heeft mogelijk een negatieve impact. De geïnterviewden stellen dat zij graag zien dat de afhankelijkheid van het buitenland kleiner wordt en er meer innovatie in Nederland blijft. Annex 1 geeft een overzicht van recente fusies en overnamen relevant voor de Nederlandse cybersecurity-innovatieketen.

[12] De lijst met startups en scale-ups betreft een mix van kleine en grote Nederlandse ondernemingen, ondernemingen die inmiddels door andere Nederlandse of buitenlandse bedrijven overgenomen zijn en ondernemingen waarin andere Nederlandse of buitenlandse investeerders een meerderheidsbelang hebben gekregen. De informatie over cybersecurity corporates blijkt - met 30 bedrijven - incompleet te zijn. In het overzicht worden naast Nederlandse bedrijven ook internationale bedrijven meegenomen met een Nederlandse participatie, internationale bedrijven die in Nederland geregistreerd zijn maar verder geen (onderzoeks- of innovatie-) activiteiten hebben en Nederlandse bedrijven die inmiddels door internationale bedrijven of investeringsfondsen overgenomen zijn.

[13] www.startupdelta.org

Het totale aantal voor deze studie relevante uitvindingen vertoont over de periode 2005–2017 een groei, maar laat een duidelijke negatieve afwijking van de opwaartse trend zien voor de periode 2007–2010. Deze tijdelijke terugval manifesteert zich met name ook in het aantal uitvindingen afkomstig uit de VS. Wanneer naar het aantal uitvindingen over de gehele periode wordt gekeken dan valt op dat het aantal uitvindingen afkomstig uit de VS groeit en dat de afstand van de VS tot China en de EU28 toeneemt. De EU28 en China zijn inmiddels naar elkaar toegegroeid dankzij een nagenoeg constant aantal uitvindingen uit de EU28 en een groeiend aantal afkomstig uit China. De bijdrage van China is sterk toegenomen in de periode 2005–2014, maar deze groei wekt de indruk dat zij voor de meest recente jaren afzwakt. Voor de EU28 geldt dat het aantal uitvindingen over de gehele periode nagenoeg constant is gebleven en ook Nederland heeft een vergelijkbaar nagenoeg constant aantal uitvindingen. 16 Nederlandse bedrijven en één kennisinstelling (TNO) hebben patenten op hun naam staan.

Kader 4: Omvang aantal uitvindingen van Nederlandse actoren. Bron: (CWTS, 2019).

Het is niet eenvoudig de omvang van onderzoek en innovatie door de cybersecurity-industrie in Nederland te duiden. Gegevens over bijvoorbeeld R&D uitgaven specifiek aan R&D ontbreken.[14] Om het innovatiegehalte van deze cybersecurity-bedrijven te beoordelen is een aantal (alternatieve) proxies gebruikt voor deze studie:[15]

a. Een eerste proxy is het aantal uitvindingen op het gebied van cybersecurity. Uit de patentenanalyse over de periode 2005-2014 (CWTS, 2019) zijn er 17 bedrijven met een (gedeeltelijk) domicilie in Nederland geïdentificeerd die uitvindingen op het gebied van cybersecurity op hun naam hebben staan (zie Kader 4). Wanneer wordt gekeken naar het aantal partners waarmee gezamenlijk uitvindingen worden gedaan zijn Philips en NXP duidelijk de Nederlandse ‘spinnen in het web’.
b. Een tweede proxy is de deelname aan internationale onderzoeks- en innovatieprogramma's. In de gedeeltelijke analyse van de Nederlandse deelname aan cybersecurity-onderzoek binnen het EU-kaderprogramma tussen 2000 en 2019, komen weer bedrijven zoals Philips en NXP naar voren, net als Forescout Technologies B.V. en Technolution (zie Annex 2 - Annex 4).
c. Een derde proxy zijn innovatieprijzen. Als voorbeeld om deze methode te illustreren is de KvK Innovatietop 100 genomen: een prijs voor innoverende MKB-bedrijven die uitgereikt wordt. De innovaties worden door deskundigen beoordeeld en er is geen (prijs)geld aan de KVK Innovatie Top 100 verbonden.

[14] Het Technisch Weekblad publiceer jaarlijks een overzicht van R&D-uitgaven en R&D personeel van de grootste R&D performers in Nederland. De informatie is samengesteld op basis van de gegevens die bedrijven zelf opsturen. Om een beeld te schetsen van onderzoek en innovatie in de cybersecurity sector worden ter illustratie de uitgaven aan R&D, en ingezet R&D personeel voor enkele voor dit onderzoek relevante bedrijven weergegeven uit de TW lijst: voor het jaar 2018: 1 ASML 1.078 mil, 6.610 fte; 3 KPN 365 mil, 1.350 fte; 5 NXP Semiconductors 213mil, 1.043 fte; 8 Thales Nederland 136 mil., 811 fte; 19 Nedap NV 26 mil, 265 fte; 24 Technolution BV 17,1 mil, 93 fte; 28 ASM International NV 13,3 mil, 36 fte; 29 Neways Electronics 12,6 mil, 149 fte.

[15] De eerste twee proxies refereren aan kennis die wordt gegenereerd en toegepast binnen een ‘ traditioneel innovatiemodel’, zie hoofdstuk 5. Het innovatiemodel voor de derde proxy is niet nader te duiden op basis van de onderliggende informatie.

Annex 5 geeft een overzicht van geselecteerde bedrijven in de periode 2015-2019, hun technologie(en) en andere relevante informatie.[16]

Bijzonder aan het cybersecurity-domein is dat ook individuen zich organiseren in samenwerkingsverbanden als open softwareontwikkeling 'communities' of de 'ethical hacker community' om daarmee een belangrijke bijdrage te leveren aan innovatie in de keten. Ethische hackers (oftewel white hat hackers) zijn security-onderzoekers en -experts die een belangrijke rol vervullen bij het ontdekken van kwetsbaarheden in software, hardware en digitale systemen.[17] Ethische hackers in Nederland kunnen gebruik maken van een wereldwijd netwerk met fysieke ontmoetingsplekken waar geëxperimenteerd en kennis gedeeld wordt.[18] Daarnaast kunnen ze, individueel of via cybersecurity crowdsourcing platforms zoals Zerocopter of HackerOne, door organisaties voor bug bounties, penetration testing en hackatons ingezet worden. Het Coordinated Vulnerability Disclosure leidraad (NCSC, 2018) schept het kader voor het verantwoord delen van informatie over ontdekte kwetsbaarheden.

Kader 5: Niet-traditionele actoren betrokken bij onderzoek en innovatie.

3.3 Secundaire actoren

In deze paragraaf worden 'secundaire actoren' beschreven, die een rol hebben in de governance van de innovatieketen en het onderzoek en innovatie bijvoorbeeld sturen, ondersteunen of initiëren.[19]

3.3.1 Overheid – nationaal, regionaal en lokaal

Naast de eerdergenoemde kennis actoren zijn met name overheidspartijen, zowel op nationaal, regionaal en lokaal als op internationaal niveau, bepalend in het innovatieproces van cybersecurity in Nederland.

Deze actoren zijn belangrijk om de strategie (mede) te bepalen, kennis te helpen ontwikkelen, toekomstanalyses te doen, vroegtijdige R&D te voeden, initiatieven en activiteiten te stimuleren, of kaders en regels te zetten. Incidenteel doet deze categorie actoren mee als partner in (internationale) onderzoeks- en innovatietrajecten.

Op nationaal niveau zijn in deze context het meest relevant: het ministerie van J&V (waaronder het WODC, Politie, OM, FIOD, NFI, NCTV, NCSC, de Cyber Security

[16] Voor al deze bedrijven geldt dat het onderzoek heeft plaatsgevonden op TRL9 (zie hoofdstuk 6), en hun innovaties vallen meestal in de categorie sustaining (zie hoofdstuk 4). Deze methodologie om het innovatiegehalte van bedrijven te beoordelen heeft nader onderzoek nodig.
[17] De betekenis van het woord hacker heeft in de loop der tijd een verandering meegemaakt. Tegenwoordig heeft het woord vooral negatieve connotaties, maar dat is niet altijd het geval geweest. Volgens een van de eerste internet security glossaries was de oorspronkelijke betekenis van het woord "someone who figures things out and makes something cool happen" of later "Someone with a strong interest in computers, who enjoys learning about them, programming them, and experimenting and otherwise working with them". https://tools.ietf.org/html/rfc4949
[18] Voor vestigingen in Nederland, zie www.tkkrlab.nl.
[19] Het overzicht refereert aan Nederlandse secundaire actoren, maar ook op internationaal niveau zijn er relevante organisaties. Voorbeelden zijn: de Europese Commissie, ENISA, de Joint Research Centres (m.n. Ispra & Seville), ECSO, EOS, Europol, Eurojust, de European Central Bank, INTERPOL (IGCI), NAVO, GFCE, European Institute for Statistics & Probability Or Stochastic Operations Research And Their Applications (EURANDOM) en het European Space Research & Technology Centre (ESA).

Raad), het ministerie van BZK (waaronder de AIVD), het ministerie van EZK (waaronder het DTC en RVO), het ministerie van OCW, het ministerie van Defensie (waaronder DCC, MIVD, KIXS, JIVC), het ministerie van Buitenlandse Zaken (BuZa), en het ministerie van Infrastructuur en Waterstaat (IenW) (waaronder RWS).

De meest relevante beleidsdocumenten en bijbehorende instrumenten van bovengenoemde ministeries worden in detail beschreven in een separaat hoofdstuk (hoofdstuk 9). Een aantal actoren met een bijzondere rol op het gebied van cybersecurity wordt hieronder in meer detail weergegeven.

De NCTV is onderdeel van het ministerie van J&V. De NCTV heeft tot taak de nationale veiligheid te versterken en maatschappelijke ontwrichting te voorkomen. De NCTV ontwikkelt de cybersecurity-strategie en bevordert de publiek-private samenwerking op dit gebied. Het CSBN is een jaarlijkse publicatie van de NCTV die tot stand komt in samenwerking met publieke en private partners, en de wetenschap. Daarnaast coördineert, ontwikkelt en evalueert NCTV het beleid en de maatregelen inzake cybersecurity, waaronder de uitvoering van de Nederlandse Cybersecurity Agenda (NCSA).[20]

Het NCSC van het ministerie van J&V heeft een rol in het voorkomen en beperken van maatschappelijke ontwrichting door cyberdreigingen en -incidenten en het versterken van de digitale weerbaarheid van de samenleving. Het NCSC functioneert als nationaal Computer Emergency Response Team (CERT); doet analyses en technisch onderzoek naar aanleiding van cyberdreigingen en -incidenten; en voert het secretariaat van de publiek-private samenwerking op het gebied van cybersecurity.[21]

De Cyber Security Raad (CSR) is een nationaal en onafhankelijk adviesorgaan van het kabinet en is samengesteld uit vertegenwoordigers van publieke en private organisaties en de wetenschap. De CSR zet zich op strategisch niveau in om de cybersecurity in Nederland te verhogen.

Het Nationaal Bureau voor Verbindingsbeveiliging (NBV) doet o.a. onderzoek naar technische maatregelen op het gebied van informatiebeveiliging (software, hardware, cryptografie, netwerk(architecturen)).[22] Het NBV is onderdeel van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD).

Het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) in Utrecht,[23] is een onafhankelijke stichting die partijen ondersteunt met kennis en advies op maat bij verschillende (cyber)veiligheidsvraagstukken. Het Centrum valt onder de verantwoordelijkheid van het ministerie van J&V.

3.3.2 Beroeps- en belangenorganisaties

Nog een belangrijke groep van actoren in de cybersecurity-innovatieketen zijn beroeps- en belangenorganisaties. Cyberveilig Nederland (CN) is de belangenvereniging van de Nederlandse cybersecuritysector.[24] Cyberveilig

[20] www.wetten.overheid.nl

[21] idem

[22] www.aivd.nl

[23] www.hetccv.nl

[24] www.cyberveilignederland.nl

Nederland is in 2018 door Computest, Fox-IT, Guardian 360, Hoffmann, Motiv, Northwave, QSight IT en Zerocopter opgericht en had een jaar na oprichting ruim 40 leden. CN stelt zich als doelen het vergroten van de digitale weerbaarheid van Nederland en het verhogen van de kwaliteit en transparantie binnen de cybersecurity-sector. De meeste leden van Cyberveilig Nederland bieden diensten aan in met name de categorie Bescherming'' (bijv. IAM, training, awareness, red teaming, business continuity, DevOp, end-point protection, etc.), gevolgd door 'Detectie (bijv. surveillance, monitoring & alerting, threat intelligence, etc.), ''Identificatie' (Risk & Asset management, security strategy, security frameworks); 'Reactie' (incident response, forensics) en 'Herstel' (disaster recovery).[25, 26]

De Commissie Cybersecurity van de brancheverenigingNL digital signaleert ontwikkelingen op het gebied van cybersecurity die relevant zijn voor de ICT-branche. Daarnaast adviseert de commissie het bestuur van NLdigital over standpunten en activiteiten. Daarbij bespreekt de commissie ook de inbreng van NLdigital in de CSR.[27]

3.3.3 Think tanks

Nederland kent ook een aantal instellingen met een *think tank* functie of activiteiten, en die op basis van onderzoek een bijdrage leveren aan de maatschappelijke discussie en het politieke oordeelsvorming o.a. rondom cybersecurity-innovatie. Voorbeelden daarvan zijn het Rathenau Instituut,[28] het Nederlands Instituut voor Internationale Betrekkingen Clingendael, The Hague Center for Strategic Studies (HCSS), de Stichting Toekomstbeeld der Techniek (STT).

De Nederlandse burger (te benoemen als 'civil society') is nog maar zeer beperkt aanwezig het cybersecurity-innovatie proces. Het spanningsveld tussen innovatie in dit domein en de vragen en de eisen die vanuit de civil society worden gesteld (zie hoofdstuk 2), wordt incidenteel doch met enige regelmaat zichtbaar. Voorbeelden hiervan zijn de discussies rondom het gebruik van biometrie om online fraude te bestrijden, het gebruik van algoritmes om crimineel gedrag te voorspellen, het gebruik van *zero days* door de inlichtingen- en veiligheidsdiensten, of het ontwikkelen en promoten van zwakke

[25] De indeling van Cyberveilig Nederland is gebaseerd op het NIST-framework.
[26] Andere relevante actoren, niet specifiek op de cybersecurity-sector gericht, zijn ondernemingsorganisatie VNO-NCW, de Nederlandse Kamer van Koophandel, FME de ondernemersorganisatie voor de technologische industrie; het CIO Platform Nederland, de vereniging voor de CIO/CDO, hun 'peers' en IT-professionals van grote gebruikers van digitale technologie in Nederland; het Platform voor Informatie Beveiliging, de beroepsorganisatie voor informatiebeveiligers in Nederland; en NOREA, de beroepsorganisatie van gecertificeerde IT-auditors in Nederland en beheerder van het register van gekwalificeerde IT–auditors.
[27] De volgende organisaties maken deel uit van de Commissie Cybersecurity van NLdigital: 1U, Atos, Aurio ICT, BT Nederland, Capgemini, CGI, Cisco Systems, Compumatica Secure Networks, Connected Information Systems, Dell EMC, Digidentity, EMC Computer Systems, Facebook, FortyTwo Security, Google, Group 2000, Hewlett Packard Enterprise, Hoffmann Cybersecurity, Huawei Technologies, IBM, Intel Security, Juniper Networks, Kahuna Network Solutions, KPN IT Solutions, Microsoft, Motiv IT Masters, Ordina, Schuberg Philis, Sectra Communications, SevenP, Software Improvement Group, SQNetworks, Storro, VASCO Data Security, Veridium, VMware, Ziggo Services. www.nldigital.nl.
[28] Het Rathenau Instituut onderzoekt nieuwe technologische ontwikkelingen en de bijbehorende kansen en risico's. Daarnaast geeft en analyseert het feiten en cijfers over het innovatie- en wetenschapssysteem in Nederland. Het Rathenau Instituut draagt bij aan (politieke) oordeelsvorming door het gevraagd en ongevraagd informeren van bijvoorbeeld het parlement, regering en beleidsmakers, bedrijven, wetenschappelijke instellingen, maatschappelijke organisaties en burgers. Het instituut doet dit op basis van wetenschappelijke analyses van maatschappelijke en bestuurlijke vraagstukken.

encryptiestandaarden (‘key escrow’) (ETSI, 2018). Er wordt echter relatief weinig sociaalwetenschappelijk of multidisciplinair onderzoek vanuit deze perspectief uitgevoerd (zie hoofdstuk 4), en een aantal technologische cybersecurity-innovatie loopt het risico om inbreuk op andere fundamentele rechten te doen (in het bijzonder op het recht op privacy en de vrijheid van meningsuiting). De GDI Foundation, Bits of Freedom en de Consumentenbond zijn enkele organisaties die de ‘civil society’ (kunnen) vertegenwoordigen.

Kader 6: 'Civil society' in het innovatieproces.

4 Op welk gebied?

4.1 Inleiding

Dit hoofdstuk schetst een beeld van de gebieden waarop de primaire actoren inzetten bij het doen van onderzoek en innovatie. Daarbij worden twee componenten onderscheiden: de richting van het onderzoek (welk onderzoeks- of technologieveld of toepassingsgebied wordt geadresseerd) en het doel (waarvoor wordt de gecreëerde kennis ingezet).

De resultaten in dit hoofdstuk leunen sterk op informatie verkregen middels verschillende kwantitatieve methoden, aangevuld met input vanuit de interviews. In de praktijk zijn er weinig bestaande rapporten en studies die duiden op welk gebied de Nederlandse actoren in de keten onderzoek en innovatie uitvoeren.

Opgemerkt moet worden dat dit onderzoek in zijn algemeenheid wel in staat is gebleken inzicht te geven in de in de (relatieve) omvang van onderzoek en innovatie (zoals beschreven in hoofdstuk 3), als ook in de richting en het doel zoals hierboven geïntroduceerd, maar niet om een eenduidig en objectief beeld van de kwaliteit daarvan te schetsen. Ook andere studies bieden geen inzicht in waar de Nederlandse innovatieketen nu werkelijk goed in is. De geïnterviewden geven aan dat de kennisbasis goed is op een beperkt aantal onderwerpen, maar onvoldoende voor de uitdagingen waar we voor staan. Er is echter geen eenduidige visie is op wat nu precies die uitdagingen zijn.

4.2 Richting van onderzoek en innovatie door actoren in de keten

Onderzoek en innovatie op het gebied van cybersecurity door de actoren in de keten kent vele modaliteiten. In hoofdstuk 5 wordt dit beschreven als een breed spectrum van verschijningsvormen van onderzoek en innovatie. Dit spectrum heeft als extremen aan de ene kant het volledig open model (bijvoorbeeld de ontwikkeling van open-source softwareontwikkeling, waarbij kennis vrij toegankelijk is en niet kan worden geclaimd), en aan de andere kant 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 omschrijven 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.

De analyse heeft geen informatie opgeleverd waarmee onderzoek en innovatie in het gesloten model nader kan worden geduid. Hiervoor zijn andere methoden noodzakelijk dan die in dit onderzoek gebruikt zijn.

Met behulp van de bibliografische analyse uitgevoerd in het kader van dit onderzoek (CWTS, 2019) is richting van onderzoek en innovatie in het traditionele model wel nader te duiden:

- Wetenschappelijke publicaties op het gebied van cybersecurity vinden voornamelijk plaats in de wetenschapsvelden ‘computer science disciplines’ en

'communicatie'. Relatief minder relevant lijken 'criminology & penology' en 'mathematics interdisciplinary applications'.
- Op basis van de in de dataset voorkomende octrooiclassificatie codes, kunnen ook de meest relevante technologiegebieden die betrekking hebben op de uitvindingen in het cybersecurity domein worden geïdentificeerd. De volgende technologiegebieden zijn duidelijk aanwezig: (1) de transmissie van digitale informatie, (2) draadloze communicatie, o.a. Wi-Fi-netwerken, (3) het verwerken van digitale informatie en (4) beeldcommunicatie. Naast deze grote clusters zijn er meerdere minder omvangrijke clusters zichtbaar.

De analyse van de verschillende internationale onderzoeks- en innovatieprogramma's zoals geïntroduceerd in paragraaf 3.2.4 geeft ook inzicht in de richting van 'collaborative research' (zie Annex 2 en Annex 4). In de praktijk is het bijbehorende innovatieproces te beschrijven als een traditioneel onderzoeks- en innovatiemodel.
- In de context van het internationale onderzoek-en-innovatieprogramma ITEA zijn voor de periode 2000 - 2019 in totaal 10 cybersecurityprojecten geïdentificeerd waarin Nederlandse actoren actief waren (zie ook H7). De meest voorkomende technologieën in die projecten waren: Internet of Things (IoT), open source software, AI/machine learning, cyber-physical systems, security automation.
- In het EU-Kaderprogramma voor R&D&I (het belangrijkste financieringsinstrument van de Europese Unie) participeren Nederlandse actoren sinds 2000 in projecten die refereren aan cybersecurity. In een eerste verkenning zijn 69 cybersecurityprojecten geïdentificeerd voor de periode 2000-2019. Deze projecten zijn ingediend op 23 verschillende 'cybersecurity topics' (onderwerpen in de 'call' tekst, waaronder Cyber Security for SMEs, local public administration and Individuals, Addressing Advanced Cyber Security Threats and Threat Actors & Cryptography, Cybersecurity en Trustworthy ICT) en die een aantal specifieke cybersecurity technologieën adresseert (bijvoorbeeld Cryptografie, IoT, privacy, Cyber-crime/security/terrorism, forensics, human factors, IT security, security-by-design, cyber-physical systems, toekomstgerichte cybersecure architectures).
- In de context van het EU-SME Instrument (een voorbeeld van een EU-financieringsinstrument specifiek gericht op innovatieve MKB-bedrijven) zijn voor de 2014 - 2021 slechts 4 Nederlandse deelnemers geïdentificeerd aan projecten die innovaties rondom cryptografie, AI, ML, Physical Unclonable Function (PUF) en IoT adresseren.
- Onder de verschillende programma's van EIT Digital (een ander EU-instrument dat zich op innovatieve MKB-bedrijven richt) zijn voor de periode 2010-2019 in totaal 6 Nederlandse innoverende actoren geïdentificeerd in projecten die zich richten op encryptie, mobile authenticatie, security by design, automated network & situational awareness platforms voor cyber-resilient Industrial Control Systems (ICS).

De bovenstaande projecten zijn van technische aard. Dit beeld wordt ook bevestigd door de interviews. De perceptie bij de geïnterviewden is dat de meeste cybersecurity-onderwerpen die onderzocht worden vaak technologisch van aard zijn en niet refereren aan de meer sociaal maatschappelijke aspecten van cybersecurity. De publieke financieringsinstrumenten van bijvoorbeeld

internationale onderzoeksprogramma's zijn bepalend voor de onderzoeksrichting en/of -onderwerp van projecten, en de samenstelling van het onderzoeksteam. Op basis van de resultaten van de interviews kan geconcludeerd worden dat het accent vaak ligt op vormen van toegepast onderzoek met relatief weinig ruimte voor curiosity-driven en fundamenteel cybersecurity-onderzoek.

De geïnterviewden suggereren ook dat veel pure player startups (jonge bedrijven die primair cybersecurity-activiteiten verrichten) zich meer richten op het ontwikkelen van softwareoplossingen voor cybersecurity en minder op hardware. De zogenoemde partial players die zich voornamelijk op andere domeinen richten (search, payments, health) bieden daarbij ook cybersecurity-oplossingen.

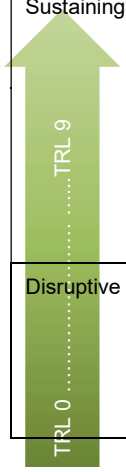
Om onderzoek en innovatie in het open innovatiemodel te analyseren is experimentele methode toegepast: de zogenaamde GitHub analyse (zie (TNO, 2019a) en (TNO 2019b)). GitHub is (een van) de grootste online platforms waar deelnemers hun bijdragen aan opensource projecten kunnen delen. Het is daarmee een voorbeeld van een open innovatie-ecosysteem. De cybersecurity-onderwerpen met een (mogelijke) Nederlandse bijdrage zijn heel gevarieerd: van data-analysis en data-manipulation tot encryption en data mining voor cybersecurity; van virtuele omgevingen waarin cyber-physical systemen worden gesimuleerd tot handleidingen en andere hulpmiddelen voor deelnemers aan een cyber challenge.

4.3 Doel van onderzoek en innovatie door actoren in de keten

Om te kunnen duiden waarvoor de door de actoren uit de keten gecreëerde kennis ingezet wordt ingezet, wordt een raamwerk geïntroduceerd waarmee onderscheid kan worden gemaakt tussen: a) een categorie *sustaining*-innovatie, die zich richt op het voorkomen van, het anticiperen op en herstellen van verstoring, uitval en misbruik van ICT; en b) een categorie *disruptieve*-innovatie, die zich richt op structurele, radicaal nieuwe vormen van cybersecurity (zie Figuur 1).

De eerste categorie van *sustaining*-innovatie valt verder uiteen in twee subcategorieën. Te weten: a) incrementele of reactieve innovatie (als antwoord op een bestaand cybersecurityprobleem); en b) proactieve innovatie (anticiperend op potentiele cybersecurity issues). De categorie *sustaining*-innovatie is meer probleem gedreven (de basis of aanleiding van innovatie ligt in de markt, of het adresseert een concreet probleem met een innovatieve oplossing).

De categorie *disruptieve*-innovatie is met name, maar niet uitsluitend, onderzoek gedreven (curiosity-driven- en basisonderzoek).



TYPE	DESCRIPTION	APPLIED TO THE CYBER DOMAIN	Positive innovation	Negative innovation (black-hat hackers, state & non-state actors, etc.)
Sustaining	Evolutionary (incremental)	Reactive/Defensive cyber innovation (e.g. intrusion detection)	x	?
	Revolutionary (breakthrough)	Pro-active/Offensive cyber innovation (e.g. automated intrusion prevention systems, post-quantum encryption, etc.)	x	x Zero-sum innovation?
Disruptive	(radical structural change, new cyber paradigms)	Structural cyber innovation (e.g. security-by-design)	x	x

Figuur 1: Cybersecurity innovatiemodellen. Bron: TNO, op basis van (Bower & Clayton, 1995)

Op basis van de interviews kan verder worden geconcludeerd dat innovatie-activiteiten door met name bedrijven in de Nederlandse keten gericht zijn op *sustaining*-innovatiemeer specifiek gaat het dan vooral om zogenaamde ‘incrementele of reactieve innovatie’ (innovatie die antwoord probeert te vinden op een bestaande cybersecurity problematiek) en in mindere mate ‘proactieve innovatie’ (innovatie die probeert te anticiperen op potentiele/toekomstige cybersecurity issues). De geïnterviewden stellen dat wat mist als basis voor het cyberveilig houden van Nederland in de toekomst *disruptive*-innovatie is. Ook hier moet echter worden opgemerkt dat er geen eenduidige visie is op wat nu precies cyberveilig is.

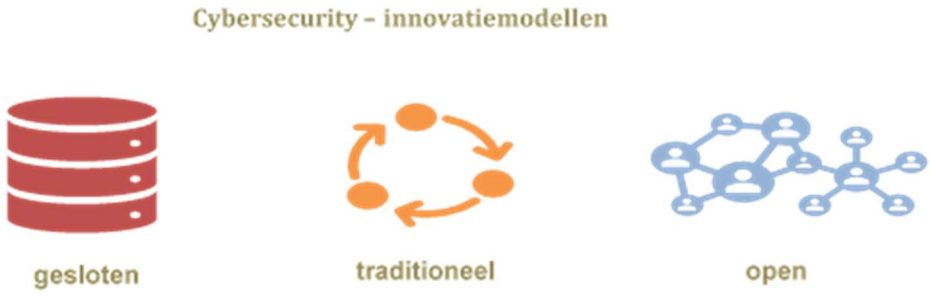
5 Onder welk innovatiemodel?

5.1 Inleiding

Onderzoek en innovatie in cybersecurity wijkt af van de meer traditionele sectoren van de economie. Dit is onder andere ingegeven door het feit dat het een relatief nieuw en breed containerbegrip is waar verschillende sub-sectoren onder kunnen worden verenigd en de toepassingen een weg vinden naar vele andere sectoren. De samenstelling van de sector lijkt daarnaast ook divers; met grote maar ook veel kleine en startende ondernemingen.

Om de verschillende modaliteiten van onderzoek en innovatie in de keten te kunnen duiden is een model geïntroduceerd waarmee de verschillende verschijningsvormen kunnen worden beschreven. De basis voor de indeling is de manier waarop de actoren ‘verbonden zijn’ in het doen van onderzoek en innovatie: hoe ze samen werken, en hoe ze kennis delen.

Het model refereert aan een breed spectrum van vormen van innovatie, met als extremen aan de ene kant het volledig open model (bijvoorbeeld de ontwikkeling van open-source software, waarbij kennis vrij toegankelijk is en niet kan worden geclaimd) en aan de andere kant 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 omschrijven 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 (zie Figuur 2).



Figuur 2: Drie cybersecurity innovatiemodellen van gesloten, traditioneel naar open

Het model heeft een prominente rol in de methodologie, als basis voor het verzamelen van informatie en het inzetten van met name de meer kwantitatieve onderzoeksmethoden (zie TNO, 2019a). Het wordt daarnaast in verschillende hoofdstukken toegepast als basis om informatie te kunnen structureren (en dan met name in hoofdstuk 4 en hoofdstuk 7).

In dit hoofdstuk worden de gesloten, open en traditionele innovatiemodellen nader beschreven, op basis van de analyse van bestaande literatuur en rapporten en aangevuld met de resultaten van de interviews. Op basis van met name de

interviews wordt vervolgens beschreven hoe innovatie in de praktijk is vormgegeven.

5.2 Innovatiemodellen in het cybersecurity innovatieketen

5.2.1 Gesloten innovatiemodel

(Porter, 1990) geeft een aantal argumenten die actoren in de keten (en dan met name bedrijven) gebruiken om een gesloten innovatiemodel te omarmen. Door een gesloten model te hanteren kunnen organisaties zich gemakkelijker differentiëren ten opzichte van hun concurrenten, kunnen ze de toetreding van nieuwe concurrenten effectiever onder controle houden, kunnen ze substituut producten of diensten ontwikkelen en aanbieden; en kunnen ze efficiënter de invloed van leveranciers en kopers onder controle houden.

In de context van het cybersecurity-domein geldt als additioneel argument dat een gesloten innovatiesysteem een zekere mate van integriteit en vertrouwelijkheid van informatie maar ook van systemen (cybersecurityoplossingen) waarborgt.

Er zijn verschillende methoden om de resultaten van onderzoek en innovatie afgeschermd te houden. (CWTS, 2019) stelt dat geheimhouding, mits goed georganiseerd, een goedkope methode is om bedrijfsgeheimen te beschermen. Daarnaast verruimen non-disclosure agreements en trade secrets wetgeving de mogelijkheden voor actoren om een gesloten innovatiemodel te omarmen.

Apple is een voorbeeld van een verticaal geïntegreerd technologiebedrijf dat een (vooral) gesloten innovatiemodel hanteert om innovatieve cybersecurity en privacy oplossingen te ontwikkelen. Door de afscherming en vertrouwelijkheid van deze gesloten vorm van innovatie, zijn verder geen kennis en inzichten opgehaald op welke onderwerpen gesloten wordt geïnnoveerd of met wie samenwerk wordt in een gesloten innovatiemodel.

5.2.2 Open innovatiemodel

In (Chesbrough & Appleyard, 2007) wordt gesteld dat de digitale revolutie nieuwe en radicaal verschillende manieren van innoveren mogelijk heeft gemaakt. Het open innovatiemodel, dat nauw verbonden is met het jaren negentig fenomeen van open source software, is daar een voorbeeld van. Het open model is als een collectieve vorm van creativiteit, waarbij de kennis van individuen gebundeld wordt in gezamenlijke innovatieprojecten. Vrijwillige deelname, ad-hoc participatie, transparantie, netwerkeffect, internationale karakter, vrije toegang tot data en de kennis van andere deelnemers, open standaarden en kosteloze licenties en geen exclusieve rechten op het innovatieproduct waar voortdurend aan geïtereerd wordt, zijn enkele karakteristieken van het open model. In (Diffy, 2003) wordt gesteld dat cybersecurity zich zeer goed leent voor het open innovatiemodel.

Op basis van bovenstaande, maar ook op basis van eigen inzichten en ervaringen omarmt TNO de hypothese dat de kans groter is dat juist binnen een open innovatiemodel disruptieve innovaties ontstaan (bijvoorbeeld nieuwe cybersecurity én privacy-by-design architecturen voor IoT). De waarde die op deze wijze gecreëerd wordt kan de attributen van een publiek goed hebben (CPB, 2016). De haalbaarheid en duurzaamheid van het (onderliggende business) model van open

innovatie zijn in de loop der tijd vaak in twijfel getrokken. In sommige gevallen heeft het model zich bewezen, bijvoorbeeld bij de ontwikkeling van open source code. Het feit dat tegenwoordig niet uitsluitend vrijwilligers bijdragen aan het gezamenlijk ontwikkelen van open source software, maar ook grote technologiebedrijven daarop inzetten, kan worden beschouwd als additioneel bewijs van de haalbaarheid van dit open innovatiemodel. Een omstreden tendens is echter dat enkele belangrijke open innovatieplatforms overgenomen zijn door grote technologiebedrijven.[29, 30]

Dankzij het actieplan “Nederland Open in Verbinding” (NOiV) uit 2007 (Ministerie van EZK, 2007) behoort Nederland tot de Nederland hoort bij de pioniers op het gebied van adoptie van dit open innovatiemodel in deze context. De Rijksoverheid stimuleert middels dit actieplan (zonder te verplichten), sinds 2007 overheidsorganisaties om open source software en open standaarden te gebruiken.

Er zijn voorbeelden van succesvolle open innovatie initiatieven op het gebied van cybersecurity in Nederland:

- De oprichting van het crowdsourcing cybersecurity hacker platform Zerocopter. Beleid rondom ‘coordinated responsible disclosure’ heeft daarin een rol gespeeld, door o.a. de activiteiten van ethical hackers te legitimeren.
- XS4ALL (onderdeel van KPN) ontwikkelt mee aan open source projecten, zoals Debian GNU/Linux, Blender en Python. Het biedt daarnaast klanten gratis licenties voor softwarepakketten en virusscanners van bijvoorbeeld F-Secure.
- Het SecurityMatters Expertisecentrum in Eindhoven, waarin proprietary kennis met betrekking tot netwerkmonitoring van operationele technologie van het onlangs door Forescout overgenomen bedrijf SecurityMatters beschikbaar wordt gesteld.
- TIBER-NL is een voorbeeld van succesvolle open procesinnovatie. Het threat intelligence-based ethical red- teaming (TIBER),[31] is een gids voor ethisch hacken van betalingsverkeer van financiële instellingen. Het is ontwikkeld door de Nederlandsche Bank en de financiële sector. Dit initiatief is naast CBEST (UK), de inspiratie geweest voor een Europeescybersecurity en -resilience testraamwerk.[32]
- De Nederlandse bijdragen aan GitHub zijn beschreven in paragraaf 4.3, en in (TNO, 2019b).

Kader 7: Voorbeelden toepassingen open innovatie in Nederland.

Tegelijkertijd worden er zorgen geuit over de (security)risico’s die het gebruik van open source code met zich meebrengt. Deze kunnen zich voordoen door bijvoorbeeld het bewust gebruiken van open source code met bekende kwetsbaarheden in andere complexe applicaties, het gebrek aan aansprakelijkheid van de ontwikkelaars en van de integrators, de mogelijkheid om kwaadaardige code toe te voegen.

[29] in 2018 werd GitHub door Microsoft overgenomen voor ruim 7 miljard dollar. Ook in 2018 werd het open source software bedrijf RedHat door IBM overgenomen voor een bedrag van 34 miljard. Tien jaar eerder, in 2008 werd MySQL, een open-source relational database management system, door Sun Microsystems/Oracle overgenomen voor een bedrag van 1 miljard dollar.
[30] Het overnemen van open innovatie initiatieven door grote commerciële bedrijven wordt in de literatuur als “co-opting” aangeduid. Co-opting wordt vaak als een negatieve ontwikkeling beschouw omdat het kan resulteren in het inperken van innovatie.
[31] www.computable.nl
[32] www.ecb.europa.eu

5.2.3 Traditioneel innovatiemodel

In de context van wat in dit onderzoek als het traditionele innovatiemodel wordt aangeduid, claimen actoren de resultaten van hun onderzoek in patenten en middels publicaties in wetenschappelijke literatuur. Zeker patentgedrag is zeer sectorspecifiek: in de semiconductor industrie, waar kennis een basis is voor concurrentie, wordt bijna alle kennis vastgelegd. In de meer traditionele machinebouw, met unieke eindproducten, bijna niets (Hippel, 1988). Het publicatie- en patentgedrag van de actoren in de cybersecurity wordt beschreven in (CWTS, 2019).

Publicaties, en zeker patenten, vormen de basis voor samenwerking in onderzoek en innovatie. Op basis daarvan kan worden vastgelegd welke kennis actoren inbrengen in een innovatietraject en kan de in de context van het project ontwikkelde kennis worden toebedeeld aan (een van de) deelnemende actoren (de zogenaamde ‘foreground’ en ‘background knowledge’). Zij vormen daarom bij uitstek de basis voor samenwerkingsverbanden tussen de primaire actoren zoals benoemd in paragraaf 3.2, al dan niet samen met de overheid, al dan niet publiek gefinancierd. Voorbeelden van deze samenwerkingsverbanden zijn beschreven in Annex 2 - Annex4.

Publiek-private samenwerkingen op het gebied van innovatie worden in de Nederlandse context ook wel aangeduid als het Triple Helix innovatiemodel. The Hague Security Delta (HSD) beschrijft in (HSD, 2018) de karakteristieken van een typisch Nederlandse (cyber) security Triple helix-samenwerking als volgt:

- Het aangaan van een triple helix-samenwerking is slechts één optie voor een organisatie om haar ambities te realiseren;
- Triple helix-samenwerkingen zijn gericht op het realiseren van meerdere doelen;
- Triple helix-samenwerkingen hebben een tijdelijk karakter;
- Partijen blijven onafhankelijke entiteiten en hebben onderling geen hiërarchische verhouding;
- In een triple helix-samenwerking verschillen de partijen in functie, doelen, ambitie en praktijken;
- Partijen richten samenwerking aan de hand van netwerkmanagement in;
- Partijen regelen legitimiteit als onderdeel van governance in”.

Kader 8: Karakteristieken van Nederlandse (cyber) security innovatiemodel op het gebied van, als voorbeeld van het traditionele innovatiemodel.

5.3 Innovatie in de praktijk: open, gesloten of traditioneel?

Op basis van het literatuuronderzoek en de kwantitatieve methoden toegepast in dit onderzoek zijn het open en traditionele innovatiemodel goed te beschrijven en te illustreren met voorbeelden (zoals beschreven in de verschillende hoofdstukken en bijlages van dit rapport). Voor een beschrijving van het gesloten model echter moet gebouwd worden op de interviews.

Uit die interviews blijkt dat eigenlijk elke actor (overheid, onderzoeksinstelling, groot bedrijf of startups) in enige mate aan gesloten innovatie doet binnen het cybersecurity-domein. Zo blijkt dat bijvoorbeeld startups bij (deel) oplossingen soms heel gesloten innoveren. Ook kan in sommige gevallen ervoor gekozen worden om een eindoplossing niet voor anderen openbaar te maken. Onderzoeken vanuit universiteiten worden soms ook in een meer gesloten innovatiemodel uitgevoerd om dezelfde reden. Universiteiten zijn vooral bezig met fundamenteel onderzoek,

maar doen ook aan toegepast onderzoek omdat zij onderzoek doen voor opdrachtgever (zoals ministeries), waarin niet alleen fundamenteel onderzoek van hen gevraagd wordt. Met name in de tweede vorm van onderzoek kan de behoefte voor afscherming van innovatie door de risico's voor veiligheidswaarborging zorgen voor gesloten innoveren. Daarnaast is het zo dat voor onderzoeksinstellingen die meer aan competitief of pre-competitief onderzoek doen, op bepaalde momenten ook gesloten geïnnoveerd wordt. Zo lijkt het dat er gezien kennisopbouw van fundamenteel, toegepast, competitief naar pre-competitief eenzelfde lijn getrokken kan worden, van zelden tot soms, gedeeltelijk tot volledig gesloten innoveren. Een ander belangrijk inzicht dat uit de interviews naar voren komt, is dat binnen het cybersecurity- innovatielandschap niet zonder gesloten innovatie gewerkt kan worden. Afhankelijk van de uitdaging en mogelijke oplossing, hoeft dit niet per se gedurende het hele proces te zijn. Het gaat bij gesloten innovatie dus niet zo zeer om veel samenwerking, maar meer om het betrekken van kennis en expertise bij uitdagingen.

Het onderzoek laat zien dat de innovatieketen een veelheid aan vormen van innovatie kent; van volledig open tot volledig gesloten. Binnen innovatietrajecten worden vaak verschillende innovatiemodellen gebruikt. Zo kan open-software in gesloten innovatie geïntegreerd worden of komt er uit gesloten innovatie een oplossing die uiteindelijk terecht komt in een open innovatietraject.

Uit het onderzoek komt verder naar voren dat er geen Nederlandse actoren zijn die hun innovatieproces volledig gesloten implementeren. Dit wordt mede veroorzaakt door dat er veel kleine(re) actoren in de keten zijn die de capaciteit niet hebben om alle kennis intern te ontwikkelen. Grote partijen zijn in zijn algemeenheid vaak 'partial players' en deze hebben (vooralsnog) niet de wens om het hele proces intern uit te voeren.

In de keten wordt ook gewerkt binnen een open innovatiemodel waarin nieuwe en externe actoren betrokken raken, zoals in het geval van open source softwareontwikkeling. Deze vorm van softwareontwikkeling is in de sector in sommige gevallen een valide businessmodel. Nog vaker wordt open source code geïntegreerd in innovatieve cybersecurity-oplossingen. Het faciliteren van open source creëert in deze context economisch gewin als ook disruptieve innovatie.

6 Waar op de TRL-schaal?

6.1 Inleiding

Om de keten nader te duiden wordt ook geanalyseerd waar de primaire actoren in het innovatieproces hun onderzoeks- en innovatieactiviteiten uitvoeren. Als basis wordt daarvoor de TRL-schaal genomen (en meer in het bijzonder de interpretatie daarvan volgens European Association of Research & Technology Organisations (EARTO), zie Figuur 3). De informatie is verkregen middels de interviews, aangevuld met resultaten van de analyse van relevante literatuur en rapporten. Dit hoofdstuk beschrijft de resultaten van deze analyse.

Cluster	TRL	H2020 terminology	EARTO reading	EARTO definition and description
Invention	TRL1	Basic principles observed	Basic principles observed	Basic scientific research is translated into potential new basic principles that can be used in new technologies
	TRL2	Technology concept formulated	Technology concept formulated	Potential application of the basic (technological) principles are identified, including their technological concept. Also the first manufacturing principles are explored, as well as possible markets identified. A small research team is established to facilitate assessment of technological feasibility.
Concept validation	TRL3	Experimental proof of concept.	First assessment of feasibility of the concept and technologies	Based on preliminary study, now actual research is conducted to assess technical and market feasibility of the concept. This includes active R&D on a laboratory scale and first discussions with potential clients. The research team is further expanded and early market feasibility assessed.
	TRL4	Technological validity in a lab	Validation of integrated prototype in a laboratory	Basic technological components are integrated to assess early feasibility by testing in a laboratory environment. Manufacturing is actively researched, identifying the main production principles. Lead markets are engaged to ensure connection with demand. Organisation is prepared to enter into scale up, possible services prepared and a full market analysis conducted.
Prototyping and incubation	TRL5	Technology validated in relevant environment (industrially relevant environment in the case of KETs)	Testing of the prototype in a user environment	The system is tested in a user environment, connected to the broader technological infrastructure. Actual use is tested and validated. Manufacturing is prepared and tested in a laboratory environment and lead markets can test pre-production products. Fist activities within the organisation are established to further scale up to pilot production and marketing
Pilot production and demonstration	TRL6	Technology demonstrated in relevant environment (industrially relevant environment in the case of KETs)	Pre-production of the product, including testing in a user environment	Product and manufacturing technologies are now fully integrated in a pilot line or pilot plant (low rate manufacturing). The interaction between the product and manufacturing technologies are assessed and fine-tuned, including additional R&D. Lead markets test the early products and manufacturing process and the organisation of production is made operational (including marketing, logistics, production and others).
	TRL7	System prototype demonstration in an operational environment.	Low scale pilot production demonstrated	Manufacturing of the product is now fully operational at low rate, producing actual commercial products. Lead markets test these final products and organisational implementation is finalized (full marketing established, as well as all other production activities fully organized). The product is formally launched into first early adopter markets.
Initial market introduction	TRL8	System completed and qualified	Manufacturing fully tested, validated and qualified	Manufacturing of the product, as well as the product final version is now fully established, as well as the organisation of production and marketing. Full launch of the product is now established in national and general early majority markets.
Market expansion	TRL9	Actual system proven in operational environment (competitive manufacturing in the case of KETs; or in space)	Production and product fully operational and competitive	Full production is sustained, product expanded to larger markets and incremental changes in the product create new versions. Manufacturing and overall production is optimized by continuous incremental innovations to the process. Early majority markets are fully addressed.

Figuur 3: TRL-niveaus en hun interpretatie. Bron: (EARTO, 2014).

6.2 Actoren en hun onderzoeks- en innovatieactiviteiten op de TRL-schaal

Uit het onderzoek blijkt dat de actoren uit het innovatiesysteem ook binnen de cybersecurity-innovatieketen opereren waar dat te verwachten is:

- Universiteiten en NWO-instituten zijn vooral terug te vinden in de lagere TRL-niveaus (TRL 0 - 3). De Technische Universiteiten innoveren voornamelijk tot en met TRL 4, maar verleggen ook meer en meer hun scope tot en met TRL 7.[33]
- De Toegepast Onderzoek Organisaties (TO2) richten zich met name op TRL 4 tot TRL 7. Als het gaat om cybersecurity springt TNO eruit; in beperkte mate doet ook NLR aan cybersecurity-innovatie.

[33] HBO instellingen hebben een specifieke rol in het Nederlandse innovatiesysteem. Nader duiding van hun rol en relevante in de cybersecurity innovatieketen vereist additioneel onderzoek.

- Bedrijven zijn nauwelijks direct betrokken bij fundamenteel onderzoek. Zij opereren meestal vanaf TRL 4. Er is echter sprake van een zekere mate van concentratie van hun activiteiten tussen TRL 4 en 6. Het onderzoek laat verder zien dat er in Nederland nauwelijks bedrijven actief zijn die het hele innovatieproces van TRL 0 - 9 zelfstandig kunnen uitvoeren.
- Ook startups en MKB-bedrijven opereren vanaf TRL 4. Op basis van zowel de data-analyse als de interviews is de conclusie aannemelijk dat ze in mindere mate actief zijn in de hoge TRL-niveaus 7 - 9. Een mogelijke verklaring is dat veel van deze bedrijven moeilijk zelfstandig voorbij TRL-niveau 6 komen. Dat kan betekenen dat er vooral producten worden ontwikkeld waar (nog) geen markt voor is en individuele partijen nog niet in willen investeren. Dit gebrek aan financiering in deze fase heeft tevens tot gevolg dat het voor deze partijen lastig is ontwikkelde prototypes in een realistische omgeving te testen en door te ontwikkelen - de zogenaamde ‘valley of death’. Opgemerkt dient te worden dat sommige actoren als expliciete strategie hebben om na het succesvol ontwikkelen van een prototype zich te laten overnemen door een grotere gevestigde (soms buitenlandse) partij.

7 Met wie: samenwerking in de innovatieketen

7.1 Inleiding

Dit hoofdstuk beschrijft de samenwerking in de keten tussen de primaire actoren bij het doen van onderzoek en innovatie. Omdat de keten onderhevig is aan voortdurende verandering, ingegeven door ontwikkelingen in de onderliggende technologie en door veranderingen in de samenstelling van de actoren, gaat samenwerking niet vanzelf. De volgende paragraaf beschrijft enkele randvoorwaarden die door de overheid zijn gecreëerd en actoren uit de keten zelf om samenwerking mogelijk te maken. De daaropvolgende paragraaf beschrijft verschillende entiteiten en platformen die zijn opgericht of ontstaan met als doel het ondersteunen van deze samenwerking. Het hoofdstuk sluit af met een beschrijving van samenwerking in de praktijk, gespecificeerd naar innovatiemodel (zie hoofdstuk 5) en niveau op de TRL-schaal (hoofdstuk 6).

De resultaten van dit hoofdstuk berusten op een analyse van de literatuur, interviews. Met behulp van verschillende kwantitatieve methoden is deze informatie getoetst en aangevuld.

7.2 Randvoorwaarden voor samenwerking

In de context van R&D en innovatie is de rationale voor samenwerking duidelijk: door het delen van kennis en capaciteit kunnen ook de kosten worden gedeeld, waardoor onderzoek dat individuele actoren zich niet kunnen veroorloven nu wel kan worden geïnitieerd (zie (Heide, 2011). Dit maakt dat ook de primaire actoren in de keten een incentive hebben om te zoeken naar partners.

Vormen van marktfalen die geassocieerd worden met het doen van onderzoek verschaffen de overheid ook een legitieme basis om dit te ondersteunen (zie (Europese Commissie, 2014)). De overheid heeft daarnaast nog een rationale om samenwerking in de keten te bevorderen in de context van cybersecurity: door het sturen van samenwerking kan de overheid de vraag- en aanbodzijde van onderzoek en innovatie beter op elkaar afstemmen, waardoor de effectiviteit van (interventies gericht op het ondersteunen van) innovatie in de keten wordt verhoogd.

De overheid kan samenwerking tussen de primaire actoren afdwingen door interventie. Bijvoorbeeld door eisen te stellen aan financiële ondersteuning voor onderzoek en innovatie. Hoofdstuk 9 beschrijft de huidige instrumenten van de Nederlandse overheid en adresseert hierbij ook dit element. Maar de overheid kan ook op een indirecte manier samenwerking faciliteren: door het creëren van de juiste randvoorwaarden.

Deze paragraaf beschrijft een aantal van deze randvoorwaarden (maar is zeker niet volledig - alleen die initiatieven worden genoemd die specifiek zijn voor de keten). Opgemerkt dient te worden dat deze niet allemaal geïnitieerd zijn door de overheid.

Zoals hierboven benoemd bestaan er ook voor de primaire actoren incentives om zich te organiseren en de juiste randvoorwaarden te creëren voor samenwerking.[34]

Centrum	Initiatiefnemers	Partners	Vestiging	Focus
Cyber Intelligence Center	Deloitte		Den Haag	Cyber intelligence
Het Expertisecentrum Cyberweerbaarheid[35]	Het Platform Veilig Ondernemen en de Brightlands Smart Services Campus in	Ondernemend Limburg, Centraal Bureau voor de Statistiek, Universiteit Maastricht, Open Universiteit, Hogeschool Zuyd, Leeuwenborgh-Arcus, CybersecurIT, Huis voor de Sport, Burgerkracht, Politie KPN	Heerlen.	Cybersecurity scan voor MKB: ondersteuning door studenten van Leeuwenborgh-Arcus
SecurityMatters[36] (aangekondigd)	ForeScout		Eindhoven	Expertisecentrum netwerkmonitoring van operationele technologie
Nederlands Cyber Collectief[37]	Sparklab / Nationale Nederlanden	Ondernemers en bedrijven	Den Haag	Co-creatie centrum van de cybersecurity-sector: onderzoek, kennisdeling, durfkapitaal, voor en met ondernemers en bedrijven in cybersecurity

Tabel 2: Expertise- en kenniscentra.

[34] Paragraaf 7.2 benoemt expliciet standaarden en certificaten, maar ook keurmerken kunnen een rol spelen. PerfectDay van verzekeraar National Nederlanden is van plan om in 2019 een cyberkeurmerk voor het MKB te ontwikkelen. De ontwikkeling van het keurmerk is een publiek-private samenwerking waarbij ook het Verbond van Verzekeraars betrokken is.
Twee andere Cybersecurity Keurmerken worden door het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) ontwikkeld: een keurmerk dat bestaat uit een risicomodel voor de inschatting van cybercrime; en een ander keurmerk dat de vakkundigheid en betrouwbaarheid van een cybersecurity dienstverlener beoordeelt. Dit wordt ontwikkeld samen met het Verbond van Verzekeraars, VNO-NCW, MKB-Nederland, CIO Platform Nederland, NL Digital (voorheen Nederland ICT), Cyberveilig Nederland en Partnering Trust en met de steun van het ministerie van EZK, het ministerie van J&V en de Politie.
[35] www.computable.nl
[36] www.computable.nl
[37] www.nederlandscybercollectief.nl

7.2.1 Expertise- en kenniscentra

Expertise- en kenniscentra vormen een basis voor kennisdeling, en daarmee innovatie op het gebied van cybersecurity. Er worden steeds meer dergelijke centra opgericht: soms als initiatieven van de private sector en soms als public-private partnerships (zie Tabel 2 voor een aantal voorbeelden).

7.2.2 Standaardisatie

Standaarden vormen een belangrijke basis om de vraagkant en aanbodkant van onderzoek en innovatie af te stemmen. Een andere belangrijke actor in de innovatieketen zijn standaardisatie-organisaties, zowel om bepaalde innovaties te standaardiseren als processen in het cybersecurity-domein (WODC, 2015).

NEN is het nationaal normalisatie-instituut. Namens Nederland is NEN lid van alle Europese en mondiale normalisatienetwerken. NEN doet actief mee aan bijvoorbeeld ‘ISO/IEC JTC 1/SC 27 - Information security, cybersecurity and privacy protection’ en de Europese 'Cyber Security Coordination Group' (CSCG).[38]

NEN en individuele experts uit het bedrijfsleven en kennisinstellingen (bijvoorbeeld TNO) doen mee aan verschillende initiatieven van de drie Europese Standaardisatie Organisaties (3ESO's) en van andere internationale standaardisatiegremia. Onder de voor dit onderzoek relevante initiatieven vallen: i) ‘CEN/CLC/JTC 8 - Technical body Privacy management in products and services for the security industry’; ii) ‘CEN/CLC/JTC 13 - Cybersecurity and Data Protection’ (gezamenlijk initiatief met ISO en IEC op het gebied van data protection, information protection, security techniques met focus op cybersecurity);[39] iii) het Technical Committee on Cybersecurity (TC CYBER) van de derde Europese standaardisatieorganisatie, ETSI.[40, 41] De drie ESO’s doen incidenteel mee als partner of stakeholder in R&D en andere innovatietrajecten van de lidstaten.

Er bestaan ook veel standaarden voor informatiebeveiliging (zoals ISO 27001 - de internationale ISO norm voor informatiebeveiliging; NEN 7510, een branche-specifieke Nederlandse norm voor informatiebeveiliging in de zorg) en er komen steeds meer standaarden bij (zoals het ISO-IEC 30141 - internationale norm voor Internet of Things toepassingen dat sinds kort van kracht is, aangekondigde inhoudelijke aanpassingen in de ISO 27001 norm als gevolg van de impact van nieuwe technologieën zoals blockchain, quantum computing, AI).

De EU Cybersecurity Act voorziet een centrale rol voor het nieuwe EU-Agentschap voor cybersecurity bij het stroomlijnen van een steeds groeiend aantal standaarden en om verdere versnippering te voorkomen.

Andere initiatieven worden buiten de traditionele standaardisatie organisaties genomen en zijn meer op vormen van procesinnovatie gericht. Een voorbeeld

---

[38] www.iso.org
[39] www.cencenelec.eu, www.cen.eu, www.cen.eu
[40] De 9 focusgebieden (key areas) van TC CYBER zijn: understanding the cyber security ecosystem, IoT security and privacy, cyber security for critical national infrastructures, protection of personal data and communication, enterprise and individual cyber security, cyber security tools, support to EU legislation, forensics, and quantum-safe cryptography.
[41] www.etsi.org

daarvan is TIBER-NL, een threat intelligence-based ethical red- teaming en initiatief van de Nederlandse financiële sector, dat, naast CBEST (UK), de inspiratie is geweest voor een Europees cybersecurity en -resilience framework. Baseline Informatiebeveiliging Overheid (BIO), dat sinds 2019 van kracht is, is een ander voorbeeld van een bestuurlijk gezamenlijk normenkader voor informatiebeveiliging binnen de overheid.

Open standaarden voor web-technologieën worden ook door andere fora ontwikkeld, zoals IETF, W3C, WHATWG en Ecma International. Stichting NLnet is een van de Nederlandse bijdragers aan deze categorie standaarden (waaronder GSM security, Tor Hidden Services, GNUnet, GPLv3, DNSSEC, secure real-time communications, NoScript, Unhosted free space optics, Serval project and OpenDocument Format). Stichting Vrijschrift host het internationale *'Translation Project'* dat bedoeld is om activiteiten van ontwikkelaars en vertalers van vrije software te coördineren. Open standaard initiatieven zijn van bijzonder en groeiend belang vanuit een cybersecurity en privacy perspectief.

7.2.3 Certificatie[42]

Met een systeem van certificering hoopt de EU een grote bijdrage te leveren aan de digitale veiligheid in Europa. Het is één van de uitwerkingen van de EU Cybersecurity Act (Verordening 2019/881). De EU ziet een sterk groeiende afhankelijkheid van de economie en de samenleving van de digitale infrastructuur en dat zorgt voor sterk toenemende risico's. Om dat het hoofd te kunnen bieden, komt de EU met een systeem van certificering van belangrijke actoren in het cybersecurity-domein. Met dit systeem hoopt de EU een grote bijdrage te leveren aan een betere bescherming van data. Met een centraal model van certificering, ontstaat meer transparantie op de kwaliteit van ICT-producten en diensten als het gaat om cybersecurity, neemt het vertrouwen toe in de digitale markt en digitale innovatie en wordt de samenwerking tussen bedrijven uit verschillende landen veel eenvoudiger. Met deze stap levert de EU mogelijk een puzzelstukje voor het ecosysteem in opbouw.

De publiek-private samenwerking Qualification of Information Security professionals (QIS) is in 2013 gestart om een certificatiestelsel te ontwikkelen voor cybersecurity professionals in Nederland.[43] De organisaties van QIS (ABN Amro, AkzoNobel, Cybersecurity Raad, ECP, EY, ING, KPN, Ministerie van Justitie/NCTV, Ministerie

[42] Opgemerkt dient te worden dat naast de in deze sub-paragraaf benoemde vormen van certificering er verschillende relevante opties voor personeel certificatie bestaan, waaronder: EC Council Licensed Penetration Tester; Certified Ethical Hacker; Certified Computer Hacking Forensic Investigator en ISC2 Certified Information Systems Security Professional. Uit interviews blijkt dat de opinies over de kwaliteit en nut hiervan sterk uiteen lopen. Daarnaast wordt vanaf 2019 wordt ook AVG-Certificering verwacht.

[43] Onderdeel van het certificatiestelsel zijn de beroepsprofielen die door onderwijsinstellingen voor mbo, hbo en wo de basis kunnen zijn voor het ontwikkelen van opleidingsprofielen met leerdoelen en doorlopende leerlijnen met loopbaanperspectieven die aansluiten bij de eisen voor professionaliteit in het vakgebied. Het stelsel sluit aan op de Europese standaard voor ICT-competenties (e-CF, EN16234) en de internationale standaarden voor persoonscertificatie (ISO-17024) en management van informatiebeveiliging (de ISO-27000 serie). Door aan te sluiten op internationale standaarden sluit het certificatiestelsel aan bij internationale ontwikkelingen, zoals in Europa ECSO (European Cyber Security Organisation van de Europese Unie) en in de US (NIST, NICE). Door QIS zijn met landen van de Europese Unie, de Verenigde Staten en Canada op meerdere bijeenkomsten de resultaten gedeeld en besproken. www.dcypher.nl

van BZK, PvIB, Rabobank, CIO Platform, CIP, MKB, NRTO, HBO-i, VSNU, NOREA, KNVI, VNO-NCW) hebben een uniform, eenduidig en transparant certificatiestelsel ontwikkeld dat toepasbaar is in alle sectoren van de Nederlandse economie. Het certificatiestelsel is opgezet overeenkomstig de structuur die andere beroepsgroepen hiervoor hanteren. Het certificatiestelsel is het instrument voor het meten van een erkend en herkenbaar niveau van vakbekwaamheid dat aansluit bij de dagelijkse beroepspraktijk van cybersecurity professionals in Nederland. Nederland is met het QIS certificatiestelsel en de beroepsprofielen op basis van e-CF competenties voorloper binnen Europa.

7.3 Ondersteunen van samenwerking: entiteiten en platformen

Naast bovengenoemde randvoorwaarden zijn ook specifieke entiteiten en platformen opgezet die actief proberen de actoren uit de keten te laten samenwerken op het gebied van onderzoek en innovatie. Deze zijn vaak geïnitieerd door de overheid, met andere actoren. Maar deze andere actoren nemen ook gezamenlijk zelf het initiatief.

7.3.1 Nationale, regionale en lokale initiatieven

dcypher is het Nederlands platform voor hoger onderwijs en onderzoek op het terrein van digitale veiligheid. dcypher agendeert en coördineert zowel wetenschappelijk als praktijkgericht cybersecurity-onderzoek aan de hogescholen en legt verbindingen “tussen betrokkenen uit de publieke- en private sector bij het hoger onderwijs en onderzoek”.[44] De ministeries van J&V, EZK en OCW en het NWO-gebied Exacte Wetenschappen zijn oprichters van dit platform.

De Cybersecurity Alliantie is een initiatief van het ministerie van J&V. De CS Alliantie is in 2018 als het platform van de publiek-private samenwerking voor een digitaal weerbaar Nederland opgericht.[45] De CS Alliantie is aangekondigd in de NCSA. Het dagelijks functioneren van de alliantie wordt door ECP - Platform voor de Informatie Samenleving uitgevoerd. De CS Alliantie faciliteert concrete kortlopende projecten die maximaal negen maanden duren.

The Hague Security Delta (HSD) fungeert als nationaal veiligheidscluster en vormt een netwerk van bedrijven, overheden en kennisinstellingen. HSD stimuleert en faciliteert kennisdeling en helpt bij het opzetten van innovatieprogramma’s waar partijen vanuit het gehele veiligheidsdomein in mogen participeren. HSD is mede-organisator van o.a. de Cyber Security Week en de International Cyber Security Summer School.[46]

Stichting NLnet is een particuliere stichting die bekend staat om het financieren van open source software en standaardisatiewerk.[47] NLnet heeft bijgedragen aan internet standaarden (waaronder GSM security, Tor Hidden Services, DNS security, secure real-time communications NLnet stelt microgrants beschikbaar, geeft advies en biedt toegang tot een internationaal netwerk van experts.

---

[44] www.nwo.nl
[45] www.cybersecurityalliantie.nl
[46] www.thehaguesecuritydelta.com
[47] www.nlnet.nl

SURF is een ICT-coöperatie van ruim 100 onderwijs- en onderzoeksinstellingen in Nederland, richt zich o.a. op het ontwikkelen van kennis over cybercrime, wet- en regelgeving over datagebruik, privacy en veiligheid. SURF verkent de potentie van nieuwe technologieën en werkt aan proactieve bescherming van de infrastructuur en data". Daarbij wordt samengewerkt met initiatieven zoals het programma Integraal Veilig Hoger Onderwijs (IVHO).[48]

SURFsara is een onderdeel van SURF en de aanbieder van een nationale e-infrastructuur aan onderzoekers bij universiteiten, universitaire medische centra en alle overige onderzoeksinstellingen in Nederland.[49] Deze entiteit slaat een brug tussen onderzoek en een geavanceerde ICT en faciliteren wetenschappelijk onderzoek en ontplooien innovaties voor het bedrijfsleven. SURFsara ondersteunt onderzoek met geoptimaliseerde software en algoritmes voor onderzoek, duurzame opslag en toegankelijkheid van data.

Het Digital Trust Center (DTC) is in 2018 opgericht door het ministerie van EZK en heeft als missie Nederlandse MKB-bedrijven weerbaarder te maken tegen toenemende cyberdreigingen. Het DTC doet dit door het delen van kennis, informatie en advies, het ontwikkelen van tools (zoals de Basisscan Cyberweerbaarheid) en het stimuleren van samenwerking. Het DTC coördineert het Cyberweerbaarheidsnetwerk.[50] De eerste regionale samenwerkingsverbanden binnen het netwerk zijn in 2018 vastgelegd en daarin "werken ondernemers samen met andere organisaties aan het vergroten van de cyberweerbaarheid, binnen en tussen niet-vitale branches, sectoren en regio's."[51]

Het Cyberweerbaarheidsnetwerk is in 2018 van start gegaan met als overkoepelend doel de digitale veiligheid van het niet-vitale bedrijfsleven te bevorderen.[52] Middels dit initiatief moet een landelijk dekkend stelsel van informatieknooppunten voor ondernemers ontstaan waar ze "terecht kunnen voor kennis, dreigingsinformatie, best practices en handelingsperspectief op het terrein van cybersecurity."[53]

- Ook vitale sectoren mogen zich aansluiten en onderdeel van het netwerk worden met name om hun kennis en expertise aan de niet vitale sectoren over te dragen. Eerdere initiatieven hebben zich inmiddels hierbij aangesloten, zoals het Cyber Synergie Schiphol Ecosysteem (CYSSEC), ondersteund door de Nationaal Coördinator Terrorismebestrijding; FERM (een initiatief van Deltalinqs, gemeente Rotterdam, Port of Rotterdam, Politie), een platform in de Rotterdamse haven om bedrijven digitaal weerbaar te maken en Connect2Trust, een initiatief van nationale en internationale bedrijven die in Nederland actief zijn.
- De samenwerkingen zijn zeer divers en uitgebreid, met als deelnemers: (inter)nationale bedrijven, lokale en regionale overheden, belangenorganisaties, etc.
- Binnen cybersecurity-innovatietrajecten wordt getracht om de samenwerking verder uit te breiden naar onderzoeks- en opleidingsinstellingen. Voorlopig

[48] www.surf.nl
[49] www.surf.nl
[50] www.digitaltrustcenter.nl
[51] www.digitaltrustcenter.nl
[52] De vervaldatum van dit beleidsexperiment is verlengd tot 1april 2021.
[53] www.officielebekendmakingen.nl

hebben slechts drie van de negen samenwerkingsverbanden in dit netwerk trajecten voorzien of al lopen op het gebeid van cybersecurity-innovatie (zie Tabel 3).

Samenwerkingsverband	Oprichting	Deelnemers	Focus
Cybersecurity Center Maakindustrie	2018	Novel-T (uitvoerder), Saxion Hogeschool, Universiteit Twente, CIO Platform, Koninklijke Metaalunie, Ten Hag Advies, BOOST, Tesorion, HTSP, Provincie Overijssel, Demiroz consultancy, Actemium, Sincerus	Regionaal/ nationaal & sectoraal
Cyberweerbaarheid door samenwerking in Noord-Nederland	2018	Regio Noord Nederland (Groningen Drenthe en Friesland) (Stichting Cybersafety Noord Nederland, Stichting Cyber security centrum Noord Nederland, DataDiensten Fryslân. De Friesland zorgverzekeraar, Connect.frl., Bedrijvenvereniging west (Groningen), Samenwerking Noord, Provincie Groningen, Provincie Fryslan, Provincie Drenthe	Regionaal
CYSSEC (Cybersecurity Synergie Schiphol Ecosysteem) -	2016	Alle actieve organisaties op het Schiphol-gebied met een werkgroep van 12 organisaties (publiek en privaat, MKB en grootbedrijf).	Lokaal

Tabel 3: Het Cyberweerbaarheidsnetwerk – regionale samenwerkingsverbanden per juli 2019.

Novel-T is een Knowledge Transfer Office (KTO) van Universiteit Twente en Hogeschool Saxion, opgericht als een public-private partnership in samenwerking met Regio Twente, Gemeente Enschede en de Provincie Overijssel. Novel-T speelt een belangrijke rol in de regionale innovatie-ecosysteem van Oost Nederland. Security is één van de focus gebieden van Novel-T. Op het gebied van cybersecurity biedt Novel-T (in samenwerking met het Cybersecurity Centrum voor de Maakindustrie) ondernemers kennis, tools en ondersteuning om hun eigen cybersecurity goed te organiseren (zoals een cyberweerbaarheid scan) en is een ISAO (Information Sharing and Analysis Organization) opgezet. Onder de partners bevinden zich het FME, Metaalunie, VMO, OostNL en CIO platform. Novel-T komt voort uit het programma ‘Digital Trust Centre’ dat eind 2017 door het ministerie van EZK samen met het ministerie van J&V is gestart.

Binnen de verzekeringsbranche zijn meerdere samenwerkingsbanden rondom cybersecurity innovatie ontstaan, met name rondom Het Verbond van Verzekeraars (VvV) en Nationale Nederlanden. Het gaat vaak om een combinatie van product, proces en marketing innovatie met een hoog TRL-niveau en in de categorie *sustaining innovatie*. Daarnaast worden vanuit de branche ook kennisdisseminatie activiteiten georganiseerd.

Het VvV is de brancheorganisatie. Het verbond heeft een aantal programma's ontwikkeld, waaronder een educatieve cybergame[54] (samen met TU Delft) voor werknemers in de verzekeringsbranche.

Het Centrum voor Verzekeringsstatistiek (CvV) van het VvV speelt een belangrijke rol bij innovatie op het gebied van oplossingen en dienstverleningsconcepten die de digitale weerbaarheid van de verzekeraars zelf zou kunnen verbeteren, waaronder een cybersecurity maturity scan voor verzekeraars.

VvV onderzoekt o.a. de geschiktheid van het inzet van kunstmatige intelligentie (AI) voor fraudedetectie. Om dit te kunnen onderzoeken is het Data Competence Center[55](DCC) opgericht, een samenwerkingsverband van het VvV, Stichting CIS (het Centraal Informatie Systeem van in Nederland werkzame verzekeringsmaatschappijen) en Stichting EPS/PV (Stichting Efficiënte Processen Schadeverzekeraars./Processen Verbaal).

Ook individuele verzekeraars zijn op dit gebied actief, waaronder verzekeraar Nationale Nederlanden (NN). Sparklab[56] is het innovatielab van NN. Uit Sparklab is een startup ontstaan, PerfectDay,[57] die cybersecurity diensten aan MKB-bedrijven bieden. De diensten richten zich niet op technische cybersecurity-oplossingen maar op het bieden van advies over interne processen en compliance van de MKB-bedrijven en op de z.g. human factors (gedrag van eigen medewerkers) die bij kunnen dragen aan hun cyberweerbaarheid. Sparklab heeft ook een branche-overstijgende initiatief genomen voor het Nederlands Cyber Collectief.[58] Doel van het Collectief is om een co-creatie centrum van de cybersecurity-sector te worden. Consultancies zoals Deloitte en andere bedrijven zijn daarbij betrokken.

Kader 9: Samenwerking op het gebied van verzekeringen.

Het Cyber Security Centre Metropool Regio Amsterdam (CSCMRA) is opgericht als een public private partnership: een samenwerkingsverband van onderwijs en het bedrijfsleven in de Regio Amsterdam. Het werk van het CSCMRA richt zich op het verbeteren van cybersecurity onderwijs. Daarnaast zal binnen het CSCMRA ook

[54] www.verzekeraars.nl
[55] www.verzekeraars.nl
[56] www.vvponline.nl
[57] Dit bouwt op eerdere pilots van Delta Lloyd (inmiddels overgenomen door Nationale Nederlanden). Delta Lloyd had in 2017 een tijdelijke pilot uitgevoerd met een cyberverzekering voor MKB-bedrijven. Crisismanagement, dataherstel, aansprakelijkheid, bedrijfsschade en verlies van geld, maakten deel uit van het modulair product .
[58] www.nederlandscybercollectief.nl

een Cyber Security Innovatielab worden ontwikkeld samen met het bedrijfsleven, MBO, HBO en WO.[59]

Het Shared Research Programma (SRP) Cybersecurity is een onderzoeks- en innovatieprogramma waarin TNO en haar partners samenwerken met als doel de cybersecurity te verbeteren door middel van innovatieve technologieën en processen. De huidige partners van het programma zijn TNO, ABN AMRO, Rabobank, ING, Achmea en de Volksbank[60].

7.3.2 Sectorale samenwerkingen: enkele voorbeelden

In de private sector wordt ook in nationaal en internationaal verband samengewerkt aan cybersecurity-innovatie. Een voorbeeld uit vele, uit de energiesector is het European Network for Cyber Security (ENCS). ENCS coördineert standaardisatie initiatieven, toegepast onderzoek, en andere activiteiten van haar leden en partners (Nederlandse en Europese bedrijven, kennisinstellingen).

Veel cybersecurity-innovatie komt ook uit de financiële sector, en ook in deze context zijn een aantal interessante voorbeelden te noemen; zoals die geïnitieerd door De Nederlandsche Bank (zoals TIBER-NL voor red teaming); als ook het Verbond van Verzekeraars (zie Kader 9).

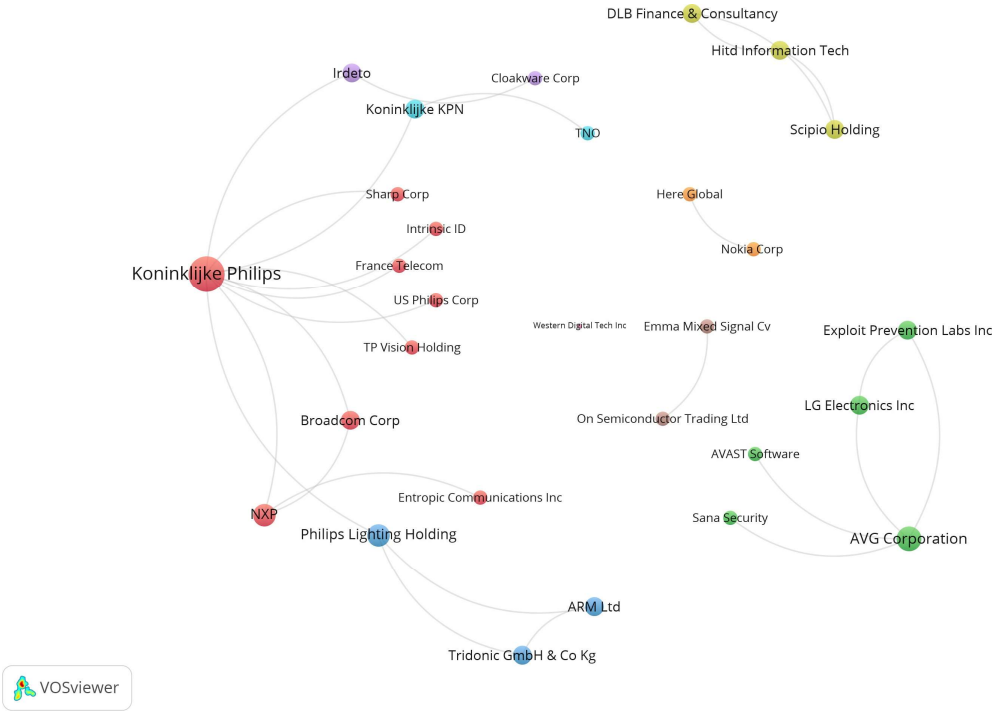
7.4 Samenwerken in de praktijk

De bibliografische analyse (CWTS, 2019) heeft ook inzicht gegeven in samenwerking binnen een traditioneel innovatiemodel (zie hoofdstuk 5). Samenwerking kan ook uitmonden in het samen publiceren of in het gezamenlijk aanvragen van octrooien of het gezamenlijk publiceren in wetenschappelijke tijdschriften of in conferentieverslagen. De netwerken van de samenwerking van Nederlandse actoren op het gebied van uitvindingen is weergegeven in Figuur 4 en op het gebied van wetenschappelijke publicaties in Figuur 5.[61]

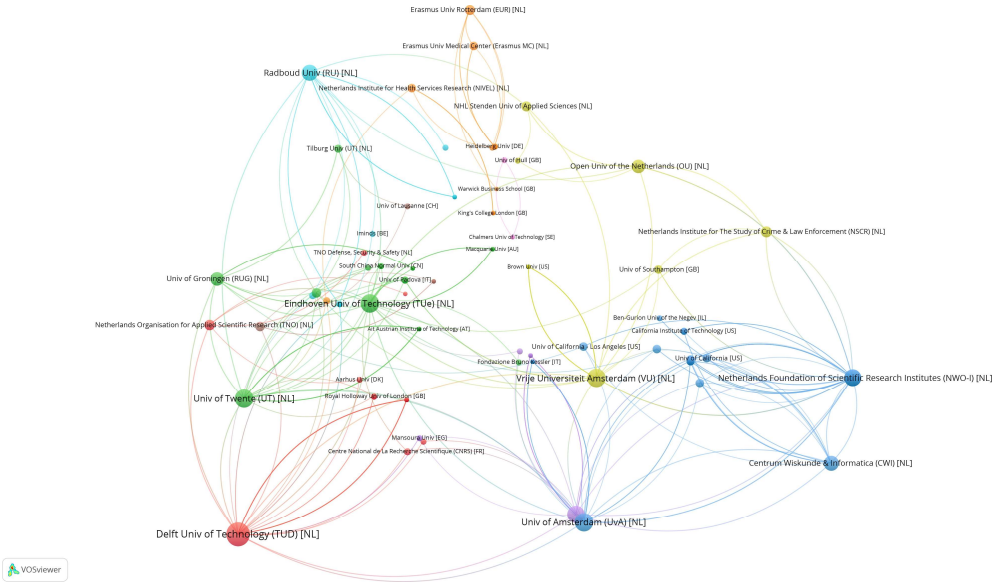
[59] Onder de initiatieven: i) (2018-2019) Practoraat Cyber Security in samenwerking met het lectoraat Cybersafety aan de NHL (Noordelijke Hogeschool Leeuwarden); en ii) (2018-2019) Doorlopende leerlijn Cyber Security: mbo - ad - hbo – wo - Het ROC van Amsterdam en de Hogeschool van Amsterdam werken samen met bedrijven in de publiek private samenwerking van het Cyber Security Centre MRA aan een doorlopende leerlijn cyber security. Deze leerlijn begint bij het ROC van Amsterdam en krijgt een vervolg in een AD opleiding en een volledig HBO-opleiding aan de HvA. Er zijn tevens gesprekken geïnitieerd om een research master opleiding te ontwikkelen, die door de HvA en de VU aangeboden gaat worden (2019). Samen met het Cyber Security Centre Metropoolregio Amsterdam ontwikkelt de Hogeschool van Amsterdam (HvA) de Ad Cybersecurity, een nieuwe tweejarige hbo-opleiding.

[60] www.tno.nl

[61] Voor het maken van deze figuren is gebruik gemaakt van het programma VOSviewer (www.vosviewer.com). Een compleet overzicht van het aantal samenwerkingspartners op basis van gezamenlijk publiceren van wetenschappelijke artikelen of het gezamenlijk aanvragen van octrooien van de Nederlandse actoren staat vermeld in het CWTS rapport. Ook de gedetailleerde overzichten van deze samenwerkingsrelaties per Nederlandse actor zijn te vinden in hetzelfde rapport.



Figuur 4: Samenwerkingsverbanden van Nederlandse actoren bij uitvindingen



Figuur 5: Gezamenlijke publicatie relaties - co-publicaties - van Nederlandse actoren

Uit de citatieanalyse blijkt dat de technische universiteiten Delft, Eindhoven en Twente de meeste wetenschappelijke publicaties op hun naam hebben staan. Zij zijn ook de zwaartepunten wanneer wordt gekeken naar samenwerkingsrelaties.

Gezamenlijk publiceren van wetenschappelijk artikelen door Nederlandse actoren gebeurt doorgaans met partners buiten Nederland.

In de context van het internationale onderzoeks- en innovatieprogramma ITEA zijn tussen 2000 en 2019 tien cybersecurityprojecten geïdentificeerd waaraan Nederlandse partners meegedaan hebben. In deze projecten hebben de 33 geïdentificeerde Nederlandse actoren binnen uitgebreide internationale verbanden samengewerkt (gemiddeld 4,7 landen en 22 partners per project). De meest actieven partijen waren TU Eindhoven, Philips Electronics, Thales, Technolution, TNO, en Almende (zie Annex 2).

De kwantitatieve analyse, maar ook overige literatuur en resultaten van de interviews, maakt duidelijk dat het niet mogelijk is te spreken van dé cybersecurity-innovatieketen in Nederland: er wordt op een veelheid aan onderwerpen geïnnoveerd, en per onderwerp ontstaan specifieke samenwerkingsverbanden. Het gevolg is dat er meerdere samenwerkingsverbanden - micro-ecosystemen - zijn ontstaan, en dat er steeds nieuwe micro-ecosystemen bijkomen (zie Kader 10). Zo ontstaan er natuurlijke hubs rondom bedrijven (zie Kader 11), al dan niet met kennisinstellingen waar bepaalde innovatie wordt gepusht via kunstmatige hubs.

Samenwerking in de keten is echter geen vanzelfsprekendheid. Alle respondenten geven aan dat de samenwerking in de keten moeizaam verloopt. Er wordt wel samengewerkt, maar dat is dan vaak ad-hoc en voor een relatief korte periode op een onderwerp waar de partijen op dat moment even behoefte aan hebben. Als de doelen gehaald zijn, wordt de samenwerking ook weer vrij snel beëindigd.

De interviews duiden op een brede overeenstemming over de noodzaak om meer samenwerking te bewerkstelligen tussen kennisinstellingen, bedrijfsleven en overheid. Het gaat bij cybersecurity om complexe problematiek en de geïnterviewden geven aan dat het steeds lastiger wordt om daar zonder betrokkenheid van anderen adequate producten en diensten op te ontwikkelen.

Uit de interviews kwam ook naar voren dat samenwerking tussen gevestigde bedrijven en startups moeilijk tot stand komt. Startups zijn terughoudend als het gaat om samenwerking met grote gevestigde partijen omdat zij veronderstellen dat zij de macht en middelen ontberen om te kunnen profiteren van samenwerking. Maar ook universiteiten werken weinig samen met startups. Dit lijkt ingegeven door verschillen in tijdshorizon voor onderzoek en ontwikkeling.

De verschillende actoren uit de keten adresseren ieder een deel van de kennisontwikkeling van idee tot product. De belangrijkste rationale voor veel van de publieke kennisinstellingen voor het doen van onderzoek is het verbreden en verdiepen van de kennisbasis in Nederland. Private partijen daarentegen innoveren voornamelijk om hun concurrentievermogen te vergroten. Het ‘cyberveilig maken van Nederland’ is voor de keten als geheel geen uitgangspunt voor het doen van onderzoek en innovatie.

Startups en MKB-bedrijven geven verder aan dat ze niet of nauwelijks samenwerken met andere partijen, zoals bijvoorbeeld universiteiten. Op die manier blijft veel innovatie onzichtbaar voor andere spelers in de keten, zolang deze startups er niet in slagen om een product naar de markt te brengen.

Hoewel de publieke kennisinstellingen geacht worden zich meer te richten op het toepassen en naar de markt brengen van kennis (valorisatie), blijkt in de praktijk dat dit moeilijk van de grond komt. Uit de recent door TNO en NWO uitgevoerde sterkte-zwakte analyse blijkt bijvoorbeeld dat het lastig is om samenwerking met in Nederland gevestigde cybersecurity-bedrijven op een structurele, meerjarige wijze vorm te geven (TNO-NWO 2019).

Begin jaren 2000 is het concept van een digitaal (business) ecosysteem ontstaan. In een discussiepaper van de Europese Commissie uit 2002 werd de visie van het digitale business ecosysteem neergelegd.[62] Met de visie werd beoogd om alle bedrijven, en met name de MKB-bedrijven in de EU te laten profiteren van de nieuwe economische kansen die, de toen nog relatief nieuwe ICT, met zich mee zouden brengen: meer innovatie, meer groei, meer banen. Door een bredere adoptie van ICT zouden spontaan nieuwe verbindingen tussen én netwerken van technologische-, economische- en kennisactoren ontstaan. Deze zouden een economisch bevorderend, transformerend effect hebben. Een op open source software gebouwde infrastructuur zou het proces faciliteren. Lokale initiatieven zouden zich vrij, verder uitbreiden naar sectorale, regionale, nationale, en internationale netwerken van netwerken. Als belangrijkste uitdagingen voor het bereiken van de visie werden beschouwd: tekort aan kennis, skills, en entrepreneurship; tekort aan technologische oplossingen en interoperabiliteit; investeringskosten; complexiteit van regelgeving; en te kort aan kapitaal. De visie werd daarna verder theoretisch uitgewerkt en praktisch geïmplementeerd. Het ecosysteem-paradigma werd later ook in andere dan het digitale domein toegepast. In het visiedocument werd echter geen aandacht besteed aan de (cybersecurity)risico's die zouden kunnen ontstaan door een steeds grotere complexiteit en wederzijdse afhankelijkheid.

Kader 10: Wat is een innovatie-ecosysteem?

Uit het onderzoek komt verder naar voren dat er onvoldoende coördinatie en samenwerking is in kennisontwikkeling en -uitwisseling tussen de actoren in de keten van lage naar hoge TRL-niveaus. Hierdoor zijn er aanwijzingen dat kennis 'op de plank blijft liggen' en onbruikbaar wordt omdat het veroudert.

Wanneer actoren op eigen initiatief wel kiezen voor samenwerking op het gebied van onderzoek en innovatie in de keten, dan is dat meestal op ad-hoc basis en van relatief kortstondige duur. De meeste samenwerking is hierbij gericht op technologieontwikkeling. Partijen vinden elkaar op een onderwerp en wanneer dat tot succes heeft geleid, wordt de samenwerking niet automatisch voortgezet op nieuwe onderwerpen. Uit de interviews komt ook naar voren dat de duur van de samenwerking wordt bepaald (en verder beperkt) doordat de investeringen in innovatieprocessen in de sector binnen twee jaar rendement moeten opleveren. Het is daardoor lastig om op een thema een langdurige samenwerking aan te gaan.

[62] www.digital-ecosystems.org

Steeds meer strategische samenwerkingsverbanden van uitsluitend industriële partners zijn ontstaan op het gebied van cybersecurity (maar nog niet structureel). In sommige gevallen gaat het om gezamenlijke inspanningen van industriële partners als gevolg van nieuwe wetgeving en om te compenseren voor het gebrek aan specifieke standaarden op dat gebied. Dit kan leiden tot bepaalde vormen van procesinnovatie, maar ook marketinginnovatie. Een voorbeeld hiervan is de strategische samenwerking rondom het GRCcontrol softwareproduct van het bedrijf CompLions die oplossingen biedt voor digital governance, risk compliance cybersecurity en privacy. Atos, Cofian, Grip IT, Northwave en Traxion zijn enkele partners in dit samenwerkingsverband. Afnemers van het product zijn overheidsinstellingen, banken, verzekeraars, andere industriële bedrijven en zorgpartijen.

Een andere categorie van strategische samenwerkingsverbanden van uitsluitend industriële partners kan tot product en marketing innovatie leiden. Met name kleine softwareleveranciers die zeer gespecialiseerde oplossingen ontwikkelen, maken hier gebruik van door gezamenlijk complementaire cybersecurity deel-producten als één complete oplossing aan te bieden en op deze manier beter aansluiten op de marktvraag.

Ook rondom individuele actoren, zoals grote bedrijven of multinationals, kunnen mini-innovatie ecosystemen ontstaan waarin wordt samengewerkt in onderzoek en innovatie. KPN is daarvan een voorbeeld. Cybersecurity, naast IoT, networks of the future en data & analytics, is een van de innovatieprioriteiten van KPN. Cyber security diensten, automated breach analysis, home network security, analytics software, human factor, post quantum cryptografie, future networks, next generation security en quantum internet zijn slechts enkele innovatieonderwerpen die samen met een gevarieerd netwerk van Nederlandse en internationale partners ontwikkeld worden.

Binnen de CISO labs werkt KPN samen met enkele Nederlandse universiteiten aan (post-quantum) cryptografische oplossingen; samen met TU Delft wordt gewerkt aan een Border Gateway Protocol (BGP) observatory prototype voor verbeterde monitoring en threat intelligence; next-generation security onderzoek wordt uitgevoerd binnen één van de EU Quantum Technology Flagship projecten - de Quantum Internet Alliance - dat al een eerste quantum backbone link gelegd heeft tussen Den Haag en Delft. Guest Hacker programma's en de Cyber Central foundation (2017) - een samenwerking tussen KPN en Cisco, Dearbytes and McAfee - zijn andere initiatieven van KPN.[63]

Via KPN Ventures wordt ook in (internationale) cybersecurity startups geïnvesteerd. Op dit gebied is ook een samenwerking aangegaan met het Security of Things Fund. Overnames van innovatieve bedrijven (bijv. DearBytes and QSight IT) en investeringen (bijv. in Cybersprint en SecurityMatters) zijn andere relevante activiteiten van KPN.

Kader 11: Mini-ecosystemen rondom individuele actoren.

Uit de interviews komt ook naar voren dat de op cybersecurity-innovatie gerichte samenwerking vooral plaatsvindt tussen universiteiten, TNO en de grotere (deels buitenlandse) bedrijven. Startups en MKB-bedrijven zijn in deze context nauwelijks in beeld: zij werken individueel op hun eigen stukje van de TRL-schaal. Dit beeld lijkt te worden onderschreven door een analyse van de op het innovatieve MKB-bedrijven gerichte EU-programma's van EIT Digital. Voor de periode 2010-2019 zijn slechts zes Nederlandse innoverende actoren geïdentificeerd.[64] Het valt daarbij op dat binnen de context van deze instrumenten de geïdentificeerde actoren niet of

[63] www.quantum-internet.team

[64] De deelname van MKB-bedrijven in Europees onderzoek in het cybersecurity-domein lijkt in zijn algemeenheid gering. Aan het op het MKB gerichte EU-SME Instrument zijn er voor de periode 2014-2021 bijvoorbeeld slechts vier Nederlandse actoren geïdentificeerd.

nauwelijks samenwerken met andere MKB-bedrijven, hoewel daar wel de mogelijkheid voor is. De inschatting van de geïnterviewden is dat er mogelijk nog veel ‘verborgen’ en ongebruikt innovatievermogen in de keten zit, met name bij startups en kleine ondernemingen.

In Nederland zijn veel samenwerkingen in het domein van cybersecurity nog gericht op informatiedelen over mogelijke dreigingen en incidenten, om zo de bewustwording en het kennisniveau van de samenleving te verhogen (Verhagen, 2016). Denk aan samenwerkingen tussen partijen in de financiële sector, het NCSC en Nederlandse opsporings-, inlichtingen- en veiligheidsdiensten. Een goed voorbeeld hiervan zijn de Information Sharing and Analysis Centers (ISACs). Wat opvalt is dat deze samenwerkingen specifiek zitten op informatiedelen en het netwerk vergroten, maar vaak niet op samen innoveren.

8 Waarom: drivers en barriers voor innovatie

8.1 Inleiding

Dit hoofdstuk beschrijft de incentives maar ook de barriers voor de primaire actoren in de keten om aan onderzoek en innovatie te doen. Beleidsincentives door de overheid (beleidsinitiatieven en de bijbehorende set van instrumenten) zijn, op verzoek van het ministerie van EZK apart beschreven, in hoofdstuk 9.

Onderzoek en innovatie wordt ook gestuurd door wet en regelgeving die de aspecten (zie hoofdstuk 2) van cybersecurity adresseert (zie (Meulen, 2015)). Er is veel veranderd op dit gebied in de afgelopen jaren. Een rapport van het Rathenau Instituut (Munnichs et al., 2017) stelt echter dat “Wetgevingstrajecten […] te veel tijd in beslag [nemen] en de technologische ontwikkelingen op het gebied van ICT gaan te snel.” Het rapport wijst er echter vervolgens wel op dat zorgplichten en aansprakelijkheidswetgeving een grote rol spelen in het garanderen van de veiligheid van digitale producten. Annex 6 beschrijft de voor de Nederlandse context meest relevante wetten en regels. In het kader van dit onderzoek worden deze als een gegeven beschouwd, en niet nader geanalyseerd.

Dit hoofdstuk leunt op de resultaten van de analyse van de literatuur en met name de interviews. Een gevolg is dat het onderzoek weinig (additionele) drivers heeft gevonden voor innovatie. Daarnaast ontbreken kwantitatieve gegevens om opinies en meningen in perspectief te kunnen plaatsen.

8.2 Drivers

Een belangrijke driver voor onderzoek en innovatie is de grote vraag naar cybersecurity-oplossingen. De brede aandacht voor, onder andere, cybercrime en in het oog springende incidenten zorgen voor een sterk groeiende vraag naar cybersecurity-producten (Meulen, 2015).[65] Zo worden de kosten bijvoorbeeld “[van] cybercrime [voor] onze economie [geschat op] circa €10 miljard per jaar.”[66] Volgens cijfers uit een meer recente studie van het CBS (CBS, 2018) had in 2018 86% van de middelgrote en grote bedrijven in Nederland een vorm van ICT-beveiliging. Dit werk werd vaak uitbesteed aan externe leveranciers: door 37% van de grootste bedrijven en 69% van de middelgrote bedrijven. Afnemers van cybersecurity-producten en -diensten hebben een voorkeur voor Nederlandse leveranciers.

Debt- en equity financiering zijn een essentieel element voor een goed functionerend innovatie-ecosysteem. Uit de interviews komt naar voren dat de sector ervaart dat dit voldoende aanwezig is. Een mogelijke verklaring is dat de perceptie van private financiers is dat de rendementen op hun investeringen

[65] (Collier, 2019) stelt dat het er op lijkt dat als de vitale infrastructuur wordt geraakt, de meeste kosten bij de burgers terecht komen en niet bij de private eigenaren van de infrastructuur en er sprake is van marktfalen voor cybersecurity. Dit is iets waar de overheid sterk beleid op zou moeten maken: “Government has to lead the way and intervene more directly by bringing its influence and resources to bear to address cyber threats” (Collier, 2019).
[66] Bron: FD van 13/09/2019: “Het is tijd voor een Deltaplan Cybersecurity” (www.fd.nl).

(gegeven de bijbehorende risico's) in de ontwikkeling van cybersecurity-oplossingen beter zijn dan in andere sectoren. Dit lijkt ingegeven door het feit dat het domein nog relatief jong is en dat innovatie sterk kennis en technologie gedreven is. Dit impliceert echter niet dat dat er geen behoefte is aan additionele publieke financiering in de vorm van bijvoorbeeld subsidies voor het adresseren van vormen van marktfalen die geassocieerd wordt met het doen van onderzoek en innovatie.[67]

Data van De Nederlandse Vereniging van Participatiemaatschappijen (NVP) verschaft een gedetailleerd beeld van durfkapitaalinvesteringen in Nederland. Op basis van de NVP data zijn er voor de periode 1994-2018 in totaal 84 voor het cybersecurity-domein relevante durfkapitaal investeringen geïdentificeerd. Dat is 1,6% van het totaal aantal durfkapitaal investeringen. Annex 7 geeft een uitgebreide beschrijving van durfkapitaal voor cybersecurity in Nederland.

8.3 Barriers

De resultaten van de interviews suggereren dat de output van de innovatieketen onvoldoende is om de cyberveiligheid voor Nederland voldoende te waarborgen. Maar daarbij dient wel opgemerkt te worden dat er geen eenduidig beeld bestaat van wat dan nu precies het concept 'cyberveilig' is en dientengevolge hoe dit zou moeten worden ingevuld.

Veel partijen zijn daarnaast van mening dat de keten niet de bijdrage aan de Nederlandse economie genereert die in potentie mogelijk is. De overheid kan een rol spelen in deze context, maar de interviews wijzen erop dat één van de barrières (voor effectief beleid) is dat de overheid als geheel geen eenduidige visie heeft op de rol voor cybersecurity in de Nederlandse samenleving en de economie, en (dientengevolge) geen eenduidige beleidsdoelen stelt als basis om de innovatieketen te versterken.

De geïnterviewden benoemen als barrière voor innovatie verder verschillende tekortkomingen in beleid. Deze tekortkomingen worden benoemd in hoofdstuk 10.

De resultaten van het onderzoek duiden er verder op dat, naast het gebrek aan heldere beleidsdoelen, de output van de actoren wordt geremd door een gebrek aan sturing en coördinatie over de hele innovatieketen heen. De geïnterviewden refereren in deze context aan versnippering van initiatieven en een gebrek aan focus.

De innovatieketen is niet één groot ecosysteem, maar bestaat uit verschillende micro-ecosystemen georganiseerd rondom bijvoorbeeld een specifieke toepassing,

[67] Een theoretische onderbouwing voor de rol van de overheid in deze context is te geven op basis van gedragseconomie. Uit de interviews komt naar voren dat in algemene zin geldt dat bij onderzoek en innovatie in de sector vaak sprake is van een financieringsgat tussen dat wat actoren en externe financiers willen investeren op basis van hun perceptie van het potentiële rendement op hun investeringen in cybersecurityoplossingen en de kans op falen van het onderliggende onderzoek, en de bijbehorende kosten van de bijbehorende innovatietrajecten. Er zijn verschillende vormen van marktfalen die bijdragen aan dit financieringsgat. Dit vormt een rationale voor overheidsinterventie (zie (Heide, 2011)).

technologie of locatie. In de praktijk lijkt er nog onvoldoende uitwisseling van informatie en kennis tussen deze micro-ecosystemen.

Het gebrek aan samenwerking tussen universiteiten, het bedrijfsleven en de overheid wordt door veel van de geïnterviewden gezien als een beperkende factor voor succesvolle innovatie. Dit wordt ook bevestigd voor de Nederlandse cybersecurity-innovatieketen in de literatuur (Hendriks et al., 2016). Samenwerking en de onderliggende oorzaken van de moeilijkheden daarvan in de Nederlandse context worden uitgebreid beschreven in hoofdstuk 7.

De sectoren in de Nederlandse economie die worden gedreven door hoogwaardige technologie worden in zijn algemeenheid gehinderd door een gebrek aan goed opgeleide mensen). Dit geldt zeker ook voor de cybersecurity-sector in zijn algemeenheid (Hendriks et al., 2016), en meer nog voor de onderliggende onderzoeks- en innovatietrajecten in deze sectoren. De cybersecurity-innovatieketen probeert dit te adresseren door het opzetten van academies waar mensen die niet direct de juiste achtergrond hebben worden getraind om de juiste kennis en vaardigheden te verwerven. Opgemerkt dient daarbij te worden dat het doel van deze academies niet per se is om met de uitstroom aan mensen de innovatiecapaciteit te versterken. Dit onderzoek geeft verder geen eenduidig beeld over de omvang van het tekort.

Hoewel de vraag naar cybersecurity-oplossingen te groot is om het hoofd te kunnen bieden aan de zich steeds ontwikkelende dreiging, laat het onderzoek tevens zien dat de gebruikers steeds meer moeite hebben om de laatste ontwikkelingen op dit gebied te implementeren. Het gaat hier om beperkingen in de absorptiecapaciteit van zowel bedrijven als overheid. De geïnterviewde leveranciers van cybersecurity-oplossingen vragen zich soms af of hun klanten wel toe zijn aan het implementeren van de resultaten van hun innovatieprocessen. Oplossingen worden gezien als “te vooruitstrevend, en te vergaand”. Er is in brede zin een gebrek aan kennis en mensen, ook wat betreft continuïteit in mensen, om de snelle veranderingen in het domein te kunnen volgen en nieuwe toepassingen te implementeren. Dit beperkt niet alleen het toepassen van bestaande oplossingen, maar ook toekomstige innovatie, doordat de kennisvraag niet goed gearticuleerd wordt en de bijbehorende innovatieprocessen niet goed begeleid worden. Het bemoeilijkt ook het formuleren van adequaat kennis- en innovatiebeleid.

Cybersecurityleveranciers zouden hun producten graag willen door ontwikkelen in samenwerking met de klant, maar dat blijkt in de praktijk moeilijk. De bovengenoemde beperkte vraagarticulatie en absorptiecapaciteit bemoeilijkt dat. Maar ook de beperkte mogelijkheid van schaalbaarheid in Nederland ten opzichte van andere landen (Hendriks et al., 2016).

De geïnterviewden suggereren verder dat innoveren makkelijker wordt als zij meer inzicht zouden hebben in de dreigingen die afkomen op Nederland. De overheid kan daar zelf het voortouw in nemen door bijvoorbeeld veel meer en gedetailleerder dreigingsinformatie te delen.

Als laatste vermoeden de geïnterviewden dat veel onderzoek en innovatie in Nederland stokt doordat veel Nederlandse innoverende partijen worden gekocht door buitenlandse actoren. Innovatie raakt zo uit zicht, en de Nederlandse primaire actoren kunnen in dat geval ook niet meer verder bouwen op de resultaten van deze ondernemingen.

9 Cybersecurity: beleid en instrumentarium

9.1 Inleiding: scope van de inventarisatie

In dit hoofdstuk worden de instrumenten beschreven die onderzoek en innovatie in de gehele cybersecurity-innovatieketen adresseren. Om deze vormen van publieke interventie nader te kunnen duiden start het hoofdstuk met een inventarisatie van het beleid dat het kader vormt voor de set van publieke interventies.

Voor deze analyse wordt beleid gedefinieerd, op basis van (De Heide, 2011), (Schram et al., 2004) en (Howlett & Ramesh, 2003)), als: "[…] a deliberate plan of action by a government to guide decisions and achieve rational outcomes which are set out in broad objectives and goals." Een beleidsinstrument "[…] translates the plan of action and its accompanying objectives and goals as defined by a public policy into concrete interventions." Deze interventies kennen verschillende modaliteiten: subsidies, regelgeving, belastingvoordelen, etc.[68]

De inventarisatie beperkt zich niet tot instrumenten die het genereren en toepassen van kennis ondersteunen in de cybersecurity-innovatieketen. Ook publieke interventie betreffende de financiering van het vermarkten van kennis is meegenomen. Beleid dat niet specifiek cybersecurity adresseert, maar wel (middels bijbehorende publieke interventies) het innovatiegedrag van actoren in de keten tracht te beïnvloeden is ook meegenomen in de inventarisatie. Instrumenten die vormen van marktfalen in de kapitaalmarkt voor de financiering van onderzoek en innovatie op het gebeid van cybersecurity adresseren zijn beschreven in hoofdstuk 8.

In deze analyse zijn de instrumenten beschreven aan de hand van de volgende elementen:

i) Eigenaar en uitvoerder;
ii) Doelgroep / Actor: de partij die een beroep kan doen op de regeling;
iii) Belangrijkste voorwaarden om in aanmerking te komen;
iv) Innovatiemodel (open / gesloten / traditioneel);
v) Fase in het innovatietraject;
vi) Doel (kennisontwikkeling, kennisdisseminatie, etc.);
vii) Beschikbaarheid;
viii) Bedrag dat o.b.v. de regeling kan worden gevraagd;
ix) Stapelbaar met andere financieringsregelingen;
x) Overige opmerkingen;
xi) Vindplaats voor meer info.

De inventarisatie is gericht op instrumenten die op het moment van de inventarisatie (juli 2019) 'open' zijn: actief en inzetbaar voor het initiëren van onderzoek en innovatie gerelateerde activiteiten van de actoren in de cybersecurity-innovatieketen. Instrumenten die 'gesloten' zijn, maar die naar verwachting wel een rol zullen spelen in de toekomst, zijn ook beschreven.

[68] Merk hierbij op dat wanneer beleidsdoelstellingen worden geprioriteerd, en gelinkt aan specifieke instrumenten en bijbehorende budgetallocaties, men vaak spreekt van programma's.

Voor de beschrijving van beleid geldt hetzelfde als voor de beschrijving van instrumenten: alleen die initiatieven zijn meegenomen die tot doel hebben het huidige gedrag van de actoren in de keten te beïnvloeden. Voor de beleidsinitiatieven is beschreven welk departement verantwoordelijk is en wat het specifieke doel is.

De instrumenten uit de beleidsmix vormen incentives voor de actoren in de cybersecurity-innovatieketen om ook daadwerkelijke te innoveren. Het hoofdstuk sluit af met een beschrijving van de perceptie van gebruikers (actoren) van de toepasbaarheid van het instrumentarium, op basis van de resultaten van de interviews. Deze beschrijving vormt geen evaluatie van de doeltreffendheid of doelmatigheid van het instrumentarium.

De inventarisatie gaat niet in op regionale beleidsinitiatieven en interventies die de cybersecurity-innovatieketen adresseren.[69] Europees beleid en instrumentarium is slechts op hoofdlijnen beschreven.

9.2 Beleid (strategie en bijbehorende onderzoeksprogramma's)

9.2.1 Specifiek beleid op het gebied van Cybersecurity

Er is geen specifiek onderzoeks- en innovatiebeleid ten behoeve van de cybersecurity-innovatieketen.[70] Onderzoek en innovatie is onderdeel van specifiek beleid dat cybersecurity als een breed concept adresseert, of van generiek onderzoeks- en innovatiebeleid. De meest relevante ministeries in deze context zijn het ministerie van EZK, met de Rijksdienst voor Ondernemend Nederland (RVO) als verantwoordelijke voor de uitvoering van de regelingen, het ministerie van OCW, NWO als verantwoordelijke voor het uitvoeren van regelingen, het ministerie van J&V en het ministerie van Defensie.[71] Daarnaast voeren ook BuZa en BZK eigen programma's uit.

Het beschrijven van relevant en recent cybersecurity-gerelateerd beleid begint met de Kamerbrief over Informatie- en communicatietechnologie van juni 2018

[69] Zie bijvoorbeeld als regionaal initiatief: Roadmap Next Economy (Zuid Hollands Investeringsplatform), hier hangt ook een agenda aan: www.mrdh.nl. Daarnaast hebben enkele provincies subsidieregelingen voor interregionale grensoverschrijdende MKB cybersecurity-innovatieprojecten, zoals DIGIPRO en IPRO-N in Zuidoost-Nederland (Gelderland, Oost-Brabant en Limburg) en in Noord-Nederland (Drenthe, Flevoland, Overijsel, Friesland of Groningen). Deze regionale subsidieregelingen zijn gericht op innovatie met partners uit Duitsland en ondersteunen innovatieve bedrijven van conceptontwikkeling tot het bouwen van een prototype of projectontwikkeling.

[70] Dat wil zeggen: geen structureel beleid specifiek gericht op het ondersteunen van cybersecurity gerelateerd onderzoek en innovatie.

[71] NWO - een zelfstandig bestuursorgaan met als taak het bevorderen van wetenschappelijk onderzoek met wetenschappelijke en maatschappelijke impact. NWO levert een actieve bijdrage aan verschillende onderdelen van het nationale wetenschaps- en innovatiebeleid. NWO vervult verschillende rollen, waaronder het financieren, programmeren, samenbrengen en ondersteunen van wetenschappelijk onderzoek.

(ministerie van J&V, 2018b).[72, 73] Deze stelt dat: “Het kabinet …stevig in[zet] op het vergroten van de kennisbasis van cybersecurity en neemt …deze signalen [daarom] zeer serieus. In het regeerakkoord […] is € 95 miljoen structureel opgenomen voor de versterking van cybersecurity. Van dit bedrag is voor 2019 € 3,5 miljoen beschikbaar voor kennis en innovatie en vanaf 2020 een bedrag van € 5,5 miljoen.”

Bovengenoemde Kamerbrief noemt verder dat “Ter uitvoering van [de ambities met betrekking tot uitgaven aan cybersecurity-onderzoek] worden in de [Nederlandse Cyber Security Agenda] NCSA concrete maatregelen geformuleerd voor cybersecurity.”[74] De NCSA is geen specifiek onderzoeks- en innovatie beleidsinitiatief, maar het benoemt wel “[…] kennisontwikkeling als een van de zeven hoofdambities op het terrein van cybersecurity voor de komende jaren. Het versterken van voldoende en hoogwaardige ontwikkeling van zowel fundamenteel als toegepast cybersecurity-onderzoek is hiervoor cruciaal. Gericht multidisciplinair onderzoek over de gehele kennisketen heen dat zowel naar oplossingen voor de langere als kortere termijn kijkt, is van het grootste belang, zo vindt dit kabinet.”

De “Nationale Cybersecurity Research Agenda 2018 (NCSRA III)” is in bovengenoemde context benoemd als het kader voor de uitgavenambitie op het gebied van onderzoek en innovatie in de keten. De NCSRA III definieert vijf pijlers voor cybersecurityonderzoek en -ontwikkeling in Nederland: “ontwerpen, verdedigen, aanvallen, governance en privacy. Het heeft een multi- en interdisciplinair karakter (computerwetenschappen, techniek, sociale wetenschappen en geesteswetenschappen) dat antwoord moet bieden op de actuele en toekomstige problematieken in het cyberdomein.” De agenda is opgesteld door het in 2016 opgerichte dcypher; een platform van “onderzoekers, hackers, docenten, studenten, producenten, gebruikers en beleidsmakers in Nederland om kennis en kunde over cyberveiligheid te verbeteren.” De NCSRA is een agenderend document en niet een programmerend document voor de actoren in de innovatieketen. De NCSRA wordt echter ook gebruikt als basis voor, bijvoorbeeld, het formuleren van calls van NWO en de Nationale Wetenschapsagenda (NWA) of als kader voor onderzoek door ministeries (bijvoorbeeld van de NCTV / NCSC van het ministerie van J&V). Het vormt daarmee het belangrijkste kader voor een groot deel van het fundamenteel onderzoek op het gebied van cybersecurity in de innovatieketen.

De Kamerbrief stelt verder dat het kabinet structureel extra geld ter beschikking stelt voor onderzoek en innovatie (dus additioneel aan bovengenoemde ambities zoals geformuleerd in het regeerakkoord) via de NWA, het vernieuwde missiegedreven topsectoren en innovatiebeleid. Deze beleidsinitiatieven zijn generiek (d.w.z. dat zij niet specifiek cybersecurity als beleidsdoel benoemen),

[72] Kamerbrief van F.B.J. Grapperhaus, minister van Justitie en Veiligheid getiteld “Aanpak Cybersecurity kennisontwikkeling en onderzoeksinvesteringen” (26643-544) van 26/06/2018. Zie www.tweedekamer.nl.
[73] Het thema cybersecurity is ook opgenomen in de Nederlandse Digitaliseringsstrategie, van juni 2018 (Kamerstuk 26 643, nr. 541). Dit beleidsdocument benoemt ook cybersecurity, maar refereert niet specifiek aan onderzoek en innovatie op dit gebied.
[74] (NCTV, 2018a): Kamerstuk 26 643, nr. 536. Zie www.zoek.officielebekendmakingen.nl.

maar de actoren uit de keten worden wel geadresseerd. Beide initiatieven worden in de volgende paragraaf nader beschreven.

Bovengenoemde Kamerbrief benoemt ook Horizon 2020 (en het daaropvolgende Horizon Europe) als structurele additionele en generieke bron van financiering van onderzoek en innovatie. Deze Europese Kaderprogramma's zijn wat betreft structuur uniek: zij zijn beleid zowel als instrument. De kaders voor onderzoek en innovatie die gefinancierd worden via Horizon 2020 op het gebied van cybersecurity worden nader geduid in het "Digital Single Market Directive",[75] en de "Cybersecurity Act".[76]

Opgemerkt dient te worden dat, omdat de uitgaven van bovengenoemde generieke middelen niet gelabeld zijn (door bijvoorbeeld het ontbreken van een eenduidige definitie van cybersecurity), het niet inzichtelijk is (te maken) hoeveel publieke middelen er nu naar de actoren in de cybersecurity- innovatieketen stromen.

Behalve bovengenoemde structurele additionele investeringen benoemt de Kamerbrief van juni 2018 ook een serie incidentele investering in cybersecurity kennisontwikkeling:

- Een bedrag van iets meer dan € 1,5 miljoen "wordt gevormd door bijdrages verdeeld over 2018 en 2019. Verschillende andere departementen hebben aangegeven nog een deelname en een (aanvullende) bijdrage te overwegen. Het ministerie van OCW beziet via NWO een mogelijke verdubbeling van dit bedrag vanuit de NWA. […] Het ministerie […] draagt via NWO ook bij aan een brede nationale cybersecurity onderzoeksoproep vanuit het Kennis en Innovatiecontract ICT 2018 - 2019 [als onderdeel van het 'oude' topsectorenbeleid (zie hier onder)]. Deze oproep wordt momenteel ontwikkeld door NWO in samenwerking met het Nationaal Regieorgaan voor Praktijkgericht Onderzoek SIA, het platform dcypher, Team ICT en de Topsector Creatieve Industrie."
- Met een onderzoekoproep van ca. €5 miljoen wil NWO tegemoet komen aan de behoefte om brede (interdisciplinaire) onderzoekssamenwerking op het gebied van cybersecurity te faciliteren.
- Tot slot is, tijdens de behandeling van de begroting van het ministerie van J&V voor het jaar 2018, een amendement aangenomen waarin wordt geregeld dat € 410.000 wordt vrij gemaakt voor open source encryptie projecten om daarmee de ontwikkeling en versterking van encryptie te ondersteunen.

Naast de beleidsinitiatieven in bovengenoemde Kamerbrief is het in het kader van dit onderzoek ook belangrijk de 'Defensie Cyber Strategie 2018' (ministerie van Defensie, 2018a) te benoemen. Ook dit beleidsdocument beschrijft een brede strategie voor de rol en toepassing van cybersecurity, in dit geval voor het ministerie van Defensie. Onderzoek en innovatie worden daarin echter wel specifiek benoemd: "Defensie intensiveert vanaf 2019 de middelen voor onderzoek op het terrein van cyber [tot] bijna 6,5 miljoen euro per jaar. Daar waar mogelijk wordt dat samen met andere departementen gedaan, zoals ook is aangekondigd in de Nederlandse Digitaliseringsstrategie. Defensie voert samen met een aantal

[75] www.eur-lex.europa.eu.
[76] www.eur-lex.europa.eu.

andere partijen een studie uit naar de opzet, vorm en organisatie van een in 2019 op te richten ‘Cyber Innovation Hub’, waarin departementen, onderzoeksinstellingen en bedrijven samen werken aan gezamenlijke en geprioriteerde veiligheidsvraagstukken op het gebied van cyber(security). Het doel van de Cyber Innovation Hub is cyberkennis en -kunde in Nederland te versterken, innovaties en experimenten te faciliteren en een ecosysteem van partners te bouwen, om zo bij te dragen aan het reduceren van cyberdreigingen.” De NCSRA vormt ook in dit geval een belangrijk kader voor het onderzoek kennisontwikkeling zoals benoemd in de Defensie Cyber Strategie 2018.

Het ministerie van BZK heeft in 2017 de Internationale Cyberstrategie gelanceerd (BZK, 2017). Het document introduceert een zestal actielijnen: economische groei en ontwikkeling van het internet, effectieve internet ‘governance’, verdere versterking van cybersecurity, bestrijding van cybercrime, internationale vrede, veiligheid en stabiliteit en rechten en internetvrijheid. Voor de financiering speelt de (jaarlijkse) Homogene Groep Internationale Samenwerking (HGIS) -nota een belangrijke rol (BZ, 2018).

In de Rijksbegroting 2019 benoemt het ministerie van BZK een aantal initiatieven die aan cybersecurity refereren. Zo gaat er in 2019 structureel € 8 miljoen extra naar de AIVD voor de aanpak van digitale dreigingen, spionage en sabotage. In 2020 is dit nog eens € 9 miljoen en in 2021 gaat het om € 12 miljoen. Dit komt bovenop het bedrag dat bij het regeerakkoord structureel is gereserveerd voor cybersecurity. Een deel van dit extra budget wordt ingezet voor uitbreiding van de personele capaciteit en ICT-voorzieningen om de dreiging van digitale aanvallen op vitale infrastructuur in West-Europa te adresseren. Een deel wordt ook ingezet om bijvoorbeeld het bestaande pakket aan digitale voorzieningen, standaarden en afspraken zoals DigiD aan te passen aan de moderne tijd, met inachtneming van eisen wat betreft toegankelijkheid en veiligheid.[77]

9.2.2 Generiek Onderzoeks- en Innovatiebeleid

De Kamerbrief over Informatie- en communicatietechnologie van juni 2018 benoemt als pijlers voor innovatie binnen de cybersecurity-innovatieketen verschillende generieke beleidsinitiatieven op het gebied van onderzoek en ondersteuning van bedrijvigheid. In de Nederlandse context adresseert dit bedrijvenbeleid, naast bijvoorbeeld de ‘framework conditions’ voor ondernemers, ook bedrijfs-georiënteerd onderzoek. Dat laatste refereert niet alleen aan directe versterking van innovatiecapaciteit van bedrijven, maar ook aan onderzoek dat bijdraagt aan het adresseren van maatschappelijke uitdagingen. De verantwoordelijk op dit terrein ligt bij EZK, RVO voert de regelingen uit. Het Nederlandse onderzoeksbeleid heeft een veel bredere scoop: het refereert ook aan bijvoorbeeld meer fundamenteel onderzoek door universiteiten en kennisinstellingen. De verantwoordelijkheid voor dit beleid ligt bij het ministerie van OCW en NWO voert de regelingen uit. De beleidsdocumenten die het bedrijvenbeleid en onderzoeksbeleid beschrijven verwijzen naar elkaar: het zijn geen losstaande initiatieven.

[77] BZK heeft voor het implementeren van voor het ministerie specifieke initiateven de zogenaamde Agenda Digitale Overheid - NL DIGIbeter geïmplementeerd. Deze adresseert het contact tussen overheid en burgers en ondernemers. Merk op dat de Agenda Digitale Overheid niet refereert aan cybersecurity: hiervoor wordt verwezen naar de Nederlandse Cyber Security Agenda.

9.2.2.1 Onderzoeksbeleid - OCW

De contouren van het huidige Nederlandse onderzoeksbeleid bouwen op twee beleidsdocumenten: de nota “Wetenschapsvisie 2025. Keuzes voor de toekomst” uit november 2014 (ministerie van OCW, 2014), en “De waarde(n) van weten Strategische Agenda Hoger Onderwijs en Onderzoek 2015-2025” uit juni 2015 (ministerie van OCW, 2015). Op basis van het regeerakkoord en de daarin aangekondigde additionele uitgaven voor onderzoek zijn de beleidscontouren geactualiseerd en verder geconcretiseerd in de Wetenschapsbrief “Nieuwsgierig en betrokken - de waarde van wetenschap” van januari 2019.

Het belangrijkste stuk uit bovengenoemde beleidsdocumenten in de context van deze analyse is de zogenaamde Nationale Wetenschapsagenda (NWA). Deze is het resultaat van een kabinetsopdracht van 2015 aan de “Kenniscoalitie”,[78] op basis van beide bovengenoemde strategieën voor de periode 2015 - 2025, om een verbindende agenda voor onderzoek in Nederland te ontwikkelen. De uitvoering van het programma voor de NWA is belegd bij NWO, waarbij de andere partijen van de Kenniscoalitie de raad van advies vormen. De NWA wordt gebruikt om een deel van de intensivering van de publieke middelen, zoals aangekondigd in het regeerakkoord, te alloceren.

De NWA adresseert vragen die vanuit de maatschappij aan de wetenschap gesteld zijn. Door deze vragen lopen ‘routes’, die deelverzamelingen van vragen betreffen. De NWA-routes zijn uitgewerkt in het portfolio voor Onderzoek en Innovatie. De routes identificeren de terreinen waarop de Nederlandse wetenschap bij uitstek het verschil kan maken.

De 25 routes vormen zelf-organiserende netwerken die belangrijke wetenschappelijke, maatschappelijke en economische vraagstukken in de samenleving agenderen en onderzoeken. De routes worden georganiseerd door routetrekkers en boegbeelden. Via de routes van de NWA kunnen consortia voorstellen indienen en daarmee financiering aanvragen. Vanaf eind 2018 kunnen wetenschappers onderzoeksvoorstellen indienen voor de NWA. Ook consortia rondom het thema cybersecurity kunnen hieraan meedoen omdat het thema cybersecurity past binnen meerdere routes van de NWA.

9.2.2.2 Bedrijvenbeleid - EZK

Met het bedrijvenbeleid ambieert het kabinet om een “een uitmuntend concurrerend ondernemings- en vestigingsklimaat [te creëren] dat bedrijven stimuleert om duurzaam en innovatief te ondernemen.” Daartoe heeft het een gecombineerde strategie ontworpen, met een algemeen spoor dat is gericht op het ondersteunen van alle ondernemingen en een meer specifiek en gericht spoor, dat zich meer richt op het versnellen van de maatschappelijke transities.

Het generieke spoor omvat het stimuleren van innovatie, betere regelgeving, het vergroten van de toegang tot kapitaalmarktfinanciering (o.a. via de oprichting van Invest-NL), goede publieke dienstverlening voor bedrijven, het wegnemen van knelpunten bij menselijk kapitaal en op (fiscale) ondersteuning van ondernemers.

[78] De Kenniscoalitie bestaat uit de universiteiten (VSNU), hogescholen (VH), universitair medische centra (NFU), KNAW, NWO, VNO-NCW, MKB-Nederland en de instituten voor toegepast onderzoek (TNO/TO2). Deze organisaties stelden gezamenlijk, op basis van een brede uitvraag aan de Nederlandse samenleving, de Nationale Wetenschapsagenda op.

Het specifieke spoor richt zich op de maatschappelijke transities en de daarvoor van belang zijnde sleuteltechnologieën in de topsectoren met een missiegedreven innovatiebeleid. Het kabinet zet daarbij in op de realisatie van missies op de maatschappelijke thema's energietransitie en duurzaamheid; landbouw, water en voedsel; gezondheid en zorg; veiligheid, en bij de sleuteltechnologieën die de technologische (kennis)basis vormen voor het aanpakken van deze uitdagingen.

Ter illustratie van de omvang van het bedrijvenbeleid: de totale financiële middelen op de EZK-begroting bedragen zo'n € 9,9 miljard in 2019. Het grootste deel, namelijk € 8,9 miljard, gaat naar het generieke spoor: fiscale ondernemerschapsstimulering. Daarvan gaat € 2,7 miljard naar fiscale innovatiestimulering (zoals de WBSO en de Innovatiebox, zie hier onder). Voor niet-fiscale stimulering, het specifieke spoor, is ongeveer € 0.9 miljard beschikbaar voor onder meer uit directe subsidies om innovatie en ondernemerschap te bevorderen, bijdragen aan kennisinstituten (TNO, GTI's en STW) en uitvoeringsorganisaties (zoals RVO.nl).

Een belangrijk element in het specifieke spoor is het vernieuwde "Missiegedreven topsectoren en innovatiebeleid", zoals beschreven in de Kamerbrief van maart 2019 (ministerie van EZK, 2019a).[79] In deze brief wordt gesteld dat "[de] economische kansen van maatschappelijke uitdagingen en sleuteltechnologieën staan centraal in het missiegedreven topsectoren- en innovatiebeleid. [Doel van het beleid is] een concrete vertaling van maatschappelijke uitdagingen naar missies en vervolgens in een gezamenlijke aanpak om die missies te realiseren. [Daartoe zullen] de topsectoren [worden gekoppeld] aan deze missies en innovatievragen."[80]

In het kader van missiegedreven topsectoren en innovatiebeleid worden zogenaamde Kennis- en Innovatieagenda's (KIA's) opgesteld: vier op door het kabinet vastgestelde maatschappelijke thema[81] en één voor sleuteltechnologieën. Eén van de maatschappelijk thema's is relevant voor deze analyse: voor het thema Veiligheid is een specifieke missie Cyberveiligheid geformuleerd met als doelstelling: "Nederland is in staat om op een veilige wijze de economische en maatschappelijke kansen van digitalisering te verzilveren. Door in te zetten op het ontwikkelen van cybersecurity kennis en innovatie streeft Nederland ernaar om binnen vijf jaar in de top 10 van zowel de Global Cybersecurity Index als de National Cyber Security Index te staan."[82]

In de KIA's wordt voor de komende jaren aangegeven op welke kennis- en innovatieopgaven de topsectoren willen inzetten en wat daarbij de prioriteiten zijn. Het initiatief voor het opstellen van deze agenda's ligt bij de topsectoren, in samenspraak met alle relevante partners uit het veld, zoals bedrijven, departementen, de brede wetenschap, kennisinstellingen, NWO en regionale overheden. Daar waar er sprake is van synergie tussen de bottom-up benadering van de NWA en het missiegedreven innovatiebeleid zal deze worden benut. De KIA's kijken ook naar de synergie met Europese en mondiale programma's.

---

[79] Kamerbrief over missiegedreven Topsectoren- en Innovatiebeleid van 26/04/2019, zie www.rijksoverheid.nl.
[80] De Topsectoren zijn: i) High Tech Systems and Materials ii) Agri & Food; iii) Chemie; iv) Creatieve Industrie; v) Energie; vi) Life Sciences & Health; vii) Logistiek; viii) Tuinbouw & Uitgangsmaterialen; ix) Water.
[81] De maatschappelijke thema's zijn: i) Energietransitie en Duurzaamheid; ii) Landbouw, Water en Voedsel; iii) Gezondheid en Zorg; en iv) Veiligheid.
[82] De KIA Veiligheid is in oktober 2019 verschenen, zie www.hollandhightech.nl.

De KIA's zijn in juli 2019 afgerond en hebben een looptijd van vier jaar hebben (2020-2023), met een mogelijkheid tot tussentijdse aanpassing na twee jaar. De KIA's voor de maatschappelijke thema's worden geconcretiseerd in zogenaamde Kennis- en Innovatiecontracten (KIC's), waarin afspraken worden vastgelegd tussen overheden, bedrijfsleven, kennisinstellingen en mogelijk maatschappelijke organisaties over de inzet en verdeling van publieke en private middelen voor onderzoek en over valorisatie en marktcreatie. De afgelopen vier jaar werd daarin voor € 10 miljard aan publieke en private middelen geïnvesteerd. De inzet voor de komende jaren is nog niet definitief bepaald. Op 11 november 2019 is het KIC vastgesteld en ondertekend. De looptijd zal gelijk zijn aan die van de bijbehorende KIA's, met de mogelijkheid tot een tussentijdse aanpassing na twee jaar. Hierbij wordt onder andere gelet op de noodzaak tot tussentijdse actualisatie waarover partijen commitment kunnen afgeven. Voor de sleuteltechnologieën wordt de KIA vertaald in zogenaamde Meerjarige Programma's (MJP's). In deze MJP's zullen digitale technologieën zoals *artificial intelligence, cybersecurity* en *blockchain* een belangrijke rol innemen. In opzet en uitvoering zijn de MJP's vergelijkbaar met de KIC's.

9.3 Instrumentarium

Bovenstaande beleidsinitiatieven richten het instrumentarium en daarmee de publieke interventie, met als doel het gedrag van de actoren in de cybersecurity-sector te beïnvloeden en daardoor de beleidsdoelstellingen te halen. Deze paragraaf bevat een zo compleet mogelijk overzicht van in Nederland beschikbare en relevante instrumenten voor het financieren van de kennisopbouw voor, ontwikkeling en het vermarkten van cybersecurity-technologie die voortkomt uit de keten. In Annex 12 en Annex 13 worden de meest relevante instrumenten vervolgens in detail beschreven in 'factsheets' (in tabelvorm).

Publieke financiële ondersteuning voor onderzoek op het gebied van cybersecurity door kennisinstellingen is niet beperkt tot het instrumentarium zoals benoemd in Tabel . Universiteiten bijvoorbeeld ontvangen middelen uit de eerste geldstroom, dat zij vrij kunnen inzetten voor onderzoek binnen bepaalde faculteiten.[83] De NWO-instituten Nederlands Studiecentrum Criminaliteit en Rechtshandhaving (NSCR) en Centrum voor Wiskunde & Informatica (CWI) voeren ook publiek gefinancierd fundamenteel onderzoek uit op het gebied van cybersecurity. TO2 instellingen ontvangen een Rijksbijdrage die zij inzetten op dit gebied. TNO bijvoorbeeld heeft de Samenwerkingsmiddelen Onderzoek (SMO), die worden ingezet voor "samenwerkingsvormen voor kennisontwikkeling in ecosystemen t.b.v. de kennisbasis in Nederland", en (ook) gebruikt worden als cofinanciering in EU- of PPS-projecten.[84] Deze vorm van publieke financiering van innovatie op het gebied van cybersecurity is niet opgenomen in het overzicht omdat bovengenoemde organisaties de besteding van deze middelen autonoom bepalen of aan de hand van vraagsturing.

[83] De meest relevante universiteiten in deze context zijn de 3 TU's, de VU Amsterdam en de Radboud Universiteit Nijmegen.

[84] Daarnaast heeft TNO het zogenaamde Early Research Program (ERP), waarmee nieuwe kennis wordt ontwikkeld ter versterking van de technologiepositie waarmee TNO, samen met kennispartners en stakeholders, een belangrijke bijdrage kan leveren aan verschillende dringende maatschappelijke uitdagingen. In de praktijk wordt dit instrument nog niet ingezet voor onderzoek op het gebied van cybersecurity, maar dit is wel mogelijk.

De overheid kan ook via contractonderzoek actoren financieren in de cybersecurity-innovatieketen. De Europese Commissie doet dit bijvoorbeeld via zogenaamde “calls for tender”, en ook de nationale overheden zetten tenderprocessen op om kennis in te kopen. Ook deze vorm van financiering wordt niet (volledig) beschreven in het overzicht van Tabel 6 omdat het niet gezien kan worden als een structureel instrument om onderzoek en innovatie in de keten te ondersteunen.

Op basis van het overzicht van Tabel 6 kunnen geen conclusies worden getrokken over, bijvoorbeeld de breedte en mate van compleetheid van de set van instrumenten. Het feit dat bijvoorbeeld bepaalde TRL-niveaus, soorten innovatie, of actoren worden geadresseerd door veel instrumenten wil niet zeggen dat de publieke interventie afdoende is op deze dimensie. Het aantal instrumenten bijvoorbeeld zegt niets over de omvang van de beschikbare financiële ondersteuning, of de actoren en onderzoeks- innovatieactiviteiten die worden geadresseerd.

Tabel 6. Overzicht instrumentarium

Instrument	**TRL**									**Innovatiemodel**			**Doelgroep / Actor**		
	1	2	3	4	5	6	7	8	9	Open	Trad.	Gesloten	Bedrijven	Kennis.	Anders
Fiscaal															
WBSO						■	■	■	■		■	■	■		
Innovatiebox						■	■	■	■		■	■	■		
Risicodragend kapitaal en leningen															
Dutch Venture Initiative				■	■	■						■			Finan-ciers
Seed Business Angel regeling voor startups	■	■	■	■	■	■	■	■	■			■	■		
Vroege Fase Financiering (VFF)				■	■	■	■					■	■		
Innovatiekrediet MKB							■	■	■			■	■		
Garanties															
Borgstelling MBK kredieten (BMKB)				■	■	■	■	■	■	■	■	■			Banken
Prijsvragen en subsidies															
Small Business Innovation Research (SBIR) Cybersecurity						■	■	■	■	■	■	■	■		
MKB-innovatiestimulering Regio en Topsectoren (MIT)					■	■	■	■	■	■	■	■	■	■	
Veiligheid Innovatie Competitie (VIC)				■	■	■	■	■	■		■	■	■	■	
Defensie Innovatie Competitie (DIC)					■	■					■	■	■		
Subsidieregeling Cyberweerbaarheid								■	■		■	■	■		
Eurostars: subsidie internationale marktgerichte R&D				■	■	■	■			■	■	■	■		
EFRO (Europees Fonds voor Regionale Ontwikkeling)	■	■	■	■	■	■	■	■	■	■	■	■	■	■	
Opdrachten															
Defensie Technologie Projecten					■	■	■				■	■	■	■	

Instrument	**TRL**									**Innovatiemodel**			**Doelgroep / Actor**		
	1	2	3	4	5	6	7	8	9	Open	Trad.	Gesloten	Bedrijven	Kennis.	Anders
Cofinanciering															
H2020 (Secure societies / ICT / MKB programma / Fast-track to innovation)	■	■	■	■	■	■	■	■	■	■	■	■	■	■	
ITEA3 (Information Technology for European Advancement)					■	■	■	■	■		■	■	■	■	
European Defence Fund (European Defence Industrial Development Programme (EDIDP) en de Preparatory Action for Defence Research (PADR)	■	■	■	■	■	■	■	■	■	■	■	■	■	■	
Topconsortia voor Kennis en Innovatie Toeslag (PPS-Toeslag)				■	■	■	■			■	■	■	■	■	
CODEMO: Commissie Defensie Materieel Ontwikkeling						■	■	■	■		■	■	■		
Overheidsfinanciering															
NWO-calls	■	■	■							■	■			■	
NWO/NWA ORC	■	■	■							■	■			■	
Risicodragend Verkennend Onderzoek (RVO)	■	■	■	■							■	■		■	

9.4 Instrumenten in de praktijk: conclusies

Op basis van de interviews wordt in deze paragraaf de set van instrumenten die de cybersecurity-innovatieketen adresseert nader geanalyseerd. Deze analyse is geen volledige evaluatie van hun impact. Het is een nadere duiding van hun geschiktheid, op basis van een analyse van de perceptie van de actoren uit de keten van de bruikbaarheid van de instrumenten voor hun respectievelijke onderzoeks- en innovatieproces. De analyse wordt aangevuld met bevindingen uit de literatuur. De set van interviews en de beschikbare literatuur is zodanig dat alleen de beleidsmix als geheel en op een hoog abstractieniveau kan worden beschreven. Enkele instrumenten worden individueel besproken omdat hun omvang maakt dat ze belangrijk zijn voor innovatie in zijn algemeenheid. Deze paragraaf moet dientengevolge worden gezien als een startpunt voor de volgende fasen van een onderzoek naar de cybersecurity-innovatieketen.

De cybersecurity-innovatieketen wordt niet geadresseerd door één specifiek instrument, maar door een uitgebreide verzameling van veelal generieke interventies. Het beeld dat de geïnterviewden hebben over de bruikbaarheid van deze instrumentarium is verdeeld, en wijkt verder af op een aantal aspecten:

- Publieke kennisinstellingen en grotere ondernemingen lijken hun weg naar publieke ondersteuning te kunnen vinden. Zij doen dit op basis van hun eerdere ervaringen, omdat zij de capaciteit hebben op zoek te gaan naar geschikte instrumenten of misschien wel omdat de beleidsdoelstelling beter aansluit bij hun specifieke karakteristieken.[85] Kleinere ondernemingen (en dat zijn in de praktijk vooral ‘pure players’) ervaren het instrumentarium echter als sterk gefragmenteerd en slecht aansluitend bij hun specifieke wensen. De interviews duiden op een grote mate van onbekendheid met de instrumenten en de mogelijkheden die deze bieden.
- Veel van de instrumenten uit de beleidsmix focussen op het ondersteunen van technologische ontwikkelingen. Cybersecurity gaat veel verder dan dat: het betreft bijvoorbeeld ook het gedrag van gebruikers. De interviews suggereren de scope van de instrumenten te verbreden naar andere wetenschapsvelden.
- De set van instrumenten lijkt zeer breed, met interventies gericht op alle TRL-niveaus en gericht op het totale spectrum van innovatiemodaliteiten (van open tot gesloten). In de praktijk echter lijken de instrumenten zich te focussen op specifieke en traditionele doelgroepen uit de aanbodzijde (kennisinstellingen, bedrijven), in plaats van op een brede set van actoren alle geledingen van de keten (inclusief gebruikers zoals banken, politie, etc.).
- De procedures van, met name, Europese programma’s worden door veel van de geïnterviewden gezien als uitermate complex en tijdrovend. De tijd tussen indiening en toekenning van deze trajecten kan oplopen tot meer dan 8 maanden. De ontwikkelingen echter gaan zo snel dat de onderliggende onderzoeksvraag in veel gevallen tegen die tijd al niet meer relevant is.
- Private investeringen moeten daarnaast al binnen twee jaar een zekere *return on investment* opleveren. De breed opgezette en langlopende Europese onderzoeksprojecten resulteren dientengevolge niet in tijdige resultaten.

[85] Als voorbeeld om dit te illustreren: het is mogelijk dat bijvoorbeeld de taal / bewoording van bijvoorbeeld EU calls beter aansluit bij het de context van kennisinstellingen dan bij die van kleine ondernemingen.

- De set van instrumenten en bijbehorende regelgeving die onderzoek met en door bedrijven ondersteunen zijn onderhevig aan voortdurende veranderingen. Dit maakt het voor kleine ondernemingen, die niet frequent gebruik maken van publieke financiering, lastig kennis en ervaring op te bouwen met het aanvragen en toepassen van bepaalde instrumenten. Het (herhaaldelijk) gebruik van deze instrumenten wordt dientengevolge een intensief proces, dat veel capaciteit vergt.
- De geïnterviewde bedrijven stellen dat de opzet van bijvoorbeeld een specifiek loket voor toegang tot publieke ondersteuning voor de cybersecurity-innovatieketen hen zou kunnen helpen. Kennisinstellingen zien zo'n loket ook als een platform om samenwerking tussen de verschillende actoren in de keten te kunnen faciliteren. Een 'real-time' overzicht van in een jaar actieve en geplande calls waarin ook de voorwaarden worden vermeld zou ook door de private partijen in de keten zeer gewaardeerd worden.
- Wat met name de kleinere private partijen missen is een Nederlands instrument dat directe samenwerking tussen een kennisinstelling en een bedrijf subsidieert.
- Veel van de verschillende actoren die zijn geïnterviewd onderschrijven het belang van langjarige programma's om continuïteit in onderzoek te waarborgen. De snelle (technologische) ontwikkelingen vereisen echter ook meer flexibiliteit in de programmering dan nu gebruikelijk is.
- Zoals gesteld in de brief van de cybersecurity onderzoeksgemeenschap blijft de omvang van publieke uitgaven aan (fundamenteel en toepassingsgericht) cybersecurity gerelateerd onderzoek in Nederland, zoals die wordt gealloceerd via de Rijksbijdrage en 1ste geldstroom aan de publieke kennisinfrastructuur, achter bij landen in Europa, maar zeker ook daarbuiten.[86] Dit heeft een impact op de keten zelf (op de aantrekkelijkheid voor mensen en investeringen), maar ook voor de cyberveiligheid en -onafhankelijkheid van Nederland.
- Voor software-gerelateerde cybersecurity-producten geldt dat het door ontwikkelen van een idee naar gebruik - de fase waarin het product kan bewijzen dat het werkt ("proof on concept") - moeilijk is te financieren. Als deze horde in het innovatieproces genomen is, dan is verdere uitrol en opschaling - de fase waarin de return op de investeringen wordt bewerkstelligd - veel gemakkelijker. De perceptie bij de geïnterviewden is dat er voor deze fase weinig geschikte instrumenten beschikbaar zijn. De huidige set adresseert deze fase, dicht bij de markt, vooral met leningen en garanties. Voor bedrijven echter is de onzekerheid over de uitkomsten van het innovatietraject te groot om de verplichtingen, die veel van dit soort instrumenten met zich mee brengen aan te gaan. Zij zien daarom meer in directe financiering van deze fase (subsidies).
- De SBIR-regeling zou een rol kunnen spelen om bovengenoemd punt te adresseren, maar het levert geen volledige oplossing: voor sommige van de geïnterviewden is de vraag van de overheid toch te zeer leidend in het proces. De SBIR-regeling wordt wel zeer gewaardeerd door de respondenten, omdat het weldegelijk een belangrijk deel van het innovatietraject ondersteunt, maar

[86] Brief van 24/10/2017 getiteld: "Behoud en Versterking Nederlandse Cybersecurity Capaciteit - De noodzaak tot Nederlandse zelfredzaamheid gebaseerd op de nationale behoefte aan eigen hoogwaardige expertise, via kennisontwikkeling en circulatie" door Herbert Bos, Michel van Eeten, en Bart Jacobs.

bovenal omdat de tijd tussen aanvraag en toekenning met 8 weken wordt ervaren als goed werkbaar. De onzekerheid over de voortzetting van de regeling specifiek voor de cybersecurity-innovatieketen wordt gezien als een gemiste kans om de innovatieketen te versterken.

- Met de SBIR-regeling neemt de overheid in de praktijk een rol op zich als "launching customer".[87] Hierbij doet de overheid, net als bij regulier contractonderzoek, een uitvraag naar kennisontwikkeling, maar met het specifieke doel als eerste afnemer een bijdrage te leveren aan het verder succesvol naar de markt brengen van nieuwe producten. Het ministerie van Defensie heeft de rol van *launching customer* expliciet benoemd in de Defensie Industrie Strategie 2018 (ministerie van Defensie, 2018b):[88] "De focus ligt hierbij op producten die bijdragen aan de bescherming van wezenlijke veiligheidsbelangen. Het vertrouwen in Nederlandse producten bij buitenlandse overheden kan worden vergroot als aangetoond is dat de Nederlandse overheid het product operationeel toepast. Voor exportdoeleinden, zeker in de defensie- en veiligheidsmarkt, is dergelijk vertrouwen van groot belang. Daarmee kunnen nieuwe, innovatieve producten sneller bij een groter publiek terecht komen." Dit onderzoek geeft onvoldoende inzicht in de omvang en (daarmee de) relevantie van dit instrument voor het versterken van de cybersecurity-innovatieketen, maar de interviews duiden erop dat intensivering van deze rol de cybersecurity-innovatieketen verder zou kunnen helpen. Opgemerkt dient te worden dat deze rol moet passen binnen het kader van de aanbestedingsregels voor de overheid, en dat lijkt in de praktijk een brede toepassing nog te beperken.
- De belangrijkste bron voor publieke financiering van privaat onderzoek (Business Expenditure on R&D (BERD)) zijn de fiscale

[87] Zie (Dialogic, 2017). Het rapport geeft een beschrijving van de rol van het ministerie van Infrastructuur en Waterstaat als aanjager van de vraagzijde van innovatie. Het geeft daarnaast een goede theoretische beschrijving van de karakteristieken van zo'n rol.

[88] De Defensie Industrie Strategie 2018 stelt dat: "Bij verwerving [door het ministerie van Defensie in de rol van launching customer] geldt als uitgangspunt dat de Aanbestedingswet 2012 (AW2012) of de Aanbestedingswet op defensie en veiligheidsgebied (ADV) wordt toegepast. Zowel binnen de AW2012 als de ADV zijn er verschillende aanbestedingsprocedures die ingezet kunnen worden afhankelijk van de aard en inhoud van de opdracht en specifieke behoeften verbonden aan de opdracht. Daarnaast bevatten beide wetten uitzonderingsbepalingen op grond waarvan de aanbestedingswet niet behoeft te worden toegepast. Daarnaast bestaat de mogelijkheid om een prijsvraag uit te schrijven of kunnen raamovereenkomsten worden afgesloten. Aanvullend daarop staan in de ADV enkele specifieke bepalingen op het punt van gegevensbeveiliging en bevoorradingszekerheid die in de aanbestedingsprocedure kunnen worden toegepast en de nodige eisen stelt aan deelnemende marktpartijen en de wijze waarop een opdracht wordt uitgevoerd. In bijzondere gevallen kan – in afwijking van bovengenoemd uitgangspunt – indien de bescherming van de wezenlijke veiligheidsbelangen van het Koninkrijk dit vergt een beroep op artikel 346 VWEU worden gedaan. In dat geval hoeven de procedures van de AW2012 of de ADV niet te worden gevolgd. Voor een beroep op artikel 346 VWEU moet aan enkele voorwaarden worden voldaan. Dit betreft de volgende vier voorwaarden: (1) een wezenlijk belang van nationale veiligheid verzet zich tegen toepassing van de ADV, (2) het betreffende materieel moet voorkomen op een lijst van militair materieel uit 1958 wanneer de verwerving ziet op militair materieel, (3) de civiele markt mag niet worden verstoord en (4) de maatregel moet noodzakelijk en proportioneel zijn. Dat laatste betekent onder meer dat onderbouwd moet worden waarom de mogelijkheden die de ADV biedt niet voldoende zijn om de wezenlijke belangen van nationale veiligheid te kunnen waarborgen."

stimuleringsmaatregelen (WBSO en Innovatiebox).[89] De geïnterviewden refereren echter niet aan deze maatregelen als het gaat over het financieren van hun innovatieactiviteiten. Dit lijkt ingegeven door het feit dat in de praktijk deze instrumenten niet goed toepasbaar lijken voor innovatieprocessen waarin 'digitalisering' een belangrijke rol speelt. Ze lijken daarmee beperkt effectief in het stimuleren van onderzoek in een deel van de cybersecurity-innovatieketen.

- Het CPB (CPB, 2018) stelt bijvoorbeeld dat: "Bij de WBSO moeten bedrijven vooraf een aanvraag indienen, moet de eigen bijdrage aan het onderzoek goed gedefinieerd zijn en zijn alleen eigen R&D-activiteiten subsidiabel. Bij open en gedigitaliseerde R&D kan dit een struikelblok zijn – soms moet een bedrijf snel reageren en is er geen tijd om vooraf WBSO aan te vragen. En een bedrijf dat in samenwerking met andere bedrijven opensourcesoftware ontwikkelt, kan moeilijk vooraf aangeven wat het zelf doet. […] Ten slotte worden nieuwe producten steeds meer digitaal; denk aan een robotstofzuiger of AI-toepassingen in auto's. Bij de WBSO wordt desondanks onderscheid gemaakt tussen fysieke producten/processen en programmatuur, zowel bij de indiening van de aanvraag als bij de beoordeling van de aanvraag." Dit laatste refereert aan een herdefinitie van wat 'programmatuur' is en wat kan worden geadresseerd middels de WBSO. De meest recente evaluatie van het instrument stelt (Dialogic, 2019): "Met de verduidelijking van de omschrijving van programmatuur vanaf 2016 is aan de groei van de projecten met zwaartepunt programmatuur een einde gekomen. Gerekend over de gehele periode [van evaluatie] 2011-2017 is het aandeel van de sector Industrie in het aantal WBSO-gebruikers afgenomen (van 32% tot 23%) en het aandeel van de sector Informatie en Communicatie toegenomen (van 9% naar 21%)." Dit suggereert een beperking in de bruikbaarheid van de WBSO door een deel van de cybersecurity-innovatieketen als instrument voor het financieren van onderzoek. Ondanks deze beperking lijkt de WBSO wel een relevant instrument voor de keten. De evaluatie stelt dat: "Het belang van digitale concepten zoals kunstmatige intelligentie en 'machine learning' (en bijbehorende programmeertalen) in WBSO-aanvragen neemt snel toe en manifesteert zich in zeer uiteenlopende sectoren."
- Het CPB (CPB, 2018) stelt verder dat: "De Innovatiebox bevoordeelt het gesloten innovatiemodel. Een voorwaarde voor de Innovatiebox is dat het bedrijf beschikt over een 'immaterieel activum'; dit kan een octrooi, kwekersrecht of WBSO-verklaring zijn. Verder moet de bedrijfswinst toegerekend kunnen worden aan het immateriële activum. Voor een bedrijf dat kennis deelt met andere bedrijven of dat winsten behaalt uit complementaire producten kan het moeilijker zijn om hieraan te voldoen. De Innovatiebox geeft zo een (onbedoelde) prikkel aan bedrijven om te kiezen voor het gesloten innovatiemodel." Als cybersecurity wordt gezien als een maatschappelijke uitdaging, dan is een essentiële voorwaarde voor het ondersteunende missiegedreven innovatiebeleid dat het samenwerking in de innovatieketen ondersteund (zie (Goetheer et al., 2018)). Als zodanig lijkt de Innovatiebox minder geschikt voor de cybersecurity-innovatieketen.

.

[89] Ter illustratie in 2016 is een kleine 2% van BERD gefinancierd middels directe publieke financiering, en meer dan 30% door fiscale instrumenten. Voor de jaren na 2016 zal dit niet wezenlijk anders zijn.

10 Onderzoek functioneren cybersecurity-innovatieketen: conclusies

Dit hoofdstuk bevat de conclusies van de studie naar het functioneren van de cybersecurity innovatieketen in Nederland. Het hoofdstuk is zo opgeschreven dat het kan worden gelezen zonder kennis te nemen van de voorgaande hoofdstukken, als een uitgebreide samenvatting van het gehele onderzoek.

10.1 Inleiding: context en methodiek van het onderzoek

TNO heeft, op verzoek van EZK, een onderzoek uitgevoerd naar het functioneren van de cybersecurity-innovatieketen in Nederland. De conclusies van dit onderzoek worden in dit hoofdstuk samengevat aan de hand van de onderzoeksvragen die bij aanvang zijn geformuleerd om de analyse te structureren: wie innoveert, op welk gebied, onder welk innovatiemodel, waar op de TRL-schaal, met wie, en waarom (wat zijn de incentives voor bedrijven om te innoveren, en wat beperkt hen daarin)?

Het concept cybersecurity gaat in de kern over informatiebeveiliging: het waarborgen van de confidentialiteit, integriteit en beschikbaarheid van data. In brede zin zijn er verschillende niveaus van cybersecurity te benoemen: van specifieke technische toepassingen om data te beveiligen tot maatregelen die gericht zijn op het beschermen van de fundamentele rechten van burgers in het digitale domein. Globaal kunnen de volgende niveaus worden onderscheiden:

- waarborgen vertrouwelijkheid, beschikbaarheid integriteit van informatie;
- waarborgen vertrouwelijkheid, beschikbaarheid integriteit van netwerken en systemen;
- waarborgen van vertrouwelijkheid, beschikbaarheid integriteit van diensten, producten en processen;
- waarborgen van economische en bestuurlijke processen;
- waarborgen van veiligheid en integriteit van de samenleving;
- waarborgen van waarden en grondrechten.

Er is geen eenduidige definitie van het concept cybersecurity die breed wordt gedragen door de actoren uit de innovatieketen zelf, of de bijbehorende governance-structuur. Hoofdstuk 3 beschrijft het cybersecurity-domein, alsmede de werkdefinitie van het CBS die is gehanteerd in de context van dit onderzoek.

Kader 12: Cybersecurity

Uit het onderzoek is gebleken dat niet eerder een vergelijkbare exercitie naar het functioneren van de gehele Nederlandse innovatieketen heeft plaatsgevonden. Dat lijkt ingegeven door het feit dat het domein relatief jong is en veel dynamiek kent. Hierdoor is er nog geen eenduidige en breed gedragen definitie van wat cybersecurity nu precies is (zie Kader 12). Door het ontbreken van een duidelijke afbakening is er geen informatie te vinden in traditionele (bestaande) bronnen en databases, voor indicatoren zoals ‘uitgaven aan R&D’ door de actoren in de cybersecurity-innovatieketen (zie Kader 13).

Om het verzamelen van de benodigde informatie mogelijk te maken is een methodiek ontworpen, bestaande uit kwalitatieve en meer objectieve kwantitatieve methoden, om deelaspecten van de keten te analyseren. Deze methodiek kan dienen als basis voor een structurele monitoring en evaluatie van de cybersecurity-innovatieketen. Het resultaat van dit onderzoek is daarom te beschouwen als een nulmeting. De methodiek is beschreven in een separaat document (zie (TNO, 2019)). Dit document gaat ook specifiek in op de voor- en nadelen van de onderliggende methoden.

Bestaande classificaties voor het verzamelen van gegevens in databestanden van bijvoorbeeld het CBS of Eurostat (zoals bijvoorbeeld NACE) kennen geen classificatiecodes die de cybersecurity-sector representeren. Door het ontbreken van een eenduidige definitie is het daarnaast ook buitengewoon complex om in de onderliggende microdata de relevante spelers te identificeren. Een onoverkomelijk probleem in deze context is echter het schatten van de omvang van cybersecurity gerelateerde activiteiten van zogenaamde 'partial players'- actoren voor wie cybersecurity niet tot de 'core' van hun activiteiten behoort - zoals bijvoorbeeld banken. Dit maakt het in de praktijk onmogelijk een correcte schatting te maken van de totale omvang van cybersecurity-innovatie op verschillende indicatoren op basis van bovengenoemde databestanden.

Kader 13: Het gebruik van bestaande databronnen.

Voor de implementatie van de methodiek is een team van experts van verschillende onderzoeksvelden bijeengebracht, die in de loop van het onderzoek een gezamenlijke taal en werkmodus heeft gevonden. Een klankbordgroep met vertegenwoordigers uit de keten, aangevuld met enkele externe experts, heeft het onderzoeksproces ondersteund door het tussentijds beoordelen van de deelresultaten en het geven van suggesties voor verbeteringen en informatieverzameling. De klankbordgroep is zodanig samengesteld dat het een brede vertegenwoordiging is van actoren uit de innovatieketen, als ook experts op het gebied van beleidsmonitoring en -evaluatie (zie hoofdstuk 1).

De conclusies in dit hoofdstuk vormen de basis voor aanbevelingen voor het versterken van de cybersecurity-innovatieketen. Deze worden beschreven in hoofdstuk 9.

10.2 Conclusies

De nu volgende sub-paragrafen geven een kort overzicht van de resultaten van het onderzoek, gestructureerd aan de hand van bovengenoemde onderzoeksvragen: wie innoveert, op welk gebied, op welke manier, met wie, en waarom? Opgemerkt dient te worden dat sommige van deze conclusies bouwen op verschillende onderliggende hoofdstukken. Als zodanig is dit hoofdstuk niet alleen een samenvatting, maar ook een weergave van een nadere analyse en synthese van de onderzoeksresultaten.

De bij elkaar gebrachte kennis levert inzichten in het functioneren van de keten, maar roept ook nieuwe vragen op, die op hun beurt weer vragen om een nadere verdieping en uitwerking. De analogie die het onderzoeksteam in deze hanteert is de volgende: “De cybersecurity-innovatieketen is als een donkere kamer. Die belichten we met verschillende methoden. Er is niet één methode die de hele kamer kan belichten, en de gecombineerde methoden belichten ook niet de gehele kamer.” Dit impliceert bijvoorbeeld dat de conclusies die getrokken worden over het functioneren van de gehele keten gepresenteerd worden met een bepaalde mate van onzekerheid.

Kader 14: Leeswijzer conclusies.

10.2.1 Wie innoveert?

Op basis van de verschillende methodieken die zijn toegepast in het kader van dit onderzoek komt naar voren dat het Nederlandse cybersecurity-innovatielandschap heel divers is en bestaat uit een grote verscheidenheid aan categorieën actoren, samenwerkingsverbanden en initiatieven die direct of indirect een bijdrage leveren aan cybersecurity-innovatie:

- In de bibliografische analyse die is uitgevoerd door het CWTS (zie Kader 15) zijn uit de patenten dataset (die bouwt uit data uit de periode 2005 - 2014) en de sample van wetenschappelijke publicaties 51 actoren geïdentificeerd in Nederland die betrokken zijn bij onderzoek en innovatie (CWTS, 2019). Een derde van deze actoren (17) - vooral bedrijven, waaronder Philips, NXP, Irdeto en KPN - heeft uitvindingen geregistreerd binnen het domein cybersecurity. TNO is de enige kennisinstelling met zowel relevante patenten als publicaties.
- Onder meer uit de Sterkte-Zwakteanalyse (TNO-NWO, 2019) volgt dat de Nederlandse universiteiten en kennisinstellingen een gevestigde reputatie op het gebied van (cyber)security-onderzoek hebben, en beschikken over uitgebreide internationale netwerken. Zij scoren hoog wat betreft omvang van publicaties en citaties. De CWTS analyse laat zien dat meeste publicaties (tijdschriftartikelen en conferentieartikelen) in de periode 2005 - 2017 staan op naam van TU Delft, TU Eindhoven, TU Twente, VU Amsterdam, UVA, Radboud Universiteit en Leiden Universiteit.
- De Nederlandse cybersecurity-industrie is divers, en kan als volgt gekarakteriseerd worden:[90]
    - De cybersecurity-industrie bestaat uit zogenaamde ‘pure players’ - bedrijven die alleen cybersecurity gerelateerde activiteiten uitvoeren - als ook ‘partial players’ - actoren voor wie cybersecurity niet tot de ‘core’ van hun activiteiten behoort. Voor beiden is onderzoek en innovatie belangrijk, maar wel vanuit

[90] Het onderzoek heeft ook geen eenduidig beeld opgeleverd van wat dit nu betekent voor innovatie op het gebied van cybersecurity.

een andere uitgangspositie: geld verdienen aan de diensten; of als essentieel onderdeel van het veilig houden van de eigen bedrijfsprocessen of producten.
    - Er vinden veel overnames plaats in de sector, zowel door Nederlandse als internationale bedrijven. Deze overnames worden ook door bedrijven gedaan die zich niet exclusief op cybersecurity-producten richten - de zogenaamde 'partial players'. Het onderzoek heeft geen inzicht opgeleverd in wat de effecten zijn van deze overnames op innovatie in de keten.
    - Naast grote bedrijven als ASML, die zich voornamelijk op hardware (zoals halfgeleiders) richten, komen er steeds meer startups bij, die met name softwarematige cybersecurity-oplossingen ontwikkelen. Ongeveer 6% van de startups in dit specifieke segment is de afgelopen twee jaar opgericht en ongeveer 10% is een eenmanszaak.
- Bijzonder aan het cybersecurity-domein is dat ook individuen zich organiseren in samenwerkingsverbanden als open software ontwikkeling 'communities' of de 'ethical hacker community' om daarmee een belangrijke bijdrage te leveren aan innovatie in de keten.

10.2.2 Op welk gebied?

Nederlandse actoren leveren een grote bijdrage aan het totale onderzoek op het gebied van cybersecurity. Wat het aantal wetenschappelijke publicaties betreft waaraan door medewerkers van Nederlandse instellingen is meegewerkt, komt van de 28 EU-lidstaten Nederland direct na de grotere landen (het Verenigd Koninkrijk, Duitsland, Frankrijk en Spanje) en duidelijk vóór de andere lidstaten. Ook wanneer Nederland wordt vergeleken met alle op het gebied van cybersecurity actieve landen dan behoort zij tot de meest actieven. Het aantal wetenschappelijke publicaties, waarbij auteurs van Nederlandse instellingen betrokken zijn, vertoont een iets sterkere groei tussen 2005 en 2014 in vergelijking tot de EU28. Wetenschappelijke publicaties op het gebied van cybersecurity vinden voornamelijk plaats in de wetenschapsvelden 'computer science disciplines' en 'communicatie'. Relatief minder relevant lijken 'criminology & penology' en 'mathematics interdisciplinary applications'. Er is niet onderzocht of dit heeft geleid tot daadwerkelijke toepassing in cybersecurity-oplossingen.

Op grond van een additionele analyse van het internationale onderzoek-en-innovatieprogramma ITEA is een nader beeld te schetsen van actoren en richting van innovatie.[91] Aan dit Eureka programma namen tussen 2000 en 2019 in totaal 33 Nederlandse actoren deel aan tien internationale projecten. De meest voorkomende onderzoeksgebieden in deze projecten zijn: 'Internet of Things' (IoT), 'open source software', 'AI/machine learning', 'cyber-physical systems' en 'security automation'.

Op basis van de door het CWTS uitgevoerde patenten- en citatieanalyse kan geconcludeerd worden dat Nederland tot de meest relevante landen behoort wat betreft omvang van wetenschappelijk onderzoek en aantal uitvindingen (CWTS,

[91] Zie www.itea3.org.

2019).[92] Op basis van de in de dataset voorkomende octrooiclassificatie codes, kunnen ook de meest relevante technologiegebieden die betrekking hebben op de uitvindingen in het cybersecurity-domein worden geïdentificeerd. De volgende technologiegebieden zijn duidelijk aanwezig: (1) de transmissie van digitale informatie, (2) draadloze communicatie, o.a. Wi-Fi-netwerken, (3) het verwerken van digitale informatie en (4) beeldcommunicatie. Naast deze grote clusters zijn er meerdere minder omvangrijke clusters zichtbaar.

Op basis van de interviews kan verder worden geconcludeerd dat innovatie-activiteiten door met name bedrijven in de Nederlandse keten gericht zijn op wat getypeerd wordt als 'sustaining innovation': probleem-gedreven innovatie gericht op het vinden van een oplossing voor een concrete vraag uit de markt. Specifiek gaat het dan om zogenaamde 'incrementele of reactieve innovatie' (innovatie die antwoord probeert te vinden op een bestaande cybersecurity problematiek) en in mindere mate om 'proactieve innovatie' (innovatie die probeert te anticiperen op potentiele/toekomstige cybersecurity issues). Wat mist als basis voor het cyberveilig houden van Nederland in de toekomst is 'disruptive innovation'; innovatie die zich niet richt op symptoombestrijding maar op baanbrekende toepassingen die de structurele tekortkomingen in cybersecurity adresseren.

Opgemerkt dient te worden dat dit onderzoek wel in staat is gebleken inzicht te geven in de (relatieve) omvang en richting van onderzoek en innovatie in het cybersecurity-domein, maar geen eenduidig en objectief beeld oplevert van de kwaliteit daarvan. Ook andere studies bieden geen inzicht in waar de Nederlandse innovatieketen nu werkelijk goed in is. De geïnterviewden geven aan dat de kennisbasis goed is op een beperkt aantal onderwerpen, maar onvoldoende voor de uitdagingen waar we voor staan. Opgemerkt dient daarbij te worden dat er geen eenduidige visie is op wat nu precies die uitdagingen zijn.

[92] Het beeld dat de bibliografische analyse zoals uitgevoerd door het CWTS schetst wordt ondersteund door de informatie zoals gepresenteerd in de context van het TIM Innovation Monitoring Tool van de Europese Commissie: www.timanalytics.eu. Opgemerkt dient wel te worden dat hoewel de patenten database ook meer recente gegevens gebruikt, deze beperkt zijn tot EPO patenten.

In het kader van dit onderzoek heeft het CWTS een bibliografische analyse uitgevoerd om het onderzoeks- en innovatiegedrag van de actoren in de Nederlandse cybersecurity-innovatieketen nader te duiden.

Voor het onderzoek naar het innovatiegedrag van actoren in de keten is gebruik gemaakt van de meest recente operationele versie van de PATSTAT-database bij het CWTS (versie: najaar 2018). De versie van PATSTAT die is gebruikt bevat gegevens van nagenoeg alle relevante uitvindingen uit de gehele wereld waarvoor octrooiaanvragen zijn ingediend tot en met december 2016. Vanwege vertraging door de geheime fase van 18 maanden, die onderdeel is van de octrooiprocedure, of vertraging bij het opnemen van octrooipublicaties in de database is ervoor gekozen om de analyse te beperken tot de periode 2005 - 2014 om op deze wijze afkapeffecten te vermijden. Dit impliceert dat het innovatiegedrag in de periode na 2014 niet wordt gevangen in de analyse. Dit is één van de beperkingen die in zijn algemeen geldt voor statistisch onderzoek naar innovatiegedrag op basis van data op het gebied van uitvindingen. De aanname is dat het patentgedrag uit het verleden een beeld geeft van het huidige gedrag van de actoren.

Voor de analyse van het onderzoeksgedrag van actoren in de keten is gebruik gemaakt van de bij het CWTS beschikbare versies van de Web of Science database (WoS) en de Proceedings database (beide van Clarivate Analytics). Deze databases bevatten gezamenlijk een selectie van wetenschappelijke tijdschriften en conferentieverslagen die representatief wordt geacht voor het weergeven van de ontwikkelingen in de wetenschap in zijn algemeenheid. De aanname in de context van dit onderzoek is dat deze selectie ook representatief is voor het totaal aan wetenschappelijke publicaties in het cybersecurity domein. In de analyses is waar nodig rekening gehouden met verschillen tussen publicaties in conferentieverslagen en publicaties in wetenschappelijke tijdschriften. Wanneer een publicatie zowel in de WoS als in proceedings database voorkomt dan wordt zij geteld als conferentiebijdrage. In de analyses is gebruik gemaakt van publicaties uit de periode 2005–2017. Er zijn meerdere typen wetenschappelijke publicaties. In dit onderzoek zijn alleen dié publicaties meegenomen die resultaten van nieuw wetenschappelijk onderzoeken bevatten en om deze reden zijn onder meer overzichtsartikelen (review papers) buiten beschouwing gelaten.

De resultaten van het onderzoek naar het onderzoeks- en innovatiegedrag, en de methodiek die daarvoor gebruikt is, is uitgebreid beschreven het rapport van CWTS, dat de analyse heeft uitgevoerd. De rol van de bibliografische analyse in de context van het totale onderzoek is beschreven in het methodologiedocument van dit onderzoek (TNO, 2019). Dit document gaat ook specifiek in op de voor- en nadelen van de bibliografische analyse.

Kader 15: Bibliografische verantwoording.

10.2.3 Onder welk innovatiemodel?

Het onderzoek laat zien dat de innovatieketen een veelvoud van vormen van innovatie kent; van volledig open tot volledig gesloten. Binnen innovatietrajecten worden vaak verschillende innovatiemodellen gebruikt. Zo kan open-software in gesloten innovatie geïntegreerd worden of komt er uit gesloten innovatie een oplossing die uiteindelijk terecht komt in een open innovatietraject.

Het onderzoek laat verder zien dat er binnen een gesloten innovatiemodel wordt gewerkt wanneer oplossingen geheim moeten blijven. Verder zijn er geen actoren bekend die hun innovatieproces volledig gesloten implementeren. Dit wordt mede veroorzaakt doordat er veel kleine(re) actoren in het speelveld actief zijn die de

capaciteit niet hebben om alle kennis intern te ontwikkelen. Grote partijen zijn in zijn algemeenheid vaak 'partial players', en deze hebben (vooralsnog) niet de wens om het hele proces intern uit te voeren.

In de keten wordt ook gewerkt binnen een open innovatiemodel waarin nieuwe en externe actoren betrokken raken, zoals in het geval van open source softwareontwikkeling. Deze vorm van softwareontwikkeling is in de sector in sommige gevallen een valide businessmodel. Nog vaker wordt open source code geïntegreerd in innovatieve cybersecurity-oplossingen. Het faciliteren van open source creëert in deze context economisch gewin als ook disruptieve innovatie.

10.2.4 Waar op de TRL-schaal?

Uit het onderzoek blijkt dat de actoren uit het innovatiesysteem ook binnen de cybersecurity-innovatieketen opereren waar dat te verwachten is:

- Universiteiten en NWO instituten zijn vooral terug te vinden in de lagere TRL-niveaus (TRL 0 - 3). De Technische Universiteiten innoveren voornamelijk tot en met TRL 4, maar verleggen ook meer en meer hun scope tot en met TRL 7.[93]
- De Toegepast Onderzoek Organisaties (TO2) richten zich met name op TRL 4 tot TRL 7. Als het gaat om cybersecurity springt TNO eruit en in beperkte mate doet ook NLR aan cybersecurity-innovatie.
- Bedrijven zijn nauwelijks direct betrokken bij fundamenteel onderzoek. Zij opereren meestal vanaf TRL 4; maar er is sprake van een zekere mate van concentratie van hun activiteiten tussen TRL 4 en 6. Het onderzoek laat verder zien dat er in Nederland nauwelijks bedrijven actief zijn die het hele innovatieproces van TRL 0 - 9 zelfstandig kunnen uitvoeren.
- Ook startups en MKB-bedrijven opereren vanaf TRL 4. Op basis van zowel de data-analyse als de interviews is de conclusie aannemelijk dat ze in mindere mate actief zijn in de hoge TRL-niveaus 7 - 9. Een mogelijke verklaring is dat veel van deze bedrijven moeilijk zelfstandig voorbij TRL-niveau 6 komen. Dat kan betekenen dat er vooral producten worden ontwikkeld waar (nog) geen markt voor is en individuele partijen nog niet in willen investeren. Dit gebrek aan financiering in deze fase heeft tevens tot gevolg dat het voor deze partijen lastig is ontwikkelde prototypes in een realistische omgeving te testen en door te ontwikkelen - de zogenaamde 'valley of death'. Opgemerkt dient te worden dat sommige actoren als expliciete strategie hebben om na het succesvol ontwikkelen van een prototype zich te laten overnemen door een grotere gevestigde (soms buitenlandse) partij.

10.2.5 Met wie?

Het is niet mogelijk te spreken van dé cybersecurity-innovatieketen in Nederland: er wordt op een veelheid aan onderwerpen geïnnoveerd, en per onderwerp ontstaan specifieke samenwerkingsverbanden. Het gevolg is dat er meerdere samenwerkingsverbanden - micro-ecosystemen - zijn ontstaan, en dat er steeds nieuwe micro-ecosystemen bijkomen. Zo ontstaan er natuurlijke hubs rondom

[93] HBO instellingen hebben een specifieke rol in het Nederlandse innovatiesysteem. Nader duiding van hun rol en relevante in de cybersecurity innovatieketen vereist additioneel onderzoek.

bedrijven en universiteiten en kunstmatige hubs waar bepaalde innovatie wordt gepusht.

Samenwerking in de keten is echter geen vanzelfsprekendheid. De verschillende actoren uit de keten adresseren ieder een deel van de kennisontwikkeling van idee tot product. De belangrijkste rationale voor publieke kennisinstellingen voor het doen van onderzoek is het verbreden en verdiepen van de kennisbasis in Nederland. Private partijen daarentegen innoveren voornamelijk om hun concurrentievermogen te vergroten. Het ‘cyberveilig maken van Nederland’ is voor de keten als geheel geen uitgangspunt voor het doen van onderzoek en innovatie.

Hoewel de publieke kennisinstellingen geacht worden zich meer te richten op valorisatie en toepassing van kennis, blijkt in de praktijk dat dit moeilijk van de grond komt. Uit de recent door TNO en NWO uitgevoerde sterkte-zwakte analyse blijkt bijvoorbeeld dat het lastig is om samenwerking met in Nederland gevestigde cybersecurity-bedrijven op een structurele, meerjarige wijze vorm te geven.

Uit het onderzoek komt verder naar voren dat er onvoldoende coördinatie en samenwerking is in kennisontwikkeling en -uitwisseling tussen de actoren in de keten van lage naar hoge TRL-niveaus. Hierdoor zijn er aanwijzingen dat kennis ‘op de plank blijft liggen’ en onbruikbaar wordt omdat het veroudert.

Wanneer actoren op eigen initiatief wel kiezen voor samenwerking in de keten, dan is dat meestal op ad-hoc basis en van relatief kortstondige duur. De meeste samenwerking is hierbij gericht op technologieontwikkeling. Partijen vinden elkaar op een onderwerp en wanneer dat tot succes heeft geleid, wordt de samenwerking niet automatisch voortgezet op nieuwe onderwerpen. De interviews geven ook aan dat de duur van de samenwerking wordt bepaald (en verder beperkt) doordat de investeringen in innovatieprocessen in de sector binnen twee jaar rendement moeten opleveren. Het is daardoor lastig om op een thema een langdurige samenwerking aan te gaan.

Uit de interviews komt ook naar voren dat de op cybersecurity-innovatie gerichte samenwerking vooral plaatsvindt tussen universiteiten, TNO en de grotere (deels buitenlandse) bedrijven. Startups en MKB-bedrijven zijn in deze context nauwelijks in beeld: zij werken individueel op hun eigen stukje van de TRL-schaal. Dit beeld lijkt te worden onderschreven door een analyse van de op het innovatieve MKB gerichte EU-programma's van EIT Digital. Voor de periode 2010-2019 zijn slechts zes Nederlandse innoverende actoren geïdentificeerd.[94] Het valt daarbij op dat binnen de context van deze instrumenten de geïdentificeerde actoren niet of nauwelijks samenwerken met andere MKB-bedrijven hoewel daar wel de mogelijkheid voor is. De inschatting van de geïnterviewden is dat er mogelijk nog veel ‘verborgen’ en ongebruikt innovatievermogen in de keten zit, met name bij startups en kleine ondernemingen.

[94] De deelname van MKB bedrijven in Europees onderzoek in het cybersecurity-domein lijkt in zijn algemeenheid gering. Aan het op het MKB gerichte EU-SME Instrument zijn er voor de periode 2014-2021 bijvoorbeeld slechts vier Nederlandse actoren geïdentificeerd.

10.2.6 Waarom?

Drivers voor onderzoek en innovatie

Een belangrijke driver voor onderzoek en innovatie is de grote vraag naar cybersecurity-oplossingen. De brede aandacht voor, onder andere, cybercrime en in het oog springende incidenten zorgen voor een sterk groeiende vraag naar cybersecurity-producten. Zo worden de kosten bijvoorbeeld "[van] cybercrime [voor] onze economie [geschat op] circa €10 miljard per jaar."[95]

Uit de interviews komt naar voren dat de sector ervaart dat er voldoende private (debt- en equity) financiering beschikbaar is voor onderzoek en innovatie op het gebied van cybersecurity. Een mogelijke verklaring is dat de perceptie van private financiers is dat de rendementen op hun investeringen (gegeven de bijbehorende risico's) in de ontwikkeling van cybersecurity-oplossingen beter zijn dan in andere sectoren. Dit lijkt ingegeven door het feit dat het domein nog relatief jong is, en dat innovatie sterk kennis en technologie gedreven is. Dit impliceert echter niet dat dat er geen rol is voor de overheid of dat er geen behoefte is aan additionele publieke financiering in de vorm van bijvoorbeeld subsidies voor het adresseren van vormen van marktfalen.[96]

Barriers voor onderzoek en innovatie

Uit de interviews met de stakeholders komt naar voren dat zij de aanwezige incentives als beperkt ervaren. Het onderzoek van de keten heeft geresulteerd in de identificatie van de volgende barrières voor onderzoek en innovatie: i) gebrek aan visie, en gebrek aan sturing over de keten; ii) beperkte efficiëntie en effectiviteit van het bestaande instrumentarium; iii) gebrek aan goed opgeleide mensen; en iv) beperkte absorptiecapaciteit van de vraagzijde.

Gebrek aan visie, en gebrek aan sturing over de keten

De resultaten van de interviews suggereren dat de output van de innovatieketen onvoldoende is om de cyberveiligheid voor Nederland voldoende te waarborgen. Daarbij dient wel opgemerkt te worden dat er geen eenduidig beeld bestaat van wat dan nu precies het concept 'cyberveilig' is, en dientengevolge hoe dit zou moeten worden ingevuld.

---

[95] Bron: FD van 13/09/2019: "Het is tijd voor een Deltaplan Cybersecurity" (www.fd.nl).

[96] Een theoretische onderbouwing voor de rol van de overheid in deze context is te geven op basis van gedragseconomie. Uit de interviews komt naar voren dat in algemene zin geldt dat bij onderzoek en innovatie in de sector vaak sprake is van een financieringsgat tussen dat wat actoren en externe financiers willen investeren op basis van hun perceptie van het potentiële rendement op hun investeringen in cybersecurityoplossingen en de kans op falen van het onderliggende onderzoek, en de bijbehorende kosten van de bijbehorende innovatietrajecten. Er zijn verschillende vormen van marktfalen die bijdragen aan dit financieringsgat. Dit vormt een rationale voor overheidsinterventie (zie (Heide, 2011)).

Veel partijen zijn daarnaast van mening dat de keten niet de bijdrage aan de Nederlandse economie genereert die in potentie mogelijk is. De overheid kan een rol spelen in deze context, maar de interviews wijzen erop dat één van de barrières (voor effectief beleid) is dat de overheid als geheel geen eenduidige visie heeft op de rol voor cybersecurity in de Nederlandse samenleving en de economie, en (dientengevolge) geen eenduidige beleidsdoelen stelt als basis om de innovatieketen te versterken.

De resultaten van het onderzoek suggereren verder dat, naast het gebrek aan heldere beleidsdoelen, de output van de actoren wordt geremd door een gebrek aan sturing en coördinatie over de hele innovatieketen heen. De innovatieketen is niet één groot ecosysteem, maar bestaat uit verschillende micro-ecosystemen georganiseerd rondom bijvoorbeeld een specifieke toepassing, technologie of locatie. In de praktijk lijkt er nog onvoldoende uitwisseling van informatie en kennis tussen deze micro-ecosystemen.

Het doen van onderzoek en innovatie wordt in zijn algemeenheid geremd door specifieke vormen van marktfalen: positieve externaliteiten / kennisspillovers, imperfecte en asymmetrische informatie, coördinatie- en netwerkfalen, etc. De aanname is dat dit ook geld in de context van de cybersecurity-innovatieketen, en dat de onderliggende vormen van marktfalen een rationale zijn voor overheidsingrijpen. Het resulterende overheidsbeleid kan in dat geval een belangrijke impuls zijn voor de actoren om wel aan cybersecurity onderzoek en innovatie te doen. Met de bijbehorende instrumenten - de daadwerkelijke publieke interventies in de markt - kan de overheid dan trachten het onderzoeks- en innovatiegedrag van de actoren te richten.

De cybersecurity-innovatieketen in Nederland wordt in de praktijk niet geadresseerd door specifiek onderzoeks- en innovatiebeleid - dat wil zeggen: er is geen beleid specifiek gericht op het ondersteunen van cybersecurity gerelateerd onderzoek en innovatie. Onderzoek en innovatie is onderdeel van specifiek beleid dat cybersecurity als een breed concept adresseert; of van generiek onderzoeksbeleid (zoals de Nationale Wetenschapsagenda (NWA)), of generiek innovatiebeleid (zoals het bedrijvenbeleid).

Kader 16: De Nederlandse beleidscontext als incentive voor onderzoek en innovatie.

Beperkte efficiëntie en effectiviteit van bestaand instrumentarium
Uit de interviews komt verder het beeld naar voren dat de huidige set van instrumenten die onderzoek en innovatie in de keten adresseert niet effectief is:

- Publieke kennisinstellingen stellen dat de totale omvang van de financiële middelen voor cybersecurity-onderzoek en -innovatie te beperkt is om de opgave waar Nederland voor staat op dit gebied te kunnen adresseren.
- Private actoren hebben vooral moeite met de complexiteit van de instrumenten. Zij ervaren deze als ingewikkeld, met complexe procedures en regelgeving voor aanvragen en monitoring van de voortgang. De instrumenten en bijbehorende regels worden daarnaast vaak aangepast waardoor bestaande kennis over de beschikbaarheid en het gebruik van instrumenten snel achterhaald is.
- Private actoren hebben tevens kritiek op de vormgeving van de instrumenten (‘dat wat instrumenten doen’): zij missen steun voor specifieke fasen in het

innovatieproces. Voor kleine bedrijven, zoals startups, is het bijvoorbeeld problematisch de zogenaamde ‘valley of death' te overbruggen. Als deze horde in het innovatieproces genomen is, dan is verdere uitrol en opschaling - de fase waarin rendement op de investeringen wordt gerealiseerd - veel gemakkelijker. Opgemerkt dient te worden dat deze ‘valley of death’ voor cybersecurity anders is dan voor veel andere sectoren, waar innovaties vaak refereren aan (productie)procesverbeteringen. In dat geval is het voor het overbruggen van de ‘valley of death’ noodzakelijk aan te tonen dat de procesinnovatie werkt, en het product of de dienst geproduceerd kan worden. In de context van cybersecurity, en zeker als het gaat om software, is het juist noodzakelijk om de werking van de oplossing aan te tonen. Wat dan ontbreekt is een omgeving om dit uit te voeren: gebruikers (klanten) die bereid zijn het product in de praktijk te (laten) testen. De overheid zou hier een rol kunnen spelen, bijvoorbeeld als ‘launching customer’, maar de marktpartijen in de keten stellen dat deze rol onvoldoende wordt vervuld.

- De looptijd van publiek gefinancierde publiek-private onderzoekstrajecten sluit over het algemeen niet aan bij de behoeftes van bedrijven in de sector. Uit de interviews komt naar voren dat MKB-bedrijven en startups investeringen over het algemeen binnen twee jaar moeten kunnen terugverdienen. De genoemde onderzoekstrajecten hebben vaak een veel langere looptijd.
- Het huidige instrumentarium dat de keten adresseert ondersteunt vooral traditionele actoren: grote bedrijven en kennisinstellingen. Het onderzoek toont aan dat er ook andere actoren betrokken zijn bij het ontwikkelen van cybersecurity-oplossingen, die momenteel geheel buiten de scope van overheidsinterventie vallen.

Gebrek aan goed opgeleide mensen
De sectoren in de Nederlandse economie die worden gedreven door hoogwaardige technologie worden in zijn algemeenheid gehinderd door een gebrek aan goed opgeleide mensen. Dit geldt nog meer voor de onderliggende onderzoeks- en innovatietrajecten in deze sectoren. De cybersecurity-innovatieketen probeert dit te adresseren door het opzetten van academies waar mensen worden getraind om de juiste kennis en vaardigheden te verwerven. Opgemerkt dient daarbij te worden dat het doel van deze academies niet per se is om met de uitstroom aan mensen de innovatiecapaciteit te versterken. Dit onderzoek geeft verder geen eenduidig beeld over de omvang van het tekort.

Beperkte absorptiecapaciteit van de vraagzijde
Hoewel de vraag naar cybersecurity-oplossingen groot is om het hoofd te kunnen bieden aan de zich steeds ontwikkelende dreiging, laat het onderzoek tevens zien dat de gebruikers steeds meer moeite hebben om de laatste ontwikkelingen op dit gebied te implementeren. Het gaat hier om beperkingen in de absorptiecapaciteit van zowel bedrijven als overheid. Er is in brede zin een gebrek aan kennis en mensen, evenals contiuniteit van mensen, om de snelle veranderingen in het domein te kunnen volgen en nieuwe toepassingen te implementeren. Dit beperkt niet alleen het toepassen van bestaande oplossingen, maar ook toekomstige innovatie, doordat de kennisvraag niet goed gearticuleerd wordt, en de bijbehorende innovatieprocessen niet goed begeleid worden. Het bemoeilijkt ook het formuleren van adequaat kennis- en innovatiebeleid.

11 Onderzoek functioneren cybersecurity innovatieketen: aanbevelingen

Op verzoek van het ministerie van EZK bevat dit rapport een aantal aanbevelingen om de innovatiecapaciteit van de keten te versterken. Deze aanbevelingen zijn geformuleerd door het onderzoeksteam, en vervolgens getoetst tijdens een bijeenkomst van de klankbordgroep, opdat zij een bredere verankering hebben in de innovatieketen. De aanbevelingen zijn gericht op het stimuleren van de drivers en/of het wegnemen van de barrières die hoofdstuk 8 van dit rapport zijn benoemd.

De eerste set van aanbevelingen rust op het onderzoek en geeft suggesties voor de verbetering van de huidige werking van de innovatieketen. Aanvullend zijn met de klankbordgroep nog twee aanvullende aanbevelingen geformuleerd die niet direct op het onderzoek rusten, maar op de expert opinion van de leden van de klankbordgroep.

In de praktijk zijn veel van de aanbevelingen in dit hoofdstuk gericht aan de overheid. Dit wil echter niet zeggen dat de actoren in de keten geen rol hebben in het versterken van de innovatiecapaciteit van de sector. Deze scope is ingegeven door de onderliggende methodiek die gebruikt is voor dit onderzoek. De aanbevelingen bouwen sterk op de resultaten van de interviews en meer kwalitatieve literatuur. Kwantitatieve (en daarmee meer objectieve) informatie over het functioneren van de cybersecurity-innovatieketen ontbreekt vaak om bepaalde opinies en aannames in perspectief te kunnen zetten.

Voor het effectief ondersteunen van de cybersecurity-innovatieketen zou de overheid desalniettemin een aantal aanpassingen moeten doorvoeren in de huidige beleidsmix, om de effectiviteit van overheidsinterventie te vergroten:

1. De cybersecurity-innovatieketen is gebaat bij specifiek (thematisch) beleid dat structurele ondersteuning geeft aan alle actoren die een rol spelen in de bredere cybersecurity-innovatieketen.
2. De continuïteit van het instrumentarium moet worden gewaarborgd. Het instrumentarium moet meer zekerheden bieden door zowel de samenstelling, modaliteiten en regelgeving meerjarig vast te leggen. De instrumenten moeten tevens meerjarig voor inschrijving open blijven (d.w.z. geen ‘calls’ die een beperkte looptijd hebben, en op een specifiek moment sluiten).
3. De overheid zou haar rol als ‘launching customer’ in de innovatieketen moeten intensiveren.[97] De actoren vragen in deze context specifiek om voortzetting en intensivering van de SBIR-regeling voor het cybersecurity-domein.
4. Om de effectiviteit van publieke ondersteuning te vergroten zouden langjarige onderzoeksprogramma’s en bijbehorende projecten een grotere flexibiliteit moeten kennen in het aanvraagproces bij de uitvoering. Dit om

[97] Zie (Dialogic, 2017) voor richtlijnen voor de invulling van de overheid als launching customer (www.dialogic.nl).

de dynamiek in de keten beter te kunnen volgen. Dit impliceert het creëren van mogelijkheden tot kortlopende trajecten, en het tussentijds evalueren en aanpassen van trajecten. Het impliceert daarnaast ook een versimpeling in het proces van aanvragen van ondersteuning, en een verkorting van het proces van evaluatie van projectvoorstellen.

5. De overheid zou de effectiviteit van het instrumentarium kunnen verbeteren door de participatiegraad van met name kleinere ondernemingen, zoals startups, te verhogen. Dat kan bijvoorbeeld door procedures te vereenvoudigen, de bekendheid van ondersteuningsmogelijkheden te vergroten en één loket specifiek voor de cybersecurity-innovatieketen op te zetten.

Het onderzoek maakt verder duidelijk dat innovatie in het cybersecurity-domein wordt gehinderd door een gebrek aan coördinatie: tussen vraag naar en aanbod van kennis; op het gebied van samenwerking bij kennisontwikkeling en innovatie-activiteiten (van laag naar hoog TRL-niveau, en tussen de verschillende actoren in de keten); tussen verschillende micro-ecosystemen die de innovatieketen vormen. Voor een verbetering in de regie en sturing in de keten gelden de volgende aanbevelingen - waarbij alle actoren uit de keten, de overheid en de governance structuur, maar ook niet-traditionele actoren een rol hebben:

6. Voor regie en sturing is het noodzakelijk beter inzicht te hebben in het functioneren van de innovatieketen. Structurele monitoring en evaluatie is daarom vereist. De hier gepresenteerde analyse is een eerste stap in die richting, maar een follow-up is noodzakelijk, met medewerking van additionele actoren zoals het CBS, en additionele methoden om de keten op een objectieve manier te kunnen beschrijven en monitoren.
7. Om de uitwisseling van informatie en kennis binnen de veelzijdige cyberinnovatie-keten te versterken is het aan te bevelen een (virtuele) entiteit in het leven te roepen. Het lijkt het meest effectief om daarbij te bouwen op bestaande publieke en private initiatieven en organisaties en hun bijbehorende kennis, maar met inachtneming van de tekortkomingen van de huidige structuren. Het doel ervan is dat het bestaande initiatieven verbindt en eventuele witte vlekken invult, teneinde kennis, inzicht en overzicht over de gehele kennis- en innovatieketen te bundelen. Deze entiteit ontsluit kennis, helpt partijen bij het koppelen van vraag en aanbod en fungeert tevens als katalysator en aanjager, legt verbindingen tussen partijen en initiatieven en signaleert nieuwe ideeën. Actoren uit de keten - overheden, bedrijven, universiteiten, hogescholen en kennisinstellingen - zullen in een nader uit te denken governance structuur allemaal een rol moeten spelen.
8. Door het delen van dreigingsinformatie met de actoren in de keten kan de ontwikkeling van cybersecurity-innovatie worden gestuurd. Dit geeft richting aan samenwerking voor vormen van dreiging die actoren niet eenvoudig individueel kunnen oplossen. De coördinerende entiteit zoals hierboven benoemd zou hierbij een rol kunnen spelen als een mechanisme om deze informatie op een verantwoorde manier te delen.
9. De huidige beleidsmix moet worden uitgebreid om coördinatie in de innovatieketen te bevorderen. Ook niet-traditionele actoren in de keten zouden ondersteund moeten kunnen worden door de bestaande instrumenten.

10. Het instrumentarium moet daarnaast de toegang van private actoren tot de publieke kennisinfrastructuur verbeteren, ook op de hogere TRL-niveaus. Zo is publieke financiering voor één-op-één samenwerking tussen publieke en private partijen bij onderzoek en innovatie beperkt beschikbaar.

Uit het onderzoek, en dan met name uit de interviews, komt het beeld naar voren dat bovengenoemde aanbevelingen alleen niet voldoende zullen zijn om Nederland cyberveilig te maken. Een aantal meer structurele veranderingen in beleid en de bijbehorende doelstellingen zijn daarvoor noodzakelijk. De nu volgende aanbevelingen betreffen uitgangspunten en hebben te maken met (politieke) keuzes over de rol van cyberveiligheid in de Nederlandse samenleving én economie. Hiermee kan onderzoek en innovatie in de gehele keten beter worden gestuurd - iets dat nu ontbreekt volgens de geïnterviewden. Maar verdere concretisering en daadwerkelijke opvolging van deze aanbevelingen vergt nog wel een analyse die verder gaat dan dit onderzoek, bijvoorbeeld door een benchmark naar hoe dit in het buitenland wordt ingevuld.

1. De overheid moet haar rol in het cyberveilig maken van de Nederlandse samenleving heroverwegen. Het vitale belang van een veilig, betrouwbaar en beschikbaar digitaal domein betekent dat de overheid hier een bijzondere verantwoordelijkheid voor draagt. De complexiteit van het domein en de daaraan verbonden cybersecurity-uitdagingen is zo groot dat de samenleving deze niet vanzelf kan adresseren. Het is noodzakelijk dat de overheid vaststelt wat cyberveiligheid is, en welk (ambitieniveau wat betreft) beleid daarvoor nodig is. De aanbeveling is daarom, in lijn met de visie van bijvoorbeeld het World Economic Forum (WEF), aspecten van cybersecurity te beschouwen als een publiek goed (WEF, 2019).
2. In het verlengde hiervan moet ook een discussie worden gevoerd over de mate van autonomie die voor Nederland in het digitale domein zeker moet worden gesteld.[98] In lijn met de conclusies van de Wetenschappelijke Raad voor het Regeringsbeleid (WRR), is een discussie nodig over welke mate van ‘strategische autonomie’ wenselijk en haalbaar is voor Nederland (WRR 2019).

[98] In deze context wordt ook wel gesproken van ‘digitale soevereiniteit’.

Een keuze voor ‘cybersecurity als publiek goed’ (en een duidelijke invulling van ‘autonomie' in de Nederlandse context) vergroot de mogelijkheden voor de overheid om in te grijpen op het gebied van het cyberveilig maken van Nederland, en daarmee het sturen en aanjagen van onderzoek en innovatie op dit thema. Maar het impliceert ook een radicale verandering in vormgeving, governance en onderliggende filosofie van beleid en bijbehorend instrumentarium, omvang van middelen, etc.

- Eén van de belangrijkste noties in deze context is dat de publieke interventie gestuurd moet worden op effectiviteit, en niet zozeer op doelmatigheid.
- Beleid moet daarnaast inzetten op zowel sustaining als disruptive innovatie. Sustaining innovatie om de huidige dreigingen effectief het hoofd te kunnen bieden en disruptive innovatie, dat wil zeggen innovatie die zich niet richt op symptoombestrijding maar op baanbrekende toepassingen die de structurele tekortkomingen in cybersecurity adresseren. Dit is noodzakelijk om op de lange termijn de digitale weerbaarheid van de samenleving structureel te vergroten.
- Duidelijk moet worden welke kennisniveau hiervoor noodzakelijk is, wat het economisch belang van de sector is en welke capaciteit beschikbaar moet zijn om de integriteit en weerbaarheid van de samenleving op de lange termijn te kunnen waarborgen. Op grond van deze discussie kan dan een heldere kennis en innovatiebehoefte worden geformuleerd met duidelijke meerjarige missies en bijbehorend instrumentarium. Op grond daarvan kan ook worden nagedacht over wat de implicaties hiervan zijn voor bijvoorbeeld onderwijs.
- Hiertoe moet worden vastgesteld welke kennis moet worden opgebouwd (TRL 0-3), toegepast (4-6), en naar de markt gebracht (7-9).
- De overheid moet vervolgens gezamenlijke programmering van publieke (en private) partijen in het cyberinnovatie-domein vormgeven. Hierbij moet voldoende generieke financieringsruimte beschikbaar worden gesteld voor het bevorderen van disruptieve innovatie.

Kader 17: Cybersecurity als 'publiek goed', en beleidsimplicaties.

12 Literatuur

In het onderzoek een grote hoeveelheid rapporten en publicaties geraadpleegd. Hieronder de lijst waarnaar in dit uiteindelijke rapport naar wordt verwezen in de tekst.

AWTI (2018b) *Verspreiding. De onderbelichte kant van innovatie*.

Bower, J.L., Christensen, C.M. (1995). *Disruptive Technologies: Catching the Wave*. Harvard Business Review.

Centraal Bureau voor de Statistiek CBS (CBS) (2018). *Cybersecuritymonitor 2018. Een verkenning van dreingingen, incidenten en maatregelen*. CBS: Den Haag.

Centraal Planbureau (CPB) (2016) *Kansrijk Innovatiebeleid*.

Centraal Planbureau (CPB). (2018). *Digitalisering R&D*. CPB Policy Brief 2018/13.

Chesbrough, H. W., & Appleyard, M. M. (2007). *Open Innovation and Strategy*. California Management Review, 50(1), 57-76.

Collier, J. (2019). *The UK's Alphabet Soup: The Organization of Cybersecurity Actors Protecting Critical National Infrastructure*. Centre for Technology & Global Affairs. UK: n.02.

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

dcypher (2018). *NCSRA III. National Cyber Security Research Agenda*.

Dialogic (2017) *Innoveren in de keten: IenW als launching customer*.

Dialogic (2019). *Evaluatie WBSO 2011 - 2017*.

Diffy W. (2003). *Risky business: Keeping security a secret*.

EARTO (2014). *The TRL Scale as a Research & Innovation Policy Tool, EARTO Recommendations*.

ENISA (2017). *ENISA overview of cybersecurity and related terminology*.

ETSI (2018). *CYBER; Middlebox Security Protocol; Part 3: Profile for enterprise network and data centre access control*. ETSI TS 103 523-3 V1.1.1

Europese Commissie (EC) (2014). *Mededeling van de Commissie, Kaderregeling betreffende staatssteun voor onderzoek, ontwikkeling en innovatie*. (2014/C 198/01)

Europese Commissie (EC) (2018). *Special eurobarometer 480*.

Europese Commissie (EC) (2019). *The Digital Economy and Society Index (DESI)*.

Goetheer, A., Zee, F. van der & Heide, M. de (2018) *De staat van Nederland innovatieland 2018. Missies en 'nieuw' missiegedreven beleid*. TNO. Den Haag.

Hansen, M., & Birkinshaw, J. (2007). *The Innovation chain.* Harvard Business Review.

Heide, M.J.L. de (2011). *R&D, Innovation and the Policy Mix*. Tinbergen Instituut Research Series (No. 508). Thela Thesis, Amsterdam.

Hendriks, A., Brand, D., Turk, K., Kocsis, V., Veld, D. in 't & Smits, T. (2016) *Economische kansen Nederlandse cybersecurity sector*. Verdonck Klooster & associates & SEO.

Hippel, E von (1988). *Sources of Innovation*. New York NY: Oxford University Press

Howlett, M. and M. Ramesh (2003). *Studying Public Policy: Policy Cycles and Policy Subsystems*. Oxford University Press.

The Hague Security Delta (HSD) (2018). *Jaarverslag 2018*.

ITU, (2017). *Measuring the Information Society Report 2017*.

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

KIA (2017) *Kennis- en Innovatieagenda 2018-2021. Maatschappelijke uitdagingen en sleuteltechnologieën. Topsectoren beleid*.

Meulen, N van der (2015). *Investeren in Cybersecurity*. RAND Europe, in opdracht van WODC.

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) (2017). *"Digitaal bruggen slaan" Internationale Cyberstrategie naar een geïntegreerd internationaal cyberbeleid*.

Ministerie van Buitenlandse Zaken (BuZa) (2018). *Homogene Groep Internationale Samenwerking -HGIS- nota 2019*.

Ministerie van Defensie (2018a). *Defensie Cyber Strategie 2018. Investeren in digitale slagkracht voor Nederland*.

Ministerie van Defensie (2018b). *Defensie Industrie strategie 2018.*

Ministerie van Defensie, Ministerie van J&V & Ministerie van EZK. (2019). *Missiedocument Veiligheid. Thema Veiligheid. Always ahead of the threat*.

Ministerie van Economische Zaken en Klimaat (EZK) (2007). *Kamerbrief Actieplan "Nederland open in Verbinding*".

Ministerie van Economische Zaken en Klimaat (EZK) (2018), Kamerbrief *"Naar een missiegedreven innovatiebeleid met impact."* Kamerstuk 33009, nr. 63.

Ministerie van Economische Zaken en Klimaat (EZK) (2019a). *Kamerbrief Innovatiebeleid*. (33 009, nr. 70), april 2019.

Ministerie van Economische Zaken en Klimaat (EZK) (2019b). *Monitor Nederland Digitaal: monitor-nederlanddigitaal.nl*.

Ministerie van Economische Zaken en Klimaat (EZK) (2019c) *Missiegedreven Topsectoren- en Innovatiebeleid*. Rijksoverheid.

Ministerie van Justitie en Veiligheid (J&V) (2018a). *Departementaal Jaarverslag*.

Ministerie van Justitie en Veiligheid (J&V) (2018b). *Kamerbrief Aanpak Cybersecurity kennisontwikkeling en onderzoeksinvesteringen*.

Ministerie van Onderwijs, Cultuur en Wetenschappen (OCW) (2014). *Wetenschapsvisie 2025. Keuzes voor de toekomst*.

Ministerie van Onderwijs, Cultuur en Wetenschappen (OCW) (2015). *De waarde(n) van weten Strategische Agenda Hoger Onderwijs en Onderzoek 2015-2025*.

Ministerie van Onderwijs, Cultuur en Wetenschappen (OCW) (2019). *Strategische agenda hoger onderwijs en onderzoek. Houdbaar voor de toekomst*.

Munnichs, G., Kouw, M & Kool, L (2017). *Een nooit gelopen race - Over cyberdreigingen en versterking van weerbaarheid*. Den Haag, voor het Rathenau Instituut.

Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) (2011). *Nationale Cyber Security Strategie 'Slagkracht door samenwerking'*.

Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) (2018a). *Nederlandse Cybersecurity Agenda (NCSA), Nederland digitaal veilig*.

Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) (2018b). *Cybersecuritybeeld Nederland 2018.*

Nationaal Coordinator Terrorismebestrijding en Veiligheid (NCTV) (2019). *Cybersecuritybeeld Nederland (CSBN) 2019*.

Nationaal Cyber Security Centrum (NCSC) (2018). *Leidraad Coordinated Vulnerability Disclosure*.

OECD (2015). *Frascati Manual 2015: Guidelines for Collecting and Reporting Data on Research and Experimental Development, The Measurement of Scientific, Technological and Innovation Activities*. OECD Publishing, Paris.

OECD/Eurostat (2018). *Oslo Manual 2018: Guidelines for Collecting, Reporting and Using Data on Innovation, 4th Edition, The Measurement of Scientific, Technological and Innovation Activities*. OECD Publishing, Paris.

Oldengarm, P & Holterman, L. (2019). *Innovatie is het onderscheid tussen een leider en een volger. Inventarisatie kennisbehoefte cybersecuritysector*. Rapport voor Cyberveilig Nederland.

Porter, M.E. (1990). *The competitive advantage of nations*. The Free Press.

Schram, A.J.H.C., H.A.A. Verbon en F.A.A.M Van Winden (2004). *Economie van de Overheid*. second ed.. Academic Service.

TNO (2019a). *Methodologie beschrijving cybersecurity-innovatieketen.* TNO 2019 R11839.

TNO (2019b). *Github experiment*. TNO 2019 R12035.

TNO-NWO (2019). *Zelfevaluatie TNO-NWO*. TNO-NWO 2019 SR.

Verhagen, H. (2016). *De economische en maatschappelijke noodzaak van meer cybersecurity. Nederland digitaal droge voeten*.

WEF (2019). *We must treat cybersecurity as a public good. Here's why.*

Zielstra, A. (2017). *TNO whitepaper cybersecurity. Slagkracht is nodig om Nederland te beschermen en economische kansen voor cybersecurity te verzilveren*. TNO: Den Haag.