Defensie & Veiligheid
Oude Waalsdorperweg 63
2597 AK Den Haag
Postbus 96864
2509 JG Den Haag

www.tno.nl

T +31 88 866 10 00
F +31 70 328 09 61

TNO-rapport

TNO 2020 R12224

EZK Verdieping Valorisatieketens: Verkenning van het ecosysteem en waardenetwerk Automated Security

Datum	December 2020
Auteur(s)	Dr. D. Tiggelman T.C.C. van Schie MA I.N. Melman MSc G.R. Jansen-Ferdinandus V. Szijarto Drs. ir. J.T. Rabbie Ir. N.E.J. Bonenkamp
Aantal pagina's	45 (incl. bijlagen)
Aantal bijlagen	1
Opdrachtgever	Ministerie van Economische Zaken en Klimaat
Projectnaam	EZK: Verdieping Valorisatieketens
Projectnummer	060.45190

Samenvatting

Cybersecurity in de Nederlandse samenleving is van steeds groter belang en daarmee ook het versterken van innovaties op dit gebied. In dit project hebben we naar de valorisatieketen van Automated Security (AS) gekeken, in het bijzonder hoe deze versterkt zou kunnen worden om daarmee de Nederlandse samenleving weerbaarder te maken tegen digitale dreigingen en verstoringen. Automated Security is een breed begrip en reikt grofweg van simpele tot zeer geavanceerde automatiseringsoplossing (producten, diensten en technieken) binnen alle fases van de cybersecurity processen (preventie, monitoring & detectie en respons), die worden ingezet voor het verlichten van de werkdruk van de (schaarse) cybersecurity specialisten en om de effectiviteit van de beveiliging vergroten.
Dit onderzoek naar de valorisatieketen van AS bestaat uit twee componenten: een marktverkenning om een schets te maken van het ecosysteem AS en een waardenetwerk analyse waarin met een brede blik naar het innovatie ecosysteem van twee (mogelijke) toepassingsgebieden wordt gekeken. Tezamen vormt dit het fundament voor de routekaart Automated Vulnerability Research (AVR). Het onderzoek is onderbouwd door literatuuronderzoek en aan de hand van interviews en gesprekken met experts. Door de aard en tijdsduur van dit verkennend onderzoek is de nadruk gelegd op het vormen van een algemeen beeld. Vervolgonderzoek is nodig om het volledige Nederlandse AS-landschap in kaart te brengen.

De marktverkenning Automated Security. Partijen zijn ingedeeld in ‘type organisatie’ (kennisinstelling, cybersecurity bedrijf of eindgebruiker) en vervolgens geplot op het ecosysteem binnen drie fases van de cybersecurity processen: preventie, monitoring & detectie en respons. Partijen ontwikkelen innovaties voornamelijk binnen de preventie en monitoring & detectie fases. Er worden diensten aangeboden binnen de categorie respons, maar er lijkt niet sterk ingezet te worden op het ontwikkelen van innovaties.
Interviews hebben geleid tot een zestal overkoepelende bevindingen: (1) invloed van automatisering op de rol van de security specialist is nog gering, (2) steeds meer bedrijven gebruiken cloudomgevingen die over geïntegreerde security tooling beschikken waardoor het aanbod en ontwikkelpotentieel verschraalt, (3) in Nederland wordt fundamenteel onderzoek gedaan naar AS door diverse vakgroepen en vanuit verschillende perspectieven, (4) de vraag naar Automated Security oplossingen is diffuus omdat klanten niet op de hoogte zijn van de mogelijkheden en vereisten, (5) de internationale markt levert vooruitstrevende automatiseringsoplossingen, en ten slotte (6) speelt *vendor lock-in* van grote technologie (Big Tech-)bedrijven bij enkele respondenten een rol in relatie tot hun aanbod of potentieel van AS-oplossingen.

De barrières voor innovaties op het gebied van Automated Security zijn: (1) gebrek aan slagkracht van Nederlandse cybersecurity bedrijven ten opzichte van Big Tech-bedrijven, (2) veelbelovende Nederlandse bedrijven en start-ups worden overgenomen door buitenlandse partijen, (3) beperkte toegang en beschikbaarheid van testdata, (4) gebrek aan sturing en visie van de overheid op het gebied van cyber security in het algemeen, (5) beperkt absorptievermogen van bedrijven om innovaties in de organisatie te implementeren.

Waardenetwerk analyse. Verder is er gekeken naar de Nederlandse financiële- en energiesector als mogelijke toepassingsgebieden van AS, met behulp van waardenetwerk analyse. Hiermee wordt het complexe innovatie ecosysteem binnen deze sectoren visueel gemaakt, waardoor we aan de hand van verschillende afbeeldingen onze bevindingen kunnen toelichten. Op basis van literatuuronderzoek en interviews hebben wij getracht het innovatie ecosysteem op het gebied van cybersecurity in kaart te brengen, waar AS innovatie een onderdeel van uitmaakt.

De waardenetwerk analyse in de *financiële sector* laat een netwerk zien waarin onder andere kennisinstellingen, cybersecurity bedrijven en consumenten van financiële diensten een rol spelen. De financiële sector is in grote mate gedigitaliseerd en er is steeds meer sprake van decentralisatie van de financiële dienstverlening. Het is ook een aantrekkelijk doelwit voor cybersecurity aanvallen, doordat er vaak direct geld mee te verdienen is. De belangrijkste bevindingen die in onze waardenetwerk analyse naar voren zijn gekomen, zijn dat: (1) er een groot aantal samenwerkingsverbanden is binnen deze sector, maar dat de regie hierover ontbreekt, (2) grootbanken vaak centraal staan in deze samenwerkingsverbanden en hiernaast nauw betrokken zijn bij cybersecurity onderzoek op universiteiten, (3) er afstemming nodig is binnen de verschillende afdelingen binnen een bedrijf om cybersecurity innovatie, bijvoorbeeld op het gebied van AS, te laten slagen, en (4) toezicht veelal is gericht op de directe financiële dienstverlener, terwijl deze steeds meer verbonden raakt met en afhankelijk is van derde partijen voor bijvoorbeeld de IT-infrastructuur. De leveranciers van deze IT-infrastructuur zijn hiernaast ook vaak Big Tech-bedrijven, welke zelf ook zijn begonnen met het leveren van financiële diensten en dit in de toekomst mogelijk willen uitbreiden. Al deze aspecten zijn in meer of mindere mate relevant om de toepassing van AS in deze sector te laten slagen.

Voor de waardenetwerk analyse van de *energiesector*, hebben we ons gericht op de elektriciteitssector als onderdeel hiervan. Kennisinstituten zijn niet opgenomen in het waardenetwerk, omdat wij geen aanwijzingen hebben gevonden dat zij actief zijn in het cybersecurity innovatie ecosysteem binnen deze sector. Een cyberaanval gericht op de elektriciteitssector kan grootschalige stroomuitval tot gevolg hebben, wat een enorme maatschappelijke impact heeft. Verder is het een sterk gereguleerde sector, waarbij de netbeheerders centraal staan in het cybersecurity innovatie ecosysteem. Samenvattend zijn de bevindingen uit onze analyse dat (1) operationele technologie (OT) cybersecurity vaak nog complexer maakt dan wanneer deze alleen gericht is op IT, alsmede dat er sprake is van een versmelting tussen OT en IT, (2) innovatie op het gebied van cybersecurity hoofdzakelijk wordt gedreven door de intrinsieke verantwoordelijkheid voor leveringszekerheid, (3) netbeheerders onderling geen concurrenten zijn, maar leveranciers bijvoorbeeld wel, wat invloed heeft op de innovatiekracht en (4) toezicht op het gebied van cybersecurity in deze sector wordt uitgevoerd aan de hand van open normen en (nog) niet is gericht op alle spelers in de leveringsketen. Verder is er naar voren gekomen dat AS in principe met open armen zou worden verwelkomd in deze sector. Voor de netbeheerders kan het aantrekkelijk zijn voor de IT (en wellicht ook de OT) bescherming, terwijl het voor de toezichthouder kan helpen bij het in kaart brengen van (systeem)risico’s.

Overeenkomsten tussen beide sectoren. Tijdens ons onderzoek is duidelijk naar voren gekomen dat het tekort aan cybersecurity personeel in beide sectoren een

acuut probleem is, wat nadelig is voor de innovatiekracht. Ook is er in beide sectoren sprake van verstrekkende digitalisatie en decentralisatie, wat nieuwe en disruptieve spelers op de markt brengt die onderdeel gaan uitmaken van de leveringsketen. Hiernaast zijn het vooral de grote partijen die het budget, personeel, kennis en incentives hebben om te innoveren op het gebied van cybersecurity. Dit geeft deze grote spelers hierdoor ook de macht om de innovatieagenda te bepalen. De kleinere partijen vallen doorgaans sneller buiten de samenwerkings- en kennisdelingsverbanden en zijn in mindere maten betrokken bij innovatietrajecten, omdat de nadruk vaak meer ligt op het opstellen van een solide basis op het gebied van cybersecurity. Een groot verschil tussen de sectoren is echter dat zowel de onderliggende motivatie als de impact van een (grootschalige) cyberaanval inherent anders is.

De resultaten van de marktverkenning en de waardeketen analyse dragen bij aan het fundament van de routekaart AVR. Het doel van de routekaart AVR is om de nationale capaciteiten op het gebied van AVR te versterken en uit te bouwen. Met de inzichten verkregen uit de analyses laten we zien welke van de gesproken partij in welke ontwikkelfase(s) een rol speelt. Daarnaast is een overzicht gemaakt van de geconstateerde ‘v*alleys of death’*. Ten slotte worden vier sporen beschreven om invulling te geven aan de routekaart: 1) Onderwijs en opleiding, 2) Versterken van samenwerking middels fundamenteel onderzoek, 3) Toepasbaar maken van producten en 4) Ontwikkelen van een fieldlab voor samenwerking.

Inhoudsopgave

1 Inleiding en context

Voor een goed functionerende en concurrerende economie en voor het algemeen vertrouwen in de digitale samenleving wordt innovatie op het terrein van cybersecurity steeds belangrijker voor Nederland. Dit geldt des te meer daar Nederland één van de meest gedigitaliseerde samenlevingen ter wereld is (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)). De strategie toont aan dat Nederland in vergelijking met andere OECD-landen vroegtijdig ministeriële (departementale) aandacht heeft verwerkt in beleidsdocumenten. Om mogelijkheden voor het versterken van de cybersecurity innovatieketen te verkennen heeft het Ministerie van Economische Zaken en Klimaat (EZK) in 2019 aan TNO de opdracht gegeven om het innovatielandschap in Nederland in kaart te brengen (TNO, 2019 R10769). Uit dit onderzoek is naar voren gekomen dat er geen sprake is van één ecosysteem, maar dat het Nederlandse cybersecurity-innovatielandschap zeer divers is. Het bestaat uit verschillende categorieën van actoren, samenwerkingsverbanden en initiatieven. Om deze ecosystemen te kunnen versterken is het van belang om voor specifieke onderdelen in kaart te brengen op welke manier innovatie plaatsvindt en waar de knelpunten liggen. EZK heeft gekozen om in deze verdiepingsslag de focus te leggen op een belangrijk onderwerp uit de submissie cyberveiligheid in de KIA veiligheid: Automated Security (AS).

De verankering van het belang van Automated Security wordt gevonden in de KIA Veiligheid en de Missie cybersecurity. Zie onderstaand kader voor een uitgebreide toelichting.

KIA Veiligheid
De Kennis- en innovatieagenda (KIA) Veiligheid is een verdere uitwerking van het maatschappelijke thema veiligheid zoals beschreven in het missiegedreven topsectoren- en innovatiebeleid. De missies uit de KIA zijn opgesteld door vakdepartementen in consultatie met vele partijen en topsectoren en vervolgens goedgekeurd door het kabinet. De uitwerking van deze missies heeft geleid tot een aantal Meerjarige Missiegedreven Innovatie Programma's (MMIP's), en moet leiden tot vele vormen van publiek-private samenwerking en het benutten van economische kansen voor grotere en kleinere bedrijven. De KIA's zijn 'first and foremost' een inventarisatie van de kennis en innovatiebehoeften bij bedrijven, departementen, de brede wetenschap, kennisinstellingen, NWO en regionale overheden.

Missie Cyberveiligheid
De KIA Veiligheid is opgesteld door betrokken topsectoren High Tech Systemen en Materialen, Creatieve Industrie, Logistiek, Water & Maritiem en Team Dutch Digital Delta. De missie cyberveiligheid stelt zichzelf ten doel dat Nederland in staat moet zijn "om op een veilige wijze de economische en maatschappelijke kansen van digitalisering te verzilveren." Kennisontwikkeling en innovatie op het gebied van cybersecurity zijn noodzakelijk om dreigingen in het digitale domein tegen te gaan. Het doel van deze missie is cyberkennis en - kunde in Nederland te versterken, onderzoek en innovatie te faciliteren en een ecosysteem van experts

en organisaties te bouwen. Om de Nederlandse cybersecurity kennisbasis te kunnen versterken is actieve, effectieve en meerjarige samenwerking over de gehele keten een randvoorwaarde.

Op het gebied van cybersecurity onderzoek en innovatie verbindt de NCSRA III 10 verschillende disciplines met elkaar via de vijf pijlers. Een van deze pijlers is Defence, waar Automated Security een onderdeel van is (Verminderen van de schaarste aan cybersecurity capaciteit: Naast opleiding en training ook automatisering van cybersecurity taken, optimaliseren van werkprocessen, pooling & sharing van cybersecurity professionals, kennis en (ondersteunende) middelen, meer focus en preventieve maatregelen, certificering en regulering van professionals).

In dit project zijn twee onderzoeken gedaan:

- *Marktverkenning*: Hierbij wordt een verkenning gedaan van het ecosysteem Automated Security door het verkennen van de markt op basis van deskresearch en interviews.
- *Waardenetwerk analyse*: Een waardenetwerk analyse kijkt met een brede blik naar een innovatie ecosysteem wat niet slechts een eendimensionaal beeld oplevert van een waardeketen gericht op één actor (zoals een waardeketenanalyse), maar brengt een complex netwerk in kaart brengt, waarin verschillende rollen zichtbaar zijn, welke met elkaar verbonden zijn door middel van waarde-uitwisselingen (financieel, personeel, etcetera).

Er wordt een verkenning gedaan van het waardenetwerk Automated Security om als fundament te dienen voor de routekaart Automated Vulnerability Research (AVR) waar in hoofdstuk 4 naar wordt verwezen.

De twee onderzoeken zijn verwerkt in dit onderzoeksrapport. In hoofdstuk 2 laten we een verkenning van het ecosysteem Automated Security zien, gebaseerd op een marktverkenning. De marktverkenning is gedaan aan de hand van deskresearch en interviews met een aantal partijen uit het ecosysteem. We laten zien in welk deel van de cybersecurity keten (preventie, monitoring/detectie tot respons) deze partijen zich in het ecosysteem bevinden, waar zij aan werken (innovatie-initiatieven) en welke barrières voor innovatie zij ervaren.
In hoofdstuk 3 beschrijven we de waardenetwerk analyse Automated Security binnen de financiële- en energiesector. Het waardenetwerk, zoals hierboven beschreven, is in kaart gebracht door deskresearch en interviews partijen uit de respectievelijke sectoren. Uit de analyse komt naar voren waar deze partijen zich in het netwerk bevinden, welke belangen een rol spelen en waar de knelpunten liggen voor innovatie op het gebied van cybersecurity binnen de sectoren. Daarnaast laten we zien of er verschillen zijn tussen het waardenetwerk van de financiële en energiesector. Waar liggen de overeenkomsten, waar de verschillen en wat zegt dit.
In hoofdstuk 4 zetten we de informatie uit de waardenetwerk analyses om tot de fundering van de routekaart AVR. Welke spelers hebben een rol binnen de vijf ontwikkelfasen (*Discovery/basic research, Technology development, Validation and demonstration, Integration and Operationalization, Deployment*), wat zijn de "*valleys of death*" om te komen tot product ontwikkeling en het gebruik daarvan en welke sporen zijn belangrijk om tot het doel van de routekaart te komen.

2 Ecosysteem Automated Security

Dit hoofdstuk beschrijft een verkenning van het Nederlandse ecosysteem met betrekking tot Automated Security. Het ecosysteem is in kaart gebracht aan de hand van een marktverkenning op basis van deskresearch en interviews. Door de breedte van het veld en de korte doorlooptijd van het onderzoek is het niet mogelijk geweest om alle relevante partijen te interviewen en is het resulterende overzicht dus niet volledig. De geïnterviewde partijen zijn echter zo gekozen dat de verschillende rollen binnen het ecosysteem vertegenwoordigd zijn. Hierdoor beslaat het resulterende overzicht toch zoveel mogelijk de breedte van het ecosysteem. In bijlage 1A staan de geïnterviewde partijen benoemd. De marktverkenning heeft zich gericht op partijen in de cybersecurity keten. De overkoepelende partijen op het gebied van beleid, toezicht en wet- en regelgeving zijn niet in het onderzoek meegenomen.

Het onderzoek is gericht op het Nederlandse innovatielandschap, buitenlandse partijen zijn dus buiten scope gelaten. In de interviews is echter wel ter sprake gekomen hoe het Nederlandse innovatielandschap zich verhoudt tot het buitenland. Bevindingen hierover zijn als resultaat in de marktverkenning opgenomen.

2.1 Introductie Automated Security

Automated Security is een veelomvattend begrip waar een grote diversiteit aan producten, diensten en technieken onder wordt geschaard. Automated Security kan worden ingezet in alle fases van het cybersecurity proces (preventie, monitoring & detective en respons). Wat al deze (deel)oplossingen gemeen hebben is dat een IT-proces en/of systeem gebruikt wordt ter vervanging van, of als ondersteuning van handmatige acties voor cybersecurity. Automatiseringsoplossingen zijn voor organisaties over het algemeen om twee redenen interessant. Deze oplossingen kunnen a) de werkdruk van (schaarse) cybersecurity specialisten verlichten en b) de effectiviteit van de beveiliging vergroten.

a) Het ontlasten van cybersecurity specialisten is belangrijk, omdat de hoeveelheid veiligheidsmeldingen en de informatie die verwerkt moet worden zo groot is dat het niet meer mogelijk is om dit handmatig te verwerken. Het ontlasten van specialisten gebeurt in de praktijk al door het automatiseren van met name low-level taken die één of twee relatief simpele vervolghandelingen vereisen. Voorbeelden van repetitieve sequentiële handelingen uit een Security Operations Center (SOC) zijn die geautomatiseerd kunnen worden: het aanmaken van tickets, het prioriteren van incidenten, false positives uit monitoring- en detectiesystemen identificeren en verwerken, statistieken opstellen, implementeren van open source pentesting tooling, informatie uit verschillende systemen kopiëren naar andere systemen, het in quarantaine plaatsen van bestanden en firewall- en DNS-regels aanpassen.
b) Automated Security oplossingen kunnen ook worden ingezet om de effectiviteit van de beveiliging van systemen te verhogen door het geautomatiseerd verzamelen, correleren en interpreteren van grote hoeveelheden data uit complexe systemen. Dit is belangrijk, omdat de aanvallende partijen ook in toenemende mate automatiseringstechnieken gebruiken. Het wordt dus steeds lastiger om alleen met handmatige verdedigingsmechanismen te werken. Het resultaat hiervan kan zijn dat een specialist gerichter onderzoek kan doen en

besluiten kan nemen op basis van de informatie die het systeem beschikbaar maakt, of dat het systeem zelfstandig handelingen onderneemt zonder tussenkomst van een mens. Machine learning technieken kunnen onderdeel zijn van Automated Security oplossingen om toezicht te houden op bijvoorbeeld afwijkingen in gedrag en instellingen van applicaties of gebruikers. Voorbeelden van grote hoeveelheden data die door middel van AS-technieken gebruikt en gecombineerd kunnen worden: informatie over kwetsbaarheden in broncodes, cyber threat intelligence feeds, gebruikersstatistieken van end-points, monitoring en (intrusion) detectie informatie van systemen en software.

De breedte van het begrip Automated Security wordt ook zichtbaar in de mogelijke oplossingen die het kan bieden. Het spectrum reikt van ‘simpele’ automatiseringsoplossingen tot zeer ‘geavanceerde’ oplossingen. . Een ‘simpele’ rule-based automatiseringsoplossing blokkeert, bijvoorbeeld, automatisch een IP-adres als de server teveel requests binnen krijgt. Een voorbeeld van een ‘geavanceerde’ oplossing analyseert met behulp van AI en machine learning technieken grote hoeveelheden threat intelligence en netwerkdata in real time om afwijkingen te detecteren in eigen systemen, en daarover de security specialist te adviseren over passende responsemaatregelen. Er bestaan echter geen heldere definities of afbakeningen om te bepalen of een automatiseringsoplossing geavanceerd is. Cybersecurity vendoren vermarkten Automated Security oplossingen veelal onder de term Security Operations and Analytics Platform Architecture (SOAPA), Security Automation Operations and Respond (SOAR) of Automated Security (intelligence) (ASI) (Gartner, 2019). Hierin wordt echter ook geen duidelijke definitie gegeven van wat deze toepassingen precies inhouden. Wat voor de één een ‘zeer geautomatiseerde oplossing’ is wordt door een andere organisatie opgevat als ‘weinig geautomatiseerd’. Beide perspectieven zijn naar voren gekomen tijdens de interviews, en ook als zodanig verwerkt in de tabel of aanvullende bevindingen in dit hoofdstuk.

2.2 Marktverkenning Automated Security

De marktverkenning van het Nederlandse innovatielandschap rondom Automated Security bestaat uit drie onderdelen:

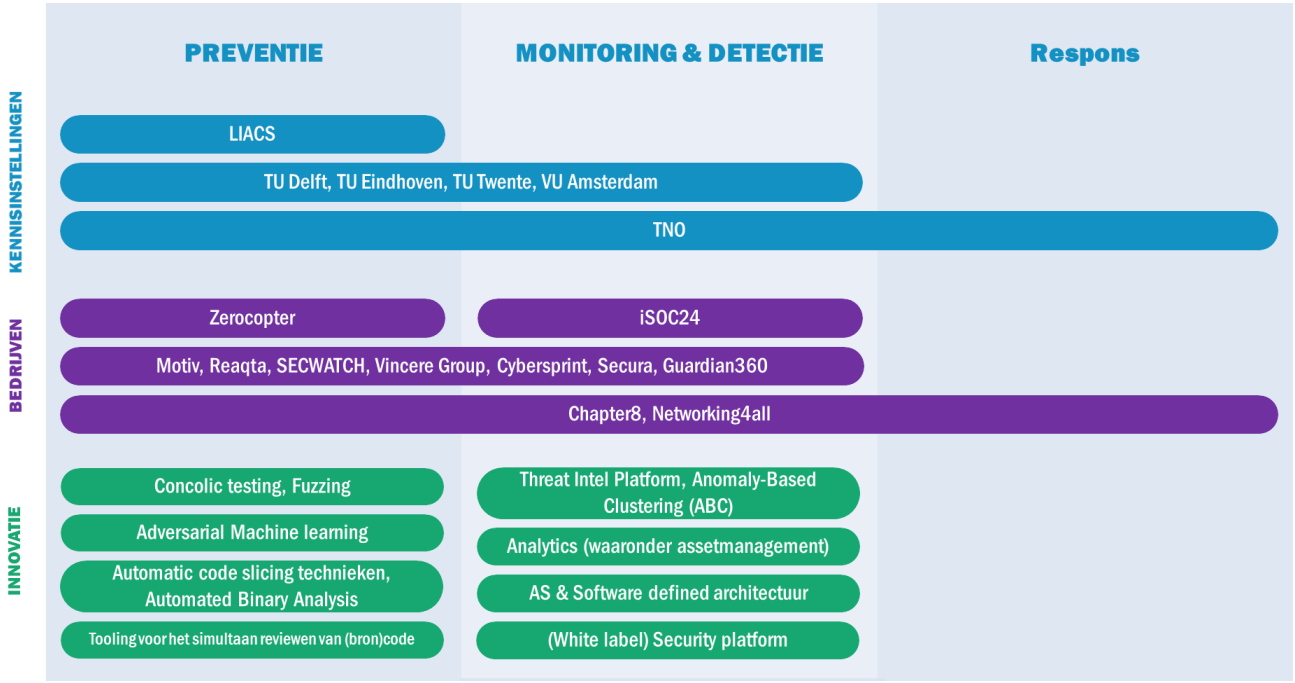
- Een overzicht van de lopende innovatie-initiatieven met betrekking tot Automated Security en de bijbehorende spelers.
- Een aantal overkoepelende bevindingen met betrekking tot Automated Security.
- Een beschrijving van de barrières binnen het ecosysteem die innovatie-initiatieven in de weg staan[1].

2.2.1 Innovatie-initiatieven

Bij het in kaart brengen van de partijen die een rol spelen in het Automated Security ecosysteem is onderscheid gemaakt tussen drie typen organisaties: kennisinstellingen, cybersecurity bedrijven en eindgebruikers. Daarnaast zijn de toepassingen waarvoor deze partijen Automated Security inzetten gecategoriseerd op basis van de categorieën preventie, monitoring & detectie en respons. Figuur 1 toont een schematische weergave van actuele partijen en toepassingsgebieden (i.e. innovatie-initiatieven) van deze verkenning van het Nederlandse Automated

[1] De barrières voor innovatie binnen Automated Security zijn niet gespecifieerd voor één van de drie categorieën van preventie, monitoring & detectie en respons. Daarom zijn deze gebundeld in een apart hoofdstuk en niet opgenomen in figuur 1.

Security innovatie ecosysteem. Binnen de categorieën kunnen organisaties een verschillende rol hebben, sommigen ontwikkelen zelf toepassingen, anderen nemen producten van andere bedrijven, die ze vervolgens aanpassen en aanbieden aan de eindgebruiker.



Figuur 1 Schets van het Nederlandse Automated Security ecosysteem, gebaseerd op de afgenomen interviews. In de bovenste helft staan de betrokken spelers geplot, in de onderste helft worden innovaties benoemd. In het volgende hoofdstuk zijn (mogelijke) eindgebruikers geplot (Waardeketen analyse).

Het overzicht uit Figuur 1 wordt in onderstaande tabel verder toegelicht, waarbij de verschillende innovatie-initiatieven in meer detail worden beschreven en zijn gekoppeld aan de partijen die aan het initiatief werken. De tabel is tot stand gekomen op basis van de afgenomen interviews en biedt geen uitputtend overzicht. In de tabel wordt een inschatting gemaakt van het Technology Readiness Level (TRL) in de kolom Innovatiefase. Het duiden van het TRL-niveau geeft inzicht in de mate waarin de innovatie of techniek op dit moment verkeert.

Ondanks dat sommige onderwerpen in de tabel ingedeeld zijn in een specifieke categorie beslaat of raakt het onderwerp vaak ook andere categorieën (bijvoorbeeld het White label Security Platform). Automated Security producten leveren vaak niet alleen een bijdrage aan de preventie, monitoring & detectie en respons categorieën, maar hebben vaak ook de data nodig die in deze categorieën wordt verzameld.

Tabel 1 Overzicht van innovatie-initiatieven en partijen, gebaseerd op de afgenomen interviews. De inhoud van de tabel geeft dus geen volledige weergave van AS-initiatieven en ontwikkelingen in Nederland. Er kunnen meer partijen of organisaties betrokken zijn per ontwikkeling of innovatie dan in deze tabel vermeld staat.

Categorie	Onderwerp	Toelichting	Innovatiefase	Gesproken partij
Preventie	Programma analyse: Concolic testing en fuzzing	Concolic testing en fuzzing zijneen softwareverificatie technieken waarmee fouten in software ontdekt kunnen worden, zodat het aantal kwetsbaarheden dat wordt veroorzaakt door fouten in code kan worden teruggebracht. Na willekeurige data (fuzz) in een programma in te voeren wordt onderzocht of het programma crashed of andere fouten vertoont.	Medium TRL-niveau. Kennisinstituten en een paar toepassingen (Microsoft SAGE). Verwachting is dat concolic testing binnen 5 jaar breed wordt toegepast. Fuzzing kent een laag en hoog TRL niveau: fuzzers worden veel gebruikt in computerbeveiliging. Er worden echter ook nog veel nieuwe toepassingen binnen deze categorie ontwikkeld.	TU Delft, VU, LIACS
	Adversarial Machine learning	Onderzoek naar de toepassing van adversarial machine learning technieken voor verdedigingssystemen die erop gericht zijn om de werking van vijandige algoritmes te herkennen en deze te verstoren.	Laag TRL-niveau. Kennisinstituten.	TU Delft
	Programma analyse: Automatic code slicing technieken	Technieken die automatisch belangrijke elementen uit grote hoeveelheden code kunnen identificeren en markeren voor nadere review en tests. Handmatig onderzoek naar onbekende kwetsbaarheden is menselijk onhaalbaar, kan inboeten aan kwaliteit, en is kosten inefficiënt	Medium tot hoog TRL-niveau. Bedrijven.	Riscure
	Programma analyse: Tooling voor het simultaan reviewen van (bron/binary)code	(Door)ontwikkelen van tooling om met meerdere personen en expertises efficiënt en hoogwaardig (bron)code te reviewen.	Medium tot hoog TRL-niveau. Bedrijven.	Riscure
	Programma analyse: Automated Binary Analysis	Geautomatiseerde analyse om fouten en kwetsbaarheden in binary code te ontdekken.	Hoog	VU

Categorie	Onderwerp	Toelichting	Innovatiefase	Gesproken partij
Monitoring en Detectie	Threat Intelligence Platform (TIP)	Tooling waarmee threat intelligence automatisch vanuit verschillende bronnen wordt gecombineerd, gevalideerd en gecorreleerd om te komen tot handelingsperspectief. Op basis van AI of vooraf gedefinieerde playbooks kunnen vanuit deze tooling ook automatische acties worden ondernomen als reactie relevante dreigingen.	Zowel laag als hoog TRL niveau: er zijn al verschillende TIP oplossingen op de markt, maar de automatische ondersteuning voor het correleren en analyseren van data en het automatisch handelen wordt nog doorontwikkeld	VTM, Northwave, Fox-IT, Telindus, iSOC24, SOCCRATES[2], TU/e
	Analytics (waaronder asset management)	Infrastructuur en het gedrag van software, hardware en menselijk handelingen adhv data in kaart brengen is een randvoorwaarde voordat AS effectief een rol kan spelen bij organisaties.	Hoog TRL-niveau	Telindus
	Automated Security technieken in samenwerking met software defined architecturen	Een IT-infrastructuur die zonder menselijk handelen aangestuurd wordt en niet gebonden is aan de onderliggende hardware. AS-oplossingen zijn daarom geen puntoplossing maar integraal onderdeel van de infrastructuur, waardoor deze zeer effectief kunnen zijn.	Medium tot hoog TRL-niveau	Telindus
	(White label) Automated Security platform	Een security platform dat verschillende AS-technieken bij elkaar brengt om organisaties in staat te stellen om geautomatiseerd cyberaanvallen sneller te ontdekken en te beantwoorden.	Laag TRL-niveau	PPS ASOP[3], SOCCRATES

[2] SOCCRATES is een EU H2020 project met 10 partners, waarvan TNO coördinator is. SOCCRATES ontwikkelt en evalueert een Automated Security platform dat via geautomatiseerde processing van monitoring informatie en threat intelligence en met afweging van business belangen een aantal geoptimaliseerde response acties voorstelt aan een SOC operator.

[3] Publiek Private Samenwerking Automatiseren van Security Operaties. Dit is een consortium van cybersecurity bedrijven, publieke organisaties en TNO dat de komende jaren werkt aan het zetten van een volgende stap in Automated Security.

Categorie	Onderwerp	Toelichting	Innovatiefase	Gesproken partij
	Automatiseren van SOC werkzaamheden	• Het automatisch filteren van false positives. Dit gebeurt nu handmatig en kost veel tijd. • Algoritmes ontwikkelen die inzichtelijk maken waarom een alarm is afgegaan. • Het automatisch genereren van 'attack stories' op basis diverse informatiebronnen. Dit zorgt ervoor dat er minder tijd nodig is om te analyseren waarom een alarm is afgegaan.	Laag TRL-niveau onderzoek zoals email spear phising (TNO) en Reasons engine (SOCCRATES).	TU/e, TU Delft, Northwave, TNO
	Intrusion Detection System (IDS)	Een geautomatiseerd systeem dat ongeautoriseerde toegang tot een netwerk of systeem detecteren. Kan vele onderliggende onderwerpen omvatten zoals 'reconnaissance detection'	Zowel laag als hoog TRL niveau: IDSs worden veel gebruikt in computerbeveiliging. Er worden echter ook nog veel nieuwe toepassingen binnen deze categorie ontwikkeld. Hoog TRL niveau IDS bevat weinig AS. Automated Security technieken in IDS momenteel laag-TRL.	VU
	Evalueren van SOC performance	In een SOC draaien veel operationele en technische processen. Het is lastig voor SOC personeel om te monitoren of al deze processen correct functioneren. Het automatiseren van een monitoringsfunctie voor SOC processen zorgt ervoor dat personeel inzicht krijgt in het functioneren van het SOC. Een dergelijke toepassing geeft ook inzicht in de toegevoegde waarde van een nieuwe tool of techniek die in een SOC wordt toegevoegd, aangezien metingen kunnen worden gedaan voor en na het toevoegen van de nieuwe tool.	Laag TRL-niveau, op dit moment wordt de omgeving gebouwd waarin de TU/e hypotheses rondom dit onderzoek wil testen.	TU/e

Categorie	Onderwerp	Toelichting	Innovatiefase	Gesproken partij
Respons	Uit de interviews komt naar voren dat er wel diensten worden aangeboden binnen de categorie response, maar niet dat er wordt ingezet op het ontwikkelen van innovaties. Het is onduidelijk of er geen behoefte is aan innovaties in deze categorie, of dat er vanwege andere redenen niet wordt geïnnoveerd in deze categorie.			

2.2.2 Overkoepelende bevindingen

Deze paragraaf beschrijft een aantal trends met betrekking tot Automated Security die van invloed zijn op het ecosysteem. Deze bevindingen zijn gedaan op basis van de interviewresultaten.

- Invloed van automatisering op de rol van de security specialist

Automatisering zal er op korte termijn niet voor zorgen dat de rol van de security specialist overbodig wordt in het cybersecurity werkveld. Veel van de toepassingen die worden ontwikkeld dienen ertoe om de security specialist bij te staan en te ontlasten, aangezien er een groot tekort is aan goed opgeleid personeel. Een respondent gaf aan dat geautomatiseerde monitoring en detectie tools doorzichtig (transparant) moeten blijven. Het is namelijk over het algemeen de security specialist die actie moet ondernemen op de resultaten van deze geautomatiseerde tools. Als de specialist geen inzicht kan krijgen in hoe een toepassing aan zijn informatie komt, heeft de toepassing uiteindelijk weinig tot geen toegevoegde waarde.

Het moment waarop Automated Security tooling gebruikt wordt heeft ook invloed op de security specialist. Wanneer Automated Security toepassingen aan een bestaande SOC/SIEM/dashboard omgeving toegevoegd worden, blijkt het een grote uitdaging te zijn de tooling op de juiste manier te implementeren. Bijvoorbeeld om de tooling te integreren in bestaande processen, de werking ervan volledig te doorgronden, of om alle functionaliteit ook daadwerkelijk te gebruiken. Deze uitdaging is niet, of in mindere mate, aanwezig als Automated Security tooling een integraal onderdeel van de beveiliging uitmaakt. Dus wanneer de tooling al wordt geïmplementeerd wanneer een IT-infrastructuur wordt opgebouwd.

- Een alomvattende cloudomgeving

Bedrijven verplaatsen in toenemende mate hun IT-infrastructuur naar een cloudomgeving, omdat het beheren van een eigen, lokale IT-infrastructuur een steeds complexere taak wordt die veel resources vraagt op het gebied van beheer en ondersteuning. Cloudomgevingen bieden over het algemeen een veilige inrichting en eenvoudig beheer voor een IT-infrastructuur. Daarnaast zorgt de geïntegreerde omgeving ervoor dat de ingebouwde geautomatiseerde security tools toegang hebben tot alle relevante data, wat de security tools zeer krachtig maakt. De keerzijde is echter wel dat klanten gebonden zijn aan de tools en informatie die de cloudleverancier bereid is te bieden. Er is dus weinig ruimte om eigen voorkeuren door te voeren. Daarnaast is het gevolg van de krachtige security tools binnen cloudomgevingen dat cybersecurity dienstverleners minder goed kunnen concurreren met deze tools. In welke mate Nederlandse partijen bijdragen aan de innovatie van security tooling voor cloudomgevingen is niet onderzocht of naar voren gekomen tijdens de interviews.

- Fundamenteel onderzoek

Automated Security is een breed onderwerp dat door meerdere universiteiten en diverse vakgroepen vanuit verschillende perspectieven wordt onderzocht. Hierbij wordt nauw samengewerkt met een aantal grote Nederlandse bedrijven, waardoor de kennisopbouw die binnen kennisinstellingen plaatsvindt snel toegepast kan worden in het bedrijfsleven.

Daarnaast tonen internationale techbedrijven grote interesse in de kennis die door Nederlandse kennisinstellingen wordt ontwikkeld. Dit uit zich in samenwerkingen in de ontwikkeling van fundamenteel onderzoek, maar ook in het opkopen van start-ups en spin-offs van de universiteiten. Dit onderstreept het hoge niveau van de kennis die binnen Nederlandse kennisinstellingen wordt ontwikkeld.

- Wie vraagt om Automated Security?

Volgens een respondent worstelen klanten van cybersecuritybedrijven met de vraag wat ze wel of niet willen automatiseren. Automated Security is een relatief nieuw concept, waarbij onbekend is welke processen reeds geautomatiseerd zijn en in hoeverre nieuwe of bestaande processen verdergaand geautomatiseerd zouden kunnen worden. Iedere sector moet beredeneren in welke processen menselijk inzicht nodig is en welke processen volledig geautomatiseerd kunnen worden. Veel tooling die automatisch naar kwetsbaarheden zoekt (vulnerability scanning), richt zich alleen op bestaande kwetsbaarheden. Voor veel eindgebruikers is het vinden en verhelpen van deze bekende kwetsbaarheden al een grote stap vooruit in de beveiliging. Er wordt door bedrijven die een lager maturity level hebben beperkt gevraagd naar methoden en technieken om onbekende kwetsbaarheden te vinden. Het vinden van onbekende kwetsbaarheden wordt nu voornamelijk aangeboden in de vorm van een ethische hacker, niet door tooling. De behoefte aan innovatie op dit onderwerp komt wel meer naar voren bij grote bedrijven en instellingen (o.a. de partijen die samenwerken in het Program on Cyber Security Innovation (PCSI), SOC van publieke en private partijen bij de Technische Universiteit Eindhoven).

- Het aanbod van cybersecurity producten en oplossingen

De internationale markt van cybersecurity bedrijven levert volgens de respondenten interessante producten en diensten. Naar hun verwachting gaan huidige onderzoeksinstituten en marktspelers (met name huidige grote internationale hardware- en softwarevendoren) ook de innovaties en producten voor Automated Security producten leveren.

Nederlandse bedrijven die geïnterviewd zijn maken kenbaar dat het veel werk kost om producten van leveranciers te kiezen. Het blijkt een uitdaging om de verschillen te duiden, informatie in te winnen over de betrouwbaarheid van het product of dienst, en de functionaliteiten na aanschaf in hun eigen omgeving te integreren.

- Vendor lock-in

Nederlandse bedrijven die leveranciers (reseller) zijn cybersecurity producten en diensten van een groot techbedrijf afnemen worden in toenemende mate gepushed om meer producten van dat specifieke bedrijf af te nemen. Een aantal geeft aan dat deze grote techbedrijven ook cybersecurity tooling aanbieden. Deze tooling kan echter alleen worden afgenomen als een duurder abonnement wordt afgesloten. Dit heeft tot gevolg dat wanneer een cybersecurity bedrijf óf een klant gewend is om

met dergelijke tooling te werken, beide partijen daarmee het duurdere abonnement moeten afnemen om een bepaalde mate van beveiliging te bereiken. Andere lock-in effecten zijn door de respondenten niet kenbaar gemaakt in de context van automated security (bijv. concurrentie effecten of uiteindelijk lagere kosten voor de afnemers of eindgebruikers).

2.2.3 Barrières voor innovatie op het gebied van Automated Security

In een eerder TNO onderzoek (2020) naar het versterken van de innovatieketen op het terrein van cybersecurity zijn vier barrières geïdentificeerd voor de cybersecurity innovatieketen als geheel.[4] De barrières die in deze marktverkenning zijn geïnventariseerd hebben daarmee gedeeltelijke overlap.

- Gebrek aan slagkracht van NL cybersecurity bedrijven in vergelijking met Big Tech-bedrijven

Cybersecurity dienstverleningsbedrijven hebben niet dezelfde middelen om op innovatie te kunnen concurreren met Big Tech-bedrijven als bijvoorbeeld Microsoft, Cisco of Symantec. Dit geldt zowel voor Nederlandse als buitenlandse cybersecurity bedrijven. Deze bedrijven kunnen niet concurreren met Big Tech omdat er onvoldoende kapitaal beschikbaar is om de innovatiebudgetten van deze grote bedrijven te evenaren.

Daarnaast kunnen Big Tech-bedrijven innoveren op basis van de producten en diensten die zij zelf produceren, terwijl cybersecurity bedrijven veelal moeten innoveren op basis van de producten van de Big Tech-bedrijven, wat de cybersecurity bedrijven op een achterstand zet in de innovatiecyclus. Hierdoor ontstaat een onderscheid tussen Big Tech partijen die producten ontwikkelen en aanbieden aan de ene kant en Nederlandse cybersecurity bedrijven die deze producten aanbieden aan hun klanten aan de andere kant.

- Buitenlandse overnames

Veel Nederlandse cybersecurity bedrijven en veelbelovende start-ups met unieke kennis worden overgekocht door buitenlandse partijen. Bekende voorbeelden zijn Fox-IT, Redsocks en SecurityMatters. Hoewel het overgenomen bedrijf binnen Nederland blijft bestaan, wordt het voor kennisinstellingen lastiger om met deze bedrijven samen te werken. Waar de bedrijven eerst samen met kennisinstellingen innovatieprojecten uitvoerden, worden deze veelal stopgezet of wordt er minder budget beschikbaar gesteld na een buitenlandse overname. Buitenlandse overnames hebben dus een negatief effect op de samenwerking tussen bedrijven en kennisinstellingen. Daarnaast is er op dit moment al een groot gebrek aan goed opgeleid cybersecurity personeel (TNO, 2020). Het wegkopen van Nederlandse bedrijven die personeel met hoogwaardige kennis in dienst hebben kan op de lange termijn een negatief effect hebben op het Nederlandse innovatievermogen en het kennisniveau, op het gebied van Automated Security en van cybersecurity in zijn geheel.

- Gebrek aan duidelijke rol van de overheid

De rol van de overheid in het ondersteunen van innovatie is onduidelijk voor cybersecurity bedrijven. Het is voor bedrijven niet duidelijk hoe keuzes om in een innovatieterrein te investeren tot stand komen, omdat er geen duidelijke missies

[4] Gebrek aan visie en sturing over de keten, huidige set van instrumenten is niet effectief, beperkt absorptievermogen, gebrek aan goed opgeleide mensen. (TNO, 2020)

door de overheidsinstellingen wordt geformuleerd. Deze bevinding strookt met het TNO rapport (2020), waarin wordt gesteld dat er vanuit de overheid een gebrek aan visie en sturing is op de rol voor cybersecurity in de Nederlandse samenleving en economie, en hoe die moet worden ingevuld.

- Cultuur van innovatie

Een respondent van een cybersecurity bedrijf gaf aan dat het lastig is om Automated Security oplossingen te laten landen bij hun klanten, aangezien de implementatie van geautomatiseerde oplossingen vaak een verandering in de organisatie van de klant vergt. De innovatiebehoefte zit dus voornamelijk bij het cybersecurity bedrijf zelf, aangezien deze beoogt door geautomatiseerde oplossingen betere dienstverlening aan te kunnen bieden en het eigen personeel te kunnen ontlasten. Dit strookt met de bevindingen uit het TNO rapport (2020), waarin wordt aangegeven dat vooral kleinere bedrijven een beperkt absorptievermogen hebben om de laatste ontwikkelingen op het gebied van cybersecurity te implementeren.

- Gebrek aan testdata en testomgevingen

Een respondent van een universiteit geeft aan dat de beperkte toegang en beschikbaarheid van testdata een barrière is voor innovatie op Automated Security technieken. Data staat aan de wieg van modellen waarmee wordt gesimuleerd en ontwikkeld. Door een gebrek aan testdata kunnen onderzoekers hun hypotheses minder uitgebreid testen en valideren. Het is een grote financiële uitdaging om als onderzoeksinstituut een testinfrastructuur in te richten.

3 Waardenetwerk analyse Automated Security

In dit hoofdstuk beschrijven we het waardenetwerk op het gebied van cybersecurity innovaties binnen de Nederlandse financiële- en energiesector. Gezien de aard en tijdsduur van deze verkenning, zijn de bevindingen uit dit hoofdstuk gebaseerd op een relatief klein aantal interviews en literatuuronderzoek. Om een volledigere beeld te vormen, is een uitgebreidere analyse nodig. De inzichten uit deze waardenetwerk analyse kunnen gebruikt worden als fundament voor de routekaart AVR, welke aan bod komt in Sectie 5.

Waardenetwerk analyse is een methode om met een brede blik naar een innovatie ecosysteem te kijken. Dit levert niet slechts een eendimensionaal beeld op van een waardeketen gericht op één actor (zoals een waardeketenanalyse), maar brengt een complex netwerk in kaart brengt. Hierin zijn er verschillende rollen zichtbaar, welke met elkaar verbonden zijn door middel van waarde-uitwisselingen. Elke rol wordt vervuld door tenminste één actor, wat bijvoorbeeld een bedrijf kan zijn. Eén actor kan vervolgens meerdere rollen aannemen. Zo kan een organisatie bijvoorbeeld zowel een IT leverancier als klant zijn binnen de context van een bepaald waardenetwerk. Het waardenetwerk laat hiermee de verschillende relaties binnen het ecosysteem zien en richt zich naast geld ook op andere waarde transacties zoals kennis, personeel en innovatiekracht. Tevens kunnen samenwerkingsverbanden en barrières inzichtelijk en visueel gemaakt worden.

Er is voor een waardenetwerk analyse gekozen, omdat het een passende methode is om een complex innovatie ecosysteem op een gestructureerde wijze en in detail in kaart te brengen. Innovatie rondom Automated Security binnen de financiële- en energiesector gebeurt met veel verschillende partijen, belangen, en samenwerkingsverbanden. Een waardenetwerk analyse kan de dynamiek van deze verbanden in meer detail weergeven dan bijvoorbeeld de klassieke waardeketenanalyse, die meer procesgericht naar een ecosysteem kijkt. Hiernaast is er in het specifiek voor de financiële- en energiesector gekozen, omdat deze sectoren aansluiten bij de aandachtsgebieden binnen het nieuwe samenwerkingsplatform voor cybersecurity kennis en innovatie (Kwartiermakers, 2020). Een kanttekening die geplaatst moet worden is dat het waardenetwerk een momentopname is van een ecosysteem dat permanent in beweging is. Om onze bevindingen actueel te houden, moet het waardenetwerk tenminste jaarlijks geëvalueerd en herijkt worden.

3.1 Methode

Hieronder volgt een korte beschrijving van de methode voor de waardenetwerk analyse die is uitgevoerd. De gehele methode met achtergrondinformatie is te vinden in het TNO rapport “AUSI: An integrated approach to Value Network Analysis” (R12144, 2013).

De methode bestaat uit vier stappen die worden aangegeven in Figuur 2. Hierna lichten we per stap toe wat het doel is.

Figuur 2 Stap-voor-stap methodische aanpak voor een waardenetwerk analyse (vertaling van figuur uit TNO, 2013)

3.1.1 *Stap 1: Deskresearch*

Het doel van de deskresearch is om stakeholders te identificeren en een basiskennis op te bouwen over het waardenetwerk, de waarden en de rollen. Om dit te bereiken wordt een literatuuronderzoek uitgevoerd. Op deze manier wordt er een beeld gevormd van de werking van het ecosysteem en de bestaande problemen vanuit een onafhankelijk, buitenstaander perspectief. Op basis van de resultaten kan een draft van het waardenetwerk getekend worden. Deze wordt als uitgangspunt gebruikt en wordt in de volgende stappen verder gedetailleerd en gevalideerd.

3.1.2 *Stap 2: Hypothese workshop*

Het doel van de hypothese workshop is om binnen het projectteam hypothesen te bespreken en op te stellen over de rollen en de belangen van de stakeholders. De hypothesen gaat over hoe het waardenetwerk werkt; wat zijn de belangrijkste rollen, waarden en belangen. Dit is een voorbereiding op de interviews met experts binnen de stakeholders in de volgende stap. Het dient als een basis voor de beoordeling van de impact voor de verschillende stakeholders. Het zorgt er ook voor dat alle teamleden een gemeenschappelijk basiskennisniveau krijgen.

3.1.3 *Stap 3: Interviews met experts*

Het doel van de interviews met experts binnen de stakeholders, in dit geval bijvoorbeeld met chief information security officers (CISOs), is om informatie te verzamelen die nodig is voor de validatie en verdere uitbreiding van het waardenetwerk. Alle belangrijke stakeholders moeten geïnterviewd worden om een genuanceerd beeld te kunnen vormen over de werking en dynamiek van het ecosysteem.

3.1.4 *Stap 4: Analyse waardenetwerk*

In de laatste stap wordt alle verzamelde informatie bij elkaar gelegd en geanalyseerd. Op basis van de uitkomsten van de interviews wordt het waardenetwerk aangepast en worden conclusies getrokken over de werking van het ecosysteem. Krachtverdeling, onbalans en waarde transacties tussen stakeholders, barrières en problemen binnen het systeem worden na deze stap duidelijk.

In de huidige analyse zijn bovengenoemde stappen deels parallel uitgevoerd om ervoor te zorgen dat de resultaten binnen de beschikbare tijd gerealiseerd konden worden. Tevens is de hypothese workshop overgeslagen en is het niet gelukt om alle belangrijke stakeholders te interviewen.

Tijdens onze interviews hebben we een aantal vragen gesteld die specifiek gericht waren op Automated Security. Echter was niet iedereen bekend met toepassingen hiervan, doordat de personen met kennis over innovatie, strategie en samenwerkingsverbanden niet altijd óók de inhoudelijke kennis over cybersecurity of Automated Security hebben. Hiernaast is de beschikbare literatuur over de toepassing van Automated Security in de financiële- en energiesector gering, gezien het jonge stadium van de technologische ontwikkeling.

3.2 Waardenetwerk analyse – Financiële sector

In deze sectie volgt de uitwerking van de waardenetwerk analyse voor de Nederlandse financiële sector. Na een korte inleiding waarin we schetsen waarom deze sector relevant en interessant is, gaan we over tot de waardenetwerk analyse zelf. Hierin laten we eerst het gehele netwerk zien, waarna we aan de hand van sub-netwerken onze bevindingen illustreren. Deze zijn allen toegespitst op cybersecurity innovaties in het algemeen, waar Automated Security een onderdeel van is. Ten slotte benoemen we een aantal bevindingen die niet (direct) in het waardenetwerk te zien zijn, maar wel tijdens ons onderzoek naar voren zijn gekomen.

3.2.1 Inleiding

De hoeveelheid aan gevoelige en waardevolle data die in de financiële sector wordt verwerkt en opgeslagen maakt het een interessant doelwit voor cyberaanvallen. Hiernaast is er ook vaak direct een korte termijn gewin te behalen: geld. In 2018 was de financiële sector wereldwijd de meest geraakte sector op het gebied van cyberaanvallen en incidenten: één op de vijf aanvallen betrof deze sector (SwivelSecure, 2018). In het Cybersecuritybeeld Nederland wordt erkend dat er momenteel op mondiale schaal een dreiging is voor de financiële sector (CSBN, 2020). Bovendien zijn de kosten van een cyberaanval en de nasleep daarvan voor de financiële sector vele malen hoger dan voor andere sectoren (BCG, 2019). De financiële crisis van 2008 is een kenmerkend voorbeeld van hoe een kwetsbaarheid in de financiële sector zich als een olievlek op mondiale schaal kan uitbreiden.

Naast de beschikbaarheid van waardevolle data in de financiële sector, is het ook een zeer dynamische sector. De invoering van innovatie-bevorderende wetgeving zoals Payment Services Directive 2 (PSD2) en de opkomst van blockchain technologie hebben de deur open gezet voor disruptieve Financial Technology (FinTech) bedrijven om toe te treden tot de markt. Hiernaast zijn vrijwel alle financiële diensten tegenwoordig digitaal. De toenemende schaal, complexiteit en onderlinge verbondenheid maakt het in steeds grotere mate praktisch onmogelijk om systeemrisico’s handmatig in kaart te brengen (PwC NL, 2018).

Bij organisaties in de financiële sector staat cybersecurity daarom steeds hoger op de bestuursagenda. Het blijkt echter lastig te zijn dit ook te implementeren in de praktijk: uit onderzoek van EY blijkt dat slechts 6% van de financiële dienstverleners zegt dat hun systemen voor informatiebeveiliging momenteel toereikend zijn voor

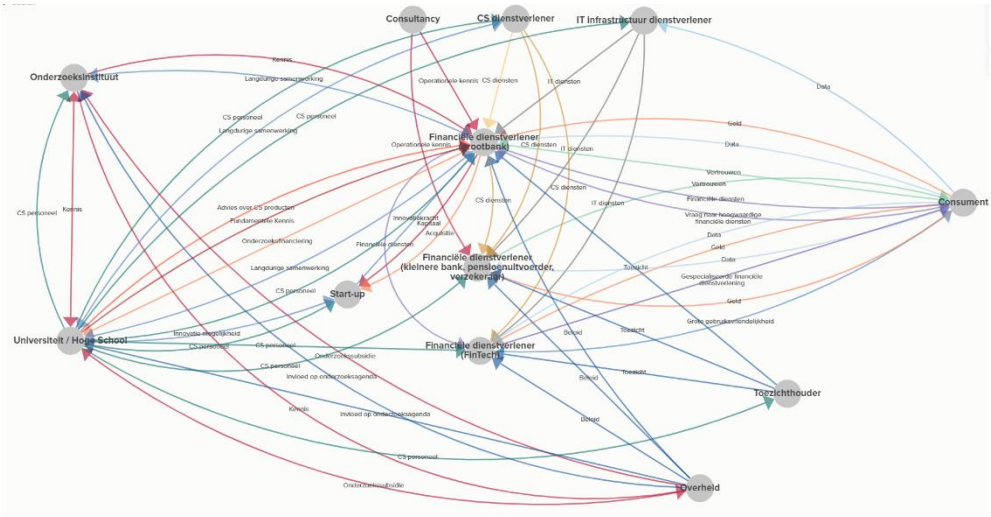
de behoeften van hun organisatie (EY, 2019). Cybersecurity innovaties zoals Automated Security kunnen helpen om de cybersecurity competenties van organisaties in deze sector te verbeteren.

Om deze innovaties te laten slagen, is het echter essentieel om in kaart te brengen hoe het innovatie ecosysteem er op dit moment uit ziet: welke rollen zijn hierbij betrokken en welke waarden wisselen zij uit, waar wordt kennis en personeel vergaard en wat zijn barrières die innovatie tegenwerken? Deze vragen beogen wij te beantwoorden met behulp van een waardenetwerk analyse.

3.2.2 Waardenetwerk analyse

Figuur 3 toont het gehele waardenetwerk dat wij in kaart hebben gebracht tijdens ons onderzoek. Hier zijn twaalf rollen te zien waartussen een groot aantal verschillende waarden worden uitgewisseld. Dit netwerk laat een schets van het innovatie ecosysteem voor cybersecurity binnen de financiële sector zien, met daarin ook de waarde transacties die plaats vinden rondom de fundamentele dienstverleningen binnen de sector.

Door de aard van deze verkenning is dit netwerk niet allesomvattends, dus zouden er enige rollen en/of waarde transacties in het netwerk kunnen ontbreken. Om het netwerk inzichtelijk te maken, wordt de analyse van het waardenetwerk per sub-netwerk toegelicht. De partijen met wie we gesproken hebben tijdens de interviews staan in bijlage 1B.

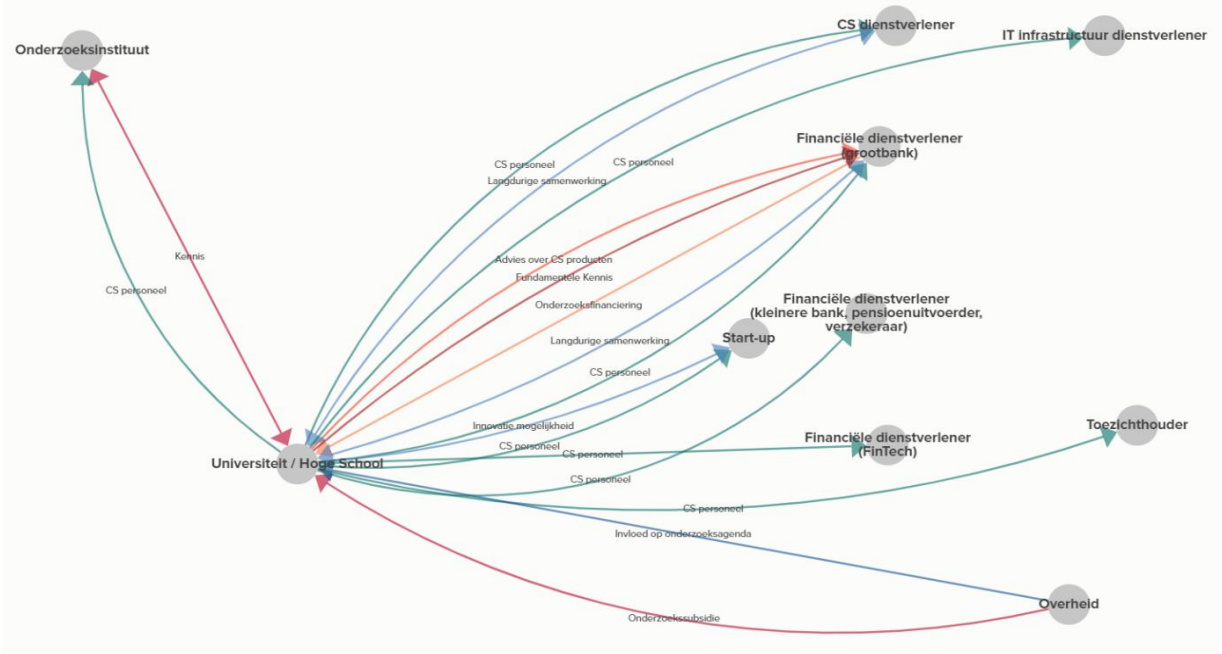


Figuur 3 **Schets van het cybersecurity waardenetwerk in de Nederlandse financiële sector.** De cirkels weergeven de rollen en de pijlen geven de waarde uitwisselingen tussen deze rollen aan. Waarden van soortgelijke types hebben, waar mogelijk, dezelfde kleur. Van links naar rechts is grofweg de leveringsketen voor de cybersecurity rondom financiële dienstverlening te zien: van fundamenteel onderzoek, tot financiële dienstverlening tot consument, met hier boven en onder de dienstverlening van derde partijen en het toezicht. In deze afbeelding bedoelen we de rol als consument in de context van consumptie van financiële producten en de rol als toezichthouder is in deze context toebedeeld aan De Nederlandsche Bank.

1 Versplintering van financiële diensten

In het overzicht van het volledige netwerk is zichtbaar dat de leveringsketen van financiële diensten in de sector versplinterd is. Er is een grote hoeveelheid rollen die deelnemen in dit netwerk, welke vervolgens aangenomen kunnen worden door

één of meerdere actoren. Deze dragen allen bij aan het tot stand brengen van een toenemend aantal digitale financiële diensten, die steeds complexer worden en (in)direct onderling verbonden kunnen zijn. De bijdrage van de betrokken partijen is beperkt tot hun eigen expertisegebied, wat vaak een niche-gebied is, en dus maar een klein deel van het geheel is. Deze versplintering kan leiden tot versnelde innovatie, omdat er sneller resultaten opgeleverd kunnen worden door de specialisatie van iedere betrokken partij, maar gaat ten koste van de transparantie. Hierdoor kunnen er ook nieuwe, onbekende cybersecurity risico's ontstaan. Het Threat Intelligence Based Ethical Red-teaming (TIBER) raamwerk dat De Nederlandsche Bank (DNB) toepast zou hierbij enige houvast kunnen bieden, doordat het kwetsbaarheden in een ondoorzichtige leveringsketen zichtbaar kan maken.



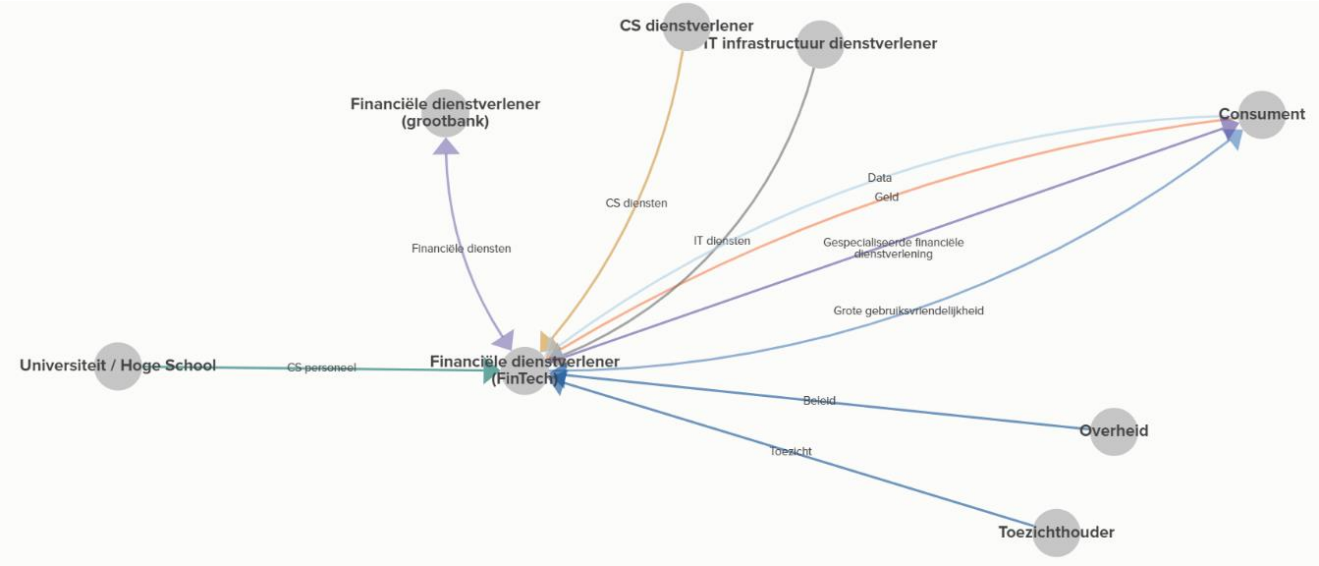
Figuur 4 **Sub-netwerk universiteiten / hoge scholen**. Hier is te zien dat deze vooral cybersecurity personeel leveren aan veel verschillende andere rollen in het netwerk. Hiernaast hebben ze ook nauwe samenwerkingen met grootbanken aan fundamenteel onderzoek.

2 Kennisopbouw en de strijd om cybersecurity personeel

Zoals te zien is in Figuur 5, leiden universiteiten en hogescholen studenten op die als personeel aan het werk gaan binnen bijna alle spelers in het ecosysteem. Doordat er een beperkt aantal studenten kiest voor een cybersecurity (of technische gerelateerde) opleiding en de vraag naar (hoog)opgeleid cybersecuritypersoneel onverminderd toeneemt, ontstaat er een schaarste in cybersecuritypersoneel in het gehele netwerk. Hierdoor moeten alle stakeholders hun best doen om de juiste professionals aan te trekken en als dit voor één partij goed lukt, gaat dit automatisch ten koste van de rest.

Daarnaast is te zien dat de onderwijsinstellingen financiering ontvangen van grootbanken voor onderzoek naar innovaties op het gebied van cybersecurity. Deze middelen worden vaak gebruikt voor de financiering van promotieonderzoek, waarmee een meerjarige samenwerking tot stand wordt gebracht. Ook zijn deze twee partijen over het algemeen betrokken in de grootschalige

samenwerkingsinitiatieven rondom cybersecurity innovaties. De kleinere partijen vallen hier doorgaans buiten (zie volgende bevinding).

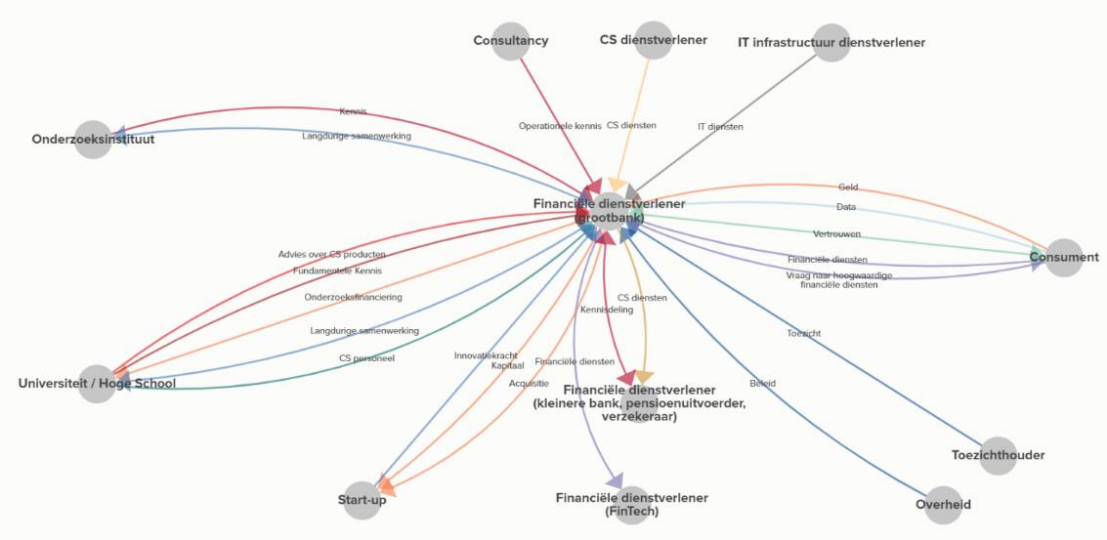


Figuur 5 **Sub-netwerk FinTech**, waarin is te zien dat ze zich vooral richten op de ontwikkeling van (gespecialiseerde) financiële productontwikkeling en buiten de kennisopbouw en deling vallen.

3 Cybersecurity niet altijd onderdeel van financiële innovatie

De (in de meeste gevallen kleine, disruptieve) FinTech bedrijven zijn over het algemeen niet sterk betrokken bij grote cybersecurity innovatietrajecten. Dit komt mede doordat ze zich vaak (nog) niet in het standaard (relatie)netwerk van de grotere spelers bevinden. Er zijn echter wel initiatieven in het leven geroepen om de innovatiekracht van FinTech bedrijven te bevorderen, zoals het Europese FinTech Action Plan en het Maatwerk voor Innovatie van de Autoriteit Financiële Markten (AFM) en DNB (zie bevinding 5).

De focus van de FinTech bedrijven is sterk gericht op eindgebruikers (consumenten) van financiële diensten. Innovatie binnen deze bedrijven wordt het meest gedreven door klantvragen en -wensen, is gericht op user experience en business modellen, en is dus niet hoofdzakelijk gebaseerd op wetenschappelijk onderzoek op het gebied van cybersecurity. Hiernaast kan er een gebrek zijn aan budget, personeel of incentives voor deze partijen om actief te innoveren op het gebied van cybersecurity: zo voelt cybersecurity soms niet als een nuttige investering omdat de terugverdientijd niet helder is en onderschatten kleinere partijen het risico dat ze lopen, denkend dat hun bedrijf niet waardevol genoeg is om doelwit van digitale aanvallen te worden (Security Magazine, 2019). Ten slotte kunnen FinTech bedrijven in sommige gevallen ook onder de radar van de (inter)nationale toezichthouders opereren (CPB, 2016), waardoor de mate van cybersecurity ongecontroleerd blijft.



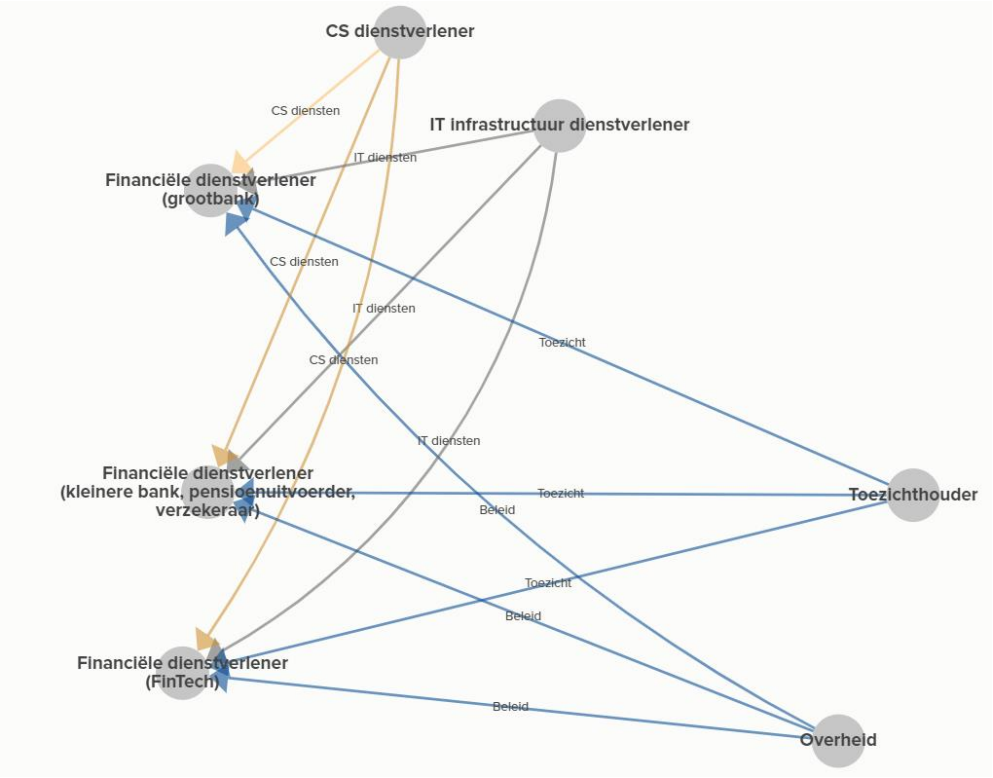
Figuur 6 **Sub-netwerk grootbanken.** Deze rol staat redelijk centraal in het waardenetwerk en wisselt een of meerdere waren uit met alle andere rollen. In het algemeen ontvangen ze veel diensten en kennis, welke ze vervolgens omzetten in productontwikkeling en kennisdeling in samenwerkingsverbanden.

4 Grootbanken hebben veel interactie

De grootste financiële dienstverleners hebben een dubbele rol in de valorisatieketen. Ze kunnen gezien worden als 'eindgebruiker' van inhoudelijke cybersecurity innovaties, maar zijn ook betrokken bij de kennisontwikkeling en het opzetten van innovatietrajecten (NVB, 2020). Hierdoor zijn ze niet volledig afhankelijk van derde partijen voor hun cybersecurity.

De grootbanken werken vooral veel samen met andere grote spelers (andere grootbanken, onderzoeksinstituten, universiteiten) met een focus op langdurige samenwerking op het gebied van cybersecurity innovatie. Al met al zorgt dit voor veel verschillende soorten waarde uitwisseling met een groot aantal rollen in het netwerk. Ook is te zien dat deze grotere spelers in veel mindere mate samenwerken met de overige kleinere banken. Als de grootbanken echter innovatieve, effectieve cybersecurity producten tot stand brengen, kunnen de kleinere spelers hiervan gedeeltelijk meeprofiteren door deze aan te schaffen zonder het benodigde onderzoeksbudget. De grootbanken hebben hierdoor echter wel de zeggenschap en de macht over welke cybersecurity innovaties meegenomen worden in de productontwikkeling.

Voor grootbanken is cybersecurity hiernaast ook een landgrensoverschrijdend thema, aangezien ze vaak actief zijn in meerdere landen of werelddelen. Hierdoor zijn ze aan de ene kant ook betrokken bij internationale samenwerkingen, maar moeten ze aan de andere kant voldoen aan zowel internationale als land-specifieke regulering (niet zichtbaar in Figuur 7).



Figuur 7 **Sub-netwerk toezicht en beleid.** Het toezicht en beleid heeft over het algemeen direct betrekking op de financiële dienstverlener zelf, welke deze vervolgens contractueel moet doorvertalen en vastleggen naar de derde partij die diensten aanlevert.

5 Toezicht gericht op financiële dienstverleners

De financiële markt is sterk gereguleerd, waarbij de dienstverleners aan veel eisen moeten voldoen, zoals de Wet op het financieel toezicht (Wft), en onder streng toezicht staan van DNB en de AFM. In artikel 3.18 van de Wft wordt beschreven dat derde partijen die betrokken zijn bij de levering van de financiële dienst hier ook aan moeten voldoen.

In sommige gevallen leveren grote technologie (BigTech) bedrijven significante delen van bijvoorbeeld de IT-infrastructuur van een financiële dienstverlener. Naast dat dit een concentratierisico met zich mee brengt (DNB, 2020) en de BigTech bedrijven hun positie als oligopolie mogelijk kunnen versterken (CPB, 2019), speelt het consumentenvertrouwen hier ook een belangrijke rol. Indien de dienstverlening van bijvoorbeeld een grootbank (in grote mate) wordt verstoord door een kwetsbaarheid die ontstaan is bij een derde partij, kan de consument het vertrouwen in de bank verliezen. Het is een opgave om dit vertrouwensverlies contractueel of wetmatig in te dekken. Ten slotte kan het toezicht binnen een landgrens soms ingewikkeld zijn, aangezien BigTech bedrijven vaak wereldwijd opereren. Om in te spelen op het complexe en dynamische ecosysteem waarin financiële diensten zich ontwikkelen, hebben DNB en de AFM samen het Maatwerk voor Innovatie opgesteld. Hierin wordt actief gekeken naar het achterliggende doel van wetgeving om zinvolle innovatie te bevorderen.

Toezicht op het gebied van Automated Security onderscheidt zich ten slotte niet van het algemene toezicht op cybersecurity: de zelfde “good practices” worden nagestreefd.
Naast de bovenstaande bevindingen, die we aan de hand van het waardenetwerk kunnen laten zien, noemen we hier nog een aantal overige bevinden die naar voren zijn gekomen tijdens onze analyse.

6 Gebrek aan orchestrator van de innovatieketen
Het is niet duidelijk wie de rol als orchestrator van de innovatieketen vervult. Hierdoor mist het overzicht van wat er zich afspeelt op welke thema’s binnen cyber security innovatie binnen het hele ecosysteem. Er bestaan samenwerkingsverbanden zoals het Partnership for Cyber Security Innovation (PCSI), het Financial Institutes – Information Sharing and Analysis Center (FI-ISAC) en publiek-private organisaties zoals de Cyber Security Raad (CSR) en het Nationaal Cyber Security Centrum (NCSC), maar er is verder weinig regie over deze samenwerkingsverbanden, waardoor het niet altijd duidelijk kan zijn wat waar wordt besproken en of er overlap is binnen deze initiatieven (CPB, 2019). Tevens kunnen er belangrijke hiaten ontstaan of relevante ontwikkelingen te laat worden opgemerkt. Hiernaast is de vraag of alle relevante partijen hierbij betrokken kunnen worden, aangezien sommige (kleinere) partijen niet het budget, de incentives of het netwerk hebben om aan samenwerkingsverbanden deel te nemen.

7 Kleine financiële dienstverleners vallen buiten de “innovatieloop”
Als deze meer betrokken zouden worden bij samenwerkingen rondom Automated Security innovatie, zou dit gunstig zijn voor het verkleinen van het systeemrisico van de sector als geheel. Door deze kleinere partijen mee te nemen in het innovatietraject en toegang te bieden tot cybersecurity kennis, kunnen ze features als Automated Security gemakkelijker in hun eigen dienstverlening implementeren (security by design). De crux is hier dat de kleine financiële dienstverleners wellicht weinig of geen incentive kunnen hebben om te innoveren op het gebied van cybersecurity, dus er moet er ook nagedacht worden hoe dit veranderd kan worden. Naar verwachting zullen kleinere partijen voornamelijk bezig zijn met het leggen van een solide fundament op het gebied van cybersecurity in plaats van innovatie.

8 BigTech is begonnen om de rol als financiële dienstverlener aan te nemen
Met initiatieven zoals Alipay of Google Pay, en in de toekomst wordt deze rol mogelijk verder uitgebreid. Dit zorgt voor nieuwe, grote spelers op de financiële markt die zowel sterktes (IT als core business) als risico’s (“too big to fail”) met zich mee brengen. Hiernaast hebben deze actoren vaak ook al de rol als IT-infrastructuur leverancier binnen het ecosysteem.

Op dit moment ontkomen zij aan het directe, strenge toezicht waar financiële dienstverleners wel onder vallen. Voor betalingsverkeer kan de huidige PSD2 wetgeving dekkend zijn, maar wat als BigTech ook verzekerings- of pensioendiensten op de markt wil brengen? Tevens kan, zoals hierboven eerder vermeld, toezicht ook ingewikkeld zijn voor deze mondiaal opererende bedrijven. Daarnaast vallen ook cryptovaluta waar BigTech aan werkt, zoals bijvoorbeeld Facebook’s Libra, buiten de Wft en is er weinig toezicht op deze geldstromen. Er is meer onderzoek nodig om vast te stellen hoe dit cybersecurity innovatie in de financiële sector kan beïnvloeden. Zo zijn BigTech bedrijven vaak voorloper op het

gebied van cybersecurity (as a service); hoe kan hier bijvoorbeeld op worden ingespeeld?

9 Afstemming tussen verschillende afdelingen binnen een bedrijf nodig om innovatie op het gebied van cybersecurity succesvol te laten zijn.
Een voorbeeld hiervan is te zien bij de interpretatie van de Algemene verordening persoonsgegevens (AVG). Als een derde partij data nodig heeft van een financiële dienstverlener welke herleid kan worden naar een persoon, zal de privacy afdeling deze data bijvoorbeeld versleutelen (hashen), wat de bruikbaarheid ervan kan verslechteren. Hiernaast is het belangrijk dat de kennis die wordt opgebouwd binnen de inhoudelijke IT afdeling, die Automated Security waarschijnlijk toejuichen, op een bepaald moment ook wordt geoperationaliseerd binnen het bedrijf om de inzetbaarheid en kennisdisseminatie te bevorderen.

3.3 Waardenetwerk analyse – Energiesector

Naast de financiële sector, hebben we ook een verkennende waardenetwerk analyse uitgevoerd in de Nederlandse energiesector. In het specifiek hebben we ons gericht op de elektriciteitssector als onderdeel hiervan. We introduceren eerst het volledige waardenetwerk, waarna we aan de hand van een aantal sub-netwerken onze bevindingen zullen beschrijven. Het waardenetwerk is gebaseerd op een relatief klein aantal interviews en literatuuronderzoek, en weerspiegelt het ecosysteem voor cybersecurity innovaties in het algemeen, waar Automated Security onderdeel van is.

3.3.1 Inleiding

De elektriciteitssector is een van de meest fundamentele vitale sectoren in Nederland. Zonder elektriciteit komen andere vitale diensten zoals betalingsverkeer, digitale communicatie en transport direct in gevaar. De energietransitie en de bijbehorende elektrificatie zal de afhankelijkheid van elektriciteit in de toekomst verder vergroten. De elektriciteitssector valt, mede hierom, onder de A-categorie binnen de vitale processen van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) . Het elektriciteitsnet is van oudsher ontworpen vanuit een gecentraliseerd, onveranderd en analoog oogpunt, terwijl deze nu juist steeds meer gedecentraliseerd, dynamisch en digitaal wordt. Het is een sterk gereguleerde sector die sinds 1998 aanzienlijk is veranderd door bijvoorbeeld de Elektriciteitswet en de Wet onafhankelijk netbeheer (ook wel de Splitsingswet genoemd), en nu onder streng beleid valt van onder andere de Netcode elektriciteit en de Wet beveiliging netwerk- en informatiesystemen (Wbni).

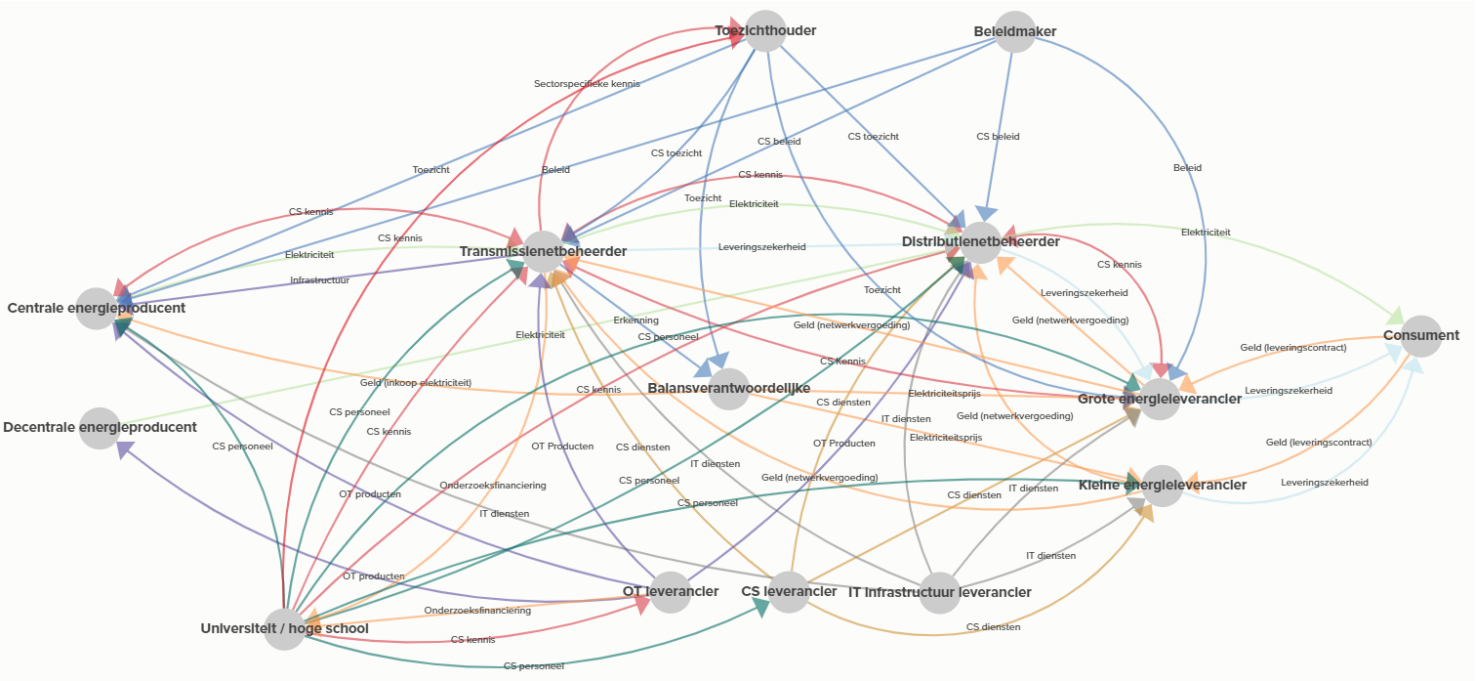
Cyberaanvallen op de energiesector nemen steeds meer toe en worden snel geavanceerder (CSBN, 2020). Twee voorbeelden omtrent gerichte aanvallen op de elektriciteitssector zijn uit de afgelopen jaren zijn:

- In 2015 en 2016 werd de energielevering in Oekraïne verstoord door destructieve malware die de stroomvoorziening stillegden (NOS, 2016).
- In 2019 werd het Noorse energie- en aluminium bedrijf Norsk Hydro slachtoffer van het LockerGoGa virus, waardoor computers van het bedrijf wereldwijd afgesloten moesten worden en geautomatiseerde processen handmatig moesten worden gedaan (Bloomberg, 2019).

Een belangrijk, onderscheidend aspect van de energiesector is het gebruik van Operationele Technologie (OT) binnen de elektriciteitsleveringsketen. OT omvat alle processen die de fysieke systemen binnen de elektriciteitsinfrastructuur aansturen. Deze zijn van oudsher ontworpen met aandacht voor (zeer) lange levensduur en stabiliteit, met weinig aandacht voor cybersecurity. Veel oudere Industrial Control Systemen, als onderdeel van de OT, bevatten hierdoor nog beperkte veiligheidsmaatregelen; toen ze werden ontwikkeld was er simpelweg nog geen dreiging van cyberaanvallen. De systemen worden echter steeds meer verbonden met het internet voor beheer op afstand en monitoring, waarbij het continu belangrijk is dat er rekening met de cyberveiligheidsmaatregelen wordt gehouden. Daarnaast, vanwege de cruciale rol van de elektriciteitssector, kan een geslaagde aanval op deze sector een grote impact hebben. Ook wordt steeds meer elektriciteit decentraal opgewekt, wat resulteert in meer kwetsbare installaties die kunnen fungeren als toegangspoort tot een groter netwerk. De combinatie van deze omstandigheden maakt de elektriciteitssector tot een aantrekkelijk doelwit voor cyberaanvallen.

3.3.2 Waardenetwerk analyse

Figuur 8 toont het waardenetwerk binnen de Nederlandse elektriciteitssector als onderdeel van de energiesector. Hierin is de leveringsketen van elektriciteit in grote lijnen te zien met hier omheen een focus op het ecosysteem voor algemene cybersecurity innovaties. Het netwerk is gebaseerd op een relatief klein aantal interviews en literatuuronderzoek, waardoor het niet allesomvattend zou kunnen zijn. Om het netwerk inzichtelijk te maken, wordt de analyse van het waardenetwerk per sub-netwerk toegelicht. De partijen met wie we gesproken hebben tijdens de interviews staan in bijlage 1B.



Figuur 8 **Schets van het waardenetwerk voor de leveringsketen en cybersecurity innovaties binnen de elektriciteitssector.** De cirkels en de pijlen geven respectievelijk de rollen binnen het ecosysteem en de waarde uitwisseling hiertussen aan. Pijlen met de zelfde kleur geven, waar mogelijk, de zelfde soort waarden aan. Van links naar rechts is centraal in het netwerk de leveringsketen van elektriciteit in grote lijnen terug te zien, met hier onder en boven de leveranciers van diensten en producten en het toezicht en beleid. De toezichthouder op cybersecurity in deze context is het Agentschap Telecom, welke toezicht houdt op de aanbieders van essentiële diensten binnen de Wet beveiliging netwerk- en informatiesystemen (Wbni). Energieproducenten vallen hierdoor wel onder toezicht, maar niet onder specifiek cybersecurity toezicht. Onder de noemer balansverantwoordelijke kunnen zowel een programmaverantwoordelijke als een aggregator vallen. Beide partijen dragen bij aan de geldstromen in het ecosysteem, maar hun rol op het gebied van cybersecurity innovaties is niet duidelijk geworden in ons onderzoek. De rol van kennisinstituten is niet zichtbaar in dit waardenetwerk, aangezien wij geen aanwijzingen hebben gevonden dat deze actief zijn binnen het cybersecurity innovatie ecosysteem in deze sector op dit moment.

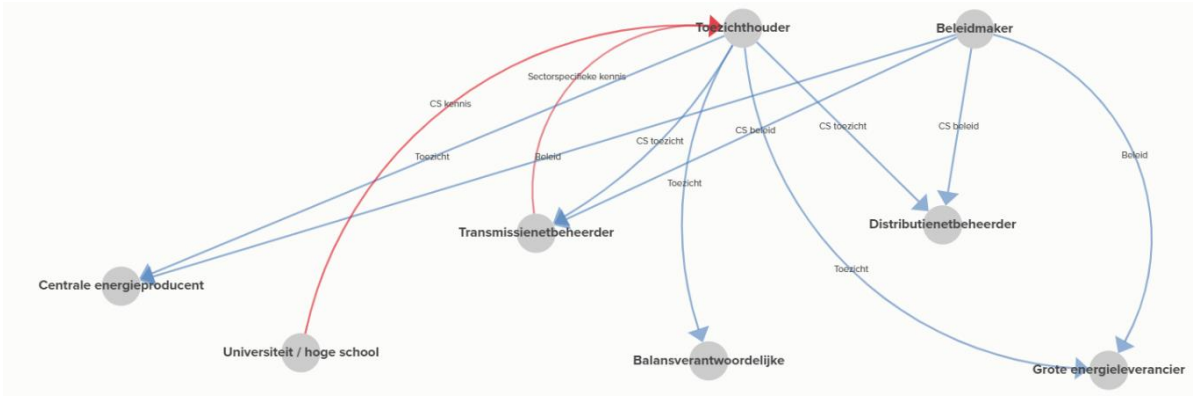
1 Cybersecurity toezicht in de energiesector en de Wbni

Sinds 2018 houdt het Agentschap Telecom (AT) toezicht op de Wbni, welke een meld- en zorgplicht met zich meebrengt. Hierin wordt het onderscheid gemaakt tussen reactief toezicht voor digitale dienstverleners (DSP's) en proactief toezicht voor aanbieders van essentiële diensten (AED's). In de elektriciteitssector behoren de transmissienetbeheerder en alle distributienetbeheerders tot de categorie AED. De andere spelers binnen het ecosysteem vallen op het moment niet onder het toezicht op de Wbni, alhoewel energieproducenten er in de toekomst wel onder zullen vallen.

Het toezicht op de Wbni geldt voor AED's in het algemeen, waar de netbeheerders in de elektriciteitssector slechts een deel van uitmaken. Hierdoor kan het toezicht bemoeilijkt worden wanneer er sectorspecifieke kennis nodig is om cybersecurity op een bepaald onderdeel van de leveringsketen te beoordelen. De bekendheid van de relatief nieuwe toezichthouder voor cybersecurity bij marktpartijen is nog wat laag, en de rol die het gaat spelen in de innovatie nog enigszins ongedefinieerd. Op het moment spelen toezichthouders een vrij kleine rol bij cybersecurity innovatie binnen de sector. De Wbni schrijft geen "checklist" voor aan eisen waaraan voldaan moet worden, maar geeft aan dat de partijen passende en evenredige, technische en organisatorische maatregelen moeten treffen, gelet op de risico's die zich voordoen, om cyberincidenten te voorkomen. Er wordt dus gewerkt met

zogenaamde open normen. Door de open normen die gehanteerd worden vanuit de Wbni, is er geen “push” vanuit deze kant voor een bepaalde innovatie. In de toekomst is het AT wel van plan om cybersecurity innovatie in de markt enigszins te sturen, door bijvoorbeeld cybersecurity dienstverleners te beoordelen op veiligheid. Aangezien er vooral toezicht wordt gehouden op de procesmatige- en systeemrisico’s, ziet het toezicht op het gebied van Automated Security er niet per se anders uit dan op andere cybersecurity gebieden. Automated Security kan zelfs juist een goede aanvulling zijn voor het toezicht, doordat ongewenste handelingen vroegtijdig ontdekt kunnen worden.

Een ander belangrijk aspect is dat de Wbni alleen geldt voor de AED’s zelf en niet voor de toeleverancier(s) van producten of diensten. Hierdoor kan er een risico bij een derde partij ontstaan waar de netbeheerder, producent of leverancier vervolgens zelf verantwoordelijk voor wordt gehouden. Cybersecurity vereisten moeten dus doorvertaald worden naar deze derde partijen. Het lastige hierin is dat bij de afname van producten de Autoriteit Consument en Markt (ACM) een andere bril op heeft voor hun eigen aspect van het toezicht op de markt, waardoor toeleveranciers ook wel of niet geaccepteerd kunnen worden. Verschillende toezichthouders werken wel samen om discrepanties tegen te gaan en om nieuwe dreigingen (bv. elektrische laadpalen) op een goede manier aan te pakken, bijvoorbeeld binnen de inspectieraad. Samenwerkingen met universiteiten in het kader van kennisopbouw komen ook voor. Ten slotte is de energiemarkt nauw verbonden met het buitenland, wat het toezicht kan bemoeilijken. Een probleem in het buitenland zou kunnen leiden tot een kettingreactie die tot Nederland reikt (RLI, 2018).

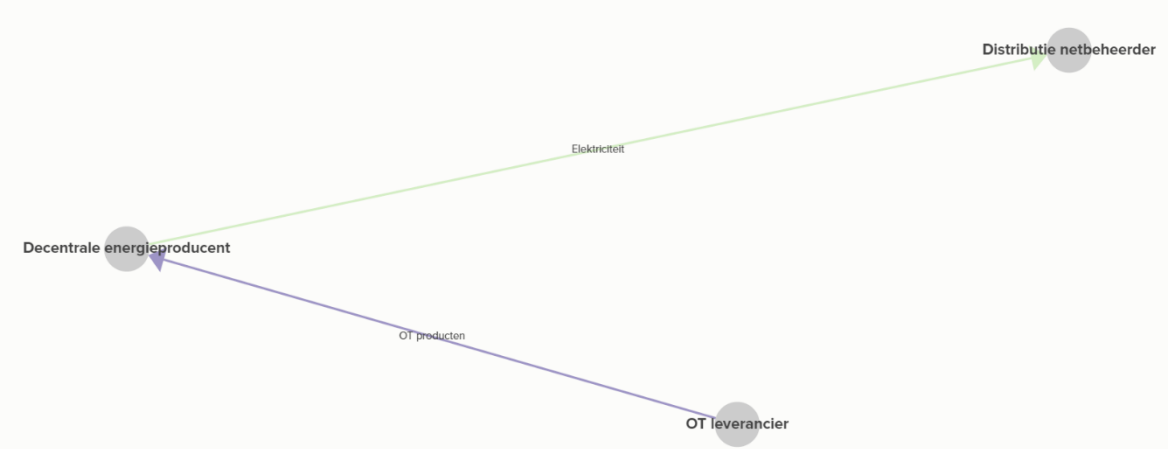


Figuur 9 **Sub-netwerk toezicht en beleid.** Hierin is te zien dat alleen de netbeheerders onder het cybersecurity toezicht en beleid van de Wbni vallen, aangezien zij zijn aangemerkt als aanbieder van essentiële diensten.

2 Disruptieve rol van decentrale producent

De cybersecurity risico’s van een paar relatief nieuwe partijen in de leveringsketen, zoals bijvoorbeeld decentrale energieproducenten, geëlektrificeerde voertuigen en Internet of Things (IoT) apparatuur, kunnen ook een risico voor het gehele energienetwerk veroorzaken door onvoorziene verstoringen van de elektriciteitsbalans. Het perspectief van een netbeheerder wordt niet altijd meegenomen in beslissingen van deze nieuwe partijen, omdat deze (nog) niet in de traditionele leveringsketen van de elektriciteitssector zitten.

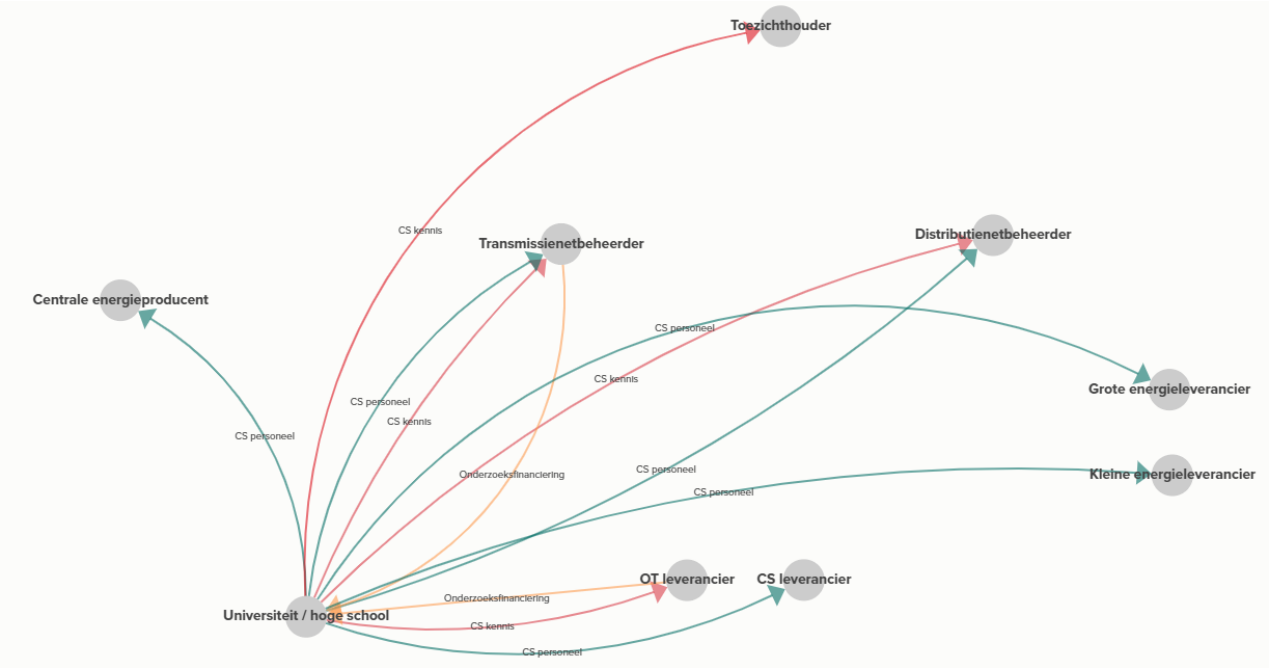
Uiteindelijk kan dit leiden tot onduidelijkheid over wie de rol als eindverantwoordelijke vervult wanneer de leveringszekerheid in gevaar komt door bijvoorbeeld een grootschalige hack van consumentenapparatuur (RLI, 2018). Op Europees niveau is er wel aandacht voor de cybersecurity van het toekomstige elektriciteitsnet, met initatieven zoals de Cyber Security Strategy for the Energy Sector en Security for smart Electricity GRIDs (SEGRID). Er is meer onderzoek nodig om te bepalen in welke mate Automated Security hierop kan inspelen.



Figuur 10 **Sub-netwerk decentrale energieproducent.** De rol binnen het ecosysteem is klein, terwijl de opgetelde impact op de elektriciteitslevering groot zou kunnen zijn.

3 Kennisopbouw en de strijd om cybersecurity personeel

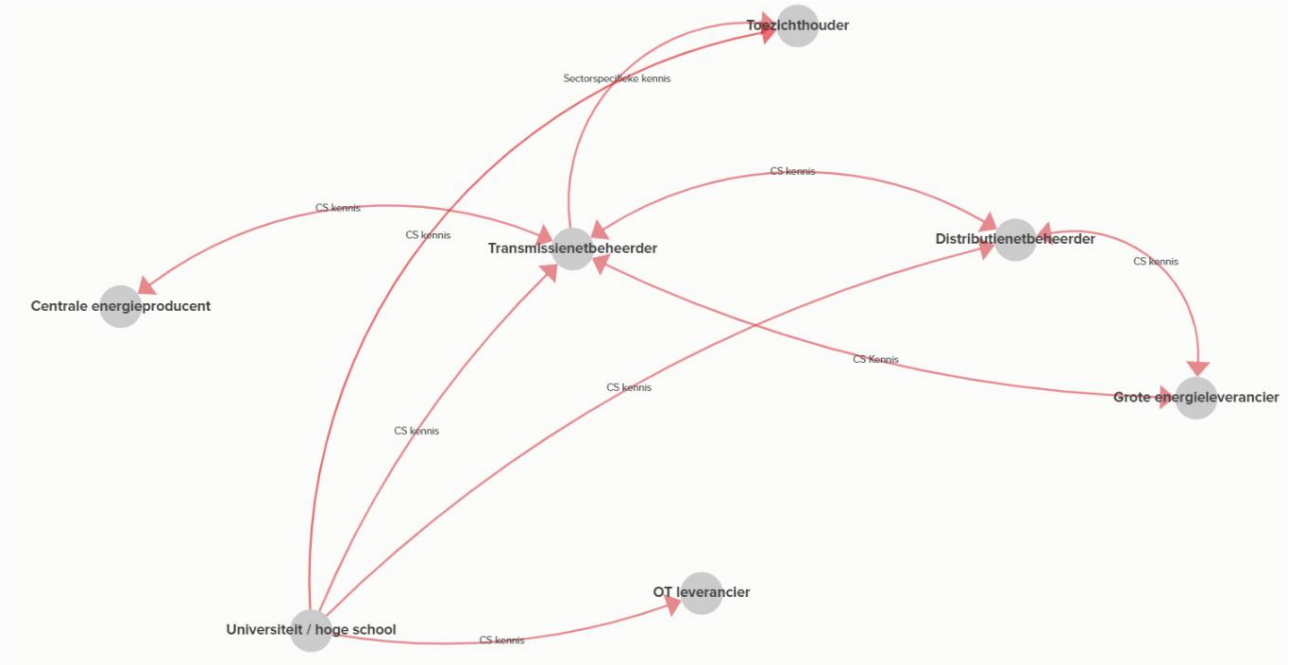
Er is een tekort aan cybersecurity personeel, terwijl alle rollen in de leveringsketen van elektriciteit met grote IT systemen te maken hebben. Beide type netbeheerders en de grootschalige energieproducenten en leveranciers moeten naast cybersecurity van hun IT ook die van de OT systemen beheren. Omdat er een steeds grotere koppeling ontstaat tussen IT en OT, zal de vraag naar cybersecurity personeel naar verwachting in de toekomst verder toenemen.
De onderwijsinstellingen zijn verder betrokken bij verschillende samenwerkingsverbanden in deze sectoren, waar bijvoorbeeld de twee typen netbeheerders en OT leveranciers bij betrokken worden. De meeste netbeheerders staan nauw verbonden met verschillende universiteiten op het gebied van cybersecurity en staan open voor innovaties op het gebied van Automated Security. Hiernaast is de transmissienetbeheerder ook actief bezig met op de hoogte blijven van de nieuwste ontwikkelingen en was deze bijvoorbeeld ook al jaren geleden betrokken bij innovaties op het gebied van *anomaly detection*. Concreet wordt er op dit moment, voor zover bij ons bekend, niet specifiek gewerkt aan onderzoek op de toepassing van Automated Security bij de transmissienetbeheerder. Naast het gebrek aan cybersecurity personeel, worden hier echter verder geen acute barrières voor gezien.



Figuur 11 **Sub-netwerk universiteiten.** Deze leveren aan veel verschillende partijen het schaarse cybersecurity personeel. Verder is er kennisuitwisseling tussen beide netbeheerderrollen en OT leveranciers.

4 Veel kennisdeling en samenwerkingsverbanden

Er is sprake van relatief veel kennisdeling, waar ook cybersecurity innovaties aan bod komen, binnen de partijen die betrokken zijn bij de leveringsketen in Nederland. Voorbeelden zijn de Energie ISAC, Netbeheer Nederland, Internationale (Europese) samenwerkingen, maar ook internationale verbondenheid op het gebied van elektriciteitslevering en productie en de identificatie van gaten in internationaal toezicht. De distributie- en transmissienetbeheerders zijn tevens betrokken bij het European Network for Cybersecurity (ENCS) en er is ook een transmissienetbeheerder community binnen Europa waar kennis wordt gedeeld. Wel is het geval dat deze kennisdeling voornamelijk tussen de netbeheerders en grote spelers plaatsvindt, omdat kleinere spelers een te hoge instap-barrière zien om toe te treden tot deze samenwerkingen. Kleine energieleveranciers vallen hierdoor bijvoorbeeld doorgaans buiten de kennisdelingsinitiatieven door gebrek aan netwerk, capaciteit of incentives. Dit kan ook een bewuste keuze zijn, doordat er intern bijvoorbeeld (nog) geen solide basis is gelegd op het gebied van cybersecurity of omwille van het vermijden van (streng) beleid en toezicht. Dit betekent ook dat de netbeheerders zelf de macht en invloed in handen hebben om bepaalde beslissingen te nemen, bijvoorbeeld in de opgestelde richtlijnen voor slimme laadpalen door ElaadNL.

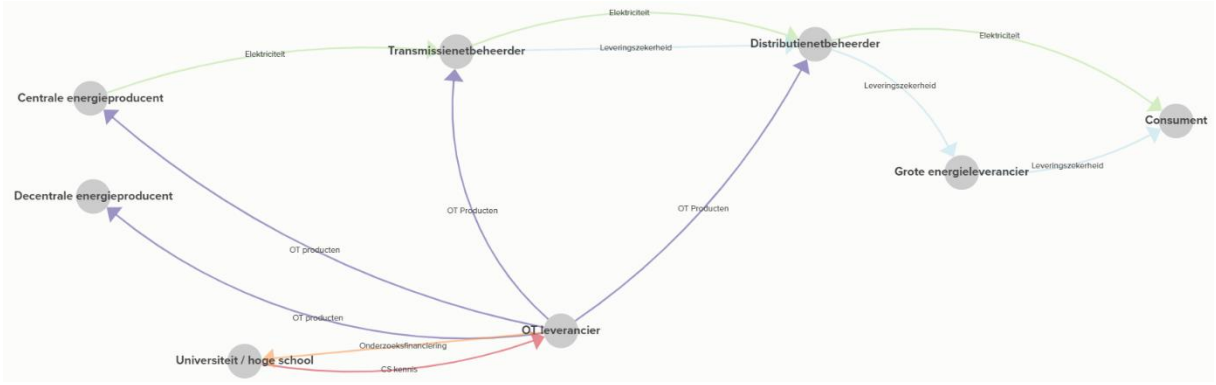


Figuur 12 **Sub-netwerk kennisdeling.** Er bestaat een breed scala aan kennisdelingsinitiatieven en samenwerkingen, waarin zowel in brede zin als specifiek voor cybersecurity kennis wordt gedeeld.

5 OT maakt cybersecurity nog complexer

De belangrijke rol van OT naast, en in combinatie met, de grote IT systemen maken de cybersecurityuitdagingen in de elektriciteitssector nog complexer. Legacy systemen zijn veel voorkomend doordat de apparatuur een hele lange levenstermijn hebben, waarbij tussentijds patchen zeer lastig of simpelweg onmogelijk is. Hierdoor ziet cybersecurity er heel anders uit voor OT dan voor de snel veranderende IT. De opkomende trend van het “slimmer” en verbonden maken van OT verkleint de kloof tussen OT en IT beveiliging. Er is meer onderzoek nodig om de vraag te beantwoorden hoe Automated Security hierop kan inspelen en of dit geschikt is voor de beveiliging van OT. Innovatie binnen de sector wordt ten slotte vaak gestuurd door een “technologie push”, terwijl een probleem-centrische aanpak in sommige gevallen beter zou passen.

Het Nationaal Bureau voor de Verbindingsbeveiliging schrijft adviezen uit voor de aanschaf van producten, maar verder moeten afnemers van OT producten zelf een afweging maken tussen prijs en veiligheid. Security by design is essentieel op het gebied van cybersecurity, maar uiteraard zit hier ook een prijskaartje aan.



Figuur 13 **Sub-netwerk OT, wat onderscheidend is aan de elektriciteitssector.** Deze kan in de toekomst echter steeds meer verbonden raken met de IT infrastructuur, waardoor cybersecurity een grotere rol gaat spelen.

Naast de bovenstaande bevindingen die we aan de hand van het waardenetwerk kunnen laten zien, noemen we hier nog een aantal overige bevinden die naar voren zijn gekomen tijdens onze analyse.

1 **Innovatie op het gebied van cybersecurity wordt gestuurd door de intrinsieke verantwoordelijkheid voor leveringszekerheid**. De ontwikkelingen worden goed in de gaten gehouden en er wordt bijvoorbeeld ook gekeken naar het opkopen van start-ups om vanuit buitenaf kennis op het gebied van digitale innovaties naar binnen te halen. Er is niet per se een push vanuit de toezichthouder om te innoveren, wat natuurlijk niet inherent nadelig hoeft te zijn.
2 **Netbeheerders zijn geen onderlinge concurrenten**, aangezien ze allemaal hun eigen aangewezen leveringsgebied hebben. Er bestaan echter wel verschillen tussen grote en kleine distributienetbeheerders. Dit is in tegenstelling tot bijvoorbeeld energieleveranciers, welke wel onderlinge concurrenten, waardoor er een verschil is in de budgetten die mogelijk zijn voor cybersecurity (innovaties).
3 **Investeringen in netbeheer zijn vaak lange termijn beslissingen** en gaan over het algemeen traag, aangezien het systeem continu draaiende moet blijven. Met name voor het vervangen van OT is veel gespecialiseerde kennis nodig, aangezien tussendoor *patchen* niet altijd mogelijk is.

Ten slotte willen we aankaarten dat we in deze analyse de gassector buiten beschouwen hebben gelaten. Twee belangrijke verschillen hierbij zijn dat er in de gassector geen sprake is van decentrale opwek en dat enige verstoring in de balans van vraag en aanbod aanvaardbaar is door toe- of afname van de druk in een gasleiding. We zijn echter niet ingegaan op de vraag of er belangrijke andere verschillen tussen de gas- en elektriciteitssector zijn die innovatie op het gebied van cybersecurity kunnen beïnvloeden. In een vervolgonderzoek zou ook gekeken kunnen worden naar de toepassing van Automated Security binnen de gassector.

3.4 Waardenetwerk analyse – Cross-sectorale bevindingen en vervolgvragen

Uit de onafhankelijke analyses van de twee sectoren zijn een aantal brede, overkoepelende of samenhangende bevindingen gekomen die relevant kunnen zijn voor de toepassing van Automated Security. Een aantal overeenkomsten die gelden voor beide vitale infrastructuur sectoren zijn:

- Er zijn binnen de sectoren zelf veel kennisdelingsinitiatieven en overkoepelend zorgt de Wbni ervoor dat cybersecurity incidenten bij de aangewezen AED's gemeld worden bij het NCSC en de bevoegde toezichthouder. Hiernaast is er ook kennisdeling tussen de verschillende ISACs en binnen de vitale infrastructuurpartijen in bijvoorbeeld de Commissie vitale infrastructuur. Is er echter voor alle betrokken partijen wel genoeg overzicht tussen al deze goedbedoelde initiatieven en welke soort kennis op welk vlak met welke andere partij gedeeld moet of kan worden? En is er behoefte aan regie, kennisdeling of samenwerking tussen al deze initiatieven?

- In beide sectoren is er sprake van opkomende versplintering van services en decentralisatie, waardoor er op steeds meer punten in het systeem data-uitwisseling plaatsvindt. Aan de ene kant leidt dit tot meer plekken met potentiele kwetsbaarheden, en aan de andere kant kan een dergelijke decentralisatie er juist voor zorgen dat een aanval in een enkel punt niet meteen de hele keten treft. Of de decentralisatie juist voor meer of minder cybersecurity risico's zorgt is dus niet direct duidelijk. Automated Security vraagt in sommige gevallen om een gecentraliseerd overzicht van de hele data leveringsketen om over het netwerk als geheel geautomatiseerd toezicht te kunnen houden. Dit roept een aantal vragen op, zoals: hoe haalbaar is dit in sectoren die steeds meer versnipperd raken? En, zeker niet onbelangrijk, is er genoeg vertrouwen in cybersecurity leveranciers om deze Automated Security oplossingen te integreren?

- In beide sectoren geldt dat er steeds meer nieuwe, disruptieve spelers de markt betreden. Deze kleinere spelers zijn zich minder bewust van de risico's die ze lopen, zijn voor cybersecurity vaak afhankelijk van derde partijen en hebben er vaak geen (ruim) budget voor. Voornamelijk de grote bedrijven binnen beide sectoren hebben de tijd, mankracht, budget en incentive om te innoveren op het gebied van cybersecurity. Dit roept verschillende vragen op:
  - Zijn deze kleinere partijen zich voldoende bewust van de risico's die zij lopen wat betreft cybersecurity? En zo niet, hoe kan er bij deze partijen voor meer bewustwording worden gezorgd en hoe kunnen zij in de kennisdeling meegenomen worden?
  - Is het wenselijk dat kleinere spelers in de leveringsketen ook meegenomen kunnen worden in cybersecurity innovaties, waaronder Automated Security, en hoe kan daarvoor gezorgd worden?

Aan de andere kant zijn er ook verschillen die we zijn tegenkomen tijdens onze analyse:

- De rol van cybersecurity verschilt aanzienlijk in de financiële- en elektriciteitssector. Een aanval op de financiële sector levert voor hackers of kwaadwillenden vaak direct geld op, waardoor de sector een groot doelwit is

van cybersecurity aanvallen. Cybersecurity, en de innovatie hiervan, komt daarom haast overal in deze keten voor. In de elektriciteitssector is de incentive voor kwaadwillenden om de levering te verstoren inherent anders: een aanval kan leiden tot grootschalige stroomuitval, met alle gevolgen van dien, in plaats van direct financieel gewin. Daarnaast berust de levering van diensten in de elektriciteitssector grotendeels op OT, waardoor veiligheid meer betekent dan alleen *cyber*security. Over deze OT zit wel een “laag” van IT, die steeds meer met de OT versmolten raakt. Het is belangrijk om deze verschillen mee te nemen bij het aanprijzen van Automated Security producten om aan te sluiten op de marktvraag binnen een sector.

- Voor beide sectoren zijn verschillende programma’s die ervoor moeten zorgen dat ze beter bestand zijn tegen cyberaanvallen. Dat roept de vraag op of en in hoeverre deze programma’s ook voor andere sectoren ondersteuning kunnen bieden. Biedt bijvoorbeeld de toepassing van het TIBER raamwerk, welke de DNB toepast in de financiële sector, ook uitkomst voor partijen binnen de energiesector en kan dit in de toekomst leiden tot zicht op risico’s die voortkomen uit gedecentraliseerde elektriciteitsproductie?

De aard van dit onderzoek is een verkenning en roept ook enkele losstaande vervolgvragen op. Zo is het lastig in te schatten hoe algemeen de bevindingen zijn: vervolgonderzoek zal uit moeten wijzen in hoeverre de bevindingen breed toepasbaar zijn. Daarnaast is het niet met zekerheid te zeggen of alle belangrijke knelpunten geïdentificeerd zijn en welke rol Automated Security kan spelen in het oplossen van deze knelpunten. In het specifiek merken we de volgende vervolgvragen op:

- Wat zijn de belangrijkste pijnpunten waar spelers in de waardeketens tegenaanlopen wat betreft cybersecurity? En kan Automated Security op dit moment waarde toevoegen om deze pijnpunten te verhelpen en op welke manier zou dat moeten gebeuren? Veel van de cybersecurity problemen die op het moment het grootst zijn voor de financiële sector, zoals phishing en onvoorzichtigheid van werknemers, worden veroorzaakt door de “human factor” (IBM, 2019). Als Automated Security ook ondersteuning biedt bij het detecteren en oplossen van deze problematiek, kan het de aantrekkelijkheid voor deze sector bevorderen.

Ook kan de rol van Automated Security voor toezichthouders in de ketens meer in kaart worden gebracht:

- In welke mate kan de toepassing van Automated Security binnen de leveringsketen van de vitale infrastructuur ondersteuning bieden in het toezicht op de gehele vitale infrastructuur door meer lokale risico’s, en daarmee het systeemrisico als geheel, zichtbaar te maken?

4 Invulling routekaart Automated Vulnerability Research

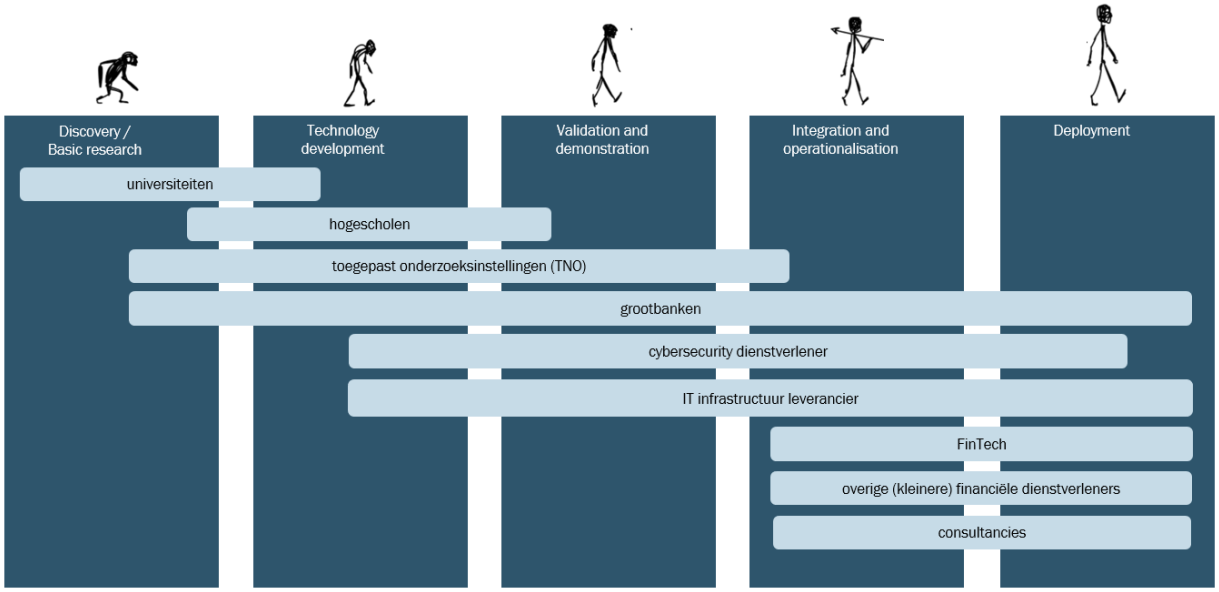
Het doel van de routekaart Automated Vulnerability Research (AVR) is om de nationale capaciteiten op het gebied van AVR te versterken en uit te bouwen, en om de achterstandspositie die Nederland ten opzichte van andere landen heeft te beperken of zelfs in te lopen. Dit vraagt om een meerjarige investering in kennis en technologieontwikkeling. De routekaart richt zich op de periode 2021 tot en met 2026, omdat in zes jaar een substantiële impuls aan het onderwerp kan worden gegeven en concrete resultaten kunnen worden behaald.

De gegevens uit de marktverkenning en waardenetwerk analyse kunnen als fundament worden gebruikt voor de routekaart. Omdat dit project input moest leveren voor de AVR routekaart, zijn de marktverkenning en waardenetwerk analyse binnen relatief korte tijd uitgevoerd. De nadruk is gelegd op het ophalen van zoveel mogelijk relevante bevindingen voor Automated security, en specifiek voor AVR. Er is echter vervolgonderzoek nodig om deze bevindingen verder te kunnen nuanceren en uit te breiden ter invulling van de routekaart. De routekaart is onderverdeeld in vijf ontwikkelfases: *Discovery/basic research, Technology development, Validation and demonstration, Integration and operationalization, Deployment*.

De indeling van de partijen binnen de vijf ontwikkelfases is gebaseerd op een doorvertaling van de inzichten die uit de waardenetwerk analyse zijn verkregen. Daarnaast zijn tijdens deskresearch en de interviews ‘v*alleys of death’* geconstateerd en plotten we ook deze, waar mogelijk, op de vijf ontwikkelfases. Als laatste zetten we de sporen uit waar mogelijke oplossingen beschreven worden voor het overwinnen van de barrières en de ‘valleys of death’, welke met de routekaart bewandeld kunnen worden.

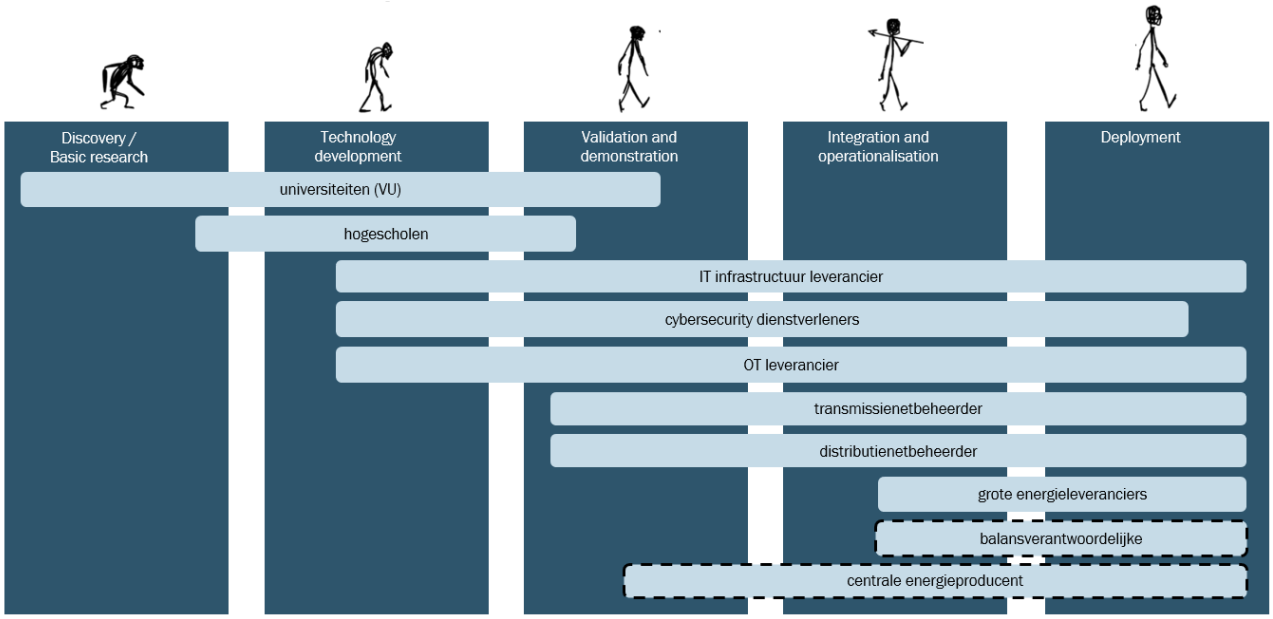
4.1 Overzicht 1: Betrokken partijen

Binnen zowel de financiële- (Figuur 14) als de energiesector (Figuur 15) zijn in alle ontwikkelfases meerdere partijen betrokken. Daarnaast spelen binnen de financiële sector in het begin van de ontwikkelfases vooral de kennisinstellingen een rol. Ook de grootbanken spelen in deze fase een rol in de vorm van het leveren van data en het aanbieden van stages, werkplekken en financiële ondersteuning. Vervolgens spelen technologie bedrijven een rol bij de ontwikkeling, validatie en demonstratie van technologieën, en het operationaliseren en implementeren van producten. Ook de eindgebruikers hebben een rol in deze fases, net zo als de cybersecurity providers, leveranciers van IT infrastructuur en consultancy partijen. Twee partijen binnen de financiële sector zijn niet te vatten binnen de ontwikkelfases maar zijn keten overstijgend, te weten de toezichthouders (DNB, AFM) en de beleidsmakers.



Figuur 14 Schets op basis van literatuuronderzoek en interviews van de partijen binnen de valorisatieketen van de financiële sector.

Tijdens deskresearch en de interviews is naar voren gekomen dat binnen de energiesector alleen de universiteiten en hoge scholen een rol spelen tijdens de eerste ontwikkelfase van technologieën, op dit moment lijken de kennisinstellingen hier geen rol in te spelen. De universiteiten en hoge scholen spelen niet alleen een rol tijdens de eerste twee fases, maar ook bij validatie en demonstratie. Het lijkt erop dat, met uitzondeling van de kennisinstellingen, alle partijen een rol spelen bij de integratie, het operationaliseren en de deployment van nieuwe ontwikkelingen. Dit beeld is ook te zien bij de financiële sector. Bij deze sector weten we dat er een rol is voor balansverantwoordelijke en de centrale energie producent. Duidelijkheid over deze rol is echter niet naar voren tijdens deskresearch en de interviews, vandaar de stippellijn in het figuur.



Figuur 15 Schets op basis van literatuuronderzoek en interviews van de partijen binnen de valorisatieketen van de energiesector.

4.2 Overzicht 2: 'Valleys of Death' tussen de ontwikkelfases

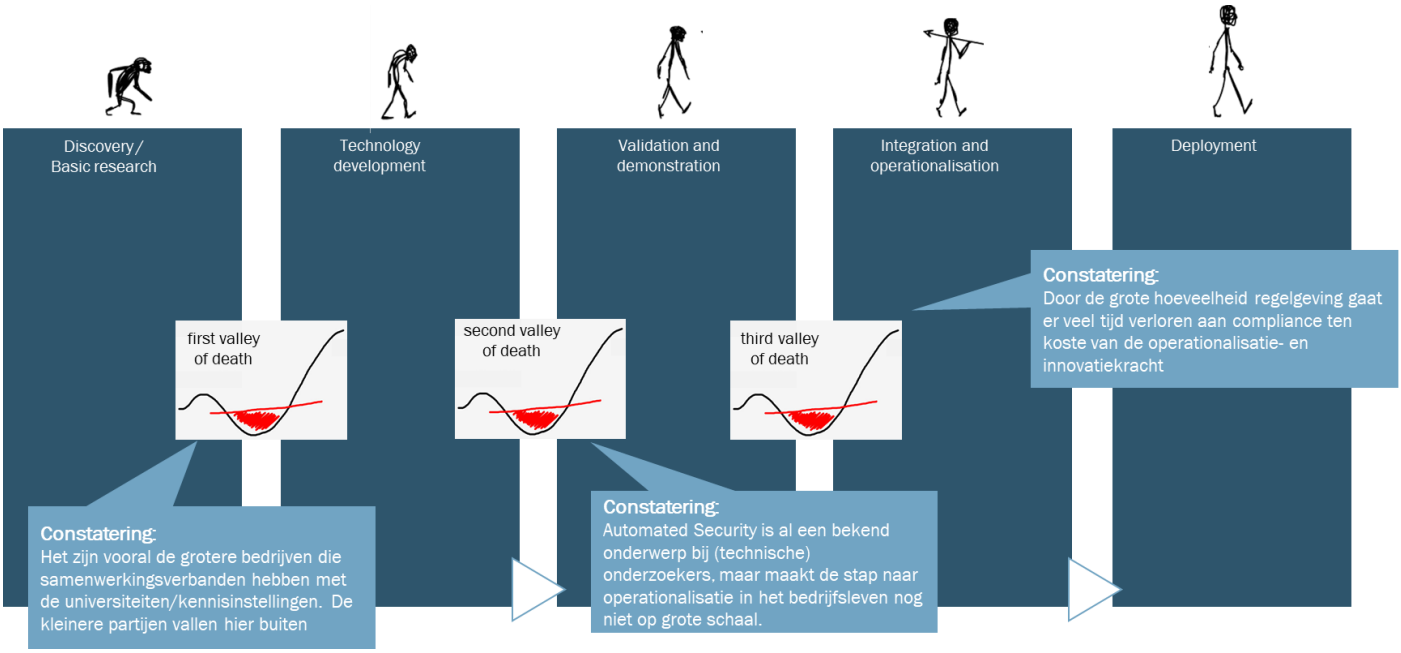
Met een '*valley of death'* bedoelen we een barrière tussen de ontwikkelfases van innovatie, welke zijn geschetst in Figuur 16. Uit de waardenetwerk analyse komt naar voren dat er een *'valley of death'* lijkt te bestaan tussen wetenschappelijk onderzoek en het ontwikkelen van technologie (tussen ontwikkelfase één en twee), vooral bij de kleinere financiële dienstverleners en kleinere energie leveranciers. Grootbanken zijn wel betrokken bij de kennisinstellingen in de financiële sector, maar kennis lijkt binnen deze organisaties te blijven en niet gemakkelijk naar de kleinere financiële dienstverleners te komen. Binnen de energiesector werken universiteiten ook vooral samen met de netbeheerders en in veel mindere mate met kleinere energie leveranciers. Dit maakt het voor de kleinere partijen lastig om de stap van fundamenteel onderzoek naar de ontwikkeling van een product te maken.

Binnen beide sectoren bestaat ook een '*valley of death*' tussen het ontwikkelde product en het valideren en demonstreren hiervan (ontwikkelfase twee en drie). Automated Security is een jong onderwerp, dat tot nu toe voornamelijk bekend is bij (technische) onderzoekers. Het valideren en demonstreren van de nieuw ontwikkelde producten in een bedrijfsomgeving gebeurt op dit moment nauwelijks. Hier kan bijvoorbeeld een gebrek aan testdata en testomgevingen een beperking vormen om te komen tot validatie van producten.

Daarnaast bestaat binnen beide sectoren een '*valley of death*' tussen het demonstreren en operationaliseren van nieuwe producten. Uit de interviews en deskresearch komt naar voren dat dit kan komen door de strenge regulaties door middel van wetten en regels binnen de sectoren. Hierdoor moet veel tijd en energie besteed worden aan compliance, waardoor minder ruimte is voor innovatie. Samen met de schaarste aan capaciteit om de stap te kunnen maken van demonstratie naar operationalisatie, maakt dit de kloof tussen deze ontwikkelfases extra groot.

De constatering van het gebrek aan (hoog)opgeleid, gespecialiseerd cybersecurity personeel dat we hierboven benoemden is echter ook een keten overstijgende *'valley of death'*, welke van toepassing is vanaf wetenschappelijk onderzoek tot en met de integratie en operationalisatie van nieuwe producten. Er is vraag naar dit type personeel vanuit de partijen die betrokken zijn bij de valorisatie, maar ook vanuit de toezichthouders en beleidsmakers in de financiële sector en vanuit de energiesector is ook vraag naar cybersecurity personeel voor OT.

Naast gebrek aan goed opgeleid personeel blijkt er geen centrale organisatie te zijn op het gebied van kennisdeling. Er zijn vele samenwerkingsinitiatieven binnen beide sectoren, maar er is geen onafhankelijke orchestrator. Tijdens de interviews uit beide sectoren komt naar voren dat meer synergie tussen de verschillende parallelle samenwerkingsverbanden zou kunnen helpen ter overbrugging van één of meerdere *'valleys of death'*. Door kennisdeling kunnen bijvoorbeeld overeenkomsten zichtbaar worden in innovaties die worden ontwikkeld, of men kan gaten ontdekken waar nog helemaal niet op geïnnoveerd wordt, terwijl daar wel behoefte aan is.



Figuur 16 De "*Valleys of Death*" in de ontwikkelfases die uit deskresearch en de interviews naar voren kwamen

4.3 Overzicht 3: Fundament voor de vier sporen

Uit de waardenetwerk analyse zijn een aantal belangrijke thema's naar boven gekomen.

- **Schaarste aan cybersecurity personeel:** binnen het gehele cybersecurity ecosysteem is een grote vraag naar cybersecurity personeel. Het gaat hierbij zowel om personeel dat nodig is tijdens de ontwikkelfases als personeel met cybersecurity kennis voor toezicht en controle. De vraag naar cybersecurity personeel richt zich vooral op de cybersecurity opleidingen binnen universiteiten en hoge scholen. Het is Interessant om te kijken welke competenties worden gevraagd door de verschillende partijen, om op deze manier een goede match

te kunnen maken met de vaardigheden van studenten bij de verschillende opleidingen. Meer aandacht van de opleidingen voor Automated Security zou kunnen helpen. Daarnaast zou wellicht meer concreet naar de lespakketten kunnen worden gekeken om de competenties van de studenten zo goed mogelijk aan te laten sluiten bij de vraag uit de markt.

- **Samenwerking/kennisdeling:** er zijn vele samenwerkingsverbanden in beide sectoren op het gebied van cybersecurity. Een centrale organisatie die sturing geeft aan deze samenwerkingsverbanden is er echter niet. Het zou interessant zijn om te kijken of een onafhankelijke orchestrator kan helpen om de innovatie te versnellen/helpen door de niches waarin wordt samengewerkt bij elkaar te brengen. Daarnaast lijkt samenwerking binnen de financiële- en energiesector vooral plaats te vinden tussen de grotere partijen. Tussen de onderzoeksinstellingen en grootbanken bestaat bijvoorbeeld een langdurige en grootschalige samenwerking. Dit draagt zowel bij aan het versterken van de ontwikkeling van fundamentele kennis op gebieden waar behoefte aan is bij de eindgebruiker, als het verbeteren van de stap naar het operationaliseren. Voor kleinere partijen (kleinere financiële dienstverleners of energie leveranciers) en partijen binnen de FinTech lijkt toetreden tot de ‘innovatieloop’ lastiger. Kleinere partijen lijken buiten deze samenwerkingsverbanden te vallen. Dit kan komen door bijvoorbeeld het gebrek aan netwerk, maar ook aan het gebrek aan capaciteit binnen deze partijen. Het is interessant om te verkennen of door het invoeren van een orchestrator rol de samenwerking met de kleinere partijen uit de sectoren vorm kan worden gegeven door het bieden van een netwerk. Door ook hun behoeften, kennis en capaciteit vroegtijdig mee te nemen in het ontwikkelproces kan de stap van fundamenteel onderzoek naar productontwikkeling én de stap naar het operationaliseren worden versterkt. Daarbij wordt de stap van fundamenteel onderzoek naar de toepassing en operationaliseren ervan samengebracht.

- **Regulering /toepassing:** binnen het cybersecurity ecosysteem is een sterke regulatie, waarbij ook grensoverschrijdend gekeken moet worden naar internationale wetten, regels en eisen. Zowel binnen de financiële- als de energiesector is sprake van een toenemende mate van decentralisatie. Dit zorgt ervoor dat op bepaalde delen van het netwerk geen toezicht wordt gehouden, wat cybersecurity issues met zich mee kan brengen. Het dichten van deze gaten in toezicht kan ook innovatie aanjagen. Het zou dus interessant zijn om te onderzoeken hoe gaten in het toezicht kunnen worden gedicht, zonder dat dit het operationaliseren van producten extra complex maakt.

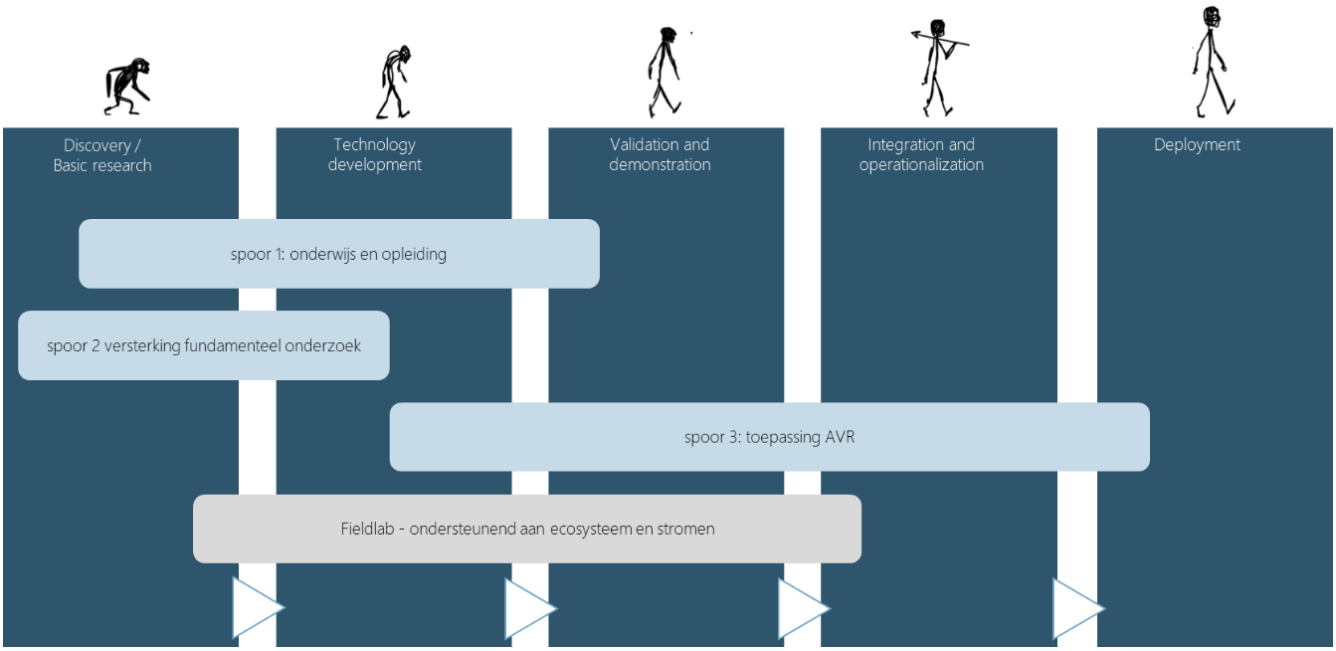
Deze bevindingen kunnen worden gevat in vier sporen om uit te werken in een routekaart. Deze sporen zijn als volgt:

1 **Onderwijs en opleiden**: meer aandacht geven aan Automated Security binnen de opleidingen kan al helpen in de kennisverspreiding bij de studenten. Het meer specifiek opleiden van studenten met een passend competentieprofiel voor de vragende partijen, kan nog een bijdrage leveren aan het verminderen van de schaarste aan cybersecurity personeel.
2 **Versterken samenwerking bij fundamenteel onderzoek**: fundamenteel onderzoek uitvoeren is essentieel voor innovatie op het gebied van Automated Security. De vraag naar onderzoek zou idealiter moeten komen van een eindgebruiker die een ontwikkeld product kan inzetten binnen de infrastructuur

van de organisatie. Samenwerkingsverbanden tussen de kennisinstellingen, partijen die producten ontwikkelen en de eindgebruikers is dus van groot belang. Wellicht is het een idee om een centrale orchestrator Automated Security te introduceren bij de al bestaande samenwerkingsverbanden, zodat deze samenwerkingsverbanden aan initiatieven binnen dit onderwerp kunnen werken. Dit kan de kloof tussen kennisopbouw en het uiteindelijk operationaliseren van producten bij de eindgebruikers verkleinen.

3 **Toepasbaar maken van producten**: Het fundamentele onderzoek moet getoetst worden op toepasbaarheid binnen concrete situaties bij eindgebruikers. Ook hier is het belangrijk om partijen in het ontwikkel traject van producten vroegtijdig samen te brengen. Daarnaast moet rekening worden gehouden met de (inter)nationale wet- en regelgeving.

4 **Fieldlab**: Er bestaat geen centrale kennisdeling tussen de bestaande samenwerkingsverbanden. Primair is een fieldlab verantwoordelijk voor informatieoverdracht en samenwerking tussen en binnen de hierboven genoemde drie sporen. Het fieldlab is geen fysieke ruimte waarbinnen wordt geëxperimenteerd, maar een virtuele ruimte waar experimenten en data kunnen worden uitgewisseld. Op deze manier kan kennis vanuit verschillende niches binnen Automated Security elkaar versterken. Dit zal bijdragen aan de drie punten die hierboven zijn genoemd. Partijen vanuit alle ontwikkelfases moeten met elkaar samenwerking om tot een goed lopende valorisatieketen te komen.



Figuur 17 Sporen routekaart Automated Vulnerability Research.

5 Bibliografie

5 Cybersecurity Weaknesses In The Banking And Finance Industry | Swivelsecure.com (2018).

AUSI: An integrated approach to Value Network Analysis (R12144) | TNO (2013).

Global Wealth Report | BCG (2019).

Cybermisdaad: wat is erger, verlies van gegevens of vertrouwen? | EY (2019).

Cybersecuritybeeld Nederland (CSBN) 2020 | Publicatie | Nationaal Cyber Security Centrum (2020).

Cyberveiligheid | Nederlandse Vereniging van Banken (2020).

De Economische en Maatschappelijke Noodzaak van Meer Cybersecurity | Cyber Security Raad (2016).

Digitale Spionage en Cybercriminaliteit Groeiende Dreiging voor Energiesector | Compact (2014).

FinTech action plan: For a more competitive and innovative European financial sector | European Commission (2018).

Hackers legden energiecentrales Oekraïne plat | NOS (2016).

IB Monitor | DNB (2020).

IBM X-Force Intelligence Index | IBM (2019).

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

Maatwerk voor Innovatie (Regulatory Sandbox) | DNB (2016).

Nordic Metals Giant Restarts Some Systems After Randomware Attack | Bloomberg (2019).

Partnership for Cyber Security Innovationn | PCSI (2020).

Werken aan digitaal vertrouwen begint voor financials bij medewerkers | PwC NL (2018).

Risicorapportage cyberveiligheid economie | CBP (2019).

Samenwerkingsplatform cybersecurity. Advies kwartiermakers. Kamerstuk 2020.

Small and Medium-sized Financial Institutions: The Security Challenges They Face Each Day | Security Magazine (2019).

Stroomvoorziening Onder Digitale Spanning | RLi (2018).

Tekort aan cybersecurity talent blijft groeien | Dutch IT-channel (2018).

TIBER: samen tegen cybercrime - De Nederlandsche Bank | DNB (2020).

Onderzoek naar het versterken van de innovatieketen op het terrein van cybersecurity | TNO (2020).

Trends en scenario’s voor de Nederlandse financiële sector | CPB (2019).

WODC | 3097 - Cybersecurity informatie-uitwisseling | WODC (2020).

6 Ondertekening

Den Haag, december 2020

Drs. K.Y. de Jong
Research manager

TNO
Networked Organisations

Dr. D. Tiggelman
Auteur

Bijlage 1. Overzicht geïnterviewde partijen

A. Marktverkenning

Riscure
TU Delft
iSOC24
Northwave
VTM
Vrije Universiteit Amsterdam (VUSec)
TU/e
Telindus
TNO

B. Waardenetwerkanalyse

Partij (eerste 5 financiële sector, rest energiesector)	**Rol**
Overkoepelende FinTech organisatie	Chief Executive Officer (CEO)
Onderzoeksinstituut	Senior Consultant 1
Toezichthouder	Supervisor IT risk en Specialist TIBER Team
Grootbank	Chief Information Security Officer (CISO)
Universiteit	Professor Governance of Cybersecurity
Onderzoeksinstituut	Senior Consultant 2
Distributienetbeheerder	Advisor Asset Management
Transmissienetbeheerder	Associate Director Safety & Security en Senior Cyber Security Advisor
Energieleverancier	Information Security Officer
OT leverancier	Technical Officer Enterprise Security
Adviesorgaan overheid	Adviseurs digitale veiligheid vitale sectoren
Toezichthouder	IT Auditors (gericht op Wbni)