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

www.tno.nl

T +31 88 866 10 00

TNO-rapport

TNO 2022 R10712

EZK Valorisatieketens: Waardenetwerk Cryptocommunicatie

Datum	September 2022
Auteur(s)	Dr. D. Tiggelman Ir. Y.J. Meijaard Drs. ir. J.T. Rabbie Drs. L.I. Soldaat Drs. V. Szijjarto Dr. ir. T.M.M. Laarhoven Drs. M.S.C. van Leuken Drs. M. Breure
Aantal pagina's	56 (incl. bijlagen)
Aantal bijlagen	2
Opdrachtgever	Ministerie van Economische Zaken en Klimaat
Projectnaam	EZK: Valorisatieketen Cryptocommunicatie
Projectnummer	060.50500

Samenvatting

Nederland is een koploper op gebied van digitalisering en moet met hoge snelheid blijven digitaliseren om deze positie te behouden. De digitalisering moet echter wel op een veilige manier plaatsvinden. Cryptocommunicatie is het fundament van veilige digitale communicatie en gegevensuitwisseling. Onder cryptocommunicatie verstaan we cryptografie in de brede zin, waarbij het nadrukkelijk gaat om cryptografie in een groter geheel van informatietechnologie en de toepassing ervan voor de uitvoering van bedrijfsprocessen. Kortom, cryptocommunicatie is de toepassing van cryptografie voor veilige verzending, verwerking, opslag, en beschermd uitwisselen van informatie.

In dit rapport beschrijven we de valorisatieketen van cryptocommunicatie, die als fundering dient voor de routekaart cryptocommunicatie. Het doel van de routekaart cryptocommunicatie is drieledig: allereerst voor de ontwikkeling van innovatieve producten en diensten op het gebied van cryptocommunicatie, daarnaast voor het bijdragen aan de economische activiteit in Nederland en als derde om de strategische autonomie van Nederland te stimuleren. Inzicht in de valorisatieketen is hierbij van belang: een economisch gezond ecosysteem en sterk functionerend waardenetwerk draagt bij aan het behalen van de doelstellingen van de routekaart cryptocommunicatie.

Dit rapport beschrijft allereerst een verkenning van het cryptocommunicatie ecosysteem, gebaseerd op een Europese marktverkenning. Vervolgens wordt de waardenetwerkanalyse cryptocommunicatie binnen de energie- en automotive sector beschreven. Tenslotte worden barrières (‘valleys of death’) geïdentificeerd en worden mogelijke oplossingen beschreven (vertaald in vier ‘sporen’). Deze bevindingen kunnen worden gebruikt bij het opstellen en aanscherpen van de routekaart cryptocommunicatie.

Marktverkenning
De marktverkenning op niveau van de Europese Unie (EU) is uitgevoerd aan de hand van literatuuronderzoek en interviews met een selectie van partijen, welke geselecteerd zijn op hun kennispositie binnen het ecosysteem. Uit zowel het literatuuronderzoek als de interviews is gebleken dat de eerder geïdentificeerde innovatie-trajecten, zoals geformuleerd in ‘Nederland Cryptoland’, sterk overeenkomen met de huidige lopende innovatie-trajecten die op de Europese markt geïdentificeerd zijn. Met name Duitsland en Frankrijk zijn sterk op het gebied van cryptocommunicatie. Nederland heeft binnen Europa ook een goede reputatie, waarbij Nederland veel samenwerkt op internationaal niveau binnen vele samenwerkingsverbanden.

In het marktonderzoek zijn verschillende barrières geïdentificeerd die door partijen worden ervaren, die de ontwikkeling van innovaties in het cryptografische landschap tegenwerken. De belangrijkste zijn:
- Tekort aan technisch personeel, met name op het gebied van innovaties;
- (Te) veel academische druk op het publiceren van wetenschappelijke publicaties binnen cryptografie;
- Te weinig investeringen in crypto-analyse;
- Belangenverstrengeling bij de ontwikkeling van standaardisatie;

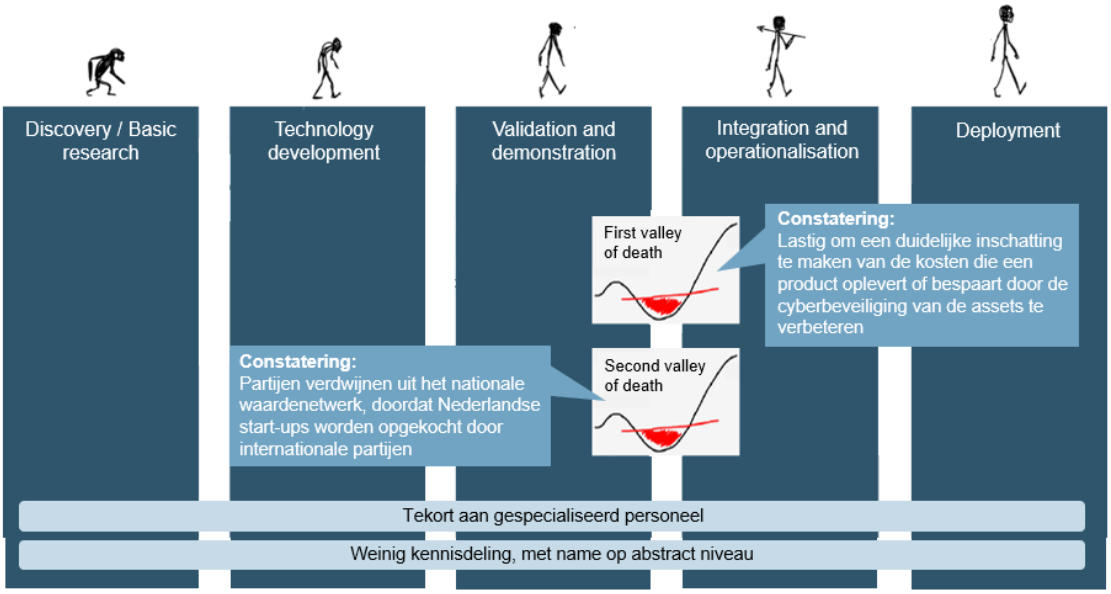
- Er is niet genoeg samenwerking tussen de verschillende EU-lidstaten;
- Crypto-agility is lastig haalbaar in hardware.

Waardenetwerkanalyse
Waardenetwerkanalyse is een gestructureerde methode waarin door een combinatie van interviews en literatuuronderzoek een innovatie ecosysteem in kaart kan worden gebracht. Hierin zijn verschillende rollen zichtbaar, welke met elkaar verbonden zijn door middel van waarde-uitwisselingen. Het waardenetwerk laat hiermee de verschillende relaties binnen het ecosysteem zien en richt zich naast geld ook op andere waarden zoals kennis, personeel en innovatiekracht. Tevens worden samenwerkingsverbanden en barrières inzichtelijk en visueel gemaakt. In dit onderzoek hebben we de waardenetwerken voor cryptocommunicatie in twee toepassingssectoren in kaart gebracht: wind op zee als onderdeel van de energiesector en (directe) 'vehicle-to-all' (V2X) communicatie als onderdeel van de automotive sector.

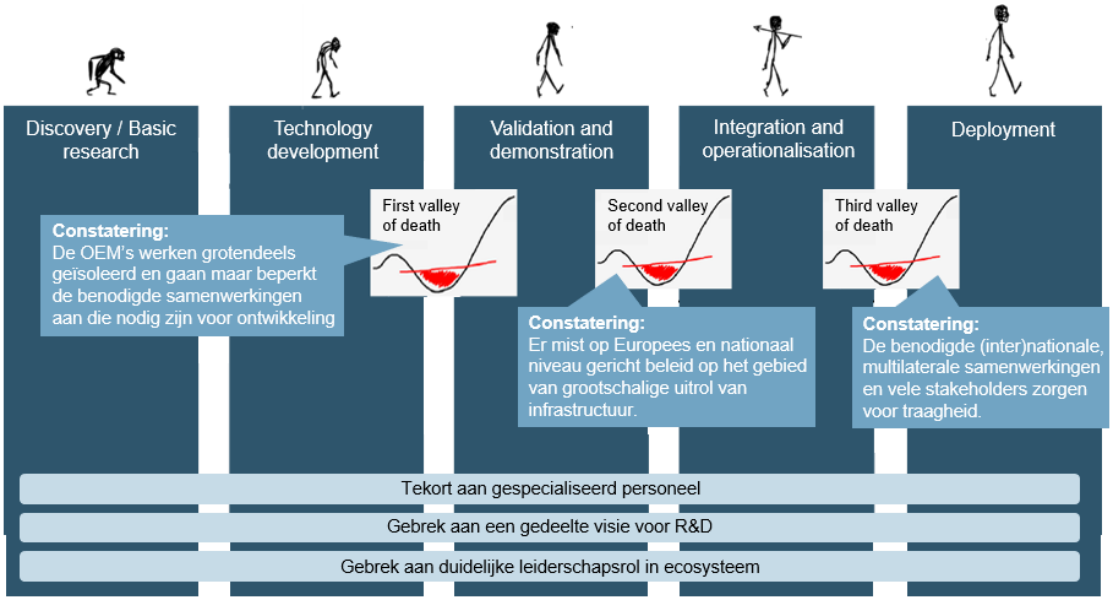
Voor wind op zee is een duidelijke valorisatieketen van kennisopbouw tot productintegratie zichtbaar. De transmissienetbeheerder staat relatief centraal in het waardenetwerk, met hiernaast een belangrijke rol voor operators van windmolenparken en leveranciers van componenten voor de infrastructuur, welke voor hun kennisopbouw samenwerken met universiteiten en andere kennisinstellingen. In deze context zijn de netbeheerder en de operators klanten die eisen kunnen stellen aan de leveranciers, waarin vereisten aan cryptografie ook meegenomen worden. Dit is een belangrijke driver voor innovatie vanuit de leveranciers. Qua beleid en toezicht vallen alle relevante partijen onder de Wet Beveiliging Netwerk en Informatiesystemen (Wbni), waardoor er geen hiaten in wetgeving zichtbaar zijn. Een van de voornaamste barrières voor innovatie is het tekort aan specialistisch personeel dat kennis heeft van zowel het cybersecurity domein als de energiesector.

In tegenstelling tot de wind op zee sector is er voor V2X onderdeel van de automotive sector nog geen waardenetwerk zichtbaar door een gebrek aan valorisatie van cryptocommunicatie. De meeste ontwikkelingen rondom (directe) V2X communicatie bevinden zich nog in de pilotfase en er is nog geen sprake van grootschalige uitrol van zelfrijdende voertuigen, waardoor er ook nog geen commerciële markt bestaat. Er zijn een groot aantal technologische en niet-technologische uitdagingen die moeten worden opgelost om deze fase te overbruggen. De belangrijkste innovatie belemmering is het inbouwen van de IT in de huidige operationele technologie; de lange levensduur van auto's (30 jaar), waardoor je voor 30 jaar relevante technologie moet inbouwen. Dit beperkt de snelheid van de innovatie. Verder is er op dit moment geen partij die het innovatie ecosysteem kan leiden. (Verkeers)veiligheid staat hiernaast hoog in het vaandel in deze sector, waardoor er kritisch wordt gekeken naar nieuwe technologieën die deze kan beïnvloeden, en er is weinig economische incentive voor bedrijven om cryptocommunicatie te implementeren in hun producten. De meeste partijen zijn hierdoor voorlopig nog afwachtend.

Fundering routekaart
Op basis van de bevindingen uit de marktverkenning en waardenetwerkanalyses zijn 'valleys of death' geïdentificeerd: barrières tussen de ontwikkelfases van innovatie.



Figuur 1 De geïdentificeerde 'valleys of death' in de ontwikkelfases die binnen de energie sector.



Figuur 2 De geïdentificeerde 'valleys of death' in de ontwikkelfases binnen de automotive sector.

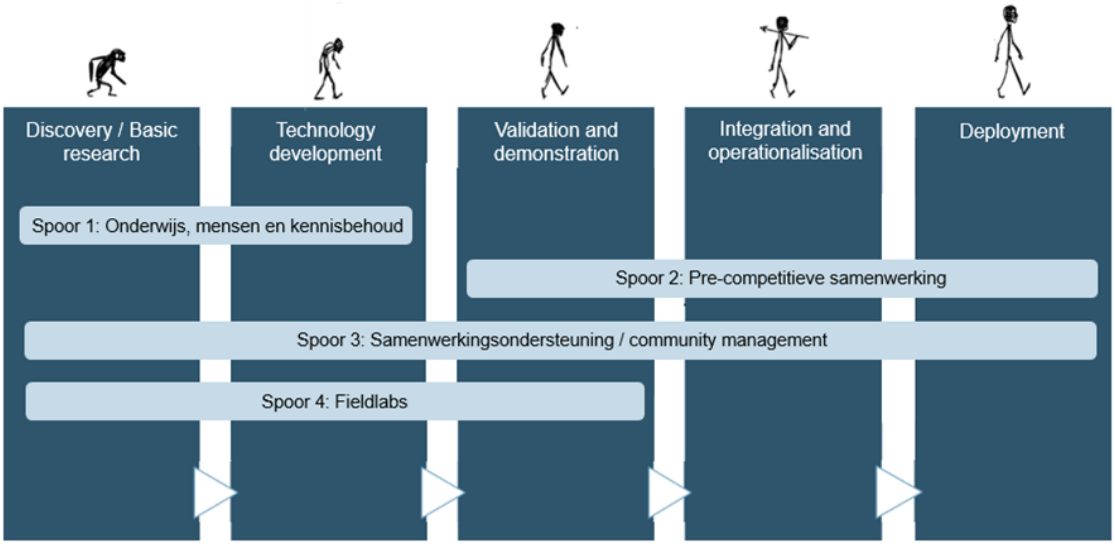
Mogelijke oplossingen voor de geïdentificeerde valleys of death zijn vertaald in vier 'sporen', welke kunnen worden gebruikt bij het opstellen en aanscherpen van de routekaart cryptocommunicatie:

1 **Onderwijs, mensen en kennisbehoud:** schaarste van gekwalificeerd personeel is een algemeen geconstateerde barrière voor de waardeketen. Concrete stappen zijn te zetten op het versterken van kennis over cryptocommunicatie binnen de sectoren; het waarborgen van (academisch) onderzoek; en het behouden van startups middels een goed vestigingsklimaat, gezonde groeimogelijkheden en specifieke regulering.

2 **Pre-competitieve samenwerking:** gemis aan een duidelijke leiderschapsrol in het ecosysteem en een gebrek aan gedeelde visie tussen partijen om prioriteiten op het gebied van R&D vast te stellen. Gerichte samenwerking, met een duidelijk leiderschap en beleid, kan deze barrières doorbreken en als zodanig de gehele markt vergroten.

3 **Samenwerkingsondersteuning / community management:** van belang is het creëren van een veilige omgeving voor samenwerking en afstemming tussen de partijen binnen het waardenetwerk. Standaardisatie op nationaal niveau (bijv. via de NEN) kan leiden tot vertrouwen en richtlijnen voor samenwerkingen. Een partij als dcypher kan hier een belangrijke rol in spelen.

4 **Fieldlabs:** de fieldlabs kunnen een veilige omgeving bieden voor open innovatie door meerdere partijen uit de sector, waarin ideeën en nieuwe technologische oplossingen vrijuit kunnen worden getest. De fieldlabs zullen een gedragen activiteit moeten zijn, waarvoor werken aan concrete, gedragen risico's leidend is. Een startpunt zijn de sectorspecifieke barrières geïdentificeerd in dit rapport.



Figuur 3 Sporen voor de Routekaart Cryptocommunicatie.

Inhoudsopgave

1 Inleiding en context

Nederland is een van de koplopers binnen Europa als het gaat om digitaliseren[1] [2], zoals met de infrastructuur van vaste en mobiele communicatie. Als Nederland koploper wil blijven, moet het zich in razendsnel tempo blijven ontwikkelen binnen dit digitale domein. Belangrijk hierbij is dat iedereen in de samenleving deel kan nemen aan de digitalisering, met de randvoorwaarde dat meer ingezet wordt op veiligheid, privacybescherming, zelfbeschikking en digitale vaardigheden. Zoals in de Nederlandse Cybersecurity Agenda[3] wordt gesteld moet Nederland in staat zijn om “op een veilige wijze de economische en maatschappelijke kansen van digitalisering te verzilveren en de nationale veiligheid in het digitale domein te beschermen.”

Het veilig houden van de systemen in onze gedigitaliseerde samenleving is dus van primair belang. Cryptografie is het fundament van digitale communicatie en gegevensuitwisseling. In Nederland is de coördinatie van innovatie op het gebied van cryptocommunicatie bij dcypher belegd, waar het een hoofdthema is dat opgepakt wordt vanuit een publiek-private samenwerking en het is een speerpunt in de Kennis- en Innovatieagenda (KIA) veiligheid, missie cyberveiligheid.[4] Onder cryptocommunicatie verstaan we de toepassing van cryptografie voor veilige verzending, verwerking, opslag en beschermd uitwisselen van informatie.[5]

In dit rapport beschrijven we de valorisatieketen van cryptocommunicatie, dat als fundering dient voor de routekaart cryptocommunicatie. De routekaart richt zich op de periode 2022 tot en met 2032 en heeft drie doelen:

1 Het ontwikkelen van innovatieve producten en diensten op het gebied van cryptocommunicatie;
2 Het bevorderen van de economische activiteit in Nederland;
3 Het stimuleren van de strategische autonomie van Nederland.

Inzicht in de valorisatieketen is hierbij van belang: een economisch gezond ecosysteem en sterk functionerend waardenetwerk draagt bij aan het behalen van de doelstellingen van de routekaart cryptocommunicatie.

In het onderzoek naar de valorisatieketen van cryptocommunicatie zijn twee methodieken gebruikt:

- *Marktverkenning*: Hierbij wordt een verkenning gedaan van het ecosysteem cryptocommunicatie door het verkennen van de Nederlandse én Europese markt op basis van literatuuronderzoek en interviews.

[1] ITU (2017), Measuring the Information Society Report, 2017 (Vol. 1).
[2] European Commission (2018), FinTech action plan: For a more competitive and innovative European financial sector.
[3] NCTV (2018), Nederlandse Cybersecurity Agenda: Nederland digitaal veilig.
[4] Topsector High Tech Systemen en Materialen (HTSM), Team Dutch Digital Delta, Topsector Creatieve Industrie, Topsector Logistiek en Topsector Water & Maritiem (2019), *Kennis en innovatieagenda (KIA) Veiligheid*, p. 26-34.
[5] Ministerie van Economische Zaken en Klimaat, TNO, CWI & dcypher (2021), Nederland Cryptoland. Startpunt routekaart cryptocommunicatie: de vier belangrijkste uitdagingen in de cryptografie.

- *Waardenetwerkanalyse*: Waardenetwerkanalyse is een methode om met een brede blik naar een innovatie-ecosysteem te kijken. Dit levert een rijker beeld op dan een waardeketenanalyse, waarin één actor centraal staat, doordat het een complex netwerk in kaart brengt. Hierin zijn verschillende rollen zichtbaar, welke met elkaar verbonden zijn door middel van waarde-uitwisselingen (geld, kennis, personeel, etc.). De waardenetwerkanalyse wordt uitgevoerd voor twee sectoren:
  - *De energiesector*: specifiek voor ‘wind op zee’;
  - *De automotive sector*: specifiek voor ‘directe communicatie’.

Dit rapport levert, naast een fundering voor de routekaart cryptocommunicatie, ook input voor de fieldlabs. Om deze redenen is het onderzoek binnen relatief korte tijd uitgevoerd. De nadruk is gelegd op het ophalen van zoveel mogelijk relevante bevindingen voor cryptocommunicatie in de brede zin tijdens de marktverkenning, en specifieker binnen de energie (wind op zee) en automotive (V2X communicatie) sector tijdens de waardenetwerkanalyse. Er is echter vervolgonderzoek nodig om deze bevindingen verder te kunnen generaliseren (naar de sectoren als geheel), te nuanceren, valideren en uit te breiden ter invulling van de routekaart.

Dit rapport bestaat uit 4 inhoudelijke hoofdstukken. Hoofdstuk 2 beschrijft de verkenning van het cryptocommunicatie ecosysteem, gebaseerd op een Europese marktverkenning. De marktverkenning is gedaan aan de hand van literatuuronderzoek en interviews met een aantal partijen uit het ecosysteem. Het resultaat hiervan is een overzicht van lopende innovatie initiatieven, actieve partijen binnen elk van de ontwikkelingen in cryptocommunicatie en de barrières die deze partijen ondervinden tijdens de ontwikkeling. Hoofdstuk 3 beschrijft de waardenetwerkanalyse cryptocommunicatie binnen de energie- en automotive sector t.a.v. de toepassing van cryptocommunicatie. Het waardenetwerk, zoals hierboven beschreven, is in kaart gebracht door een combinatie van deskresearch en interviews met 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 twee sectoren. Daarnaast worden de belangrijkste overeenkomsten en verschillen inzichtelijk gemaakt tussen de energie- en automotive sector. Hoofdstuk 4 beschrijft hoe de resultaten uit de waardenetwerkanalyse gebruikt kunnen worden bij het opstellen/aanscherpen van de routekaart cryptocommunicatie. 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' die de productontwikkeling belemmeren en welke maatregelen zijn nodig om deze te overbruggen om tot het doel van de routekaart te komen.

2 Marktverkenning Ecosysteem Cryptocommunicatie

2.1 Introductie

Onder cryptocommunicatie verstaan we cryptografie in de brede zin, waarbij het nadrukkelijk gaat om cryptografie in een groter geheel van informatietechnologie en ingebed in processen. Kortom, cryptocommunicatie is de toepassing van cryptografie voor veilige verzending, verwerking, opslag, en beschermd uitwisselen van informatie.

Binnen het cryptografie landschap zijn binnen de Nederlandse routekaart 'Nederland Cryptoland' (2021)[6], opgesteld door het Ministerie van Economische Zaken, TNO, CWI en dcypher, vier ontwikkelingen geïdentificeerd die de grootste uitdagingen vormen en de grootste kansen bieden voor de komende jaren (zie figuur 4). Langs de as van deze vier ontwikkelingen is de marktverkenning uitgevoerd. De vier ontwikkelingen zijn als volgt:

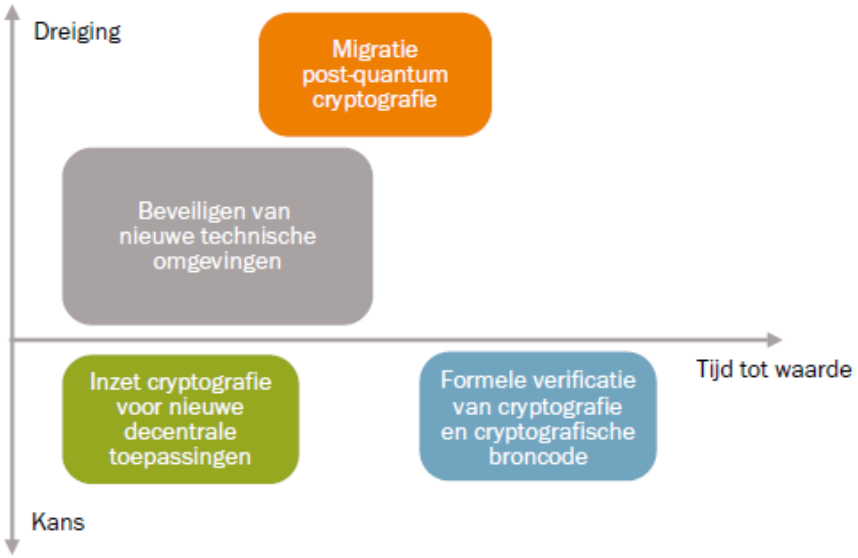
1 **Beveiligen van nieuwe technische omgevingen**: Steeds meer omgevingen worden verbonden aan de buitenwereld, denk hierbij aan OT, maar ook aan IoT-apparaten. Dit leidt tot omgevingen en producten die vaak nog onvoldoende beveiligd zijn omdat de toepassing van het security-by-design principe nog beperkt is. Dit betekent dat het nodig is om nieuwe beveiligingsproducten te ontwikkelen die geschikt zijn om te gebruiken in situaties waarin veiligheid van groot belang is.

2 **Migratie naar post-quantum cryptografie**: De ontwikkeling van de quantumcomputer brengt veelgebruikte cryptografische toepassingen in gevaar. Dit betekent dat het nodig is om te migreren naar zogenaamde post-quantum cryptografie, die bestendig is tegen aanvallen met toekomstige grootschalige quantumcomputers.

3 **Inzet van cryptografie voor nieuwe decentrale toepassingen**: De ontwikkeling van moderne multilaterale cryptografie maakt nieuwe decentrale toepassingen technisch mogelijk. Dit betekent dat er ruimte is voor nieuwe producten of diensten die gebruik maken van deze moderne cryptografie.

4 **Formele verificatie van cryptografie en cryptografische broncode**: Formele verificatie is een methode om een computer geautomatiseerd controles uit te laten voeren op cryptografische protocollen, primitieven, en hun software-implementaties. Het toepassen van technieken uit de formele verificatie op cryptografische protocollen en broncode biedt meer zekerheid over de veiligheid van cryptografische producten.

[6] EZK, TNO, CWI & dcypher (2021), *Nederland Cryptoland*.



Figuur 4 Uiteenzetting van de vier ontwikkelingen in de cryptografie, uitgesplitst in kansen en dreigingen uitgezet over de tijd.[7]

De marktverkenning van het innovatielandschap rondom cryptografie bestaat uit de volgende vijf onderdelen:

- een toelichting van de gebruikte methodiek van hoe de marktverkenning is uitgevoerd;
- een aantal overkoepelende bevindingen met betrekking tot cryptografie in het Nederlandse en Europese ecosysteem;
- een overzicht van de lopende innovatie-initiatieven binnen de vier ontwikkelingen met betrekking tot cryptografie en de bijbehorende spelers;
- een beschrijving van de barrières binnen het ecosysteem die innovatie-initiatieven in de weg staan: zowel generieke barrières als innovatie-afhankelijke barrières.
- een aantal aandachtspunten waar Europese overheden (waaronder Nederland) zich op dienen te focussen, om de ervaren barrières die in dit onderzoek naar boven zijn gekomen te verminderen of zelfs weg te nemen.

2.2 Methodiek

Eerst is literatuuronderzoek uitgevoerd om te identificeren welke spelers zich in de Europese markt bevinden en met welke ontwikkelingen in de markt zij zich bezighouden. Om de scope van het onderzoek te bepalen, zijn er een aantal criteria gehanteerd voor de selectie van onderzochte partijen, te weten:

- de kennispositie binnen het ecosysteem, waarbij in mindere mate is gekeken naar geografische spreiding;
- de spreiding over het type partijen, namelijk standaardisatie- en evaluatiepartijen, kennisinstellingen, crypto-aanbieders en productontwikkelaars;
- de spreiding over de ontwikkelingen in cryptocommunicatie en de daaronder vallende technieken.

[7] EZK, TNO, CWI & dcypher (2021), *Nederland Cryptoland*, p. 16.

Voor de Nederlandse markt is geput uit de routekaart ‘Nederland Cryptoland’. Voor verdere verdieping van het Nederlandse cryptografie landschap wordt hierbij verwezen naar die routekaart.

Naast het literatuuronderzoek zijn zes interviews uitgevoerd met geselecteerde partijen (zie bijlage A), met als doel bevindingen te verifiëren en de barrières die binnen het Europese ecosysteem worden ervaren op te halen. Naast de interviews is er nog een bredere uitvraag gedaan middels een enquête, waar drie partijen reactie op hebben gegeven (zie bijlage A en B).

Met deze marktverkenning is gestreefd naar een zo goed mogelijke *representatie* uit de Europese markt. Verder onderzoek is nodig voor het verkrijgen van een volledig beeld van het Europese cryptografie landschap.

2.3 Overkoepelende bevindingen

Uit zowel het literatuuronderzoek als de interviews is gebleken dat de eerder geïdentificeerde Nederlandse innovatie-trajecten (zoals geformuleerd in de Nederlandse routekaart ‘Nederland Cryptoland’) sterk overeenkomen met de huidige lopende innovatie-trajecten die op de Europese markt geïdentificeerd zijn. De focus verschilt hierbij wel per EU-land. In Denemarken is er bijvoorbeeld veel expertise rondom multiparty computation (decentrale toepassingen) en veel academisch onderzoek op het gebied van code-based cryptography (post-quantum cryptografie) wordt uitgevoerd in Frankrijk. Binnen de EU hebben met name Duitsland en Frankrijk een goede kennispositie op het gebied van cryptografie.

Uit de Nederlandse routekaart ‘Nederland Cryptoland’ is gebleken dat de kennispositie van Nederland goed is. Nederland heeft met name rondom post-quantum cryptografie en multilaterale cryptografie internationaal leiderschap en een uitstekende kennispositie. Daarnaast neemt Nederland deel aan een “sterk academisch ecosysteem van internationaal gerenommeerde universiteiten en kennisinstellingen waarin cryptografie in de volle breedte wordt onderzocht”.[8] Binnen het literatuuronderzoek en de interviews uitgevoerd voor deze marktverkenning wordt dit bevestigd. Nederland heeft binnen Europa een goede reputatie, waarbij Nederland veel samenwerkt. Deze samenwerking vindt plaats op zowel EU- als op mondiaal niveau. De meest toonaangevende projecten op het gebied van cryptografie in de Europese markt staan kort opgesomd in paragraaf 2.4.5., ‘Toonaangevende Europese projecten’.

Buiten de scope van deze marktverkenning, maar wel noemenswaardig, zijn de landen Zwitserland, het Verenigd Koninkrijk (VK) en Israël. Zwitserland en de VK zijn sterk vertegenwoordigd in het cryptografie-landschap. Israël is traditioneel sterk op het gebied van cryptografie en cybersecurity, wat te verklaren is door de historische spanningen met buurlanden.

[8] EZK, TNO, CWI & dcypher (2021), *Nederland Cryptoland*, p. 14.

2.4 Lopende innovatie-initiatieven binnen de Europese markt

De lopende innovatie-initiatieven binnen het ecosysteem cryptocommunicatie van de EU zijn hieronder in kaart gebracht onder de vier geïdentificeerde ontwikkelingen binnen het cryptografie landschap: beveiligen van nieuwe technische omgevingen; migratie naar post-quantum cryptografie; inzet van cryptografie voor nieuwe decentrale toepassingen; en formele verificatie van cryptografie en cryptografische broncode. Tenslotte zijn in de laatste paragraaf de meest toonaangevende Europese projecten (zowel afgerond als lopend) opgesomd.

2.4.1 Beveiligen van nieuwe technische omgevingen

Onze samenleving digitaliseert in toenemende mate en steeds meer producten zijn met elkaar verbonden via het internet en andere draadloze netwerken. Voorbeelden zijn het besturen van verlichting of het vergrendelen van een auto via een app op een smartphone, en vele andere IoT (Internet of Things) toepassingen. Hierbij neemt de vraag naar het beveiligen van nieuwe technische omgevingen toe, die in het verleden geen cryptografische oplossingen vereisten. Vaak gaat het om lightweight cryptografie: unilaterale cryptografie die moeten kunnen draaien op resource-constrained devices met beperkte rekencapaciteiten, beperkte geheugenopslag, etc. Dit vraagt vaak om nieuwe afwegingen in het ontwerpen en kiezen van toepasbare cryptografische methoden, omdat verschillende toepassingen weer specifieke beperkingen met zich meebrengen en specifieke eisen stellen aan de cryptografische oplossingen. Bovendien geldt in veel van deze low-end toepassingen het kostenplaatje als belangrijkste overweging, en vaak moet er daarom voor gezorgd worden dat de cryptografie bijna geen overhead geeft. Hiertoe vindt ook een continue ontwikkeling en optimalisatie van cryptografische hardware plaats.

2.4.2 Migratie naar post-quantum cryptografie

Al sinds de jaren ’90 is bekend dat de quantumcomputer een serieuze bedreiging vormt voor een groot deel van de huidige cryptografische technologieën: met het bestaan van een grootschalige quantumcomputer zouden vele cryptografische methoden die nu gebruikt worden makkelijk kunnen worden gekraakt. Het bouwen van zo een grootschalige quantumcomputer blijft tot op heden een uitdaging. Echter, er wordt voortgang geboekt en daarom dient men in bestaande toepassingen van cryptografie te beginnen aan een migratie naar nieuwe cryptografische methoden die wel resistent zijn tegen quantumaanvallen.

Het gebied van quantum-resistente cryptografie kan momenteel worden opgesplitst in vijf stromingen van oplossingen met verschillende eigenschappen:

1 *Lattice-based cryptography* is gebaseerd op wiskundige roosters, en is één van de voornaamste kandidaten voor het ontwikkelen van praktische post-quantum cryptografie, vanwege de algehele efficiëntie en veelzijdigheid: daar waar andere methoden vaak sterk zijn op één gebied (bijv. snelheid van encryptie/decryptie) en minder sterk op andere gebieden (bijv. sleutelgroottes) is lattice-based cryptografie een goede allround kandidaat. Voorbeelden hiervan zijn Kyber[9] (encryptie), Dilithium[10], en Falcon[11] (handtekeningen).

[9] https://pq-crystals.org/kyber/
[10] https://pq-crystals.org/dilithium/
[11] https://falcon-sign.info/

2 *Code-based cryptography* is gebaseerd op de moeilijkheid van decoderingsproblemen, die ook voorkomen in de theorie van zogenaamde error-correcting codes. Deze stroming is de oudste binnen de post-quantum cryptografie, met het McEliece schema[12] daterend van eind jaren '70. Vanwege dit lange bestaan, maar de wat mindere efficiëntie dan lattice-based cryptografie, wordt deze stroming vooral gezien als geschikt voor toepassingen met hoog-gerubriceerde informatie (HGI).

3 *Hash-based cryptography* is gebaseerd op de moeilijkheid van het inverteren van cryptografische hashfuncties. Deze hashfuncties worden breed gebruikt in verschillende cryptografische toepassingen, zoals het opslaan van wachtwoorden en het detecteren van gecompromitteerde integriteit van gegevens. Er is groot vertrouwen in de veiligheid van cryptografie gebaseerd op hashfuncties, aangezien er nooit fundamentele zwaktes zijn gevonden. Het SPHINCS-schema[13] is één van de kandidaten voor de post-quantum standaardisatie van NIST.

4 *Multivariate cryptography* is gebaseerd op de moeilijkheid van het vinden van oplossingen voor systemen van multivariate vergelijkingen. Net als de hash-based en code-based cryptografie leidt deze stroming onder de iets mindere efficiëntie, in dit geval op het gebied van sleutelgroottes; verschillende pogingen zijn er gedaan om de cryptografie efficiënter te maken (bijv. Rainbow[14]), maar de additionele structuur heeft steeds geleid tot zwaktes in de beveiliging[15]. Een betrouwbaar, maar minder efficiënt systeem, is unbalanced oil and vinegar (UOV).[16]

5 *Isogeny-based cryptography* is gebaseerd op elliptische krommen en hun isogenies. Deze richting is relatief erg nieuw, en lijdt nog onder trage encryptie/decryptie-algoritmes, maar biedt net als de (niet-post-quantum) cryptografie gebaseerd op elliptische krommen goede efficiëntie op het gebied van sleutellengtes en ciphertexts. Voorbeelden hiervan zijn SIKE[17] en CSIDH.[18]

Soms wordt als alternatief voor post-quantum cryptografie ook de quantum cryptografie genoemd, waarvan de veiligheid gebaseerd is op de onmogelijkheid van bepaalde operaties in de quantumfysica (no-cloning theorem). Systemen als quantum key distribution (QKD) worden door verschillende partijen onderzocht, maar bieden op dit moment geen reëel alternatief voor post-quantum cryptografie. Dit vanwege o.a. de noodzakelijkheid voor gespecialiseerde quantumhardware; uitdagingen op het gebied van lange afstandscommunicatie; authenticatie; en problemen met praktische implementaties. Het gebruik van QKD wordt afgeraden door onder andere de nationale veiligheidsdiensten van Nederland[19] en Duitsland[20].

---

[12] https://classic.mceliece.org/
[13] https://sphincs.org/
[14] https://www.pqcrainbow.org/
[15] Beullens, W. (2022), 'Breaking Rainbow takes a weekend on a laptop', *Cryptology ePrint Archive*, Paper 022/214.
[16] Goubin, L., Kipnis A. & J. Patarin (1999), 'Unbalanced Oil and Vinegar signature schemes', *Advances in Cryptology – EUROCRYPT '99*, p. 206-222.
[17] https://sike.org/
[18] Castryck, W. & T. Lange, et al. (2018). 'CSIDH. An efficient post-quantum commutative group action', *ASIACRYPT 2018*, p. 395-427.
[19] Algemene Inlichtingen- en Veiligheidsdienst (AIVD) (2021), *Bereid je voor op de dreiging van de quantumcomputers*.
[20] Federal Office for Information Security (BSI) (2021), Quantum-safe cryptography: Fundamentals, current developments and recommendations.

2.4.3 Inzet van cryptografie voor nieuwe decentrale toepassingen

Nieuwe cryptografische methoden maken het mogelijk om de eigenaar van gevoelige data te scheiden van de partij die met de data gaat werken (berekeningen of verificaties uitvoert), zonder dat degene die met de data werkt meer leert over de data dan de eigenaar van de data toestaat. Dit biedt een variëteit aan nieuwe mogelijkheden, waarbij partijen bijvoorbeeld gezamenlijk berekeningen kunnen uitvoeren op gevoelige data, zonder dat de veiligheid van de onderliggende privacygevoelige data in gevaar komt.

Binnen het gebied van de decentrale toepassingen worden de volgende stromingen geïdentificeerd:

1 *Secure multiparty computation (MPC)* gaat op technisch vlak over het gezamenlijk berekeningen uitvoeren op gevoelige input-data met verschillende partijen, zonder dat deze gevoelige data gedeeld hoeft te worden met alle partijen. Vaak willen verschillende partijen bepaalde berekeningen doen op bijvoorbeeld persoonsgegevens om voorspellende modellen te optimaliseren, maar is dit door de Algemene Verordening Gegevensbescherming (AVG) en andere privacywetgeving onmogelijk. Het gebruik van MPC biedt hierbij een mogelijke oplossing.

   Binnen MPC zijn er verschillende methoden die in de praktijk gebruikt worden. Homomorphic encryption maakt gebruik van encryptiemethodes waarbij berekeningen gedaan kunnen worden op versleutelde data, zonder de data eerst te ontsleutelen. Als opkomend subgebied hierin is nog fully homomorphic encryption te identificeren, waar arbitraire berekeningen gedaan kunnen worden op versleutelde data. Dit gaat echter in de praktijk ten koste van efficiëntie en praktische haalbaarheid. Secret sharing is een alternatieve stroming waarbij gevoelige data als het ware wordt opgedeeld, waarbij elk deel niets weggeeft over de data die het bevat. Deze opgedeelde data worden vervolgens verspreid over verschillende partijen, met als resultaat dat geen van de partijen de data kan inzien, maar wel gezamenlijk de data kunnen verwerken. Dit is mogelijk door middel van gezamenlijke berekeningen over hun deel van de data.

2 Op een hoger niveau gaat *self-sovereign identities (SSI)* over het veilig en privacy-vriendelijk delen van persoonlijke informatie, waardoor de privacy van individuen in de digitale samenleving wordt verbeterd. De gebruiker krijgt in dit model meer controle over het delen van zijn eigen gegevens. Deze gegevens staan opgeslagen op een mobiele applicatie: de SSI-wallet. De gegevens worden opgeslagen met hun bijbehorende zekerheden, zoals de herkomst en integriteit van deze gegevens. Hierdoor kunnen de gegevens voor zowel gevoelige informatie (bijvoorbeeld BSN, medische gegevens) als ongevoelige informatie (bijvoorbeeld Netflix login) gebruikt worden.

   Door de gebruiker meer controle te geven over zijn gegevens en de hoeveelheid informatie die gedeeld wordt te minimaliseren, wordt er voldaan aan het programma ‘Regie op Gegevens’ en de AVG. Om controle, privacy en informatiebeveiliging te garanderen, wordt er gebruik gemaakt van cryptografie. Er wordt binnen SSI verschillende cryptografie toegepast, waaronder versleuteling, digitale handtekeningen, de eerdergenoemden zero-knowledge proofs, en distributed ledger technologies.

3 *Distributed ledger technologies (DLT)* omvat onder andere blockchains en ring signatures en gaat over decentrale registers waarbij op meerdere plekken dezelfde informatie (vaak publiekelijk ter verificatie) is opgeslagen. Door het gebruik van versleuteling en digitale handtekeningen zijn de gegevens beschermd. Bovendien is de informatie niet op één plek opgeslagen, maar verdeeld over verschillende nodes in het netwerk, waardoor er geen 'single point of failure' is. Met behulp van zero-knowledge proofs kan op een publieke manier de integriteit van de blockchain bevestigd worden. DLTs worden gebruikt in cryptocurrencies, maar ook in multiparty computation en self-sovereign identities.

4 Het gebruik van *zero-knowledge proofs (ZKP's)* is op technisch vlak in opkomst. ZKP's zijn wiskundige bewijzen die een partij kan produceren om te bewijzen dat privacygevoelige data aan bepaalde eisen voldoet, zonder de data daadwerkelijk weer te geven. Een voorbeeld van het gebruik van ZKPs binnen SSI is dat klanten in de supermarkt kunnen bewijzen dat zij 18 jaar of ouder zijn, zonder leeftijd of geboortejaar prijs te geven. Dit onderwerp komt naast binnen SSI veel terug in de context MPC, om te bewijzen dat berekeningen op versleutelde data juist zijn uitgevoerd. Dit speelt ook een grote rol in DLTs, om te bewijzen dat een update van de ledger aan alle regels van het onderliggende protocol voldoet zonder te veel details over de bijbehorende update vrij te geven.

2.4.4 Formele verificatie van cryptografie en cryptografische broncode

Deze ontwikkeling wordt ook wel computer-aided cryptografie (CAC) genoemd, aangezien computers helpen met het checken van het ontwerpen, analyseren en implementeren van cryptografie. Hierbij wordt de kracht van automatisering gebruikt om methodische stappen door een computer uit te laten voeren, in plaats van dit aan een mens over te laten. Dit onderwerp is onder te verdelen in de volgende drie technieken:

1 *Formele verificatie van cryptografische primitieven.* Het bewijzen van de formele correctheid en veiligheid van een primitieve (bijvoorbeeld een encryptiemethode) kost in de praktijk erg veel moeite, zowel om de correctheid te bewijzen als voor een ander om dit bewijs te verifiëren. Deze bewijzen zijn verder vaak erg technisch van aard, waardoor een kleine fout (bijvoorbeeld het niet beschouwen van een randgeval) makkelijk gemaakt wordt. Door dit proces te automatiseren kan de primitieve efficiënter en zonder fouten worden geverifieerd.[21]

2 *Formele verificatie van cryptografische protocollen.* Op een hoger niveau dienen high-level protocollen correct te werken, waarbij deze vaak gebruik maken van verschillende low-level cryptografische technieken. Tooling zoals ProVerif[22] laat de gebruiker de beveiligingseigenschappen van een cryptografisch protocol geautomatiseerd bewijzen met behulp van een

[21] Barbosa, M. & G. Barthe, et al. (2019), 'SoK: Computer-Aided Cryptography', *Cryptology ePrint Archive,* 1393.
[22] https://opam.ocaml.org/packages/proverif/

computer. Een voorbeeld hiervan is de VPN WireGuard geverifieerd door INRIA met CryptoVerif.[23]

3 *Formele verificatie van cryptografische implementaties*. Tenslotte is het van belang het onderscheid te maken tussen de cryptografische algoritmes (vaak gegeven in pseudocode) en daadwerkelijke implementaties van deze algoritmes in een specifieke programmeertaal. Het correct implementeren van cryptografie is noodzakelijk, vanwege de fouten die bij de implementatie gemaakt kunnen worden die de veiligheid van het hele systeem kunnen compromitteren.

   Naast dat een implementatie juist moet zijn, is het van nog groter belang om rekening te houden met zogenaamde 'side-channel attacks'. Door bijvoorbeeld te kijken naar de tijd die het kost om een decryptie uit te voeren, kan een aanvaller uit een naïeve implementatie misschien halen dat de privésleutel bepaalde bits op 0 heeft staan. Het formeel verifiëren van cryptografische implementaties gaat daarom vaak ook over het bevestigen dat de implementatie niet kwetsbaar is voor side-channel attacks. Als voorbeeld hiervan wordt de library libjade[24] gebruikt om te garanderen dat een implementatie van een cryptografische primitieve constant-time en memory-safe is.

2.4.5 Toonaangevende Europese projecten

In figuur 5 zijn verschillende projecten op EU-niveau weergegeven op het gebied van cryptografie, gebaseerd op deskresearch en de gehouden interviews (zie bijlage A). Hieronder lichten we een aantal toonaangevende projecten uit. We hebben gekozen om deze projecten kort toe te lichten omdat ze samen alle ontwikkelingen behandelen. KYBER-VESI, PRESERVE en EVITA gaan over de toepassingsgebieden van de waardenetwerk analyse (wind op zee en automotive). Deze projecten vallen onder de ontwikkeling *beveiligen van nieuwe technische omgevingen*. De andere projecten hier genoemd gaan over de andere drie ontwikkelingen binnen het cryptocommunicatie ecosysteem.

- Horizon Europe (2013-2020) en (2021-2027)[25]
  Een EU-programma dat beoogt samenwerking te faciliteren en de impact van onderzoek en innovatie in het ontwikkelen, ondersteunen en implementeren van EU-beleid te versterken, op het gebied van mondiale uitdagingen. Hieruit zijn (en worden) verschillende projecten gefinancierd met betrekking tot innovaties in de cryptografie. Deze projecten gaan onder andere over de migratie naar post-quantum cryptografie[26], het beveiligen van nieuwe technische omgevingen

[23] Bhargavan, K. & B. Blanchet, et al. (2019), 'A mechanised cryptographic proof of the WireGuard Virtual Private Network protocol', *Inria Paris*, p. 50.
[24] https://github.com/formosa-crypto/libjade
[25] https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en
[26] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/horizon-cl3-2022-cs-01-03;callCode=HORIZON-CL3-2022-CS-01;freeTextSearchKeyword=;matchWholeText=true;typeCodes=1;statusCodes=31094501,31094502,31094503;programmePeriod=null;programCcm2Id=null;programDivisionCode=null;focusAreaCode=null;destination=null;mission=null;geographicalZonesCode=null;programmeDivisionProspect=null;startDateLte=null;startDateGte=null;crossCuttingPriorityCode=null;cpvCode=null;performanceOfDelivery=null;sortQuery=sortStatus;orderBy=asc;onlyTenders=false;topicListKey=callTopicSearchTableState

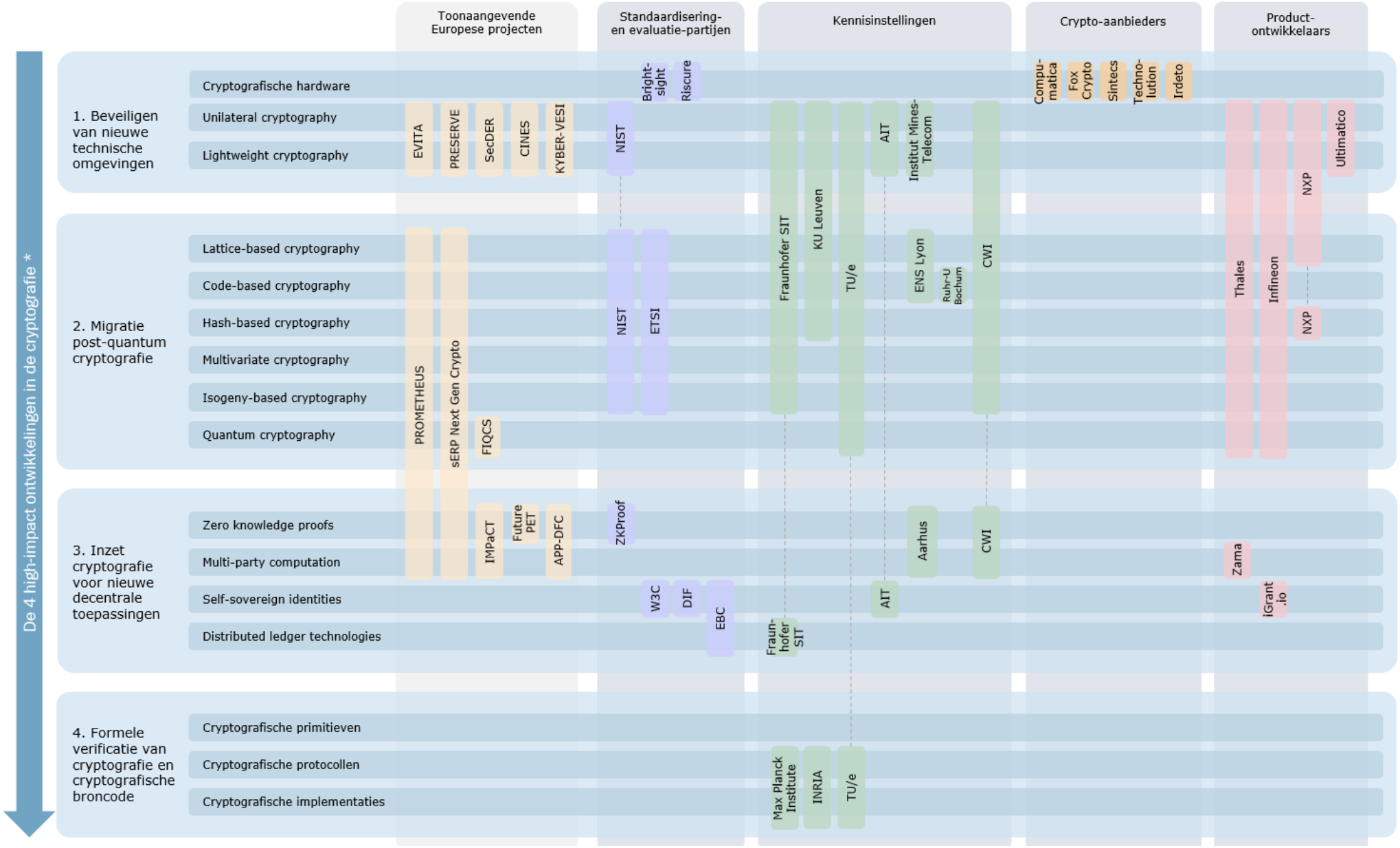
(met post-quantum cryptografie)[27] en homomorphic encryption[28]. Hieronder vallen ook PROMETHEUS en PRIViLEDGE.

- PROMETHEUS (heden)[29]
  'Privacy preserving post-quantum systems from advanced cryptographic mechanisms using lattices'. Onderzoeksproject dat momenteel wordt uitgevoerd door CWI, met externe fundering en verschillende (internationale) partners.
- PRIViLEDGE (2018-2021)[30]
  Realisatie van cryptografische protocollen voor het ondersteunen van privacy, anonimiteit en efficiënte gedecentraliseerde consensus voor DLT's.
  Gefinancierd door de EU, hebben verschillende EU partijen uit de fintech- en blockchain-domeinen bijgedragen aan het cryptografisch onderzoek.
- KYBER-VESI (2016-2018)[31]
  Gecoördineerd door het Finse onderzoeksinstituut VVT, ten behoeve van de ontwikkeling van assessment tooling en richtlijnen die de cyberveiligheid van de watervoorziening moet verbeteren. Deze tooling is momenteel beschikbaar gesteld binnen de Finse watersector en dient als instrument om de continuïteit van de watervoorziening in Finland te waarborgen.
- PRESERVE (2011-2015)[32]
  Ook wel 'Preparing SEcuRe Vehicle-to-X Communication Systems', heeft als doel gehad bij te dragen aan de veiligheid en privacy van toekomstige vehicle-to-vehicle en vehicle-to-infrastructure communicatiesystemen.
- EVITA (2008-2011)[33]
  Getrokken door Fraunhofer Institute for Secure Information Technology en werd medegefinancierd door de EU, voor het ontwerpen, verifiëren en prototypen van een architectuur voor automotive onboard networks.

2.4.6 Overzicht

Op de volgende pagina (figuur 5) wordt een overzicht weergegeven van de spelers die zich in de Europese markt bevinden, waarbij een inschatting is gemaakt van het deel van de markt waar zij zich mee bezighouden. Dit overzicht geeft niet een volledig overzicht van het Europese cryptografie landschap weer, maar is bedoeld als een zo goed mogelijke *representatie* van de Europese markt. De weergegeven partijen zijn geselecteerd op hun kennispositie binnen het ecosysteem, waarbij in mindere mate is gekeken naar geografische spreiding binnen de EU. Het lijkt erop dat Nederlandse crypto-aanbieders zich voornamelijk richten op het ontwikkelen van cryptografische hardware. Een verklaring hiervoor is dat de andere ontwikkelingen een lager TRL hebben, waardoor het nog lastig is daar concrete producten in aan te bieden.

[27] https://cordis.europa.eu/project/id/946280
[28] https://cordis.europa.eu/project/id/644209
[29] https://www.h2020prometheus.eu/
[30] https://cordis.europa.eu/project/id/780477
[31] https://www.vttresearch.com/en/news-and-ideas/new-tools-water-utility-cyber-security-kyber-vesi-project
[32] https://www.preserve-project.eu/
[33] https://www.evita-project.org



Figuur 5 Overzicht van belangrijke spelers die zich in de Europese markt bevinden, waarbij een inschatting is gemaakt van met welk deel van de markt zij zich bezighouden. Dit overzicht is niet compleet en dient ten eerste aanzet.

2.5 Barrières voor innovaties in het cryptografische ecosysteem

In dit marktonderzoek zijn er verschillende barrières geïdentificeerd die door partijen worden ervaren, die de ontwikkeling van innovaties in het cryptografische landschap tegenwerken. Deze barrières zijn met name opgehaald met de gehouden interviews (zie bijlage A). Er wordt een onderscheid gemaakt tussen algemene barrières, dat wil zeggen barrières die toepasselijk zijn binnen het hele cryptografische ecosysteem, en barrières die ontwikkeling-afhankelijk zijn.

De algemene barrières die geconstateerd zijn, zijn als volgt:

- *Tekort aan technisch personeel.* Een terugkomend probleem dat in alle interviews naar voren is gekomen is dat het voor partijen lastig is om personeel te vinden met kennis over ontwikkelingen en innovaties in de cryptografie waar nu aan gewerkt wordt. Deze innovaties zitten vaak ook niet in het curriculum van bachelor- of masteropleidingen, omdat het als een niche wordt beschouwd en er liever meer tijd wordt besteed aan het overdragen van kennis over klassieke cryptografie.
- *“Publish or perish” in de academische wereld.* Door de druk op het publiceren in de academische wereld wordt er voornamelijk tijd en geld gespendeerd aan het onderzoeken van iets dat publiceerwaardig is. Dit gaat ten koste van het documenteren van de ontwikkelde software en het onderzoeken van belangrijke, maar minder spectaculaire onderwerpen, of het rapporteren van “negatieve” resultaten. Hierdoor lopen onderzoekers vaak tegen dezelfde problemen aan, zoals het zelf moeten uitvinden hoe de software werkt. Bijvoorbeeld bij cryptanalyse is het ook een waardevol resultaat als een cryptografische techniek na een bepaalde tijd nog steeds niet gebroken is, hoewel dit niet publiceerbaar is.
- *Te weinig investeringen in cryptanalyse.* Omdat er vanuit de industrie vaak alleen geïnvesteerd wordt in cryptografie waar geld aan verdiend kan worden (nieuwe, efficiëntere methoden die het bedrijf zelf kan gebruiken), wordt er weinig geïnvesteerd in cryptanalyse: het onderzoeken van kwetsbaarheden in algoritmen of systemen. Het aantonen dat een systeem kwetsbaar is levert tenslotte geen praktisch voordeel op. Aangezien gedegen cryptanalyse een cruciale rol speelt bij het opzetten van veilige cryptografie en het bouwen aan vertrouwen in de onderliggende methoden, is het belangrijk dat er daarom wel via andere wegen in cryptanalyse wordt geïnvesteerd.
- *Belangenverstrengelingen bij standaardisatie.* Bij standaardiseringen zitten vaak een groot aantal organisaties samen aan tafel om standaarden te maken. Deze organisaties hebben eigen belangen en voorkeuren voor bepaalde standaarden, wat voor frictie en vertraging kan zorgen.
- *Niet genoeg samenwerking binnen de EU.* Onderzoek naar nieuwe cryptografische ontwikkeling wordt voornamelijk gedaan vanuit eigen organisaties, waar er weinig samenwerking is tussen verschillende EU-lidstaten.
- *Crypto-agility is lastig haalbaar in hardware.* Om flexibel te zijn met cryptografie, en makkelijk over te kunnen schakelen op andere cryptografie, zijn vaak extra ruimte en componenten nodig om verschillende cryptografische methoden te ondersteunen. In de praktijk wordt daardoor uit kosten- en prestatieoverwegingen vaak gekozen voor één methode en lopen innovaties

vertragingen op omdat hardware compleet vervangen moet worden om nieuwe cryptografie te ondersteunen.
- *Prioriteiten.* Bedrijven lopen over het algemeen een groter (financieel) risico bij problemen met huidige cryptografische methoden en met de security architectuur eromheen, dan met het wel/niet meedoen met nieuwe cryptografische innovaties. Veel bedrijven hebben het innoveren daarom niet hoog op hun agenda staan en besteden die aandacht liever aan het oplossen van andere security-problemen.

2.5.1 Barrières voor het beveiligen van nieuwe technische omgevingen

In de interviews met verschillende partijen zijn de volgende problemen geïdentificeerd binnen de innovatieve nieuwe technische omgevingen:
- *Hardware-updates en certificeringen.* Omdat hardware vaak specialistisch gemaakt wordt en geoptimaliseerd wordt voor bepaalde toepassingen, is het lastig om veranderingen/updates uit te voeren over de cryptografie die op bepaalde hardware gebruikt/ondersteund wordt. Bovendien wordt hardware vaak gecertificeerd, en vereist nieuwe hardware nieuwe certificering, waardoor vaak gekozen wordt om de oude hardware te blijven gebruiken.
- *Launching customer.* Bij sommige ontwikkelingen ontbreekt het aan een “launching customer” die ervoor zorgt dat een product (goed) gemaakt wordt en ervoor zorgt dat een nieuw product daadwerkelijk op de markt komt.

2.5.2 Barrières voor de migratie naar post-quantum cryptografie

In de gesprekken met partijen die actief zijn in de migratie naar post-quantum cryptografie zijn de volgende barrières geïdentificeerd:
- *Het wachten op standaardisatie.* Door problemen met patentdreigingen heeft de Amerikaanse standaardisatie-organisatie NIST ruim een half jaar vertraging opgelopen met het aankondigen van de standaarden voor toekomstige post-quantum cryptografie. Omdat bedrijven in willen spelen op de nieuwe standaarden, wachten bedrijven de standaardisatie af en lopen bedrijven dus ook vertraging op in de migratieplannen.
- *Weinig regelgeving.* Veel bedrijven zien cryptografie meer als een kostenpost waar nu eenmaal aan voldaan moet worden; zolang een product compliant is aan standaarden zijn bedrijven tevreden. Aangezien er op dit moment nog weinig/geen regelgeving is omtrent post-quantum security, hebben veel bedrijven deze migratie nog niet op hun agenda staan.
- *Weinig awareness over de urgentie.* Quantumaanvallen en de bijbehorende lange termijn risico’s vereisen vrij technische, specialistische kennis. Veel partijen beschikken niet over deze kennis om te weten hoe urgent deze migratie nodig is. Eindgebruikers moeten awareness krijgen over de risico’s en de bijbehorende kosten van het niet op tijd migreren naar post-quantum cryptografie.

2.5.3 Barrières voor decentrale ontwikkelingen

Binnen het onderwerp van de decentrale ontwikkelingen zijn de volgende barrières geïdentificeerd:
- *Missende kennis cryptografen over wetgeving.* Hoewel cryptografen vaak wel de technische kennis in huis hebben over wat er technisch mogelijk is, weten zij meestal niet welke wettelijke beperkingen er gelden omtrent het (versleuteld) uitwisselen van data voor bijvoorbeeld toepassingen met MPC.

- *Missende kennis van wetgevers over cryptografie.* Ook andersom is er vaak ontbrekende kennis: wetgevers weten wellicht wel wat bijvoorbeeld de implicaties zijn van de AVG op het uitwisselen van persoonlijke data, maar niet hoe cryptografie hierbij wel/niet kan bijdragen om toch bepaalde processen mogelijk te maken binnen de wetgeving.
- *Onduidelijkheid over standaardisatie.* Er is nog veel onduidelijkheid over wat er precies gestandaardiseerd moet worden voor MPC, en er is nog geen kritieke massa voor het standaardiseren van SSI. Standaardisatie is nodig voor het kiezen van veilige parameters en het juiste gebruik van deze methodes.

2.5.4 Barrières voor formele verificatie in de cryptografie

Tenslotte hebben we de volgende barrières geconstateerd met betrekking tot het onderwerp formele verificatie:

- *Tools worden ad-hoc gemaakt, zonder documentatie.* Vaak moet er hierdoor veel tijd geïnvesteerd worden om deze tools te begrijpen en te gebruiken en om eerder behaalde resultaten te hergebruiken. Dit hangt samen met het momenteel lage Technology Readiness Level (TRL) van dit innovatiegebied en het feit dat er vanuit de academische wereld over het algemeen minder prioriteit wordt gegeven aan het bouwen van goed-gedocumenteerde tools.
- *Weinig interesse in concrete verificatie voor academici.* Samenhangend met het lage TRL wordt het meeste werk verzet in de academische wereld, maar tegelijkertijd is er in deze wereld weinig interesse om concrete protocollen van bijvoorbeeld commerciële partijen te analyseren, omdat dit vaak geen publiceerbaar resultaat is op een academische conferentie. Het toepasbaar maken wordt niet gedaan door academici en er moeten nog stappen gezet worden voordat de technieken breed in de industrie gebruikt kunnen worden. Bovendien bevatten concrete protocollen vaak een enorme hoeveelheid aan potentiële toestanden, die stuk voor stuk geverifieerd moeten worden. Dit maakt het onzeker of intensief onderzoek op enig moment tot een resultaat leidt.
- *Te weinig awareness over deze tools.* Er is veel onbekendheid rondom het bestaan van de tools voor formele verificatie, en hoe deze tools gebruikt kunnen worden om meer zekerheid te krijgen over de correctheid van de implementaties.
- *Duidelijkheid over te verifiëren functionaliteit.* Voor het formeel verifiëren van cryptografische functionaliteiten op hardware moet van tevoren bekend en duidelijk zijn welke functionaliteiten er allemaal zijn. Vaak is er weinig transparantie vanuit de hardware-kant, zodat er meer functionaliteiten zijn dan er gedocumenteerd zijn. Dit leidt in de praktijk soms tot incidenten, zoals Spectre en Meltdown[34].

2.6 Aandachtspunten voor het wegnemen van de ervaren barrières

Op basis van de waargenomen barrières die ervaren worden binnen het Europese ecosysteem van cryptografie, heeft TNO een aantal aandachtspunten op lange termijn geformuleerd waar landen binnen de EU (waaronder Nederland) zich op dienen te focussen, om de ervaren barrières die in dit onderzoek naar boven zijn gekomen te verminderen of zelfs weg te nemen.

[34] https://meltdownattack.com/

- **Meer gekwalificeerd personeel opleiden, aantrekken en behouden**
  Eén barrière die herhaaldelijk genoemd werd in de gevoerde interviews, was het gebrek aan gekwalificeerde mensen en de moeilijkheid om nieuwe mensen aan te trekken die innovaties vorm kunnen geven. Concrete aandachtspunten die hierbij horen zijn:
  - Het opleiden van meer studenten op het gebied van cryptocommunicatie;
  - Het erop aansturen dat er in het curriculum van universitaire opleidingen meer aandacht gaat naar relevante innovaties;
  - Het aantrekken van meer cryptografische experts naar Nederland en/of Europa;
  - Het zorgen voor een aantrekkelijk werkklimaat, zodat cryptografische experts binnen Nederland en/of Europa blijven.

- **Overheid als launching customer**
  Bij sommige ontwikkelingen ontbreekt het aan een “launching customer” die ervoor zorgt dat een product (goed) gemaakt wordt en ervoor zorgt dat een nieuw product daadwerkelijk in de markt komt. De overheid zou deze rol op zich kunnen/moeten nemen om innovaties te stimuleren.

- **Minder academische druk op wetenschappelijke publicaties binnen cryptografie**
  Om te voorkomen dat problemen met bepaalde aanpakken/methoden steeds herontdekt worden, en dat kennis over deze tegenslagen verloren gaat, is het belangrijk om onderzoek dat uiteindelijk niet tot een “positief” resultaat leidt ook te documenteren. Er staat veel druk op academici binnen Europa om te publiceren. Onderzoek dat leidt tot resultaten die niet publiceerbaar zijn, wordt vaak niet gepubliceerd of überhaupt gedocumenteerd. Tevens zijn sommige academici betrokken bij standaardisatietrajecten, die vaak niet tellen als “publicaties” en daarom minder aantrekkelijk zijn voor het stimuleren van een academische carrière. Concrete aandachtspunten die hierbij horen zijn:
  - Het stimuleren van het daar waar mogelijk documenteren van ‘negatieve resultaten’;
  - Het stimuleren en waarderen van andersoortige bijdragen aan ontwikkelingen binnen de cryptografie, zoals standaardisatie-initiatieven;
  - Het verlichten van de publicatiedruk op academici werkend aan cryptocommunicatie, die bijdraagt aan de exclusieve focus op publiceerbare resultaten.

- **Meer investeringen in cryptanalyse**
  Daar waar “constructieve” cryptografie (het bouwen van nieuwe protocollen) vaak wel opgepikt en gestuurd wordt vanuit de industrie vanwege commerciële belangen, is er vanuit een commercieel oogpunt weinig interesse om te werken aan cryptanalyse (d.w.z. het kraken van systemen en het testen van de veiligheid). Dit terwijl het analyseren van de veiligheid van cryptografie een essentieel onderdeel is van het ontwikkelproces. Concrete aandachtspunten die hierbij horen zijn:
  - Het investeren in meer cryptanalytisch onderzoek, vanuit academisch oogpunt, om de kwaliteit van de cryptanalyse te waarborgen;
  - Meer samenwerkingen aangaan met relevante industriële partners met betrekking tot onderzoek over ‘constructieve’ cryptografie.

- **Regulering op het gebied van de post-quantum migratie**
  Daar waar voor experts duidelijk is dat de migratie naar quantum-veilige oplossingen noodzakelijk is (en voor bepaalde toepassingen zelfs urgent), speelt vanuit de industrie vooral *compliance* een rol: zolang aan alle wettelijke voorwaarden wordt voldaan, hoeft er niet verder geïnvesteerd te worden in cryptografie. Hierbij is het daarom wenselijk dat Europese overheden duidelijke regelgeving opstellen over een (verplichte) tijdige migratie naar quantum-safe systemen, zodat de industrie kan voldoen aan wet- en regelgeving.

- **Stimulering van crypto-agile oplossingen**
  Momenteel worden cryptografische methoden vaak gehardcode in software- en met name hardware-oplossingen, waardoor latere aanpassingen aan de cryptografie lastig te realiseren zijn. Hierbij ligt de oorzaak deels in missende kennis over de voordelen van flexibele oplossingen, en deels in bewuste keuzes om tijd en geld te besparen door voor één oplossing te kiezen en deze optimaal te implementeren. Door de voordelen van crypto-agile oplossingen beter te benadrukken, en eventuele missende kennis aan te vullen, zou de industrie beter kunnen inspelen op crypto-agility.

- **Kennisuitwisseling tussen cryptografie-experts en regelgevers op het gebied van decentrale toepassingen en privacywetgeving**
  Door deze verschillende partijen meer kennis uit te laten wisselen, krijgen beide partijen een beter inzicht waar mogelijkheden tot cryptografische innovatie liggen in verschillende domeinen, waar wetgeving als de AVG deze innovatie fundamenteel in de weg staat, en waar beide partijen samen kunnen werken om de innovatie daadwerkelijk te realiseren m.b.v. de juiste methoden.

3 Waardenetwerkanalyse cryptocommunicatie

In dit hoofdstuk beschrijven we de waardenetwerkanalyses op het gebied van cryptocommunicatie binnen de Nederlandse automotive- en energiesector. In het bijzonder richten we ons op directe communicatie binnen de automotive sector en wind op zee binnen de energiesector. Onze bevindingen zijn gebaseerd op een combinatie van interviews en literatuuronderzoek en kunnen gebruikt worden ter aanvulling voor de Routekaart Cryptocommunicatie[5], welke aan bod komt in hoofdstuk 4.

Waardenetwerkanalyse is een methode om met een brede blik naar een innovatie ecosysteem te kijken.[35] Dit levert een rijker beeld op dan een waardeketenanalyse, waarin één actor centraal staat, doordat het 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 maar ook een uitvoeringsorgaan van de overheid kan zijn. Het waardenetwerk laat hiermee de verschillende relaties binnen het ecosysteem zien en richt zich naast geld ook op andere waarden zoals kennis, personeel en innovatiekracht. Tevens kunnen samenwerkingsverbanden en barrières inzichtelijk en visueel gemaakt worden.

Een waardenetwerkanalyse is ook een geschikte methode om een complex innovatie ecosysteem op gestructureerde wijze in kaart te brengen. Innovatie op het gebied van cryptocommunicatie binnen de wind op zee en automotive sector vindt plaats aan de hand van veel verschillende partijen, belangen, relaties en kennisgebieden. Een waardenetwerkanalyse kan de dynamieken van deze verbanden in meer detail weergeven dan bijvoorbeeld de klassieke waardeketenanalyse, die meer procesgericht naar een ecosysteem van een enkele actor kijkt.

In dit onderzoek is ervoor gekozen om een waardenetwerkanalyse uit te voeren voor twee toepassingssectoren: de Nederlandse energie- en automotive sector. Deze zijn onderdeel van vitale infrastructuur van categorie A en B respectievelijk.[36] Voor beide geldt dat ze fysieke infrastructuur bevatten die tientallen jaren meegaan, waardoor het essentieel is dat de cyberbeveiliging en cryptografie op orde is en indien mogelijk geüpdatet kan worden. Het is namelijk niet te voorspellen welke mate van computerkracht, inclusief quantum computing, er in 2040 beschikbaar is die ingezet kan worden voor hacking. Dit is tegelijk een motivatie om naast de beveiliging van nieuwe technische omgevingen ook te kijken naar de toepasbaarheid van post-quantum cryptografie (PQC), zoals beschreven in paragraaf 2.4.2.

Een kanttekening die tot slot geplaatst moet worden is dat het waardenetwerk een momentopname is van een ecosysteem dat permanent in beweging is. Om de bevindingen actueel te houden, moet een waardenetwerk periodiek geëvalueerd en herijkt worden.

[35] Allee, V. (2008), 'Value network analysis and value conversion of tangible and intangible assets', *Journal of intellectual capital*, Vol. 9, Issue 1, pp. 5-24.
[36] https://www.nctv.nl/onderwerpen/vitale-infrastructuur/overzicht-vitale-processen

3.1 Methode

Hieronder volgt een korte beschrijving van de methode voor de waardenetwerkanalyse die is uitgevoerd. De methode bestaat uit vier stappen die worden aangegeven in figuur 6. Hierna lichten we per stap toe wat het doel is.

Figuur 6 Methodische aanpak voor een waardenetwerkanalyse.

Stap 1: Deskresearch
Het doel van de deskresearch is om stakeholders te identificeren en basiskennis op te bouwen over het waardenetwerk en de bijbehorende rollen en waarde-uitwisselingen, door middel van een literatuurstudie. Op deze manier wordt er een beeld gevormd van de werking van het ecosysteem en de bestaande problemen vanuit een onafhankelijk perspectief. Op basis van de resultaten kan een draft van het waardenetwerk opgetekend worden. Deze wordt in de volgende stappen verder gedetailleerd en gevalideerd.

Stap 2: Hypothese workshop
Vervolgens vindt er een hypothese workshop plaats. Het doel hiervan is om binnen het projectteam hypothesen over de belangen en dynamieken van de stakeholders het waardenetwerk op te stellen en te bediscussiëren. 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 in de volgende stap. Het dient als een basis voor de beoordeling van de impact voor de verschillende stakeholders. Hiernaast zorgt het er ook voor dat alle teamleden een gemeenschappelijk basiskennisniveau krijgen.

Stap 3: Interviews met experts
Hierna vinden interviews plaats met experts die onderdeel zijn van partijen die een bepaalde rol in het netwerk vervullen. In dit geval kan dit bijvoorbeeld met chief information security officers (CISOs) en/of product owners van (cryptografische) softwareproducten zijn. Het doel van de interviews met experts is om informatie te verzamelen die nodig is voor de validatie en verdere uitbreiding van het waardenetwerk. Elke expert draagt zijn eigen stukje van de puzzel bij vanuit zijn of haar eigen perspectief en dragen tezamen bij om een genuanceerd beeld te kunnen vormen over de werking en dynamiek van het ecosysteem in zijn geheel. De interviewresultaten worden tot slot waar mogelijk ook gevalideerd en verder uitgebreid met bevindingen uit de literatuur.

Stap 4: Analyse waardenetwerk
In de laatste stap wordt alle verzamelde informatie bij elkaar gevoegd 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.

De interviews zijn zo veel mogelijk gericht op de toepassing van cryptocommunicatie in beide sectoren. Als deze scope echter te smal was voor de vertegenwoordiger van een organisatie, dan zijn de vragen aangepast zodat deze op cybersecurity en veilige communicatie in zijn geheel waren gericht. Dit was de overweging om dat dezelfde dynamieken en barrières een rol spelen. Een overzicht van de partijen die we voor de waardenetwerkanalyse gesproken hebben is te vinden in bijlage A.

3.2 Toepassingssector: Wind op Zee

3.2.1 Inleiding

In het kader van de energietransitie heeft Nederland ambitieuze doelen gesteld op het gebied van de opwekking van duurzame energie. Wind op zee behoort tot vitale infrastructuur van categorie A. Vanaf land tot 12 mijl op zee geldt Nederlandse wetgeving, waarbij bescherming tegen kwaadwillende een nationale verantwoordelijkheid is.[37] Hierbuiten is het echter een grijs gebied wie verantwoordelijk is voor de bescherming van de infrastructuur.

De plaatsing van windparken gebeurt stapsgewijs en de ruimte hiervoor is beperkt, doordat rekening gehouden moet worden met de ruimte voor visserij, militair gebied, vaarroutes, zandwinning en natuurbehoud.[37] Zodra bekend is waar een windpark geplaatst kan worden, wordt een uitvraag gedaan aan private partijen om het grondgebied te pachten en het windpark daadwerkelijk te plaatsen. Dit zorgt ervoor dat windparken van verschillende, concurrerende partijen zijn, die elk hun eigen partners en uitbaters hebben. Veel van de onderdelen van windmolens zelf worden hiernaast voornamelijk in Azië geproduceerd.[38] Dit zorgt ervoor dat elk windpark zijn eigen fysieke onderdelen en, belangrijk in deze context, eigen cryptografische oplossingen kan hebben.

Onafhankelijk van welke private partij het windpark daadwerkelijk plaatst, is TenneT als transmissienetbeheerder verantwoordelijk voor de aanleg van de infrastructuur (onder andere hoogspanningskabels op zee en transformatorstations) om de verbinding met het stroomnetwerk op land te maken. Dit brengt een bekend spanningsveld mee voor de cyberbeveiliging van operationele technologie (OT), wat alle fysieke infrastructuur omvat.[39] Hier moet namelijk de afweging gemaakt worden tussen beheer op afstand en de mogelijkheid voor kwaadwillenden om via deze weg toegang te krijgen en de stabiliteit van het netwerk te verstoren.

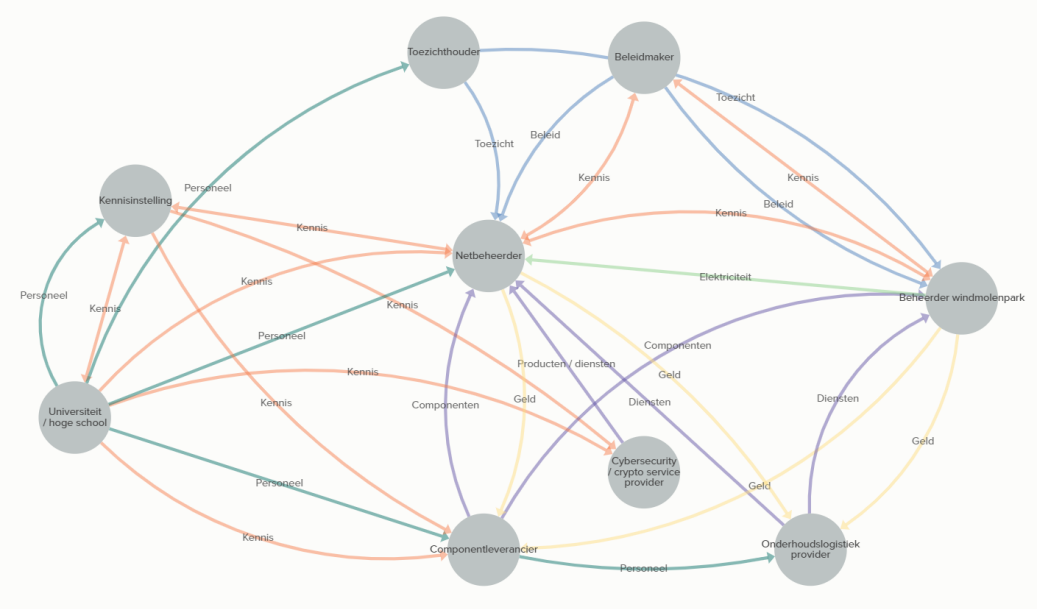
De elektriciteitsmarkt is op zijn beurt erg concurrerend, wat ervoor zorgt dat private partijen een incentive hebben om zo min mogelijk informatie te delen dat deze markt kan beïnvloeden, zoals hoe veel stroom er (naar verwachting) geproduceerd

[37] The Hague Centre for Strategic Studies (2021), *The High Value of The North Sea*.
[38] Straver, F. (2017, 29 November), Windlobby waarschuwt: Aziatische massamolen hijgt Europa in de nek. *Trouw* (https://www.trouw.nl/duurzaamheid-natuur/windlobby-waarschuwt-aziatische-massamolen-hijgt-europa-in-de-nek~b30cf380/)
[39] TNO (2019), *Succesfactoren voor digitaal veilige Operationele Technologie* (TNO 2019 R11304)

wordt en wanneer onderhoud plaatsvindt. De besloten marktdynamieken zorgen voor een gebrek aan transparantie, wat uniformiteit op het gebied van cryptografie niet ten goede komt. Bovendien zijn partijen soms genoodzaakt om bepaalde windmolens aan- of uit te schakelen indien er significant minder of meer stroom wordt geproduceerd dan verwacht, doordat hiermee de balans op het elektriciteitsnet verstoord kan worden. Deze toegang op afstand kan vervolgens gebruikt worden als aanvalsvector.

3.2.2 Resultaten

Figuur 7 toont het waardenetwerk rondom cryptocommunicatie binnen de Nederlandse wind op zee sector. Hierin is van links naar rechts de valorisatieketen van windparken op zee te zien, inclusief de onderdelen die een rol spelen voor cryptocommunicatie. Tevens zijn hierin de leveringsketen van offshore windmolens en elektriciteit in grote lijnen zichtbaar, met hier omheen het ecosysteem voor cryptocommunicatie innovaties. De rollen die vervuld worden in het ecosysteem en de waarde transacties tussen hen worden hierin gevisualiseerd met behulp van respectievelijk de knopen en de verbindingen. Het netwerk is in het specifiek gericht op rollen en transacties die specifiek bij offshore windenergie zijn betrokken en partijen die het (overige) onshore netwerk in stand houden zijn hierin niet meegenomen. Het waardenetwerk van de volledige elektriciteitssector inclusief distributiebeheerder en consumenten is beschreven in een eerder onderzoek.[40]



Figuur 7 Waardenetwerk voor de wind op zee sector.

Een aantal kenmerkende dynamieken die te zien zijn in dit waardenetwerk zijn:

- De (transmissie)netbeheerder staat qua waarde uitwisseling centraal in het waardenetwerk. Hierdoor heeft het een bepalende, sturende rol in het ecosysteem en heeft het invloed op innovatie op het gebied cryptocommunicatie. Dit komt bijvoorbeeld voort uit de eisen die zij stellen bij tenders richting marktpartijen, waarin zij enigszins sturing kunnen geven aan de prioriteiten en de ruimte voor innovatie.

[40] TNO (2020), *EZK Verdieping Valorisatieketens: Verkenning van het ecosysteem en waardenetwerk Automated Security* (TNO 20220 R12224)

- Financiering van producten waarvoor cryptografie relevant is, komt vooral vanuit beheerders van windmolenparken en de netbeheerder (de klanten in deze context).
- Er zijn geen hiaten in beleid en/of toezicht zichtbaar voor dit ecosysteem, aangezien er lijnen lopen naar de belangrijkste actoren.
- Kennis en personeel vloeien vooral vanuit universiteiten en kennisinstellingen het ecosysteem in.
- Componentleveranciers staan centraal voor levering van onderdelen van windmolens. Deze hebben vervolgens ook een rol bij het onderhoud, doordat zij hun eigen experts hiervoor inzetten.

De belangrijkste bevindingen die uit onze waardenetwerkanalyse naar voren zijn gekomen, zijn in drie groepen gecategoriseerd; algemene bevindingen, drijfveren voor innovatie en barrières. Deze worden hieronder één voor één beschreven. De bevindingen zijn deels beschrijvend over het huidige ecosysteem, maar bevatten ook voorstellen voor veranderingen die de geïnterviewden als wenselijk zien.

3.2.2.1 Algemene bevindingen

- **“Klassieke” samenkomst van operationele technologie (OT) en informatietechnologie (IT) is ook kenmerkend voor wind op zee.**
  OT is sinds oudsher cruciaal in de energiesector, maar IT is in de loop der jaren door digitalisering en automatisering ook steeds belangrijker geworden; nieuwe OT bevat *by design* IT-elementen, en IT-componenten worden toegevoegd aan oude OT. De toevoeging van IT brengt veel voordelen met zich mee (bijvoorbeeld verbeterde efficiëntie en beheer op afstand), maar er zijn ook een aantal punten waarop dit uitdagingen veroorzaakt:
  - OT-hardware moet in principe zo simpel mogelijk zijn om tientallen jaren gebruikt te kunnen worden zonder grote wijzigingen of toevoegingen, en moet zonder onderbrekingen kunnen draaien (leveringszekerheid). Voor IT is dit anders; het moet regelmatig geüpdatet worden. Het is lastig om momenten voor patching te vinden voor windmolens omdat dit een stilzetting vereist, maar het is wel vereist vanuit cybersecurity perspectief.
  - Innovatie op het gebied van OT is over het algemeen (veel) trager dan op het gebied van IT. De levenscyclus van OT-componenten is over het algemeen in orde van decennia meegaan, terwijl IT-componenten, inclusief software, soms na enkele jaren al gedateerd zijn.[41]
  - Werken met OT of IT in de energiesector vereist verschillende, specifieke kennis. De integratie van cryptografie ligt op het snijvlak hiervan, waardoor specialistische kennis van beide vakgebieden is vereist om dit goed te doorgronden. Personeel met deze kennis is schaars en tegelijkertijd erg gewild bij veel partijen in het ecosysteem.

- **Cryptocommunicatie is relatief nieuw in deze sector, maar zal een steeds belangrijkere rol spelen in de (nabije) toekomst.**
  - In onderzoeken en experimenten uitgevoerd door partijen in het ecosysteem wordt er aandacht besteed aan cryptografie voor wind op zee, maar in het algemeen moet er nog een bewustwordingsstap plaatsvinden over het belang hiervan. Omdat digitale communicatie alsmaar toeneemt in deze

[41] https://www.digitaltrustcenter.nl/informatie-advies/operational-technology

sector, zal het gebruik van goede cryptografie en innovatie hierop onvermijdelijk zijn.[42] Het thema wordt besproken in bijvoorbeeld sector-brede vergaderingen, maar het krijgt vaak nog geen hoge prioriteit.
- Er is op dit moment weinig behoefte aan innovatie in cryptocommunicatie. Transport Layer Security (TLS) wordt momenteel door veel partijen als de-facto oplossing gebruikt. De meeste communicatie kan in de praktijk dan ook goed beveiligd worden met behulp van TLS, behalve firmwarebeheer. Er is weinig vraag naar innovatieve netwerkbeveiliging vanuit de meeste partijen.
- Communicatie voor wind op zee vindt plaats via zowel WiFi als vaste bekabeling, maar de data die gecommuniceerd wordt is over het algemeen niet heel gevoelig van aard, wat de kansen op een aanval verkleint. Vooralsnog gaat de meest cruciale communicatie in deze sector niet via het internet, maar via besloten netwerken, waardoor de fysieke beveiliging van infrastructuur in de praktijk soms relevanter is dan cybersecurity, inclusief cryptografie.

- **Alle windparken staan onder toezicht van het Agentschap Telecom (AT) via de Wet Beveiliging Netwerk- en Informatiesystemen (Wbni).**
  - De grens van partijen die onder dit toezicht vallen ligt bij een productie van meer dan 100 MW. Aangezien moderne windmolens rond de 10 MW aan energie produceren, zal deze grens altijd overschreden worden voor uitbaters van offshore windmolenparken. In tegenstelling tot onshore wind bestaat het probleem van kleine, decentrale producenten die buiten het toezicht vallen dus niet in de offshore windsector.
  - Operators van windmolenparken geven aan dat op bepaalde vlakken meer toezicht en frequentere toetsing wenselijk zou kunnen zijn. Energienetwerken worden steeds dynamischer en fluctueren meer, waardoor het mogelijk gunstig kan zijn om vaker te toetsen of het netwerk nog steeds voldoet aan de beveiligingsstandaarden en –eisen. Op een substation of mid-spanning is het heel anders als een consument een windturbine bouwt t.o.v. een heel windpark op zee bijvoorbeeld.

- **Standaardisatie voor dit veld is complex en ambitieus, wat voor fabrikanten afschrikkend kan werken.**[43]
  Een aantal kaders of minimumeisen waaraan voldaan moet worden zou genoeg kunnen zijn, zodat innovatie niet wordt gelimiteerd.

3.2.2.2 Drijfveren voor innovatie

- **Leveringszekerheid en compliance aan wetgeving zijn de belangrijkste drijfveren voor innovatie op het gebied van cryptografie.**
  - De voornaamste reden om cryptocommunicatie te verbeteren is om de leveringszekerheid te vergroten, door de risico's van cyberaanvallen te minimaliseren. Er bestaan (hoge) boetes op het niet nakomen van marktafspraken over elektriciteitsleveringen, en uitval van infrastructuur op grote schaal leidt hier bovenop tot substantiële maatschappelijke schade.

[42] A. Aazami, (2021), Digitalisering en energie: Méér dan de som der delen.
[43] CE Delft, TNO en Quintel (2021), Afspraken maken: van data tot informatie, Informatiebehoeften, datastandaarden en protocollen voor provinciale systeemstudies – Deel II technische rapportage.

Voorkoming hiervan is heel belangrijk en een van de drijfveren voor innovatie.
- Eén van de belangrijkste aspecten waarop geconcurreerd wordt tussen windmolen (onderdeel) en station producenten is vooralsnog de prijs. Hierdoor wordt een afweging gemaakt tussen het niveau van de ingebouwde cyberveiligheid en de kosten hiervan. Doordat de prijs in een vrije markt bepalend is, krijgt cybersecurity niet altijd de hoogste prioriteit, zolang deze voldoet aan de minimumeisen.
- Operators van windparken en de transmissienetbeheerder doen in zekere mate onderzoek naar de impact van quantum computing en post-quantum cryptografie, maar zijn hierin vooral afwachtend op o.a. het NIST voor de publicatie van standaarden (op het moment van schrijven zijn alleen de kandidaat algoritmes bekend gemaakt). Ze innoveren zelf niet op het gebied van cryptografie en hebben over het algemeen voorkeur voor veilige en bewezen oplossingen. Hierdoor nemen ze geen leidende rol aan op het gebied van cryptografische innovatie, maar blijven ze wel op de hoogte van belangrijke trends en toekomstbeelden op dit gebied.
- Innovatie komt vooral vanuit cybersecurity dienstverleners en producenten van hardwarecomponenten. De bouw van stations en windmolens wordt vaak uitbesteed aan aannemers en onderaannemers, waarbij de vereisten op het gebied van cybersecurity niet tot in detail gedefinieerd zijn. Dit biedt ruimte voor nieuwe oplossingen en innovaties, maar wel binnen de kaders die de prijsconcurrentie creëert.
- De overheid is begonnen aan de voorbereidingen voor een Rijksbreed programma voor de implementatie van post-quantum cryptografie nu de NIST-kandidaten voor standaardisatie recent bekend gemaakt zijn. Dit zal naar verwachting een meerjarig traject zijn waarbij wordt begonnen bij de implementatie van PQC bij de overheid zelf, maar wat later ook vertaald zou kunnen worden naar de vitale infrastructuur.

- **Voor wind op zee in zijn geheel is er momenteel relatief weinig beleid, alleen een aantal Europese richtlijnen.**
  Omdat het enorm druk is op de Noordzee en het in de toekomst nog drukker gaat worden en veel informatie moet worden uitgewisseld, zit er enorme economische potentie in[37]. Gebrek aan beleid kan uiteindelijk wel een barrière worden als er niet op tijd aan gewerkt wordt.

- **Innovatie en kennisdeling worden gedreven en gestimuleerd vanuit samenwerkingsverbanden** zoals Dcypher, waarin cryptografie leveranciers, universiteiten en kennisinstellingen betrokken zijn.
  - Er wordt vanuit bijvoorbeeld operators van windparken op enige schaal kennis gedeeld met concurrenten, vooral op een hoog abstractieniveau om oplossingsrichtingen te identificeren of peer reviews uit te voeren, maar niet voor de aanschaf van bijvoorbeeld specifieke componenten (om kartelvorming te voorkomen).
  - Componentleveranciers ontwikkelen veel in-house, maar werken ook samen met universiteiten en andere leveranciers aan cyber security innovaties.
  - De netbeheerder heeft veel kennis binnen de organisatie. Desondanks zijn er in enige mate samenwerkingen met universiteiten op het gebied van cybersecurity innovatie.

  - Internationaal wordt relevante kennis ook gedeeld binnen bestaande samenwerkingsverbanden en programma's.

3.2.2.3 Barrières

- Wat duidelijk naar voren is gekomen tijdens meerdere gesprekken is het **tekort aan personeel met gecombineerde kennis van cybersecurity (IT) en het energiedomein (OT) door vrijwel de hele keten.** Er is maar een relatief klein aantal mensen met deze kenniscombinatie beschikbaar, en alle partijen in het ecosysteem concurreren met elkaar voor deze kennis.

- **Nederland heeft een vrij kleine markt op het gebied van cryptografie** en het gebeurt regelmatig dat Nederlandse cybersecurity startups worden verkocht aan het buitenland, wat deze positie verder verzwakt.[44] [45]

- **Leveringszekerheid en maintenance kunnen voor wrijving zorgen, wat ook innovatie kan limiteren.**
  - Het is een doel om OT zo simpel mogelijk te houden voor performance, en door IT toe te voegen kan het verbeterd worden, maar de koppeling met IT creëert op zijn beurt weer nieuwe veiligheidsrisico's.
  - Daarnaast moet de turbine stilgezet worden voor (groot) onderhoud, wat juist zo veel mogelijk wordt vermeden. Hoe meer patching, des te veiliger het systeem kan blijven, maar ook hoe meer impact op de levering (en hiermee de markt), waardoor patching in de praktijk vaak wordt uitgesteld.

- Het belang van cryptocommunicatie wordt vaak nog niet gezien door marktpartijen, **omdat ze vooral zijn gericht op de relatief korte termijn.** Door beleid wordt toepassing ook niet afgedwongen. Op langere termijn wordt dit naar verwachting een relevanter topic, bijvoorbeeld door de opkomst van quantum computers, maar de investeringstijdlijnen zijn nu nog te kort. Het urgentiebesef mist in zeker mate en budgetten zijn daarnaast geen bottleneck voor cybersecurity innovatie.

- **Er is op sommige vlakken beperkte communicatie tussen sommige partijen in het ecosysteem, bijvoorbeeld op het gebied van onderhoud.** Dit is relatief gefragmenteerd en gebeurt vaak één-op-één in afspraken met componentleveranciers en aanbieders van logistieke diensten. Een verbetering hiervan zou voordelen voor alle betrokkenen op kunnen leveren, waardoor ook het onderhoud van digitale systemen goedkoper kan worden.

3.2.3 Conclusies

Digitale communicatie vindt op grote schaal plaats voor de wind op zee sector en dit zal naar verwachting alleen maar toenemen in de komende decennia. De samensmelting van OT en IT brengt nieuwe veiligheidsrisico's met zich mee en vereist schaars personeel met specialistische kennis van beide domeinen. Cryptografie is een onderwerp dat regelmatig aan bod komt tijdens overleggen tussen partijen in het ecosysteem, maar het heeft geen topprioriteit. De vereisten aan cryptografische oplossingen worden vooral gesteld vanuit de

[44] https://www.agconnect.nl/artikel/techleap-dit-heeft-nederland-nodig-om-techstartups-meer-te-stimuleren
[45] https://executivefinance.nl/2022/05/buitenland-tuk-op-onze-startups/

transmissienetwerkbeheerder en operators van windmolenparken, die vervolgens beide onder beleid en toezicht vanuit de overheid vallen. Innovatie op het gebied van cryptografie wordt hierdoor met name gedreven vanuit de leveranciers van hardwarecomponenten. Uiteindelijk speelt de prijs ook een belangrijke rol bij de aanschaf van infrastructuur. Tot slot zijn er in dit onderzoek een aantal kenmerkende barrières naar voren gekomen die kunnen leiden tot concrete aanbevelingen ter invulling van de routekaart.

3.3 Toepassingssector: Automotive

3.3.1 Inleiding

De transformatieve werking van digitalisering heeft ook een enorme invloed op de automotive sector. Terwijl voertuigen overgaan van volledig mechanische apparaten naar “rijdende computers”, verandert de infrastructuur van het wegennet van statisch naar volledig dynamisch. Dit alles is nodig zodat voertuigen zowel met elkaar als met de omgeving kunnen communiceren, wat ook wel V2X communicatie wordt genoemd. V2X (vehicle-to-all) communicatie bestaat hoofdzakelijk uit V2V (vehicle-to-vehicle) en V2I (vehicle-to-infrastructure) communicatie. V2V bevordert de mogelijkheid voor autonoom rijdende voertuigen en helpt om botsingen te voorkomen, terwijl V2I gebruikt kan worden om tijds- en veiligheid kritische applicaties te realiseren zoals filestaatdetectie en om voertuigen optimaal te laten doorstromen in het verkeer, wat op zijn beurt voor minder uitstoot en files zorgt. Deze nieuwe vormen van communicatie brengen echter ook direct de behoefte voor de juiste cryptografie met zich mee. Er kan een risico ontstaan door een bestuurder te veel af te leiden met meldingen over relatief onschuldige systemen. Hoe meer advanced driver assisstance systems (ADAS) in auto’s worden ingebouwd, zoals dode hoek en parkeersensoren, hoe meer de afleidende risico`s toenemen. Het is ook van belang om te beseffen dat deze ADAS-systemen de eerste stap zijn naar zelfstandig rijdende voertuigen.

Het grootste veiligheidsrisico zit in de electronic control units (ECUs) voor het gas, de rem of het stuur[46]. Het beveiligen van communicatie waarop op hoge snelheid motieve besluiten worden gemaakt is belangrijk omdat er bij fouten mensenlevens bij betrokken kunnen zijn. Kwaadwillenden kunnen enorme schade veroorzaken als ze informatie manipuleren. Tevens biedt de integratie van communicatietechnologie zoals chips en simkaarten in auto’s, ook meer mogelijkheden voor het stelen van een voertuig, bijvoorbeeld door de digitale toegangssleutel te hacken (door een combinatie van ‘sniffing’ en ‘spoofing’). Tot slot speelt ook spionage en privacy een belangrijke rol, aangezien auto’s steeds meer gevoelige data zullen monitoren en opslaan.

Er zijn meerdere ingangen als je een auto zou willen hacken; de autofabrikant zou een ingang kunnen veroorzaken door verkeerde software of achteringangen over het hoofd te zien in de ingebouwde communicatietechnologie, maar naast autofabrikanten, zijn ook dealers en garages een mogelijke zwakke schakel. Deze hebben namelijk toegang tot de hardware en software met geavanceerde gereedschappen. Hackers kunnen gebruik maken van de minder beveiligde locaties van dealers/garages en toegang zoeken.

[46] https://www.saksen.com/insights/white-papers/automotive-security

Chips in voertuigen kunnen gehackt worden door fysieke toegang te krijgen, maar door de toenemende connectiviteit van auto's via onder andere bluetooth, WiFi en simkaarten, zijn er ook steeds meer mogelijkheden om vanaf een afstand toegang te krijgen tot het voertuig.

Als elk apparaat (zowel auto's als infrastructuur) gebruikt maakt van een cryptografische oplossing, zal single point of failure er niet voor zorgen dat een groot deel van de gebruikers in gevaar komen. Dit geldt ook voor bijvoorbeeld V2I server platforms, welke toegang kunnen bieden aan een groot aantal sensoren.[47]

Een ander risico van de cyberveiligheid van voertuigen is hun lange levensduur. Waar sommige "reguliere" IT-consumentengoederen om de 3 tot 5 jaar vervangen worden, gaan auto's makkelijk 10 tot 30 jaar mee. In deze lange tijdsduur kunnen bepaalde cryptografische algoritmes of ontsleutelingstechnieken worden ontwikkeld die eerder niet bestonden, zoals post-quantum cryptografie. De ontwikkelingen en veiligheidsbedreigingen van de samenleving gelden ook voor oudere voertuigen. Zij moeten hier mee omgaan en voldoen aan nieuwe standaarden. Het aanbieden van upgradebare hardware en software is daarom van belang, met het risico dat het patch-mechanisme zelf gehackt wordt. Voertuigen besteden namelijk een groot deel van hun tijd in openbare, onbewaakte ruimte, waardoor ze vrij toegankelijk zijn voor kwaadwillenden.

Naast cryptografie speelt ook intrusion detection prevention schemes (IDPS) een belangrijke rol in de veiligheid. Dit zijn systemen die afwijkingen in de communicatie monitoren, wat kan duiden op ongeautoriseerde toegang of manipulatie van apparaten. Deze zijn relatief makkelijke te integreren in een auto en brengen bovenal een stuk lagere kosten met zich mee. Uiteindelijk zal een combinatie van meerdere, onafhankelijke veiligheidsmechanismes voor het meest effectieve totaalpakket kunnen zorgen.

De automotive sector heeft cryptografisch gezien een aantal unieke uitdagingen, bijvoorbeeld doordat het netwerk in hoge mate veranderlijk is, alle communicatie draadloos plaatsvindt en er in een kort tijdbestek informatie moet worden uitgewisseld en beslissingen worden gemaakt.[48] Vanuit een veiligheidsoogpunt is het belangrijk dat de authenticatie van berichten en de privacy van een bestuurder gewaarborgd wordt, de informatie en communicatie ten alle tijden beschikbaar is, en het juiste niveau van geheimhouding wordt aangehouden. Alleen bepaalde partijen mogen toegang kunnen hebben tot gevoelige informatie, bijvoorbeeld de politie wanneer er een ongeval is gebeurd.
Tot slot heeft de automotive sector een erg competitieve markt, waarbij veiligheid en ADAS gebruikt worden als unique selling point. De cybersecurity van deze technologie is echter ondergeschikt aan de functie en de risico`s van onvoldoende cybersecurity zijn (nog) niet zichtbaar. OEMs zullen hier naar verwachting echter ook weinig openheid over bieden, doordat dit hun ontwikkelingen richting autonoom rijden kan schaden, waardoor het mogelijk is dat de risico`s pas achteraf zichtbaar worden wanneer het heeft geleid tot schade. Hierdoor kan het lastig zijn om de extra kosten die nodig zijn voor innovatie op het gebied van cybersecurity door te vertalen naar de klant.

[47] https://cybersecurity.ieee.org/blog/2017/06/28/christof-paar-on-why-cryptography-is-key-for-automotive-security/
[48] https://www.hindawi.com/journals/wcmc/2018/1640167/

3.3.2 Resultaten

Op basis van de waardenetwerkanalyse voor de automotive sector, is de conclusie dat het waardenetwerk voor cryptocommunicatie in de context van (directe) V2X communicatie op dit moment niet te schetsen is. De meeste projecten zitten in een pilotfase (laag TRL) en er is op dit moment geen sprake van een valorisatieketen, mede doordat wetgeving en standaarden op dit vlak nog niet bestaan. Door het vroege stadium in de (technologische) ontwikkeling, is het nog onduidelijk hoe het innovatie ecosysteem er in de toekomst uit gaat zien en welke spelers, marktdynamieken, samenwerkingsverbanden, kansen en barrières hier een rol spelen. Een waardenetwerk is daarom geen geschikt middel om het ecosysteem in kaart te brengen, aangezien de valorisatieketen nog gevormd moet worden. Hiernaast is het niet gelukt om binnen de looptijd van dit onderzoek met de twee belangrijkste Nederlandse voertuigproducenten DAF en VDL te spreken, waardoor wij niet hebben kunnen toetsen of zij deze bevindingen onderschrijven. Desondanks lichten we in dit hoofdstuk de bevindingen toe die uit het onderzoek naar voren zijn gekomen. Deze bieden een aantal interessante inzichten in de huidige dynamieken rondom cybersecurity innovatie in deze sector. De bevindingen zijn als volgt gecategoriseerd: algemene bevindingen, barrières, drijfveren voor innovatie en bevindingen rondom het ecosysteem. De bevindingen zijn deels beschrijvend over het huidige ecosysteem, maar bevatten ook voorstellen voor veranderingen die de geïnterviewden als wenselijk zien.

3.3.2.1 Algemene bevindingen

Cryptografie in de automotive sector zou een (toekomstige) markt kunnen vormen voor het benutten van de Nederlandse voorsprong op cryptografie, maar er zijn op dit moment nog een groot aantal technische en niet-technische barrières. Hierdoor bevindt innovatie voor cryptografie in de auto-industrie zich nog in een vroeg stadium (laag TRL), waarbij vooral in (Europese) consortia wordt samengewerkt tussen partijen. Onderwerpen zoals post-quantum cryptografie zijn voor alle gesproken partijen in de komende jaren niet relevant.

Zelfrijdende auto’s zullen in de toekomst niet alle sensorinformatie zelf vergaren, maar de beschikbare informatie zowel met elkaar als met de omgeving communiceren om beslissingen te maken. Het beveiligen van verbindingen en de authenticatie van de afzender van berichten zijn hierdoor voorlopig het belangrijkste doel, waarbij cryptografie slechts één van de mogelijke middelen is om deze beveiliging tot stand te brengen. Zo wordt nu vooral gebruik gemaakt van commodity protocollen: TLS en oplossingen die gebruik maken van certificaten. Deze technologieën zijn bewezen technologie; al lang in gebruik en innoveren nauwelijks. Ze zijn ook goedkoper dan moderne innovatieve cryptografie oplossingen die nog ontwikkeld moeten worden. Zolang er in de praktijk weinig tot geen communicatie plaatsvindt tussen voertuigen onderling en infrastructuur, is er geen behoefte aan innovatieve cryptografie. Het nadeel is dat de bewezen technologieën niet quantum-bestendig zijn en daarmee op termijn onveiligheid brengen bij toepassing in de voertuigen.. Het is moeilijk om een inschatting te geven van de termijn waarop deze innovatieve cryptografie relevant gaat worden. De verwachting is dat als er functionele en technische richtlijnen worden gemaakt en partijen veel samenwerken, er een sneeuwbaleffect op kan treden en er binnen een tijdsbestek van ca. 20 jaar V2X cryptocommunicatie kan plaatsvinden. Zoals hierboven benoemd zal quantum computing een bevorderende invloed hebben op

de ontwikkeling van crypto in de automotive industrie vanwege de hogere benodigde communicatie veiligheid.

Het huidige beeld is dat de vooruitgang van de cryptografische innovatie vooral incrementeel is en dat er veel tijd nodig is om de vele complexe vraagstukken in verschillende domeinen te beantwoorden. Hierin spelen een combinatie van technologische innovatie, standaardisering en beleid een belangrijke rol. De incrementele innovaties zouden versneld kunnen worden door een gedeelde langetermijnvisie voor bijvoorbeeld smart infrastructuur te vormen, in samenwerking met meerdere partijen uit het ecosysteem, en functionele afspraken te maken waarop voortgebouwd kan worden. Het recent opgestarte innovatieproject 'DITM' (Digitale Infrastructuur voor Toekomstbestendige Mobiliteit) kan hieraan bijdragen. Eén van onze bevindingen is dat er wel op korte termijn marktkansen kunnen zijn voor cryptografische producten in de smart infrastructuur. Cryptografie is namelijk op dit moment al nodig bij de smart infrastructuur om veilige en effectieve communicatie te waarborgen.

3.3.2.2 Drijfveren voor innovatie

Ondanks het grote aantal uitdagingen dat moet worden opgelost voordat de valorisatieketen gevormd kan worden, zijn er een aantal belangrijke drijfveren voor innovatie. Allereerst is het wenselijk vanuit efficiëntie oogpunt. Met zelfstandig rijdende voertuigen zouden we efficiënter rijden en een betere doorstoom van voertuigen genereren. Dat zou ook zorgen dat we minder energie nodig hebben om dezelfde afstand af te leggen[49], wat onder andere uitstootreductie tot gevolg heeft. Een volgende drijfveer voor innovatie is het verbeteren van de verkeersveiligheid, doordat (inschattings)fouten kunnen worden voorkomen of gecorrigeerd. Rijden zou in het algemeen veiliger kunnen worden doordat de gehele smart infrastructuur met elkaar in verbinding staat.[50] [51]

De elektrificatie binnen de automotive sector biedt hiernaast ook kansen voor innovatie op cybersecuritygebied. Door de innovatiedruk die ontstaat vanuit disruptieve partijen, zijn ook gevestigde bedrijven genoodzaakt om (technologisch) te innoveren om te overleven, wat kansen biedt voor de implementatie van cryptografische systemen. Tevens worden nieuwe verdienmodellen mogelijk binnen de keten, bijvoorbeeld voor het (op afstand) updaten van software. Daarnaast heeft de Europese commissie als doel gesteld om in 2025 een ononderbroken implementatie van 5G te hebben, wat een stimulans is voor de uitrol van slimme infrastructuur. Onderzoek heeft uitgewezen dat binnen Nederland in 2030 15% van de voertuigen voorzien kan zijn van SAE level 3 of hoger.[52],[53]

---

[49] Sieber, L., Ruch, C., Hörl, S., Axhausen, K. W., & Frazzoli, E. (2020). Improved public transportation in rural areas with self-driving cars: A study on the operation of Swiss train lines. Transportation research part A: policy and practice, Vol. 134, pp. 35-51.

[50] Kalra, N., & Groves, D. G. (2017), The enemy of good: Estimating the cost of waiting for nearly perfect automated vehicles.

[51] Teoh, E. R., & Kidd, D. G. (2017), 'Rage against the machine? Google's self-driving cars versus human drivers', *Journal of Safety Research*, Vol. 63, pp. 57-60.

[52] J3016_202104: Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles - SAE International

[53] Milakis, D., Snelder, M. en Arem, B. (et. al.) (2017), 'Development and transport implications of automated vehicles in the Netherlands: Scenarios for 2030 and 2050', *European Journal of Transport and Infrastructure Research,* Vol. 17, pp. 63-85.

3.3.2.3 Barrières

Over het algemeen ontbreekt er op dit moment een gedeelde visie over de ontwikkeling van V2X communicatie in de automotive sector, waardoor partijen zich onafhankelijk van elkaar voorbereiden op de komst van zelfrijdende voertuigen en slimme infrastructuur. Partijen in het ecosysteem richten zich hiernaast hoofdzakelijk op het bestaande productportfolio en kernactiviteiten.[54] De huidige marktaandeelhouders hebben een sterk merk met bijbehorende producten en ervaren momenteel veel uitdagingen, bijvoorbeeld door de impact van de pandemie en chiptekort op productielijnen. Hiernaast kunnen disruptieve technologieën machtsverschuivingen creëren die niet in hun voordeel zijn. Het is aannemelijk dat de grote marktaandeelhouders willen meeliften op het succes van early adopters. Deze lopen echter een risico, doordat de implementatie van nieuwe technologie ook imagoschade kan voortbrengen. Als er iets misgaat in de technologie en de auto als onveilig of onveiliger dan andere merken wordt ervaren door consumenten zou het merk waarde verliezen. Het introduceren van nieuwe risicovolle functies is strategisch interessanter als het beleidsmatig of door de markt wordt afgedwongen.

Ook is cybersecurity een passieve eis van veel consumenten: het wordt gezien als een minimumeis waaraan voldaan moet worden en het is slechts in beperkte mate een stimulans om een auto te kopen. Dit heeft invloed op zowel voertuigproducenten als component leveranciers. Component leveranciers geven aan dat producenten enthousiast worden van een functionaliteit als het helpt een auto te verkopen, maar niet per se extra willen betalen voor het inbouwen van cryptografie functionaliteit in chips. Deze functionaliteiten zijn soms zelfs in beginsel ingebouwd in producten, waarna klanten ze handmatig uitschakelen. Cryptografie wordt slechts gezien als een onderdeel van een geheel dat uiteindelijk veilig moet zijn.

Een aansluitende reden waardoor er minder economische druk is om te innoveren zijn de kosten. Vanwege het commerciële belang naar winst, zullen minimale veiligheidsprocedures ingebouwd worden om kosten te drukken. De prijs is vaak leidend, waardoor er wordt gekozen voor ‘minimum viable’ oplossing. De huidige innovatiekosten en de beperkte functionaliteit die cryptografie op dit moment oplevert, in combinatie met de complexiteit om de bijbehorende toename in veiligheid in monetaire waarde uit te drukken, zorgt ervoor dat het lastig is om een positieve business case te formuleren. Er is dus weinig economische incentive voor industriepartijen om zich bezig te houden met iets als cryptografie, en dit zal naar verwachting vooral door wetgeving en standaarden moeten worden afgedwongen (welke veel tijd kosten om te ontwikkelen).

De lange levensduur van auto’s zorgt ervoor dat er vanaf de productie al nagedacht moet worden over de gehele levenscyclus; technologie en/of software die ingebouwd zijn, moeten makkelijk 30 jaar mee kunnen gaan. Hierdoor moet er ook de mogelijkheid zijn om op een later moment nieuwe onderdelen en/of functionaliteiten in te bouwen. In de context van cryptocommunicatie, zullen bijvoorbeeld cryptografische protocollen geüpdatet moeten worden. Hiernaast moeten er ook (deels) retrospectief onderdelen toe worden gevoegd aan bestaande

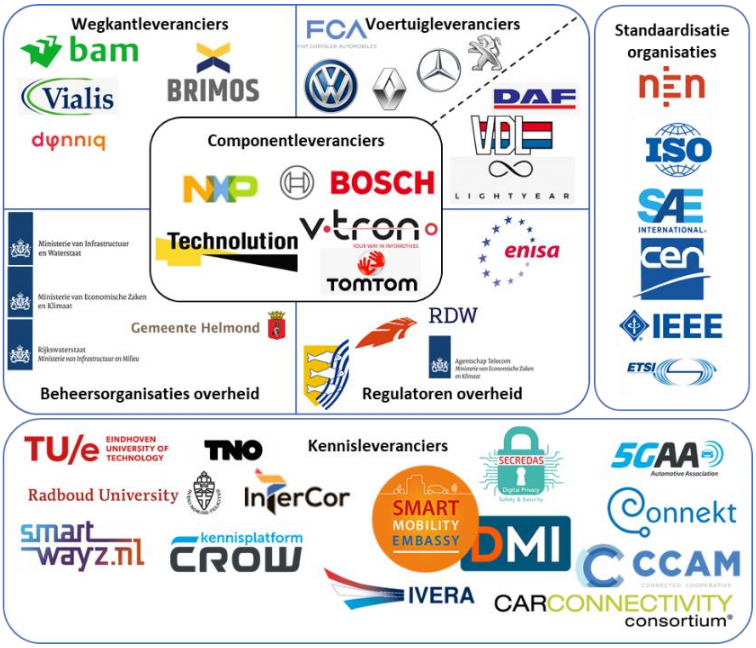
[54] Hofstätter, T., Krawina, M., Mühlreiter, B., Pöhler, S., en A. Tschiesner (2020), ‘Reimagining the auto industry’s future: It’s now or never’, McKinsey & Company (https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/reimagining-the-auto-industrys-future-its-now-or-never)

voertuigen om V2X communicatie mogelijk te maken. De huidige chiptekorten zetten in beide gevallen druk op de uitrol hiervan.

Ten slotte is er een tekort aan personeel bij cybersecuritybedrijven en is er te weinig kennis in de rest van de markt voor het absorberen van innovatie op dit gebied. De kennis en kunde zijn geconcentreerd en bovendien vaak erg specialistisch, wat remmend werkt op innovatie.

3.3.2.4 Bevindingen rondom het ecosysteem

Tijdens de interviews is ook gekeken naar de rol van de spelers binnen het landschap en daaruit volgt de volgende analyse voor de samenwerking en ecosysteem-bevordering. Een overzicht van relevante partijen binnen het (Nederlandse) ecosysteem staat weergeven in figuur 8.



Figuur 8 Overzicht van partijen die een rol spelen in het automotive ecosysteem[55].

De kennisleveranciers zoals universiteiten zijn heel actief op het gebied van cryptografie, zoals aangegeven in hoofdstuk 2, maar er mist soms een aansluiting met de markt. Ze worden bijvoorbeeld niet actief benaderd door voertuigleveranciers/ original equipment manufacturers (OEMs) om hun onderzoek naar versleuteling van berichten toe te passen op hun producten of andere kennisdeling. Voertuig-leveranciers nemen over het algemeen een passieve rol in dit ecosysteem in. Ze hebben vaak ook veel te verliezen (imago, marktaandeel) en relatief weinig te winnen omdat ze al succesvol zijn, waardoor ze terughoudend kunnen zijn in het delen van informatie. Ze willen niet alleen hun intellectueel eigendom beschermen, maar ook veilig omgaan met (klant)data. OEMs opereren hierdoor relatief geïsoleerd, terwijl er juist samenwerking nodig is tussen OEMs en omringende partijen in het ecosysteem om geïntegreerde oplossingen te ontwikkelen. Om hen te stimuleren informatie te delen kan beleid nodig zijn vanuit de overheid. Open innovatie (bijvoorbeeld open source software) kan een geschikt

[55] TNO (2022), Crypto for Automotive – WP1 Report: Toepassing cyrptografie in directe automotive communicatie (te verschijnen Q4 2022).

middel zijn om samenwerking en innovatie te stimuleren, maar de vraag is of dit lukt met de vrij conservatieve en gesloten houding van voertuigproducenten.

De regulatoren vanuit de overheid houden zich vooral bezig met risicobeheersing. Aangezien cryptografie in de automotive industrie nog niet actief speelt, houden ze nog geen toezicht op dit gebied in deze sector. De componentleveranciers geven aan dat zij volgend zijn in dit ecosysteem. Hoewel zij bijvoorbeeld chips ontwerpen met cryptografie functionaliteiten, merken zij dat de klant ze uit zet of niet geïnteresseerd is in deze functionaliteit. Standaardisatieorganisaties zoals de NEN en de ISO zijn startend in het ontwikkelen van standaarden. Leveranciers van infrastructuur zoals laadpalen zijn ook actief op het gebied van cryptografie innovatie. Zo zijn er verschillende lopende Europese initiatieven en wordt er samengewerkt in cyberconsortia. Ze geven aan dat veiligheid steeds belangrijker wordt op de laadinfrastructuur, ook vanwege aanbestedingen waar de hogere veiligheid een vereiste is.

Infrastructuur beheerders zijn vooruitstrevend binnen hun domein in de EU, maar willen geen ecosysteem trekker zijn. Het kost te veel geld en tijd om alle samenwerkingen te ontwikkelen en het ligt te ver af van de huidige taken volgens de interviews. Er is wel kennis over functionele en operationele eisen bij deze partijen, waardoor ze een belangrijke rol kunnen spelen in het opzetten van de toekomstvisie. Rijkswaterstaat stelt vooral functionele eisen, waarna de precieze invulling bij de marktpartijen ligt. Overheden, netwerkbeheerders, infrastructuurbeheerders en serviceleveranciers werken actief samen met brancheorganisaties, in bijvoorbeeld field labs en cyberconsortia.

Grote technologiebedrijven zoals Amazon en Google hebben tot slot het netwerk, de middelen en de kans om hun marktaandeel te vergroten door te investeren in slimme infrastructuur. Zij zouden een disruptieve rol kunnen innemen in het innovatie ecosysteem, maar dit roept wel vragen op rondom dataprivacy en dit ontneemt de overheid de kans om een leidende rol te nemen en standaarden te stellen.

3.3.3 Conclusie

Cryptografie zou in de toekomst een belangrijke rol voor de automotive industrie kunnen spelen, maar heeft dat op dit moment nog niet. Er zijn nog een groot aantal technologische en niet-technologische uitdagingen die moeten worden opgelost voordat er op grote schaal V2X communicatie kan worden toegepast. Volgens de interviews is op dit moment cybersecurity ondergeschikt aan functionaliteit; er is nog relatief weinig samenwerking in het ecosysteem en het speelveld is erg verdeeld. Geen van de partijen wil verantwoordelijkheid dragen wanneer het mis gaat, waardoor veel partijen naar elkaar wijzen (overheid naar industrie en vice-versa). Dit is opmerkelijk, omdat fysieke veiligheid hoge prioriteit heeft binnen het automotive ecosysteem. Concluderend kunnen we zeggen dat als er een cybersecurity-innovatie bevorderend ecosysteem moet worden opgezet, het verstandig is om spelers binnen het ecosysteem te stimuleren die al een bestaand netwerk hebben en markaandeel kunnen veroveren.

3.4 Overkoepelende resultaten

Aangezien beide sectoren behoren tot de vitale infrastructuur in Nederland, is het interessant om tot slot ook nog kort stil te staan bij de belangrijkste verschillen en overeenkomsten tussen de sectoren. Deze leiden vervolgens, samen met de vorige twee sub-secties, tot een set aan vervolgvragen die in de toekomst beantwoord kunnen worden.

3.4.1 Overeenkomsten en verschillen

Zoals vermeld in de introductie van dit hoofdstuk, behoren beide sectoren tot de vitale infrastructuur in Nederland. Dit brengt een belangrijke maatschappelijke incentive met zich mee om de cybersecurity in het algemeen goed op orde te hebben, waarbij enerzijds leveringszekerheid en anderzijds verkeersveiligheid van belang zijn. Een andere kenmerkende overeenkomst is dat beide infrastructuur bevatten (voertuigen dan wel windmolens) die tientallen jaren mee dienen te gaan, waardoor de gehele levenscyclus vanaf het eerste ontwerp moet worden meegenomen. Hier bovenop heeft grootschalige digitalisering gezorgd voor een transitie van grotendeels analoge hardware naar een systeem van complexe, digitale infrastructuur. Hierdoor is tussentijdse patching van de cybersecurity, waaronder de cryptografie, van essentieel belang is om weerbaar te blijven tegen toekomstige dreigingen. In beide sectoren wordt cybersecurity soms slechts achteraf meegenomen in de innovatiecyclus in plaats van by-design en wordt het pas gezien als een probleem wanneer er daadwerkelijk iets mankeert (‘ignorance is bliss’). Hoge innovatiekosten versterken dit issue. Tot slot geldt voor beide sectoren dat post-quantum cryptografie voorlopig nog (verre) toekomstmuziek is. Bij grote partijen staat het onderwerp al wel op de radar, maar er zijn nog geen plannen voor de concrete implementatie.

Er zijn echter ook een aantal belangrijke verschillen tussen de twee sectoren. Om te beginnen is het wind op zee-ecosysteem ‘up and running’ en zal deze de komende decennia flink worden opgeschaald[37], terwijl V2X communicatie in de automotive sector nog hoofdzakelijk in de pilot fase zit en uitrol op grote schaal van volledig autonoom rijdende voertuigen pas in de (verre) toekomst plaats zal vinden. Dit is ook kenmerkend voor de uitzonderlijk hoge complexiteit die V2X communicatie met zich meebrengt, waarbij er onder andere op technologisch, ethisch, juridisch en geografisch gebied grote vraagstukken zijn die eerst nog opgelost moeten worden. Hierdoor is het ook nog niet duidelijk hoe de V2X communicatie in de toekomst er in de praktijk uit zal zien, terwijl dit voor wind op zee al redelijk vast staat en daadwerkelijk al plaatsvindt. Ook op het gebied van externe dreiging is er een groot verschil tussen de sectoren. Windparken (en de bijbehorende infrastructuur) op zee zijn niet gemakkelijk te bereiken en de dreiging van grootschalige onderbreking van energielevering zal naar verwachting voornamelijk komen vanuit statelijke actoren. Aan de andere kant zal de benodigde infrastructuur voor V2X communicatie naar verwachting geïntegreerd worden in de bestaande infrastructuur die publiekelijk toegankelijk is. Tegelijkertijd kan er al flinke schade toegebracht worden aan mensenlevens door het hacken van één enkel voertuig, ten opzichte van één enkele windmolen. Qua onderhoud is er ook een verschil tussen de sectoren: voor wind op zee is het stilleggen van turbines een barrière om (grootschalig) onderhoud te plegen, terwijl dit voor zelfrijdende voertuigen in mindere mate geldt. Tot slot zit er een verschil tussen de twee sectoren qua incentive voor marktpartijen om de cybersecurity, en daarmee ook de

cryptografie, op orde te hebben. Voor wind op zee heeft deze veiligheid namelijk een belangrijke economische incentive (bv. marktafspraken rondom vraag en aanbod van elektriciteit), terwijl deze indirecter is voor V2X communicatie (bv. imagoschade bij ongelukken).

3.4.2 Conclusies en vervolgvragen

De waardenetwerkanalyse heeft waardevolle inzichten naar boven gebracht op het gebied van cybersecurity en (post-quantum) cryptografie voor beide sectoren. Het waardenetwerk voor de wind op zee sector laat verschillende rollen in het bestaande ecosysteem en de interacties hiertussen zien, waarmee er duidelijk een valorisatieketen zichtbaar is. Hiermee worden een set aan belangrijke drijfveren en barrières zichtbaar die resulteren in concrete aanbevelingen om innovatie binnen het ecosysteem te stimuleren. Aan de andere kant is het waardenetwerk voor de automotive sector op het moment nog niet te schetsen, aangezien innovatie op het gebied van V2X communicatie hoofdzakelijk in de pilotfase zit en er nog geen sprake is van een valorisatieketen. Desondanks heeft dit onderzoek de huidige staat van het ecosysteem in kaart gebracht en zijn een aantal belangrijke dynamieken en uitdagingen beschreven.

De bevindingen die beschreven zijn in dit hoofdstuk leiden tot een reeks vervolgvragen die aanleiding kunnen vormen voor toekomstig onderzoek. Voorbeelden van vervolgvragen zijn:

- In welke mate worden de bevindingen uit de interviews gedragen door (concurrerende) partijen die dezelfde rol aannemen in het waardenetwerk? Dit kan worden aangekaart door aanvullende, validerende interviews uit te voeren.
- Wat zijn de belangrijkste sterktes en zwaktes van het Nederlandse ecosysteem ten opzichte van andere landen? Om deze vraag te beantwoorden zouden we een waardenetwerkanalyse op internationaal niveau uit kunnen voeren, waarin bijvoorbeeld ook Frankrijk en Duitsland of de gehele Europese Unie worden meegenomen.
- Het innovatie ecosysteem in de automotive sector is relatief gefragmenteerd en het is niet gelukt om met DAF en/of VDL te spreken over hun rol als OEM. Welke partijen zijn van belang om hiernaast nog te interviewen om een volledig beeld te vormen van het Nederlandse ecosysteem?
- Welke technologische ontwikkelingen, zoals beschreven in paragraaf 2.1, zijn naast de migratie naar post-quantum cryptografie nog meer relevant voor deze twee toepassingssectoren?
- Is er behoefte aan nieuwe of aanvullende samenwerkingsverbanden of consortia om innovatie op het gebied van cryptocommunicatie in deze sectoren te verbeteren?

4 Invulling routekaart cryptocommunnicatie

Het doel van de routekaart cryptocommunicatie wordt drieledig. Allereerst voor de ontwikkeling van innovatieve producten- en diensten op het gebied van cryptocommunicatie, daarnaast voor het bijdragen aan de economische activiteit in Nederland en als derde om de strategische autonomie van Nederland te stimuleren. Een economisch gezond ecosysteem en sterk functionerend waardenetwerk draagt bij aan het behalen van de doelstellingen van de routekaart cryptocommunicatie. De bevindingen uit de marktverkenning en de waardenetwerkanalyse kunnen als fundament worden gebruikt voor de routekaart waarop verder doorgebouwd kan worden[56]. De bevindingen worden omgezet in de sporen van de routekaart, om op een gegronde manier aan de gevonden uitdagingen, de barrières en *valleys of death*, binnen de valorisatieketen te werken.

De routekaart richt zich op de periode 2022 tot en met 2032. In deze periode kunnen zich nieuwe, nog niet voorziene ontwikkelingen voordoen. Om die reden blijft het een dynamische en levende routekaart die tussentijds bijgesteld moet worden op basis van nieuwe inzichten en ontwikkelingen.

Het in dit hoofdstuk weergegeven fundament voor de routekaart cryptocommunicatie is onderverdeeld in vijf ontwikkelfases: *Discovery/basic research, Technology development, Validation and demonstration, Integration and operationalization* en *Deployment*. Voor zowel de energiesector als de automotive sector worden betrokken partijen weergeven, ingedeeld binnen de vijf ontwikkelfases. Dit is gebaseerd op een doorvertaling van de inzichten die uit de waardenetwerkanalyse zijn verkregen. Vervolgens worden voor de twee sectoren ‘valleys of death’ weergegeven, geplot op de vijf ontwikkelfases. Met een valley of death wordt een barrière bedoeld tussen de ontwikkelfases van innovatie. Ten slotte worden de mogelijke oplossingen beschreven en deze worden doorvertaald in vier ‘sporen’. In deze sporen worden mogelijke oplossingen beschreven voor het overwinnen van de barrières en de valleys of death, welke met de routekaart cryptocommunicatie bewandeld kunnen worden.

4.1 Toepassingssector: Wind op zee

4.1.1 Overzicht 1: Betrokken partijen

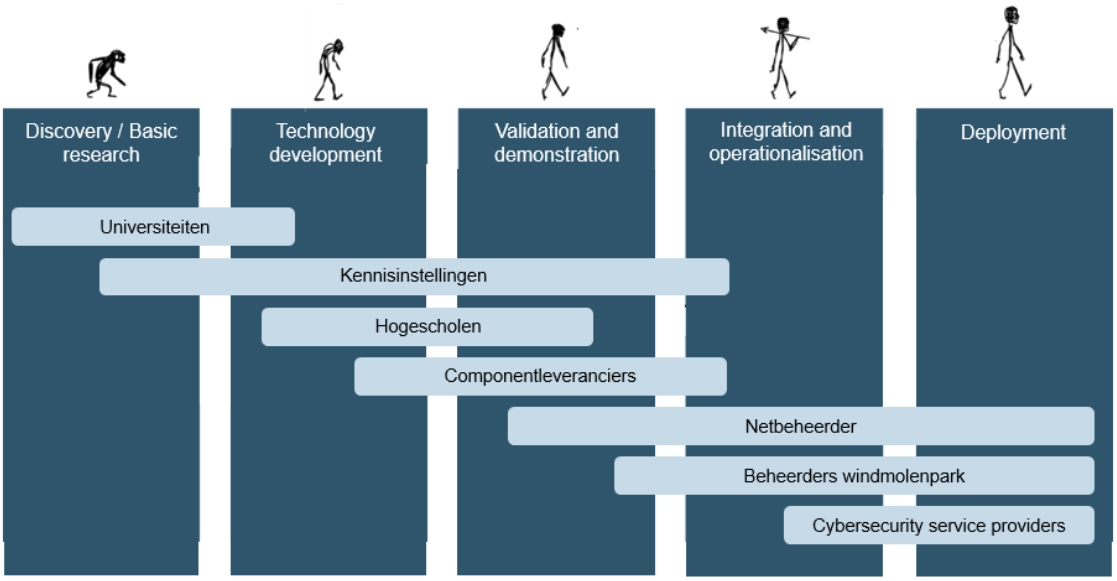
In het waardenetwerk van de energiesector (zie figuur 7, p. 27) is van links naar rechts de valorisatie van kennisopbouw door onderzoek naar productlancering en integratie te zien.[57] De (transmissie)netbeheerder staat qua waarde uitwisseling centraal in het waardenetwerk en de financiering van producten waarvoor cryptografie relevant is komt vooral vanuit beheerders van windmolenparken en de netbeheerder (de klanten). Er zijn in principe geen hiaten in beleid en/of toezicht hierop zichtbaar voor dit ecosysteem, doordat alle relevante partijen onder de Wet Beveiliging Netwerk en Informatiesystemen (Wbni) vallen. Enkele component-

[56] Zoals benoemd (zie p. 6) zijn de marktverkenning en waardenetwerk analyse binnen relatief korte tijd uitgevoerd, met als gevolg dat vervolgonderzoek nodig is om deze bevindingen verder te kunnen nuanceren, valideren en uit te breiden ter invulling van de routekaart.

[57] Het waardenetwerk van de volledige elektriciteitssector inclusief distributiebeheerder en consumenten is beschreven in vorig onderzoek: TNO (2020), *EZK Verdieping Valorisatieketens: Verkenning van het ecosysteem en waardenetwerk Automated Security* (TNO 2020 R12224).

leveranciers staan centraal voor de levering van onderdelen voor de windmolens. Deze hebben vervolgens ook een rol bij het onderhoud, doordat zij hun eigen experts hiervoor inzetten.

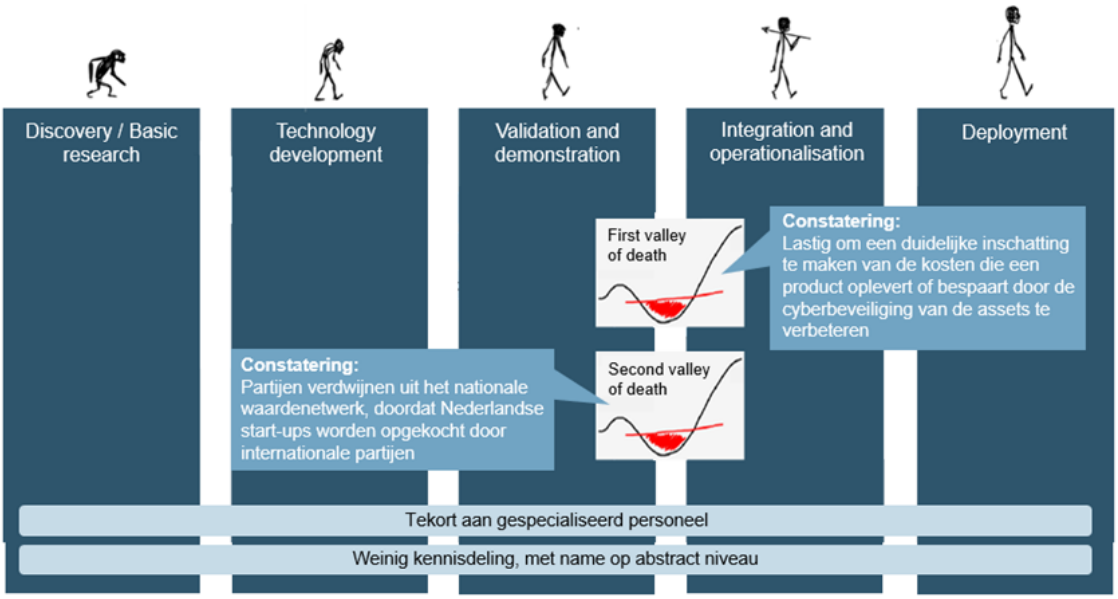
In figuur 9 zijn de rollen uit het waardenetwerk (zie paragraaf 3.2.2., p. 28) geplot op de vijf ontwikkelfases van de routekaart. Hierbij is er overlap tussen de verschillende rollen te zien tussen en binnen bepaalde pijlers, wat concrete mogelijkheden kan bieden voor kennisoverdracht en samenwerkingen.



Figuur 9 Schets op basis van de waardenetwerkanalyse binnen de valorisatieketen van de wind op zee sector.

4.1.2 *Overzicht 2: 'Valleys of death' tussen de ontwikkelfases*

De geïdentificeerde *valleys of death* binnen de energiesector zijn als volgt:



Figuur 10 De "Valleys of death" in de ontwikkelfases die binnen de energiesector uit deskresearch en de interviews naar voren kwamen.

De eerste valley of death bij de energiesector zit tussen validatie/demonstratie en integratie/operationalisatie. Deze valley of death speelt voornamelijk in de interactie tussen kennisinstellingen, netbeheerders en leveranciers. Het belang van de integratie van cryptocommunicatieproducten wordt ingezien, maar voor de daadwerkelijke integratie van producten bestaat er een kosten-baten analyse voor de betrokken partijen. Wat kost een product en wat kost de implementatie/ deployment ervan (bijvoorbeeld de kosten voor het stilzetten van een windturbine) en wat levert het uiteindelijk op? Hierbij is het met name lastig om een duidelijke inschatting te maken van de kosten van en/of besparingen door de cyberbeveiliging van de assets te verbeteren.

De tweede valley of death zit ook tussen validatie/demonstratie en integratie/ operationalisatie en speelt voornamelijk voor de cybersecurity serviceproviders. Nederland kent meerdere startups voor cryptografische producten, maar gezien er een kleine markt is, wordt de stap naar integratie/operationalisatie in de Nederlandse markt weinig gemaakt en worden de startups opgekocht door internationale partijen. Hierdoor verdwijnen deze partijen uit het nationale waardenetwerk.

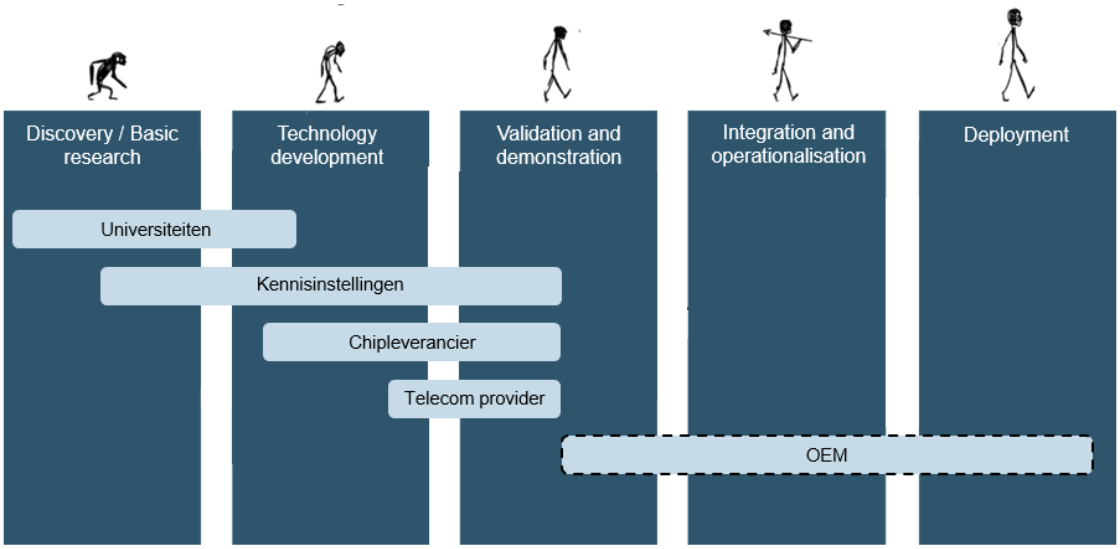
Overkoepelend over de gehele valorisatieketen spelen er twee barrières mee in deze sector:

1 Er is een (groot) tekort aan personeel dat zowel cybersecurity als cryptografische kennis heeft en specialistische kennis van de sector zelf.
2 Op sommige gebieden, zoals bij het onderhoud, is er weinig sprake van communicatie en afstemming tussen de partijen in de keten. Verbetering hiervan zouden de kosten voor onder andere patching van cryptografische producten kunnen drukken.

4.2 Toepassingssector: Automotive

4.2.1 Overzicht 1: Betrokken partijen

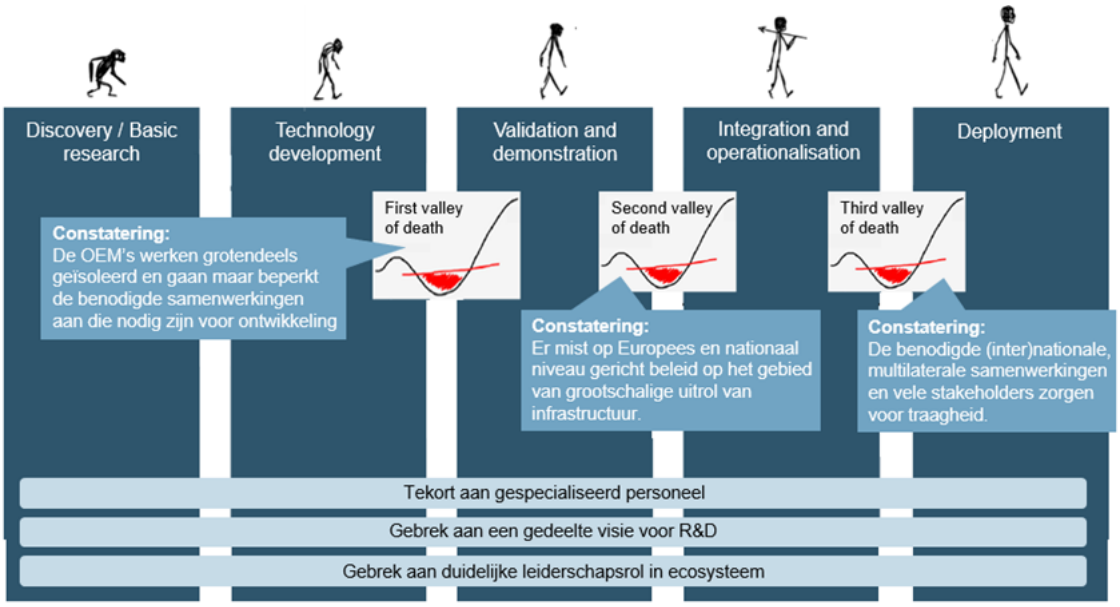
Voor de automotive sector is, zoals in het hoofdstuk hierboven beschreven, nog geen valorisatieketen in kaart te brengen. In figuur 11 is te zien dat de meeste betrokken partijen (zie paragraaf 3.3.2.4., p. 37) in deze sector in de eerste drie fases van ontwikkeling zitten. Binnen de sector is bij de gesproken partijen nog geen stap gezet naar integratie en operationalisatie (fase 4), omdat hiervoor eerst nog een aantal grote stappen moeten worden gezet op het gebied van o.a. standaardisatie, wetgeving en doorontwikkeling van de technologie. Het is nog onduidelijk hoe het innovatie ecosysteem er uit gaat zien in de toekomst en welke spelers, marktdynamieken, samenwerkingsverbanden, kansen en barrières hier een rol gaan spelen.



Figuur 11 Schets op basis van de waardenetwerkanalyse van de partijen binnen de automotive sector. Dit is geen uitputtend overzicht van alle partijen die betrokken zijn bij innovatie op het gebied van V2X communicatie, maar een greep uit de partijen die wij hebben gesproken. Het is niet gelukt om binnen de looptijd van dit onderzoek met een OEM te spreken, waardoor we de positie op basis van literatuuronderzoek hebben geschetst. NB. De infrastructuur partijen vallen ook onder de OEMs.

4.2.2 *Overzicht 2: 'Valleys of death' tussen de ontwikkelfases*

De geïdentificeerde valleys of death binnen de automotive sector zijn als volgt:



Figuur 12 De valleys of death en de meer algemene barrières in de ontwikkelfases die binnen de automotive sector uit deskresearch en de interviews naar voren kwamen.

Ten eerste is er een valley of death te vinden tussen de technologieontwikkeling en validatie/demonstratie, doordat de centrale spelers in het ecosysteem geïsoleerd werken en een afwachtende houding aannemen in samenwerkingen die leiden tot de implementatie van nieuwe producten op het gebied van cryptografie. Meer specifiek, zoals te zien in figuur 11, spelen de OEM's een zeer beperkte rol in de

onderzoeks- en ontwikkelingsfase, waardoor de overdracht van technologie naar implementatie beperkt is.

Vervolgens is er ook een valley of death tussen validatie/demonstratie en integratie/operationalisatie door een gebrek aan beleid en standaarden op zowel Europees als nationaal niveau. Doordat cryptocommunicatie geen corebusiness van OEMs is, blijft een innovatieprikkel uit.

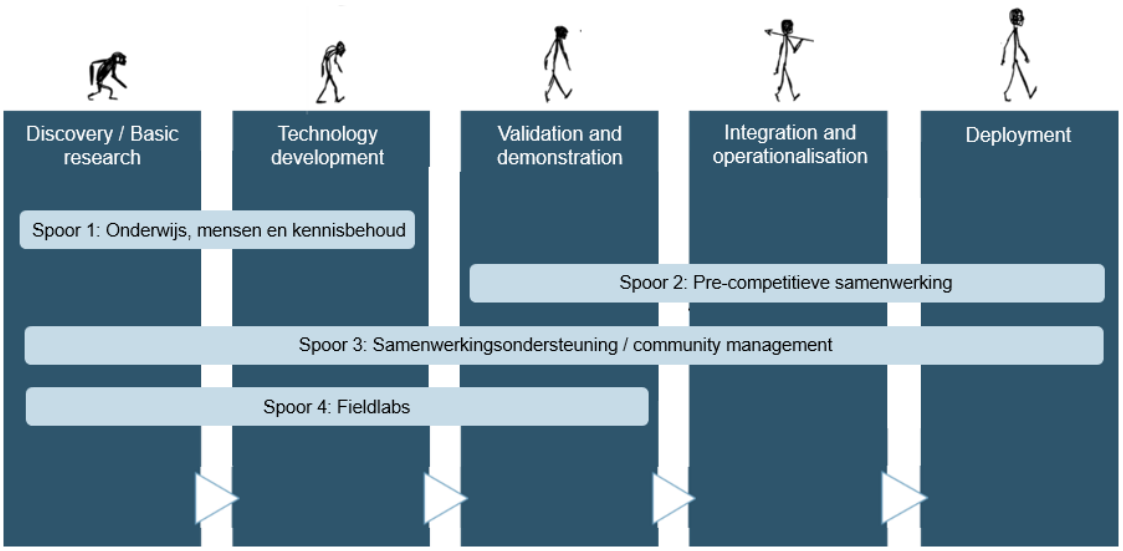
De derde valley of death is de traagheid waarmee standaarden voor toegestane deployment ontwikkeld worden. Deze ontwikkeling kost veel tijd door de benodigde multilaterale en internationale afstemming.

Overkoepelend over de gehele valorisatieketen spelen er nog twee barrières mee in deze sector:

1 de schaarste aan goed opgeleid cybersecuritypersoneel die zowel technische kennis als sectorspecifieke kennis bezitten;
2 het gebrek aan een gedeelde visie tussen partijen in het ecosysteem om de prioriteiten op het gebied van R&D vast te stellen;
3 een missende duidelijke leiderschapsrol in het ecosysteem, waarbij overheid en marktpartijen naar elkaar wijzen om de eerste stap te zetten in de ontwikkeling.

4.3 Overzicht 3: Fundament voor de routekaart cryptocommunicatie

Hieronder wordt het fundament van de routekaart uitgewerkt. Op basis van de bevindingen uit de marktverkenning en waardenetwerkanalyses zijn vier sporen opgesteld, waar in de routekaart aan gewerkt kan worden om de valorisatie van cryptocommunicatieproducten te versterken. De vier sporen van de routekaart zijn verdeeld over de waardeketen, zoals weergegeven in figuur 13. In dit hoofdstuk worden de bevindingen per spoor toegelicht en de koppeling met de barrières/valleys of death aangegeven.



Figuur 13 Sporen voor de routekaart cryptocommunicatie.

De bevindingen uit de marktverkenning en de waardenetwerkanalyse zijn ondergebracht binnen vier sector overstijgende sporen die uitgewerkt kunnen worden in de routekaart. Deze sporen zijn als volgt:

1 **Onderwijs, mensen en kennisbehoud:** schaarste van gekwalificeerd personeel is een algemeen geconstateerde barrière voor de waardeketen, deze wordt genoemd door partijen in de marktverkenning en binnen de waardenetwerkanalyses (overkoepelende barrière 1 in beide sectoren). Daarom is het blijven opleiden van specialisten belangrijk. Dit kan aangescherpt worden door het voor domein-specifieke technici aantrekkelijk te maken om zich te specialiseren in cryptografie. De sectorspecifieke kennis kan vervolgens met behulp van interne opleidingsprogramma's bij (markt)partijen worden bijgebracht. De basis van kennisbehoud zijn de universiteiten en kennisinstellingen, daardoor is het stimuleren van fundamenteel onderzoek belangrijk. Dit kan, o.a. door het aantrekken en financieren van PhD's op Nederlandse universiteiten en kennisinstellingen. Overwogen kan worden of dit 'industrie-PhD's' kunnen worden, waarbij de PhD ook deels in het bedrijfsleven onderzoek uitvoert. Verderop in de waardeketen is het van belang te werken aan het behouden van start-ups voor cryptografische producten binnen de Nederlandse markt, zodat deze start-ups binnen het nationale waardenetwerk blijven en de kennis binnen deze start-ups niet verdwijnt (de tweede geïdentificeerde valley of death in de energie sector).

   Aanbevelingen spoor 1:
   Concrete stappen zijn te zetten op het versterken van kennis over cryptocommunicatie binnen de sectoren. Hiervoor kunnen opleidingstrajecten voor professionals opgezet en aangemoedigd worden.
   Voor het behouden van een sterke kennispositie is het waarborgen van (academisch) onderzoek noodzakelijk. Hiervoor is stabiele financiering van PhD's noodzakelijk. Bijkomende voordeel kan behaald worden door de inzet van 'industrie-PhD's' om zo de kennispositie van de sector te versterken.
   Voor het behouden van startups kan de overheid sturen op een goed vestigingsklimaat, gezonde groeimogelijkheden en specifieke regulering. Een concrete aanzet is door een (gedeelde) locatie aan te bieden waarin startups en MKB-ers op ABDO-gecertificeerd niveau kunnen opereren. Hierdoor ontstaat binding aan Nederland én wordt een barrière tot het beginnen van een startup weggenomen.

2 **Pre-competitieve samenwerking:** hier gaat het om het uitvoeren van activiteiten die bijdragen aan (potentiële) marktgroei. In de barrières en valleys of death wordt benoemd dat er een gemis is aan een duidelijke leiderschapsrol in het ecosysteem, waarbij overheid en marktpartijen naar elkaar wijzen om de eerste stap te zetten in cryptocommunicatie-ontwikkelingen (de derde overkoepelende barrière in de automotive sector) en een gebrek aan een gedeelde visie tussen partijen in het ecosysteem om de prioriteiten op het gebied van R&D vast te stellen (de tweede overkoepelende barrière in de automotive sector). Gerichte samenwerking, met een duidelijk leiderschap en beleid, kan deze barrières doorbreken en als zodanig de gehele markt vergroten. Samenwerking kan plaatsvinden tussen partijen op alle ontwikkel-/TRL-niveaus, bijvoorbeeld door het ontwikkelen van een gemeenschappelijke deeloplossing, die partijen daarna individueel verder

specificeren. Marktgroei kan ook gezocht worden door onderscheid te maken tussen high- en low-assurance producten en nieuwe samenwerkingen te starten op het low-assurance domein. Daarnaast komt hier de koppeling naar voren met de eerste valley of death in de energiesector. Wanneer een eindgebruiker voor de ‘deployment’ van een eindproduct een kosten-baten analyse maakt, spelen de kosten van het product zelf een rol hierin, maar ook zeker de kosten van het implementeren/operationaliseren van het product. Indien afstemming vooraf plaatsvindt tussen de ontwikkelaar en eindgebruiker, kan hier in het ontwikkelproces al rekening mee gehouden worden.

Aanbevelingen spoor 2:
Onder aanvoering van dcypher neemt het Nederlandse ecosysteem leiderschap en zet het een stap in samenwerking door met de partijen in de waardeketen een gedeelde visie voor R&D te maken door de focus te leggen op componenten van cryptocommunicatie (modulariteit) en niet op een volledig eindproduct. Hiertoe werken academie, industrie en eindgebruikers met elkaar samen om gedeelde problemen gezamenlijk aan te pakken. Door vroege afstemming over te ontwikkelen deelproducten worden kosten/baten van het implementeren en operationaliseren van cryptocommunicatieproducten gedeeld en beheerst. Concrete pre-competitieve samenwerking kan worden vormgegeven door verschillende projecten met (een deel van) de deelnemende partijen aan de routekaart cryptocommunicatie. Logischerwijs begint deze samenwerking door het laaghangend fruit aan te pakken, met projecten waarvan de uitkomst gegarandeerd van toegevoegde waarde is. Door klein te beginnen, nieuwe gedeelde barrières te ontdekken en in het aanpakken daarvan momentum te behouden, wordt de samenwerking gaandeweg steeds verder uitgebreid.

3 **Samenwerkingsondersteuning / community management:** van belang is het creëren van een veilige omgeving voor samenwerking en afstemming (zoals innovatiemissies of conferenties) tussen de partijen binnen het waardenetwerk. De cybersecurity van het systeem als geheel is tenslotte niet de verantwoordelijkheid van slechts één of enkele partijen. Het verbinden van stakeholders zorgt voor community-building (d.w.z. nationale ‘branding’, Nederlandse branding internationaal, briefings en conferenties, sub-communities opzetten, automotive en wind op zee-partijen bij elkaar brengen, werkgroepen organiseren, etc.) en draagt bij aan awareness voor de kansen die cryptocommunicatie biedt. Zo kunnen bijvoorbeeld, door een verbetering in afstemming en communicatie tussen partijen in de waardeketen, de kosten voor patching van cryptografische producten verminderd worden (de tweede overkoepelende barrière in de energiesector) en een verbetering teweegbrengen in de overdracht van technologie naar implementatie (de eerste valley of death in de automotive sector). Standaardisatie op nationaal niveau, bijvoorbeeld via de NEN, kan ook leiden tot vertrouwen en richtlijnen voor gemeenschappelijke samenwerkingen. Visa versa is standaardisatie eenvoudiger haalbaar in een goed verbonden community (de tweede en derde valley of death in de automotive sector).

Aanbevelingen spoor 3:
Als samenwerkingsplatform kan dcypher zorgen voor een veilige omgeving (community) waarin de partijen binnen het waardenetwerk informatie met elkaar

uit kunnen wisselen en op deze manier, door meer awareness, meer begrip van de kansen van cryptocommunicatieproducten, de valorisatie van cryptocommunicatieproducten te verbeteren. Ook kan dcypher, o.a. door het organiseren van congressen en handelsmissies de reputatie van de Nederlandse crypto-industrie op Europees/internationaal gebied versterken.

4 **Fieldlabs:** het spoor pre-competitieve samenwerking is in zekere mate een technologie-push, van binnen naar buiten. Omgekeerd kan vraag gedreven technologie-pull ervoor zorgen dat nieuwe producten/dienstverlening ook daadwerkelijk land. De fieldlabs kunnen een veilige omgeving bieden voor open innovatie door meerdere partijen *uit de sector*, waarin ideeën en nieuwe technologische oplossingen vrijuit kunnen worden getest. Hierin kunnen vervolgens meerdere use-cases uitgewerkt worden, zoals het testen van de integratie van een nieuw cryptografisch product met behulp van een digital twin. Een belangrijk aspect dat hierin kan worden meegenomen is dat er naar oplossingen wordt gezocht die aansluiten bij concrete vragen uit de markt. Succesvolle implementaties kunnen hierdoor makkelijker landen in een bestaand ecosysteem.

   Aanbevelingen spoor 4:
   Wie neemt initiatief, wat gaan we doen?
   De fieldlabs zullen een gedragen activiteit moeten zijn, waarvoor werken aan concrete, gedragen risico's leidend is. Een startpunt voor de fieldlabs zijn de sectorspecifieke barrières geïdentificeerd in dit rapport. De fieldlabs hebben EZK als belangrijke aanjager, maar vallen/staan door de gedragenheid binnen de sector. De fieldlabs kunnen ook dienen als inspiratiebron voor het ontwikkelen van nieuwe producten/dienstverlening, door een korte lijn van sector tot onderzoek en ontwikkeling te creëren.

De vier beschreven sporen geven een eerste aanzet tot invulling, welke in een vervolgtraject verder dient te worden uitgediept. Het wordt aanbevolen om verder te bouwen op de bevindingen en geïdentificeerde barrières uit dit rapport. Zodoende wordt er invulling gegeven aan de routekaart cryptocommunicatie.

5 Bibliografie

- Aazami, (2021), Digitalisering en energie: Méér dan de som der delen.
- Algemene Inlichtingen- en Veiligheidsdienst (AIVD) (2021), *Bereid je voor op de dreiging van de quantumcomputers*.
- Allee, V. (2008), 'Value network analysis and value conversion of tangible and intangible assets', *Journal of intellectual capital*, Vol. 9, Issue 1, pp. 5-24.
- Barbosa, M. & G. Barthe, et al. (2019), 'SoK: Computer-Aided Cryptography', *Cryptology ePrint Archive,* 1393.
- Bhargavan, K. & B. Blanchet et al. (2019), 'A mechanised cryptographic proof of the WireGuard Virtual Private Network protocol', *Inria Paris*, pp. 50.
- Beullens, W. (2022), 'Breaking Rainbow takes a weekend on a laptop', *Cryptology ePrint Archive*, Paper 022/214.
- Castryck, W. & T. Lange et al. (2018). 'CSIDH. An efficient post-quantum commutative group action', *ASIACRYPT 2018*, pp. 395-427.
- CE Delft, TNO en Quintel (2021), Afspraken maken: van data tot informatie, Informatiebehoeften, datastandaarden en protocollen voor provinciale systeemstudies – Deel II technische rapportage.
- Ministerie van Economische Zaken en Klimaat, TNO, CWI & dcypher (2021), Nederland Cryptoland. Startpunt routekaart cryptocommunicatie: de vier belangrijkste uitdagingen in de cryptografie.
- Milakis, D., Snelder, M. & Arem, B. (et. al.) (2017), 'Development and transport implications of automated vehicles in the Netherlands: Scenarios for 2030 and 2050', *European Journal of Transport and Infrastructure Research,* Vol. 17, pp. 63-85.
- European Commission (2018), FinTech action plan: For a more competitive and innovative European financial sector.
- Federal Office for Information Security (BSI) (2021, oktober), Quantum-safe cryptography: Fundamentals, current developments and recommendations.
- Goubin, L., Kipnis A. & J. Patarin (1999), 'Unbalanced Oil and Vinegar signature schemes', *Advances in Cryptology – EUROCRYPT '99*, pp. 206-222.
- Hofstätter, T., Krawina, M., Mühlreiter, B., Pöhler, S. & A. Tschiesner (2020), 'Reimagining the auto industry's future: It's now or never', McKinsey & Company (https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/reimagining-the-auto-industrys-future-its-now-or-never)
- ITU (2017), Measuring the Information Society Report, 2017 (Vol. 1).
- Kalra, N., & Groves, D. G. (2017), The enemy of good: Estimating the cost of waiting for nearly perfect automated vehicles.
- NCTV (2018), Nederlandse Cybersecurity Agenda: Nederland digitaal veilig.
- Sieber, L., Ruch, C., Hörl, S., Axhausen, K. W. & Frazzoli, E. (2020), 'Improved public transportation in rural areas with self-driving cars: A study on the operation of Swiss train lines' *Transportation research part A: policy and practice*, Vol. 134, pp. 35-51.
- Straver, F. (2017, 29 November), Windlobby waarschuwt: Aziatische massamolen hijgt Europa in de nek. *Trouw* (https://www.trouw.nl/duurzaamheid-natuur/windlobby-waarschuwt-aziatische-massamolen-hijgt-europa-in-de-nek~b30cf380/)
- Teoh, E. R. & Kidd, D. G. (2017), 'Rage against the machine? Google's self-driving cars versus human drivers', *Journal of Safety Research*, Vol. 63, pp. 57-60.

- The Hague Centre for Strategic Studies (2021), *The High Value of The North Sea*.
- Topsector High Tech Systemen en Materialen (HTSM), Team Dutch Digital Delta, Topsector Creatieve Industrie, Topsector Logistiek en Topsector Water & Maritiem (2019), *Kennis en innovatieagenda (KIA) Veiligheid*.
- TNO (2020), *EZK Verdieping Valorisatieketens: Verkenning van het ecosysteem en waardenetwerk Automated Security* (TNO 20220 R12224).
- TNO (2019), *Succesfactoren voor digitaal veilige Operationele Technologie* (TNO 2019 R11304).
- TNO (2022), Crypto for Automotive – WP1 Report: Toepassing cryptografie in directe automotive communicatie (te verschijnen 2022).

A Overzicht geïnterviewde partijen

A.1 Marktverkenning

Tabel 1 Overzicht van de geïnterviewde partijen voor de marktverkenning.

Technische Universiteit Eindhoven (2x interview) (NL)
NXP Semiconductors (interview) (NL)
Roseman Labs (interview) (NL)
Infineon (interview) (DE)
Zama (interview) (FR)
iGrant.io (enquête) (SE)
NTNU (enquête) (NO)
Airbus (enquête) (NL, FR, ES, DE)

Zie voor de enquête: 'Bijlage B: Enquête Marktverkenning'.

A.2 Waardenetwerk analyse

Tabel 2 Overzicht van de geïnterviewde partijen voor de waardenetwerkanalyse. De eerste zeven partijen zijn gesproken voor de wind op zee sector en de onderste vier voor de automotive sector. De overige partijen hebben we voor beide sectoren gesproken.

Partij	**Rol geïnterviewde**
Siemens	Cybersecurity Specialist
Shell	Information Security Architect
Compumatica	Board Member
Ministerie van Infrastructuur en Waterstaat	Senior Information Advisor
NHL Stenden Hogeschool	Lector Digitale Weerbaarheid
European Network for Cybersecurity	Researcher
TenneT	Cybersecurity Advisor
TNO (x3)	Senior Scientist Energy Transition Studies, Program Manager Wind Energy, Senior Project Manager Automotive
Rijkswaterstaat (x2)	Kwartiermaker Offshore Expertise Centrum, Adviseur Smart Mobility
Agentschap Telecom	Inspecteurs Cybersecurity
TU Eindhoven	Professor Software Engineering
NXP	Senior Systems Architect
KPN	Technical Lead Mobility Fieldlab
ElaadNL	Cybersecurity Expert

B Enquête Marktverkenning

TNO – EU Cryptography market research
On behalf of the Dutch Ministry of Economic Affairs, TNO conducts research into the current developments on cryptography within the EU. More specifically, we are looking at various parties within the EU cryptography market (i.e. knowledge institutions, product developers, end users) to identify current developments, initiatives and barriers.

1. Current research, projects and/or initiatives of your organisation
TNO currently identifies four developments that pose the greatest challenges, and simultaneously offer the greatest opportunities, in the coming years in the field of cryptography:

- Securing new technical environments
  Due to the constant development and adoption of new technical environments, it is necessary to secure them sufficiently, before these new technical environments are suitable for use in situations where security is of great importance. This development could be carried out with common unilateral cryptography and should be achievable on the short term.

- Migration to post-quantum cryptography
  The development of the quantum computer puts widely used cryptographic systems at risk. Therefore, we need post-quantum cryptography that is resistant against future quantum attacks. However, the migration to post-quantum cryptography is a challenge for the entire valorisation chain, both on the short and long term. An additional opportunity is that through the structural migration, the crypto agility of the systems can be increased.

- Deployment of cryptography for new decentralised applications
  The emergence of multilateral cryptography has given the opportunity to develop new decentralised techniques, such as secure multiparty computation and self-sovereign identities. Developments of new, advanced cryptographic primitives such as fully homomorphic encryption further give rise to new opportunities in the area of outsourced computing on sensitive data.

- Formal verification of cryptography and cryptographic source code
  Formal verification, or computer-aided cryptography, is a method that is being used to let computers validate software implementations of cryptographic primitives. This technique can also be applied to the underlying cryptographic protocols and their implementations, providing assurance on the security of cryptographic products.

1.1. Which new technical environments has your organisation identified and which of those are addressed in your organisations current efforts in research, projects and/or initiatives?

1.2. Which post quantum cryptography migration challenges has your organisation identified and which of those are addressed in your organisations current efforts in research, projects and/or initiatives?

1.3. Which deployments of cryptography for new decentralised applications has your organisation identified and which of those are addressed in your organisations current efforts in research, projects and/or initiatives?

1.4. Which formal verification of cryptography and cryptographic source code has your organisation identified and which of those are addressed in your organisations current efforts in research, projects and/or initiatives?

1.5. Do you identify other developments for the coming years within the field of cryptography? If so, what kind of research, projects and/or initiatives does your organisation undertake in terms of this development?

2. Barriers within the cryptography market

In our current research, we are identifying barriers that are currently at play within the cryptography market. Expectations are that certain barriers specifically exist for (new) organisations to enter the cryptography market; barriers that stand in the way of (new) innovation initiatives; and barriers to translate crypto-graphic research into (embedded) cryptographic end-products.

Examples of generic barriers that we have identified so far:

- Due to a mix of stakeholders conflicts of interest can occur during standardisation.
- Not enough collaboration within the EU, many Member States want to remain independent.
- Shortage of researchers and personnel.
- Researchers have to publish papers. For researchers working in the area of formal verification of cryptography, this leads to less available time to develop documentation / tutorials of the tooling being developed on the fly, with a lack in documentation and tutorials as a consequence.
- Lack of governmental guidelines, standardisation, and rules on how to deploy new forms of cryptography.
- Currently existing security problems obstruct organisations to look into migrating towards post-quantum cryptography, as these security issues have to be fixed first.

2.1. Which barriers can you identify that exist specifically for (new) organisations to enter the cryptography market? What could be done to take away these barriers?

2.2. Which barriers can you identify that specifically stand in the way of (new) innovation initiatives? What could be done to take away these barriers?

2.3. Which barriers can you identify that exist specifically in translating cryptographic research into (embedded) cryptographic end-products? What could be done to take away these barriers?

2.4. Are there any additional barriers that you identify in the cryptography market?

3. Standardisation and regulation

In recent years various bodies have undertaken to develop and implement standardisation and regulation relating to cryptography, on an international level (such as NIST and ISO) as well as on the national level. In our research it would be very useful to know which standardisation and/or regulation is applicable to your organisation.

3.1. Which standarisation and/or regulation is applicable to your organisation?

3.2. Which interoperability issues exist, where in your opinion standarisation and/or regulation is needed?
