Fieldlab Energie & Cybersecurity

Contextanalyse

TNO Public ⟩ TNO 2023 R12804
19 Augustus 2023

ICT, Strategy & Policy
www.tno.nl
+31 88 866 00 00
info@tno.nl

TNO 2023 R12804 – 19 Augustus 2023

Fieldlab Energie & Cybersecurity

Contextanalyse

Auteurs: Shari Finner, Bart Gijsen

Rubricering rapport	TNO Public
Titel	TNO Public
Rapporttekst	TNO Public
Aantal pagina's	33 (excl. voor- en achterblad)
Aantal bijlagen	2
Sponsor	Ministerie van Economische Zaken en Klimaat
Projectnaam	FLECS - Fieldlab Energie & Cybersecurity
Projectnummer	060.50857

Samenvatting

Met de energietransitie wordt Nederland steeds afhankelijker van de leveringszekerheid van groene energie. De elektriciteitsinfrastructuur wordt niet alleen verduurzaamd, maar ook gedecentraliseerd en gedigitaliseerd. Dit zorgt voor uitdagingen met betrekking tot de stabiliteit en veiligheid van het elektriciteitsnet, die nodig is om een hoge leveringszekerheid te waarborgen. Tegelijk dienen zich nieuwe risico's aan, waaronder de dreiging van verstoring van de energie-infrastructuur door cyberaanvallen.

Om de cybersecurity in tijden van de energietransitie te waarborgen verkent TNO in opdracht van het Ministerie van Economische Zaken en Klimaat in 2022 en 2023 het cybersecurity ecosysteem binnen de duurzame energieopwekking. Nog niet alle beschikbare cybersecurity-technologie wordt in de energiesector toegepast. De intentie is daarom om een samenwerkingsvorm op te zetten waarin cybersecuritykennis en -technologie in de zich transformerende energiesector op collaboratieve wijze ontwikkeld, ofwel gedeeld, toegepast en gedemonstreerd kan worden. Het beoogde samenwerkingsverband heeft als doel om zich stapsgewijs uit te breiden, beginnend bij use cases ten behoeve van het borgen van de leveringszekerheid tot een model waarin steeds meer (internationale) economische activiteit plaatsvindt.

In dit document wordt op basis van opgehaalde informatie uit gesprekken met markt- en overheidspartijen en literatuuronderzoek de context geschetst waarbinnen het project FLECS – Fieldlab Energie & Cybersecurity – uitgevoerd wordt. Het begint met een omschrijving en analyse van het ecosysteem van hernieuwbare elektriciteitsopwekking, specifiek met de focus Wind op Zee. Vervolgens wordt de rol van cybersecurity-technologie en -partijen algemeen in de hernieuwbare energiesector en specifiek binnen de Wind op Zee sector geschetst. Op basis van deze ecosysteem schets en gevoerde interviews wordt de behoefte naar sectorale samenwerking en mogelijke invullingen daarvan beschreven.

Op basis van de **verkenning van het speelveld cybersecurity voor Wind op Zee** kunnen de bevindingen als volgt samengevat worden:

1. Grootschalige windparken zijn over het algemeen structureel beveiligd, zowel fysiek als digitaal. Grote spelers tonen vaak een redelijk volwassenheidsniveau. Voor MKB partijen daarentegen zijn prioriteit en budgetten voor cybersecurity beperkt.
2. De Wind op Zee sector kan in de toekomst door de energietransitie en evolutie van het dreigingslandschap vaker doelwit van gerichte cyberaanvallen worden, en de mogelijke impact van uitval groeit. Daarom is er structureel betere beveiliging nodig.
3. Aan de technische kant zijn de belangrijkste cybersecurity uitdagingen voor de Wind op Zee sector het veilig maken van legacy

technologie en de bekende IT cybersecurity concepten vertalen en toepassen op operationele technologie zoals windmolens.

4. Aan de organisatorisch-technische kant van cybersecurity in de Wind op Zee sector ligt de uitdaging vooral in de ketensamenwerking, standaardisatie en testen:
   - Er is i.v.m. een gesloten deur beleid een gebrek aan informatie-uitwisseling, samenwerking, normen/eisen en veiligheids-tests in de supply chain (waaronder toeleverende MKB partijen met beperktere cyber-expertise). Hierdoor is er weinig zicht op de mate van beveiliging en op verschillende risico's (kans & impact);
   - Door het missen van concrete eisen is het uitdagend voor markt-partijen om te bepalen waar en op welke manier de eerste stap-pen te zetten zijn;
   - Er is door de markt begeleiding en richting vanuit de overheid gewenst.
5. Op dit moment is er geen expliciete vraag vanuit de wind op zee markt naar technologie van cybersecurity technologie bedrijven. Daardoor is er (nog) geen specifiek aanbod. Indien een vraag vanuit de markt richting cybersecurity leveranciers gesteld wordt is te verwachten dat het aanbod zal volgen.

Uit de **verkenning van de behoefte naar sectorale samenwerking** en mogelijke invulling kan geconcludeerd worden dat er binnen de sector en vanuit de overheid verschillende behoeftes bestaan, namelijk naar:

a. het delen van operationele informatie over huidige dreigingen en uitdagingen;
b. samenwerking in de vorm van experimenten en praktijktesten;
c. pre-competitieve samenwerking om het (toekomstige) elektriciteitsnet "by design" te beschermen tegen cyber-aanvallen.

Een inventarisatie van bestaande samenwerkingsverbanden in de vorm van ISACs of fieldlabs laat zien dat er al veel cybersecurity en energie gerelateerde initiatieven bestaan. In ISACs wordt vaak operationele informatie over huidige uitdagingen in de bestaande infrastructuur gedeeld, terwijl in fieldlabs vaak experimenten, integratie en praktijktesten plaatsvinden. Er is echter nog geen samenwerkingsverband *specifiek voor cybersecurity in de Wind op Zee sector* aangetroffen. Verder lijkt er op dit moment geen samenwerkingsvorm te bestaan waarin pre-competitieve samenwerking met een duidelijk toekomstperspectief plaatsvindt, bijvoorbeeld door de ontwikkeling van architectuurdesigns voor het toekomstige elektriciteitsnet (security-by-design).

De behoefte van de sector lijkt daarom op dit moment niet in zijn geheel door bestaande overlegorganen, samenwerkingsverbanden of initiatieven vervuld te worden. Om deze reden is een nieuwe samenwerkingsvorm of een uitbreiding van bestaande initiatieven wenselijk. Deze zou in de vorm van een PPS setting vormgegeven kunnen worden met een driehoek van zowel publieke als private partijen en kennisinstellingen. In verband met de aankomende vertaling van de NIS2 Directive, de grote kavel-aanbestedingen op de Noordzee en groeiende awareness over het belang van cybersecurity en ketenveiligheid lijken de omstandigheden gunstig om nu momentum voor het vormgeven van een dergelijke pre-competitieve samenwerking te creëren.

Inhoudsopgave

Samenvatting 3
Inhoudsopgave 5
1 Inleiding 6
1.1 Achtergrond 6
1.2 Doelstelling 6
1.3 Leeswijzer 7
2 Energie en Cybersecurity 8
2.1 Het elektriciteitsnet 8
2.1.1 Overzicht elektriciteitsnet 8
2.1.2 Gekozen focus: elektriciteitsopwekking door Wind op Zee 11
2.1.3 Het speelveld van elektriciteitsopwekking Wind op Zee 12
2.2 Cybersecurity in het elektriciteitsnet 13
2.2.1 Cybersecurity van het elektriciteitsnet algemeen 13
2.2.2 Cybersecurity voor Wind op Zee 15
2.2.3 Het cybersecurity technologie aanbod voor Wind op Zee 16
2.2.4 Samenvatting: Cybersecurity voor Wind op Zee 17
3 FLECS - Fieldlab Energie en Cybersecurity 18
3.1 De behoefte aan sectorale samenwerking 18
3.2 Overzicht bestaande ISACs 19
3.3 Overzicht bestaande (field-)labs en andere testlocaties 20
3.4 Meerwaarde en positie van een Energie-Cybersecurity fieldlab FLECS 23
3.5 Suggesties voor invulling FLECS 24
3.5.1 Het mogelijke consortium & de positie van FLECS 24
3.5.2 FLECS selectie van mogelijke use-cases 26
4 Conclusies 29
5 Verwijzingen 31
Bijlagen 1
A.1 Lijst van gesproken partijen 1
A.2 Afkortingenlijst 2

1 Inleiding

1.1 Achtergrond

Door de energietransitie verandert de elektriciteitsinfrastructuur en wordt deze sterk gedecentraliseerd, verduurzaamd en gedigitaliseerd. Dit zorgt voor uitdagingen voor het in balans houden van de stabiliteit van de infrastructuur, die nodig is om de hoge leveringszekerheid te waarborgen. [1] Aanvullend aan deze uit de energietransitie voortvloeiende uitdaging dienen zich nieuwe risico's aan. Een daarvan is de dreiging van verstoring van de energie-infrastructuur door cyberaanvallen. [2] Niet alleen is er een toenemende dreiging van generieke cyberaanvallen waar belanghebbenden in de energiesector door getroffen worden, [3] maar ook de toenemende activiteit van cybersabotage door statelijke actoren toont de urgentie van deze dreiging aan. [4] [5]

Om cybersecurity uitdagingen het hoofd te bieden komt steeds meer cybertechnologie beschikbaar en wordt voortgang geboekt met het aanscherpen van beleid en regelgeving in meerdere sectoren. Daarmee wordt steeds duidelijker wat er t.a.v. cybersecurity versterkt kan worden en door wie. De volgende stap is om uit te werken hoe deze ontwikkeling gezamenlijk uitgevoerd kan worden voor specifieke toepassing in de energietransitie[1], en om hem in gang te zetten.

1.2 Doelstelling

Als gevolg van de energietransitie zal Nederland afhankelijker worden van groene energie en daarmee van de leveringszekerheid van deze groene energie. Specifiek worden er in de Klimaatwet (volgend uit Klimaatakkoord van Parijs) en de Green Deal (EU Commissie) dermate ambitieuze eisen gesteld aan vermindering van broeikasgasuitstoot, dat groene energie een zeer fors deel van de nationale energievoorziening zal worden.[2] Nederland behoort tot de kopgroep van EU-lidstaten die de Green Deal ondersteunen, [6] en ook het Nederlandse bedrijfsleven is positief over de plannen.

Tegelijk met de energietransitie vindt er een digitale transitie plaats waarin er in de maatschappij meer en meer digitale technologieën en oplossingen beschikbaar komen. Apparatuur en infrastructuren, waaronder degene die de energietransitie ondersteunen, worden gedigitaliseerd en met elkaar of met het internet verbonden om data uit te wisselen. De digitale transitie biedt grote kansen maar introduceert ook (digitale) veiligheidsrisico's. Het sterk groeiende aandeel van duurzaam opgewekte elektriciteit zal daarmee van

1.

[1] Bijvoorbeeld in [20] wordt aangegeven dat "current market offers few and under-developed wind-specific cyber-security services, products and strategies."
[2] in 2030 49%/55%, en in 2050 95% of 100% minder broeikasgassen dan in 1990, waarbij het eerste getal voor de Klimaatwet is en het tweede voor de Green Deal.

toenemend belang voor nationale veiligheid en voor de economie worden.

Om de cybersecurity in tijden van de energietransitie te waarborgen onderzoekt TNO in opdracht van het Ministerie van Economische Zaken en Klimaat in 2022 en 2023 met een selecte groep van initiatiefnemers de potentiële dreigingen en beoogt het een samenwerkingsvorm op te zetten waarin kennis en technologie op het gebied van datacommunicatiebeveiliging in de transformerende energiesector op collaboratieve wijze gedemonstreerd en toegepast kan worden. Cybersecurity-oplossingen waaronder bijvoorbeeld Automated Vulnerability Research (AVR) of cryptografietechnieken zijn mogelijke toepassingen waarmee de (nieuwe) infrastructuur beter tegen cyberdreigingen beveiligd zou kunnen worden. Echter, nog niet alle cybersecurity-technologie die op dit moment beschikbaar is wordt toegepast in de energiesector en het is in veel gevallen niet duidelijk hoe deze toepassing in het publiek-private ecosysteem met complexe waardeketens precies in zijn werk zou moeten gaan. [7] Daarom wordt verkend of een pre-competitieve samenwerking in een PPS setting, bijvoorbeeld in de vorm van een fieldlab, mogelijk is om gezamenlijk concepten te ontwikkelen en technologieën te testen. Een mogelijk samenwerkingsverband/ fieldlab zou beogen om zich stapsgewijs uit te breiden van initiële use cases ten behoeve van het borgen van de leveringszekerheid tot een model waarin steeds meer (internationale) economische activiteit zal plaatsvinden.

1.3 Leeswijzer

Dit document schetst de context waarbinnen het project FLECS – Fieldlab Energie & Cybersecurity – in 2022 en 2023 uitgevoerd is op basis van opgehaalde informatie uit literatuuronderzoek en gesprekken met markt- en overheidspartijen. Het dient als omschrijving en analyse van de rol van cybersecurity binnen het ecosysteem van hernieuwbare elektriciteitsopwekking, specifiek met de focus Wind op Zee. Het document is primair bedoeld voor FLECS-intern gebruik, ter documentatie en onderbouwing van de FLECS activiteiten, maar wordt ook beschikbaar gesteld voor een breder publiek. De gesproken partijen en een lijst van afkortingen zjin in de bijlage te vinden.

2 Energie en Cybersecurity

2.1 Het elektriciteitsnet

2.1.1 Overzicht elektriciteitsnet

De kritieke elektriciteitsinfrastructuur is een complex netwerk waarin een divers aantal stakeholders samenwerken. Fig 1 schetst de bestaande fysieke infrastructuur met daarin zowel fossiele als nieuwe duurzame elektriciteitsopwekking.

Fysieke infrastructuur

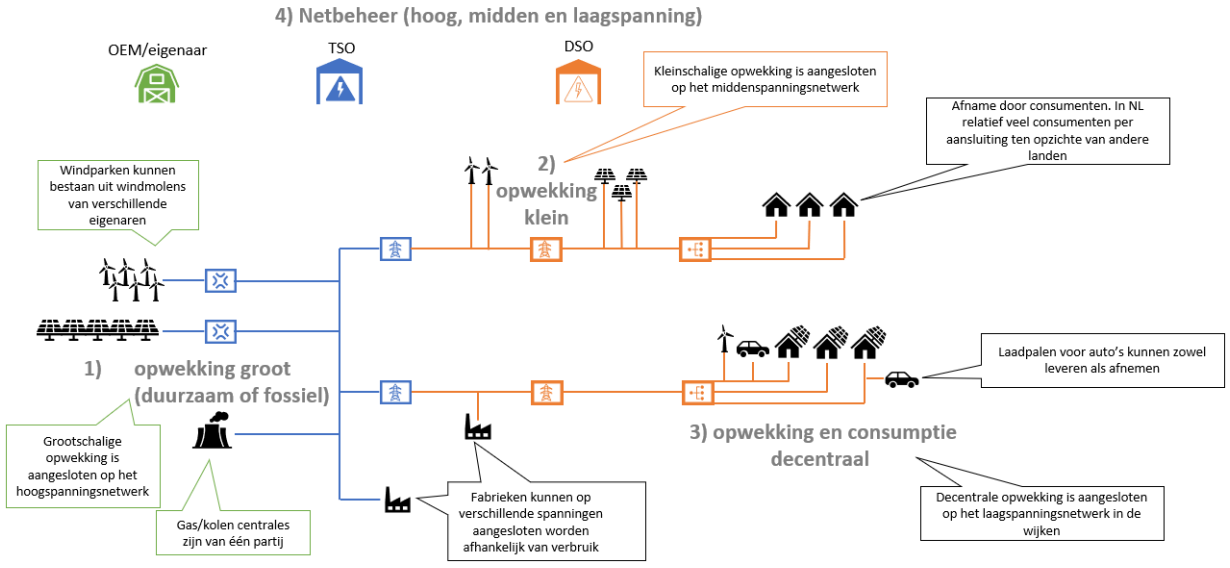


Fig 1: schematische weergave van de elektriciteits-infrastructuur

Het fysieke elektriciteitsnet in Fig 1 is onderverdeeld in vier categorieën[3]:

1) Opwekking groot;
2) Opwekking klein;
3) Opwekking (& consumptie) decentraal;
4) Netbeheer.

1.

[3] Dit onderzoek is gericht op het elektriciteitsnet als publieke nutsvoorziening. Omwille van de continue beschikbaarheid van hun stroomvoorziening richten diverse private verbruikers, zoals organisaties in vitale sectoren, data centers, ziekenhuizen, etc., ook zelfstandig functionerende noodstroomvoorzieningen in. De veiligheidsregio's en (regionale) netbeheerder spelen ten aanzien de van te treffen noodstroom-voorzieningen in geval van elektriciteitsuitval een coördinerende rol, maar de verantwoordelijkheid ligt bij de private partijen. [22] In dit onderzoek blijven noodstroomvoorzieningen buiten beschouwing.

Onder **opwekking groot** vallen grote windmolenparken op land en op zee, grote zonnepaneelparken en andere (niet duurzame) energieopwekkingscentrales. Deze grote energieparken worden vaak gebouwd door o.a. OEMs (Original Equipment Manufacturers) en beheerd door de uiteindelijke eigenaren: grote (internationale) bedrijven. **Opwekking klein** van zonne- of windenergie gebeurt op dit moment voornamelijk in lokale initiatieven op het land (bijvoorbeeld boerderijen), privaat of door stichtingen beheerd (al dan niet ondersteund door decentrale overheden).
Met **decentrale opwekking** wordt breedverspreide energie-opwekking (en -consumptie) bedoeld, bijvoorbeeld bij mensen thuis of op een bedrijventerrein. De gebruikers zijn vaak huiseigenaren die bijvoorbeeld zonnepanelen op hun dak laten plaatsen, boeren die een windturbine op hun boerderij laten installeren, of de publieke e-auto laadinfrastructuur met zonnepanelen en meerdere laadpunten in woonwijken. Over het algemeen gebruiken kleinschalige decentrale energieopwekkings-systemen massa-geproduceerde apparatuur uit oosterse landen (bijvoorbeeld China) en zijn niet zo structureel beveiligd en op veiligheid getest als de producten en eigen infrastructuur van een grootbedrijf. **Netbeheer** omvat het beheer van zowel de hoog-, midden- als laagspanningsnetten. Het hoogspanningsnet wordt beheerd door de TSO (Transmission System Operator), terwijl het midden en laagspanningsnetwerk beheerd wordt door de DSOs (Distribution System Operators). Netbeheerders zijn eind-verantwoordelijk voor de stabiliteit van het elektriciteitsnet en de continuïteit van de energielevering. Naast de netbeheerders zelf bestaan er (elektriciteits-) marktbeheerders die de vraag/aanbod afstemming doen om de balans van het net en tussen netwerken te waarborgen.

De fysieke energie-infrastructuur wordt aangestuurd met (digitale) data ten behoeve van continuïteit en optimalisatie van het net voor zowel economische als maatschappelijke doelen. Fig 2 visualiseert het netwerk aan dataverbindingen t.b.v. de aansturing van systemen in het net. Hierin is zichtbaar dat er naast dataverbindingen ter directe aansturing van controlesystemen ook data verzameld en gestuurd wordt naar een balans-verantwoordelijke partij (BVP). BVPen zijn bijvoorbeeld producenten, grootverbruikers, energieleveranciers of -handelaars. Zij zijn verantwoordelijk voor het handhaven van vraag en aanbod op de energiemarkt van hun eigen portfolio en moeten voldoen aan eisen in o.a. de Netcode elektriciteit. Als erkennende instantie controleert de TSO of de BRP voldoet aan de eisen van toetreding en uitvoering. Windparkeigenaren bijvoorbeeld zijn balansverantwoordelijke partijen en lopen kans op hoge boetes indien zij niet aan bepaalde processen voldoen (echter niet alle nodige processen zijn op alle vlakken in detail gedefinieerd). Naast de dataverbindingen ter aansturing van controlesystemen en data voor het balanceren van het elektriciteitsnet bestaan er ook verbindingen voor andere datagedreven toepassingen zoals het weer, vogelvlucht etc. Deze zijn in de uitwerking van Fig 2 en van dit rapport niet verder meegenomen.

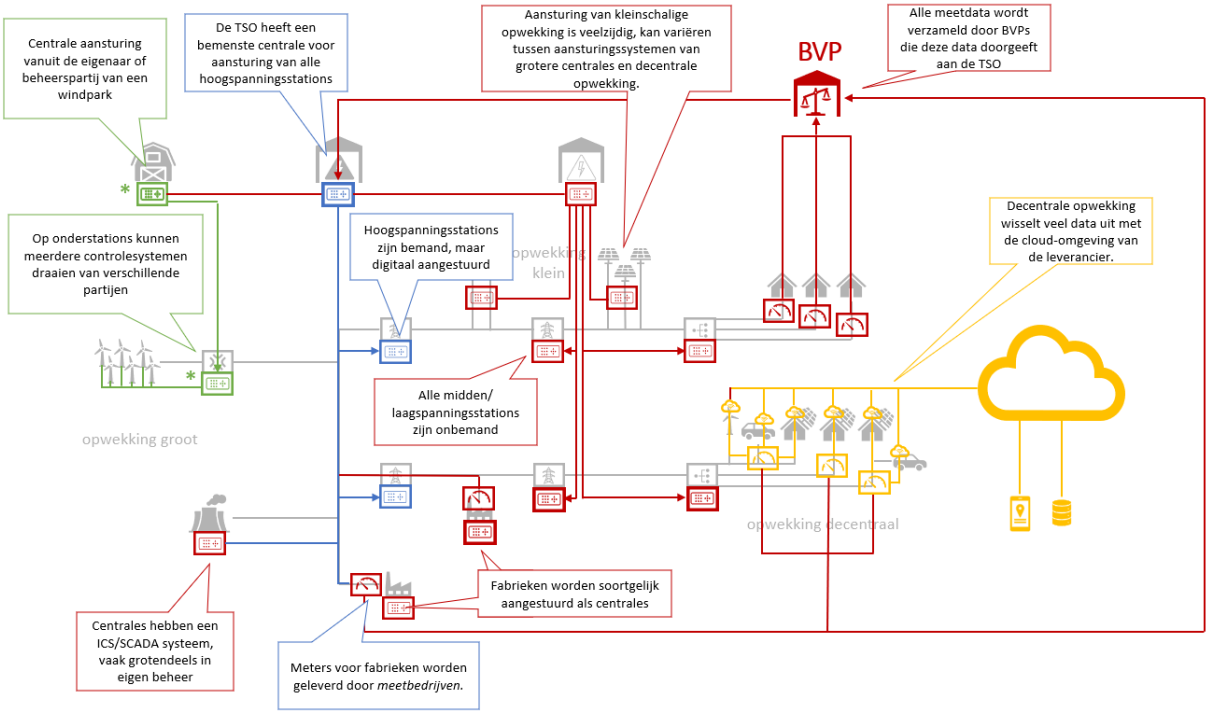


Fig 2: visualisatie van dataverbindingen in de kritieke energie-infrastructuur

De (nieuwe) elektriciteitsinfrastructuur openbaart zich als een verweven ecosysteem met een veelvoud aan functies en partijen. Wanneer een breuk in de cybersecurity zich voordoet op één plek, heeft dit mogelijk direct impact op de rest van het ecosysteem. Ook bevindt deze infrastructuur zich in een breder ecosysteem van een wettelijke context, regulatie en regelgeving vanuit publieke partijen (overheid, toezichthouders, veiligheidsdiensten, ...). Deze regulatie, wet- en regelgeving betreft zowel de elektriciteitsmarkt als ook een markt voor fysieke equipment, ICT en digitale dienstverlening. Verder omvat het ecosysteem kennisinstellingen die onderzoek uitvoeren en bijdragen aan innovatie in het verduurzamen en beveiligen van de elektriciteitsinfrastructuur.

Een grote publieke speler in dit netwerk is het Ministerie van Economische Zaken en Klimaat (Min EZK) met meerdere directies (waaronder DG Digitale Economie en DG Energie). De Nederlandse Netcode elektriciteit bijvoorbeeld wordt vastgesteld door toezichthouder Autoriteit Consument en Markt (ACM), die valt onder Min EZK.[4] Verdere toezichthouder onder Min EZK valt is de Rijksinspectie Digitale Infrastructuur (RDI). Als uitvoeringsorgaan van EZK is de Rijksdienst voor Ondernemend Nederland (RVO) betrokken, waaronder de topsectoren vallen (bijv. de Topsectoren Energie en Digitalisering, die bestaat uit onder andere het Topconsortia voor Kennis en Innovatie (TKI) Offshore Energy). Verdere ministeries die betrokken zijn bij de wet- en regelgeving rondom het elektriciteitsnet zijn het Ministerie van Infrastructuur en Waterstaat (Min IenW), het Ministerie van Justitie en Veiligheid (Min JenV) waaronder het

1.

[4] naast de nationale codes vastgesteld door ACM bestaan er ook Europese codes voor de elektriciteitsmarkt, zie ook https://www.tennet.eu/nl/de-elektriciteitsmarkt/regels-en-procedures/europese-codes

Nationaal CyberSecurity Centrum (NCSC) en de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) vallen, als ook het Ministerie voor Binnenlandse Zaken en Koninkrijksrelaties (Min BZK), waaronder ook de Nationaal Bureau voor Verbindingsbeveiliging (NBV) binnen de Algemene Inlichtingen- en VeiligheidsDienst (AIVD). Het ecosysteem van Nederlandse kennisinstellingen houdt naast de Toegepast Onderzoek Organisaties (TO2) een veeltal Nederlandse Universiteiten en hogescholen in. Welke organisaties en spelers de markten binnen het elektriciteitsdomein en het digitale infrastructuur-domein inhoudt hangt sterk af van de gekozen focus van markt en technologie. Voor de Wind op Zee sector en het specifieke onderwerp 'innovatie in cryptocommunicatie' is het waardenetwerk van publieke, private en kennisinstellingen in een recent onderzoek door TNO uitgebreid geanalyseerd en geschetst [7].

2.1.2 Gekozen focus: elektriciteitsopwekking door Wind op Zee

Alle delen van het elektriciteitsnet in Fig 1 spelen een significante rol in het borgen van de leveringszekerheid van elektriciteit, en het is van belang voor de nationale veiligheid om deze zo goed mogelijk fysiek en digitaal te beschermen. In het Klimaatplan (het beleid voor de komende 10 jaar om de doelen van de Klimaatwet te bereiken) zijn specifiek voor de opwekking en distributie van hernieuwbare elektriciteit de volgende activiteiten voorzien:

1. Stimuleren Wind op Zee: 49 TWh (2030);
2. Stimuleren hernieuwbare energie (wind en zon) op land: 35 TWh;
3. Stimuleren kleinschalige hernieuwbare productie (particuliere zonnepanelen): 10 TWh;
4. Waarborgen leveringszekerheid;
5. Investeren in voldoende elektriciteits-infrastructuur.

Daarmee zijn windmolenparken op zee op dit moment en in de toekomst tot tenminste 2050 de grootste bron van hernieuwbare energie in Nederland. Deze transitie naar hernieuwbare energie brengt uitdagingen met zich mee voor de leveringszekerheid. In [1] wordt gesteld dat de norm van een maximale onderbreking van stroomlevering van vier uur per jaar vanaf 2025 in gevaar komt, en deze uitdaging vormt vervolgens een aantrekkelijk doelwit voor gerichte (financieel of politiek gemotiveerde) aanvallen door professionele georganiseerde hackerscollectieven of statelijke actoren. [5] Mochten grote, al aan het net aangesloten windparken gehackt worden, dan zou door uitval van de stroomproductie of juist overproductie van stroom het elektriciteitsnet instabiel kunnen worden en uitvallen. Dit zou zware gevolgen hebben voor hele regio's, het land of grote delen van Europa. Door de schaal aan (geplande) opgewekte energie op de Noordzee en de uitdagingen van kwetsbaarheid en onderhoud van remote assets wordt cybersecurity voor wind op zee daarom een belangrijke voorwaarde voor een veilige kritieke energie-infrastructuur.

Kavels op de Noordzee waar aanleg van nieuwe windparken gepland is worden voortdurend openbaar aanbesteed. [8] De huidige en toekomstige tenderprocedures voor de aanleg van nieuwe windmolenparken bieden een kans voor “security-by-design” oplossingen, zodat windparken al met een focus op veiligheid ontworpen kunnen worden in plaats van dure en suboptimale retrofitting achteraf. Daarom is in het project in overleg met opdrachtgever Min EZK besloten om te beginnen het speelveld van Cybersecurity voor Wind op Zee nader te verkennen en de behoefte naar concrete samenwerking in bijvoorbeeld een fieldlab te toetsen.

2.1.3 Het speelveld van elektriciteitsopwekking Wind op Zee

Een deel van het stakeholderveld voor Wind op Zee is in Fig 3 schematisch weergegeven. De figuur toont een (niet uitputtende) selectie van relevante partijen in de Wind op Zee waardeketen, gecategoriseerd in overheidspartijen, samenwerkingsverbanden, OEMs (Original Equipment Manufacturers), elektriciteitsproducenten en netbeheerders die is bedoeld om een hoogover beeld van interacties en afhankelijkheden te geven. Door de focus op Wind op Zee zijn de midden- en laagspanningsnetbeheerders niet in Fig 3 vertegenwoordigd: zij sluiten exclusief aan op de elektriciteitsinfrastructuur van TenneT en hebben geen interactie met windpark OEMs of beheerders.

Een uitgebreide analyse van de Wind op Zee waardeketen op het gebied van cryptocommunicatie met een overzicht van de interacties en waardeuitwisselingen tussen publieke, private en kennisinstellingen is opgenomen in een recent onderzoeksrapport van TNO. [7]

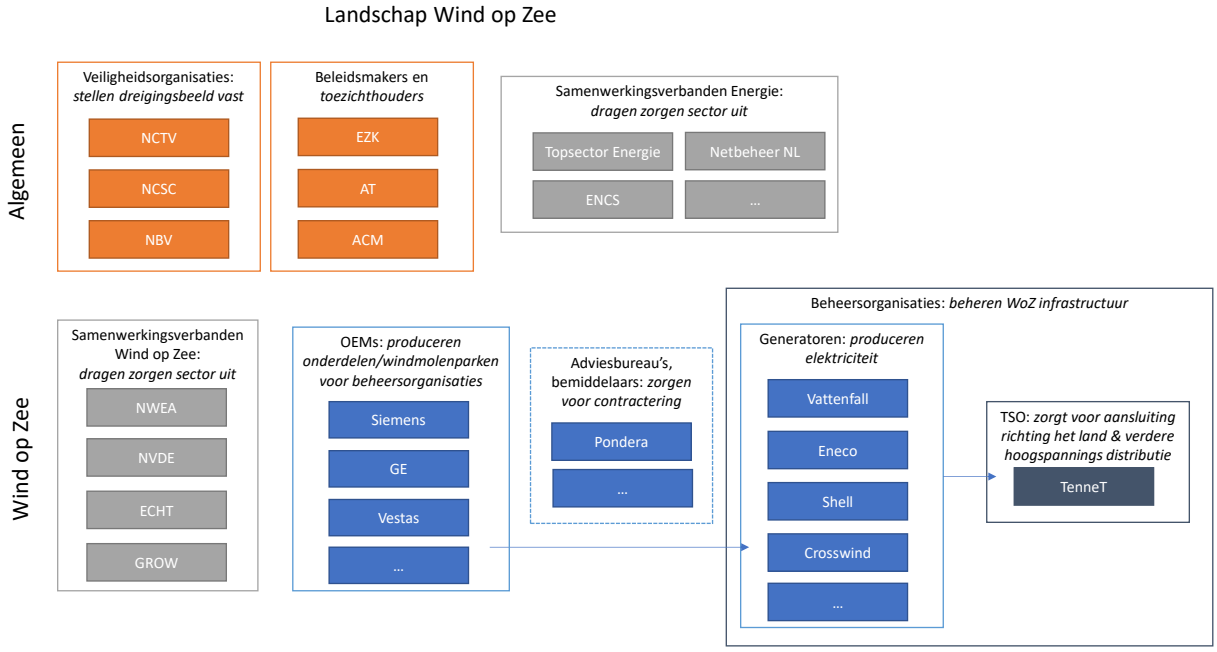


Fig 3: schematische weergave van partijen in het WoZ ecosysteem (niet uitputtend).

2.2 Cybersecurity in het elektriciteitsnet

De inhoud van dit hoofdstuk is gebaseerd op gesprekken en interviews met stakeholders in het Wind op Zee – Cybersecurity ecosysteem. Een lijst van gesproken partijen is te vinden in de bijlage.

2.2.1 Cybersecurity van het elektriciteitsnet algemeen

Netbeheerders (TSOs en DSOs) hebben een cruciale rol in het beveiligen van de elektriciteitsinfrastructuur. In interviews en verkennende gesprekken met netbeheerders ontstaat het duidelijke beeld dat zij een sterke verantwoordelijkheid voor het kritieke elektriciteitsnet voelen en zich van de noodzaak van het beveiligen hiervan zeer bewust zijn. Zo treffen zij duidelijke en zinnige maatregelen om de veiligheid van het net onder controle te hebben en te houden, en zijn hun (digitale/cyber-) beveiligingsmaatregelen gemiddeld volwassener dan die van kleinere, minder “centrale” partijen in de energiesector. In het netbeheer worden over het algemeen standaard cybersecurity oplossingen zoals cryptografie en andere good practices toegepast en wordt er onderling relevante operationele informatie uitgewisseld, met het gezamenlijke doel om het elektriciteitsnet stabiel te houden. [7] Het ENCS biedt netbeheerders een veilige samenwerkingsvorm om informatie over cybersecurity op technologisch vlak en gebied van good practices te delen en testen. De drie security programma’s van het ENCS waarin de netbeheerders samenwerken zijn: (1) Security Operations, (2) Security Architecture en (3) Security Policy. [9] Hiernaast is samenwerking en informatie-uitwisseling ook vormgegeven in ISACs (Information Sharing and Analysis Centres). [10] Ondanks de relatieve volwassenheid en de samenwerking van netbeheerders is de mate van informatie-uitwisseling beperkt door competitie en bedrijfsgeheimen, [7] en wordt cybersecurity historisch nog steeds vaak gezien als een kostenpost in plaats van een noodzakelijk bedrijfsmiddel ten gunste van de bedrijfscontinuïteit.

Ook andere grote partijen zoals energieleveranciers en OEMs hadden tot nu toe historisch gezien relatief weinig aandacht voor het onderwerp cybersecurity. Hun volwassenheid op cybersecurity vlak lijkt over het algemeen lager dan bij de netbeheerders. De aandacht voor de noodzaak van cybersecurity is de laatste jaren echter sterk groeiende, zodat ook energieleveranciers en OEMs zich aan het oriënteren zijn hoe cybersecurity maatregelen het beste vorm te geven zijn. Wat netbeheerders, energieleveranciers en OEMs gemeen hebben is dat zij allemaal te maken hebben met wereldwijde maatschappelijke ontwikkelingen die leiden tot de volgende algemene cybersecurity onderzoeksvraagstukken:

- **Toenemende digitalisering van operationele infrastructuur (IT-OT convergentie):** cybersecurity tooling die volwassen is in de IT sector (zoals het vinden van kwetsbaarheden of detectie, respons en herstel van een aanval) staat voor operationele

technologie (OT) zoals control systemen nog in de kinderschoenen. Historisch gezien waren control systems redelijk geïsoleerd van het IT netwerk, waardoor het aanvals-oppervlak klein was en er weinig cybersecurity maatregelen en tooling nodig waren. Echter, met de digitalisering van het net neemt het aantal dataverbindingen ten behoeve van optimalisatie, maintenance, grid balancing en andere (big-) data toepassingen toe, wat het aanvalsoppervlak verveelvoudigt. Huidige onderzoeksvragen richten zich op (1) hoe OT data voor datagedreven toepassingen (zoals optimalisatie) gebruikt kan worden terwijl het aanvalsoppervlak voor cyberaanvallen klein gehouden wordt, en (2) hoe cybersecurity detectie en respons tooling toegepast kan worden in het OT domein.

- Het omgaan met de **operations en maintenance van legacy-systemen**: terwijl veel onderdelen van de elektriciteits-infrastructuur, bijvoorbeeld windmolenparken, voor een levensduur van meerdere decennia gebouwd worden, doen ontwikkelingen binnen het cybersecurity gebied zich op een tijdschaal van maanden tot jaren voor. Hardware en software moet dus regulier geüpdate en gepatcht worden om veilig te blijven. (OT-) systemen moeten voor updates vaak tijdelijk uitgeschakeld worden, en er is een risico aanwezig dat bepaalde functionaliteiten na een update (tijdelijk) niet beschikbaar zijn. De prioriteit van “uptime” (operationele continüiteit) in het OT domein is vele malen hoger is dan die van het draaien van een veiligheidsupdate (“*Never touch a running system*”). Daarom zijn updates en maintenance van legacy OT systemen zoals windmolenparken of andere onderdelen van het elektriciteitsnet een grote uitdaging.
- **Ketenveiligheid**: het is voor eigenaren van delen van de elektriciteitsinfrastructuur vaak niet voldoende bekend hoe veilig geleverde hardware en software is. Daarom is er is binnen aanleveringsketens een behoefte om heldere cybersecurity eisen aan leveranciers te kunnen stellen en deze te kunnen toetsen.
- Algemene huidige cybersecurityontwikkelingen en uitdagingen in groeiende, complexe (cloud-) infrastructuren van IT, OT en IoT devices, waaronder **interoperabiliteit**, **post-quantum cryptografie migratie**, groeiende **Public Key Infrastructures**.
- Voor netbeheerders: het **balanceren van de netcapaciteit** in een dynamische, groeiende en complexer wordende elektriciteits-infrastructuur. Deze uitdaging van netbeheerders is niet specifiek cybersecurity-gerelateerd, maar vereist een robuust en (cyber-)veilig systeemdesign, gezien een succesvolle cyberaanval op het net door de beperkte “foutmarge” ernstige gevolgen kan hebben.

Naast boven genoemde uitdagingen van de grote (deels internationale) partijen zoals netbeheerders, energieleveranciers en OEMs zijn er ook andere partijen in het elektriciteitsnet met cybersecurity-gerelateerde uitdagingen. Zo is cybersecurity ook in andere kleinschalige of decentrale opwekking en consumptie van elektriciteit cruciaal. Zonnepaneelomvormers bijvoorbeeld zijn volgens een onderzoek van het RDI makkelijk te hacken en is de

mogelijkheid om hiermee verstoringen in de elektriciteitsvoorziening te veroorzaken aannemelijk. [11] [12] In het kader van dit project is echter vanwege de immense schaal van de toekomstige elektriciteitsopwekking door Wind op Zee en de kans voor security-by-design in toekomstige kavelaanbestedingen in overleg met de opdrachtgever de focus op de Wind op Zee sector gelegd.

2.2.2 Cybersecurity voor Wind op Zee

In de Wind op Zee sector passen grote internationale OEMs en energieleveranciers over het algemeen standaard cybersecurity maatregelen en tooling zoals cryptografie toe. [7] [10] Zij lijken binnen hun eigen scope een relatief hoog volwassenheidsniveau te hebben: problemen worden vaak intern opgelost. Er zijn voor het onderwerp cybersecurity ook budgetten en capaciteit beschikbaar, in de vorm dat deze partijen vaak hun eigen in-house cybersecurity experts hebben. De hoofdkantoren bevinden zich vaak niet in Nederland, maar in Duitsland of Scandinavische landen, daarom is het uitdagend om in Nederland iemand van deze bedrijven te spreken die bevoegd is om de juiste keuzes te maken.

Ook binnen de Wind op Zee sector geldt dat de mate van informatie-uitwisseling beperkt is, en dat cybersecurity historisch gezien werd als een minder belangrijke kostenpost. Dit laatste is de laatste jaren langzamerhand aan het veranderen, onder andere door de aankomende NIS2 directive en zichtbaarheid van het onderwerp door activiteiten zoals webinars en ronde tafel gesprekken. Deze activiteiten worden zowel door de Rijksoverheid (bijvoorbeeld RDI, Topsector Energie, TKI Offshore Energy), als door samenwerkingsverbanden vanuit de markt (bijvoorbeeld GROW, NWEA, GWEC, ..) geïnitieerd.

In tegenstelling tot boven genoemde grootbedrijven zijn voor kleinere spelers in de Wind op Zee sector zoals het MKB de prioriteit en budgetten voor cybersecurity over het algemeen zeer beperkt, zodat het onderwerp voornamelijk door de grote marktpartijen opgepakt wordt.

Naast de historisch beperkte prioriteit van cybersecurity is vooral de ketensamenwerking een grote uitdaging voor de cyberveiligheid van windmolenparken. [10] Door competitie binnen de markt is er een grote terughoudendheid voor samenwerking in de supply chain en heerst er een “gesloten deuren” beleid: er wordt weinig informatie over de mate van beveiliging van producten uitgewisseld. Dit in tegenstelling tot bijvoorbeeld de financiële sector waar een gentlemen’s agreement is overeengekomen om op (cyber-)security vlak niet te concurreren, en een NATO principe in de vorm van “*een aanval op één van ons is een aanval op ons allemaal*”.

Dit gebrek aan informatiedeling en samenwerking is zowel tussen OEMs onderling aanwezig, als in de aanleveringsketen tussen verschillende OEMs en windparkeigenaren. Er is binnen supply chains een sterke behoefte om duidelijkere cybersecurity eisen aan leveranciers te kunnen stellen en afspraken over

verantwoordelijkheden te maken, om te borgen dat hardware en software die geleverd wordt veilig is. Deze behoefte voelen voornamelijk windparkeigenaren als eindverantwoordelijke partijen. Echter, in de praktijk is onvoldoende bekend welke (soort) eisen dit idealiter moeten zijn, hoe de standaardisatie eruit moet zien, en op welke manier compliance met deze eisen getest, gestimuleerd of afgedwongen zou kunnen worden. Het open-norm beleid van de toezichthouder geeft hier ook geen richting aan. [13] Het vaststellen van de mate van beveiliging is dus lastig door het ontbreken van testen en samenwerking, en van een duidelijke cybersecurity-norm in de sector. Meerdere marktpartijen noemen dat hierin meer leiding door de overheid gewenst is.

Samenvattend zit de grootste cybersecurity-uitdaging voor de volwassene en leidende partijen zoals netbeheerders, OEMs en energieleveranciers in 2022 vooral in de **mate van informatieuitwisseling en de veiligheid van de ketensamenwerking**, en niet zozeer in de implementatie van al bekende standaard cybersecurity-maatregelen binnen een enkel bedrijf. [10] Dit geldt voor de algemene elektriciteitsmarkt maar ook specifiek voor de sector Wind op Zee.

2.2.3 Het cybersecurity technologie aanbod voor Wind op Zee

Zoals in Sectie 2.2.2 beschreven hebben grote (vaak internationale) partijen over het algemeen in-house experts om de cybersecurity intern binnen hun eigen scope/producten zo goed mogelijk te borgen. Dit betekent dat het **aanbod** van cybersecurity technologie in de Wind op Zee sector – vooral voor operationele technologie – voor een significant deel niet in de cybersecurity sector ligt, maar binnen de windsector zelf belegd is. Een OEM voor windmolenparken, bijvoorbeeld, is cybersecurity leverancier voor zijn eigen producten (windmolens incl. datanetwerk), maar is impliciet ook cybersecurity leverancier voor de windparkeigenaar als opdrachtgever. Echter, zoals al in Sectie 2.2.2 geschetst vindt er nog weinig informatiedeling tussen marktpartijen binnen de supply chain plaats en is onvoldoende bekend welke eisen er in deze keten gesteld en (op welke manier) getest zouden moeten worden, zodat de ketenveiligheid niet geheel bekend en hierdoor niet altijd gewaarborgd is.

Uit interviews met enkele Nederlandse cybersecurity technologieleveranciers, gevoerd in 2022, kwam naar voren dat deze bedrijven de energiesector een interessante markt vinden om cybersecurity producten voor te ontwerpen, ontwikkelen en te testen. Hier valt ook expliciet de Wind op Zee sector onder. De cyber bedrijven staan open en zijn gemotiveerd om mee te doen aan mogelijke samenwerkingsverbanden die kunnen leiden tot meer inzicht in wat er in deze sector nodig is om hun producten toe te passen en zo windparken structureel beter te beveiligen. Door de terughoudendheid en het “gesloten deuren” beleid van de sector kunnen zij echter weinig informatie verkrijgen over de huidige state of the art, hoe hun technologieën en producten precies toe te passen zijn, en waar de technische uitdagingen liggen voor

toekomstige productontwikkeling. Zodra de vraag en technische eisen zichtbaarder worden is te verwachten dat cyber technologie leveranciers open staan voor samenwerking en om hun productaanbod aan de Wind op Zee markt aan te passen.

2.2.4 Samenvatting: Cybersecurity voor Wind op Zee

Op basis van de verkenning van het speelveld cybersecurity voor Wind op Zee door middel van interviews kunnen de bevindingen als volgt samengevat worden:

1. Grootschalige windparken zijn over het algemeen structureel beveiligd, zowel fysiek als digitaal, en grote spelers in de markt tonen in hun interne operaties en producten vaak een redelijk volwassenheidsniveau. Voor MKB spelers in de Wind op Zee sector is de prioriteit en het budget voor cybersecurity beperkt, waardoor het onderwerp hoofdzakelijk door grote marktpartijen opgepakt wordt.
2. De Wind op Zee sector wordt door de energietransitie en de evolutie van het dreigingslandschap mogelijk in de toekomst vaker doelwit van gerichte cyberaanvallen, en de gevolgen van uitval groeien door de energietransitie. Daarom is er structureel betere beveiliging nodig.
3. Aan de technische kant zijn de belangrijkste cybersecurity uitdagingen voor de Wind op Zee (en algemeen in de energie-) sector:
    - Het veilig maken van legacy technologie (vulnerability scanning, patching, update van cryptografie, etc.);
    - IT/OT convergentie: de toepassing van bekende IT cybersecurity op operationele technologie zoals windmolens.
4. Aan de organisatorisch-technische kant van cybersecurity in de Wind op Zee sector ligt de uitdaging vooral in de ketensamenwerking, standaardisatie en testen:
    - De markt hanteert een gesloten deur beleid, er is een gebrek aan informatie-uitwisseling, samenwerking, normen/eisen en veiligheids-tests in de supply chain (waarbij specifiek ook de beperktere cybersecurity expertise bij toeleverende MKB partijen een risico vormt);
    - Hierdoor is er weinig zicht op de mate van beveiliging en daarmee op de verschillende risico's (kans en impact);
    - Door het missen van concrete en duidelijke eisen is het lastig voor marktpartijen om duidelijk te definiëren waar en op welke manier de eerste stappen genomen moeten worden;
    - Er is door de markt guidance/richting vanuit de overheid gewenst.
5. Er is op dit moment geen concrete vraag vanuit de wind op zee markt naar technologie van cybersecurity tech bedrijven, en daardoor is er (nog) geen specifiek aanbod. Indien een vraag vanuit de WoZ markt richting cybersecurity leveranciers gesteld wordt is te verwachten dat het aanbod zal volgen.

3 FLECS - Fieldlab Energie en Cybersecurity

Dit hoofdstuk beschrijft de opgehaalde behoefte naar sectorale samenwerking en een inventarisatie van een deel van bestaande samenwerkingsvormen. Verder wordt de mogelijke positionering en meerwaarde van een “FLECS – Fieldlab Energie & CyberSecurity” geschetst.

3.1 De behoefte aan sectorale samenwerking

Tijdens de gevoerde interviews is de behoefte aan afstemming en samenwerking geïnventariseerd. Hieruit komt een divers beeld naar voren. Tot nu toe zagen de gesproken partijen nog weinig duidelijke voordelen van uitgebreide samenwerking op cybersecurity vlak en lossen op dit moment vooral hun eigen operationele problemen op. Dit is echter met toenemende bewustwording over het belang van cybersecurity aan het veranderen. Zo wordt er in de interviews genoemd dat er in de complexe supply- en value chain betere coördinatie nodig is van sector-brede cybersecurity doelstellingen. Daarbij is ook specifiekere invulling van belang voor cybersecurity regelgeving en (open norm gebaseerde) toezicht voor de energie sector. Deze behoefte aan coördinatie komt ook naar voren bij de uitwerking van Europese regelgeving zoals NIS2 en CER naar nationale regelgeving.

Naast de hiervoor genoemde behoefte die primair gericht zijn op het “wat?", is er ook behoefte naar samenwerking ten aanzien van het “hoe?”. Om de complexe keten van de Wind op Zee sector en de algehele kritieke elektriciteits-infrastructuur tegen cyberdreigingen te beschermen lijkt een systeemaanpak over de hele keten noodzakelijk. Er is zowel aan de technische als aan de organisatorische kant behoefte naar informatiedeling en samenwerking. Vanuit het organisatieperspectief bestaat de behoefte om gezamenlijk verantwoordelijkheden, eisen en standaarden op het gebied van cybersecurity voor de Wind op Zee sector tussen de sector en de (toezicht houdende en aanbestedende) overheid te definiëren. Aan de technische kant is o.a. de ontwikkeling en doorvoering van tests wenselijk, om te bepalen of aan deze eisen en verantwoordelijkheden voldaan wordt. Ook zou er onderzocht moeten worden hoe bekende cyber technologie binnen de IT sector in het complexe speelveld van OT technologie in de Wind op Zee sector toegepast kan worden. Verder lijkt het pre-competitieve, gezamenlijke ontwikkelen en testen van zowel technologieën als concepten en designs tussen partijen in de supply chain noodzakelijk om security-by-design conceptueel goed vorm te geven.

In de interviews worden voor de inrichting en innovatie van cybersecurity in de Wind op Zee sector vooral drie specifieke samenwerkings-instrumenten genoemd die mogelijk aan de behoefte van de sector zouden kunnen voldoen: kennisdeling via ISACs, het verkrijgen van hands-on ervaring door middel van fieldlabs, en specifiek het ENCS als voorbeeld voor een sectoraal samenwerkingsverband. ISACs (Information Sharing & Analysis Centres) zijn initiatieven voor veilige en vertrouwde informatie-uitwisseling tussen sectorgenoten over bestaande operationele cybersecurity dreigingen en good practices. Het ENCS is een partnership van netbeheerders om cybersecurity informatie op technologisch vlak en gebied van good practices te delen, trainingen te organiseren of tests uit te voeren. Een fieldlab is een praktijkomgeving waarin bedrijven en kennisinstellingen gezamenlijk oplossingen pre-competitief kunnen ontwikkelen en testen.

In Secties 3.2 en 3.3 is een overzicht opgenomen van bestaande ISACs, testlocaties en andere (field-)labs die raakvlak hebben met de energie sector. Naast de in de volgende secties uitgewerkte ISACs en fieldlabs, zijn in de interviews nog andere publieke en private initiatieven en organisaties genoemd, die gerelateerd zijn aan de onderwerpen cybersecurity en Wind op Zee. Bijvoorbeeld, vanuit het oogpunt van veilige digitalisering zijn het Innovation Quarter, Hague Security Delta en dcypher belangrijke spelers, en bij die spelers groeit de aandacht voor het energie ecosysteem. Ook zijn het CIO platform Nederland en de CISO Circle of Trust als (gedeeltelijk) relevant initiatieven genoemd. Vanuit de Wind op Zee Sector groeit de aandacht voor cybersecurity vraagstukken bij organisaties zoals NWEA, Grow en GWEC. Deze organisaties en initiatieven zijn echter minder vaak in de interviews genoemd dan de hieronder beschreven initiatieven.

3.2 Overzicht bestaande ISACs

In de loop der tijd zijn er steeds meer Nederlandse en Europese ISACs opgericht en wordt de samenwerking binnen ISACs steeds meer omarmd. In Nederland zijn de meeste ISACs georganiseerd vanuit het Digital Trust Centre (DTC, als onderdeel van het ministerie van EZK) of vanuit het NCSC (onderdeel van het ministerie van JenV). [14] [15] Voor Europa wordt samenwerking in ISACs gestimuleerd door onder andere ENISA, de European Union Agency for Cybersecurity. [16] [17]

Zowel vanuit het DTC als van de Europese Commissie zijn overzichten van ISACs opgesteld. [18] [19] Een aantal relevante ISACs die raakvlak hebben met het onderwerp cybersecurity voor Wind op Zee zijn in Tabel 1 kort weergegeven.

In het tabel is te zien dat er een aantal algemene ISACs en een aantal ISACs op het onderwerp “energie” bestaan. Echter, geen van deze bestaande ISACS heeft op dit moment een specifieke focus op de sector Wind op Zee. Zo gaan EUROSCSIE en CIISI-EU over algemene ICS of algemene cybersecurity, maar hebben geen focus op het energiedomein. het Energy ISAC vitale organisaties en het EE-

ISAC hebben aandacht voor cybersecurity vraagstukken in het energiedomein, maar geen specifieke focus op *offshore* energy. Het EU maritime ISAC focust zich op cybersecurity voor het maritieme domein in de breedte, niet alleen (offshore) energie.

Tabel 1: bestaande Nederlandse en Europese ISACs die mogelijk relevant zijn voor cybersecurity in de energiesector.

Naam	Scope	Omschrijving (kopie van website)
Energy ISAC vitale organisaties[5, 6]	NL (via het NCSC)	"Wisselt tussen organisaties uit dezelfde sector gevoelige en vertrouwelijke informatie uit over incidenten, dreigingen, kwetsbaarheden en maatregelen." [14]
European Energy - Information Sharing & Analysis Centre (EE-ISAC)[7]	EU	"An industry-driven, information sharing network of trust. Private utilities, solution providers and (semi) public institutions such as academia, governmental and non-profit organizations share valuable information on cybersecurity & cyber resilience."
EuroSCSIE - European SCADA and Control Systems Information Exchange for industrial control systems[8]	EU	"EuroSCSIE supports information sharing and analysis regarding Industrial Control Systems (ICS) Supervisory Control and Data Acquisition (SCADA) systems in critical infrastructures; it was founded in 2005."
EM-ISAC - EU Maritime ISAC[9]	EU	"EU Maritime ISAC supports sharing and analysis regarding information that helps to increase the cyber resilience of the European Maritime Sector."
Cyber Information and Intelligence Sharing Initiative CIISI-EU[9]	EU	"A multilateral cyber information and intelligence sharing initiative, which brings together a community of public and private entities, to facilitate the systematic and structured sharing of vital strategic, operational and tactical cyber information and intelligence as well as good practices among themselves."

3.3 Overzicht bestaande (field-)labs en andere testlocaties

Naast de verkenning van ISACS is ook een inventarisatie van bestaande testlocaties en fieldlabs uitgevoerd. Sommigen daarvan hebben een duidelijke focus op hernieuwbare energieopwekking en/of systeemintegratie, anderen op cyberweerbaarheid of resilient system design. In Tabel 2 is de opgehaalde informatie over locaties en initiatieven weergegeven die een duidelijke link met windenergie of cybersecurity hebben. Fieldlabs die minder relevant geacht worden zijn niet opgenomen, zoals bijvoorbeeld drijvende zonnepaneelparken en andere testlocaties van o.a. TNO op het vlak van hernieuwbare elektriciteitsopwekking.

1.

[5] https://www.ncsc.nl/onderwerpen/start-een-samenwerking/zelf-een-samenwerking-starten/samenwerking-sector

[6] https://www.nctv.nl/binaries/nctv/documenten/publicaties/2015/05/01/inspectierapport-gebruik-van-beveiligingsadviezen-van-het-ncsc/CSBN+2015+-+inspectierapport-beveiligingsadviezen-ncsc-webversie.pdf

[7] https://www.ee-isac.eu/impact/

[8] https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/scada

[9] https://www.isacs.eu/european-isacs

Tabel 2: Overzicht van bestaande fieldlabs of testlocaties op het gebied cybersecurity en/of energie.

Naam	Locatie	omschrijving	betrokken partijen	relevantie voor FLECS (bijv. samenwerkingsvorm & volwassenheid)
SWITCH lab[10]	Lelystad	Klein fieldlab voor onderzoek naar grid balancing & systeemintegratie met eigen wind turbines, zonnepanelen, electrolysers, batterijen etc. SWITCH is een open faciliteit van TNO en de Universiteit Wageningen, gefinancierd uit de klimaatenveloppe. Het operationaliseren gebeurt met SMO financiering van TNO. (koppelings- en aansturings-software, sensoren, data infra).	TNO, WUR	Staat open voor cybersecurity projecten en kan de mogelijkheid faciliteren om CS concepten te testen, zonder het risico dat er schade optreedt aan grootschalige, private assets en zonder dat private partijen een kijkje in de keuken hoeven te geven. Het gebruik van SWITCH vindt plaats op projectbasis en moet uit deze projecten betaald worden middels outillage. Ook structurele partnerships behoren tot de mogelijkheden.
HESI lab - Hybride Energie Systeem Integratie[11]	Groningen	Proefopstellingen om het gedrag en de robuustheid van energie-gerelateerde technologieën, producten en diensten testen en verbeteren	EnergyGO; klanten: TNO, provincies, gemeentes, energie-leveranciers	Focus op duurzaamheid van de gebouwde omgeving: energieconcepten boven en onder de grond. Weinig tot geen raakvlak met duurzame elektriciteitsopwekking door middel van wind, hierdoor minder relevant voor FLECS.
OEC – Offshore Expertisecentrum [12]	Stellendam	Fysieke “twin” van een offshore substation als sensorplatform. Doel is het plaatsen van een veeltal sensoren ter informatievoorziening op de Noordzee over o.a. mariene ecosysteem & maritieme veiligheid	Rijkswater-staat, Min EZK, TNO, …	Focus van OEC ligt op ecologische data, monitoring van scheepvaart en hydrologische/ meteorologische informatie. Het initiatief “informatie-voorziening op de Noordzee” houdt echter in om ALLE activiteiten op de Noordzee te coördineren met betrouwbare data. Relevant voor FLECS afhankelijk van de gekozen scope.
CFNS – Connectivity Fieldlab North Sea [13]		Fieldlab waarin partijen samen aan oplossingen kunnen werken om in 2030 de Noordzee van geschikte connectiviteit te voorzien	Rijkswater-staat (Min IenW)	Focus op voldoende connectiviteit, een algemeen telecom-, data- en meet-netwerk met voldoende dekking op de Noordzee. Geen Focus op Wind op Zee, maar kan relevant zijn afhankelijk van de gekozen FLECS use case .
TIADE turbine[14]	Wieringer meer (Hoorn <-> Den Oever)	Enkele test windturbine van ware grootte, geïnstrumenteerd met veel sensoren	GE, LM wind power, TNO	Asset in privaat eigendom, kan afhankelijk van de use case wel in samenwerking gebruikt worden voor onderzoek.
GE Haliade-X[15]	Rotterdam (2e Maas-vlakte)	Enkele test windturbine van ware grootte, geïnstrumenteerd met veel sensoren	GE, TNO	Asset in privaat eigendom, kan afhankelijk van de use case in samenwerking gebruikt worden voor onderzoek

1.

[10] https://www.tno.nl/en/sustainable/renewable-electricity/system-integration-wind/electricity-grid-stable/
[11] https://www.energygo.nl/nl-NL/Projects/Show/17/hesi-lab
[12] https://www.informatiehuismarien.nl/projecten/offshore-expertise/
[13] https://www.informatiehuismarien.nl/publish/pages/193806/flyer_cnfs_nzd_def.pdf
[14] https://www.tno.nl/en/sustainable/renewable-electricity/offshore-wind-farms/innovations-large-wind-turbines-future/new-research-blade-tip-improvements/
[15] https://www.tno.nl/nl/duurzaam/hernieuwbare-elektriciteit/nieuwe-technologie-windenergie/haliade-x-windturbine/

ESP (Electrical Sustainable Power) lab[16]	Delft	In het ESP Lab werken onderzoekers samen om de transitie naar duurzame energie te versnellen.	TU Delft	De focus van het Delftse ESP lab ligt op elektriciteit maar niet specifiek op windenergie. Relevant voor FLECS door het "Control Room of the future" initiatief (volgende regel)
Control Room of the Future (CRoF) [17]	Delft	Initiatief binnen het ESP lab Delft om de integratie van nieuwe energie beheertechnologieën te testen en het elektriciteitsnet digitaal weerbaar te maken.	TU Delft, TenneT, TNO	Focus op cybersecurity en stabiliteit van het elektriciteitsnet. Zeer relevant voor FLECS, maar nog geen focus op windenergie.
Proeftuin op de Noordzee[18]	Scheveningen	testgebied van 10 x 10 zeemijl voor Datavergaring, -transmissie en -ontsluiting. Biedt mogelijkheid voor start-ups en MKB om hun innovatieve producten te testen en demonstreren	Gemeente Den Haag, KPN, TNO, TU Delft, Sailing Innovation Centre, Svašek Hydraulics, Watersport-verbond	Voornamelijk voor kleinbedrijven. Geen focus op elektriciteitsopwekking d.m.v. grootschalige windparken op zee, hierdoor beperkt relevant.
Fieldlab Zephyros[19]	Zeeland	Fieldlab voor unmanned maintenance in Wind op Zee, met onderwerpen: Conditiemonitoring & Diagnose, Veiligheid, Remote maintenance (robotica), Control Tower functionaliteit, logistiek, mensarme ontwerpen	Provincie Zeeland, HZ Hogeschool, TNO, Scalda, KM, Stork, TKI OE, North Sea Port, Min IenW, World Class Maintenance	Focus op Wind op Zee, maar geen focus op cybersecurity. Wellicht relevant voor FLECS in het kader van veilige remote conditiemonitoring.
Technical Assurance Laboratory[20]	Peterborough, UK	Technical Assurance Laboratory gericht op het testen en naleven van nieuwe slimme energie- en cyberbeveiligingsoplossingen voor de Britse markt.	CNV GL	Focus op elektriciteits- en cyber-veiligheidstests om interoperabiliteit, veiligheid en betrouwbaarheid van slimme energieproducten voor consumenten, fabrikanten en nutsbedrijven te waarborgen. Zeer relevant, maar geen focus op Wind op Zee en gevestigd in de UK.
KPMG cyber range[21]	several	Realistische cyber trainingsfaciliteit/simulator waar infrastructuur wordt gemodelleerd/gekloneerd en wordt gebruikt voor testen en (training op) incidentrespons.	KPMG	Commerciële aanbieder met significante kostprijs. Infrastructuur moet eerst voldoende realistisch gesimuleerd worden. Zou als digital twin gebruikt kunnen worden. Meer focus op training dan op software en hardware testing.

Het bovenstaande tabel laat zien dat er een aantal labs of testlocaties voor windturbines, substations en het elektriciteitsnet bestaan; deze lijken echter nog geen duidelijke focus op robuustheid en digitale veiligheid te hebben. Daar waar cyberveiligheid een

1.

[16] https://www.tudelft.nl/ewi/onderzoek/faciliteiten/esp-lab
[17] https://www.tudelft.nl/2022/tu-delft/tu-delfts-control-room-of-the-future-maakt-elektriciteitsnet-digitaal-weerbaar
[18] https://proeftuinopdenoordzee.nl/
[19] https://www.worldclassmaintenance.com/project/fieldlab-zephyros/
[20] https://www.dnv.com/news/dnv-gl-opens-first-technical-assurance-laboratory-for-smart-energy-and-cyber-security-in-peterborough-59745
[21] https://assets.kpmg.com/content/dam/kpmg/sg/pdf/2018/07/Cyber-Range-brochure.pdf

significante rol speelt (zoals het ESP lab of de KPMG cyber range) lijkt het specifieke onderwerp Wind op Zee op dit moment (nog) buiten scope te liggen. Afhankelijk van de gekozen scope en inhoud van een mogelijk samenwerkingsverband FLECS zou synergie en samenwerking met een bestaand fieldlab verkend kunnen worden. Naast boven genoemde fieldlabs bestaan er ook testlocaties in privaat eigendom van enkele marktpartijen of consortia. Zo is in de interviews genoemd dat het aannemelijk is dat een grote netbeheerder een eigen digital twin van de transportinfrastructuur onderhoudt, en dat consortia die op kavel-aanbestedingen op de Noordzee aanbieden private gezamenlijke testlocaties gebruiken om zich voldoende op een aanbesteding voor te kunnen bereiden.

3.4 Meerwaarde en positie van een Energie-Cybersecurity fieldlab FLECS

Gebaseerd op het overzicht van bestaande ISACS en fieldlabs in Secties 3.2 en 3.3 wordt geconcludeerd dat er een aantal (publiek-private) initiatieven bestaan die informatiedeling en samenwerking op het gebied van cybersecurity voor het elektriciteitsnet vormgeven. Er is binnen deze verkenning echter nog geen samenwerkingsverband specifiek voor de sector Wind op Zee aangetroffen waarin pre-competitief, samengewerkt wordt om het (toekomstige) elektriciteitsnet “by design” tegen cyber-aanvallen te beschermen. Dit betekent dat er óf een nieuwe samenwerking noodzakelijk is, of dat bestaande samenwerkingen ter vervulling van deze behoefte uitgebreid zouden kunnen worden.

De te kiezen vorm van samenwerking is afhankelijk van de behoefte en het beoogde doel. Met het doel om operationele informatie over cyberdreigingen en huidige good practices tussen (mogelijk concurrerende) partijen te delen zou een ISAC voor Wind op Zee een significant deel van de geïdentificeerde behoefte in kunnen vullen om de sector cyberveiliger te maken. Dit is in lijn met het recente onderzoek van ECHT ter verkenning van de behoefte naar sectorale samenwerking. [10] In het ECHT rapport komt ook naar voren dat de sector geen behoefte heeft naar een aparte “Wind op Zee ISAC”. In plaats daarvan gaat de voorkeur uit naar uitbouwing van bijvoorbeeld het bestaande E-ISAC en andere initiatieven, en betere communicatie en stroomlijning ertussen.

De reden dat samenwerking in een ISAC naar verwachting niet de volledige behoefte van de sector adresseert is dat in deze samenwerkingsvorm over het algemeen operationele informatie over huidige uitdagingen in de bestaande infrastructuur gedeeld wordt. De focus ligt bepaald niet op architectuurdesigns en gezamenlijke innovatie voor de toekomst. Verder is er in de sector en vanuit de overheid een aanvullende behoefte naar samenwerking in de vorm van experimenten en praktijktesten aanwezig. Voor netbeheerders wordt deze behoefte op Europese schaal grotendeels vervuld door het ENCS. Netbeheer is echter slechts een deel van het waardenetwerk van Wind op Zee. [9]

Om deze reden is naast het adresseren van operationele uitdagingen van vandaag in een brown-field omgeving (ISAC) ook een aanvullende samenwerkingsvorm wenselijk. Deze zou het doel moeten hebben om (1) ontwikkelde technologieën in de praktijk te testen, en (2) aan de voorkant innovatie uit te voeren met een visie en een duidelijk toekomstperspectief voor een green-field omgeving, bijvoorbeeld gezamenlijk ontwerp van concepten.

3.5 Suggesties voor invulling FLECS

Tijdens de interviews zijn suggesties gedaan door de gesprekspartners[22] over de mogelijke invulling van FLECS. Ook zijn inzichten uit relevante literatuur meegenomen, zoals de aangegeven rol voor testbeds in [20]. Als input voor de latere uitwerking van de inrichting van het fieldlab zijn deze suggesties in deze sectie opgenomen.

3.5.1 Het mogelijke consortium & de positie van FLECS

Een pre-competitieve samenwerking kan in de vorm van een PPS setting vormgegeven worden met het driehoek van zowel publieke als private partijen en kennisinstellingen. De publieke kant representeert hierin de belangen voor nationale veiligheid en andere maatschappelijke behoeftes zoals het verdienvermogen van Nederland en de noodzaak van de energietransitie. Publieke partijen van de Rijksoverheid zijn verantwoordelijk voor het opstellen van beleid, wet- en regelgeving en het toezicht erop. Spelers vanuit de markt moeten niet alleen aan de wet- en regelgeving van de Rijksoverheid en Europa voldoen en technologieën implementeren, maar zijn in de samenwerking ook essentieel voor de (gezamenlijke) definitie van realistische wetten en regels voor de sector. Zij kunnen onderling informatie, ervaringen en good practices uitwisselen over zowel het veilig houden van hun infrastructuur, als ook het voldoen aan specifieke eisen. Kennisinstellingen brengen meerwaarde vanuit hun innovatieperspectief en overkoepelende visie op maatschappelijke transities, maar kunnen ook toegepast onderzoek doorvoeren over hoe bekende IT technologieën toe te passen zijn in een nieuwe sector.

Gedurende de eerste verkenning naar de bereidheid voor samenwerking in een PPS setting waren de antwoorden in de private wind-op-zee sector divers, met een aantal verschillende reacties of antwoordcategorieën:

- “Waarom moet ik hiermee aan de slag? Is op dit moment niet alles in orde?”
- “Het is niet mijn verantwoordelijkheid, maar die van een andere partij.”
- “Ik wil wel, maar kan/mag/durf niet.”
- “Ik mis een reden om hiermee aan de slag te gaan, ik heb geen incentives vanuit mijn management”

1.

[22] De lijst met gesprekspartners uit het Wind op Zee – Cybersecurity ecosysteem is opgenomen in de bijlage.

- “Ontzettend interessant, hier willen wij graag aan bijdragen!”

De partijen die aangaven de noodzaak voor cybersecurity voor Wind op Zee te zien en graag bij te willen dragen gaven voornamelijk aan behoefte te hebben aan samenwerking op het gebied van standaardisatie en beleid, en op dit moment iets minder op het gebied van (gezamenlijke) technologieontwikkeling. Dit komt vermoedelijk door de aankomende wet- en regelgeving in verband met NIS2, en de terughoudendheid met betrekking tot het delen van technische informatie in de ketensamenwerking.

Verder hebben de gesproken partijen de voorkeur om toekomstige initiatieven aanvullend/ complementair aan lopende initiatieven vorm te geven in plaats van ermee te concurreren. Er wordt betwijfeld of er “iets nieuws” moet komen of dat een uitbreiding van bestaande locaties en labs voldoende is. Suggesties voor uitbreiding van bestaande fieldlabs zijn:

- CS expertise en tooling toevoegen aan bestaande energie fieldlabs
- Wind op Zee toevoegen aan cyber-energie-labs
- Bij nieuw op te richten fieldlabs of testlocaties betrokken raken om CS aspecten te waarborgen.

In het grotere ecosysteem van ISACs en andere initiatieven om FLECS heen is benoemd dat door ISACs, community building, lobbyactiviteiten en andere initiatieven juist draagvlak gecreëerd kan worden voor de uitdagingen en innovaties die vervolgens in FLECS geadresseerd worden. Dit kan het aansluiten van partijen bij het fieldlab bevorderen. Andersom kunnen deze initiatieven in de valorisatiefase van innovaties die in het fieldlab ontwikkeld zijn helpen om deze in de sector te laten landen. Een voorwaarde hierin is om naar concrete problemen/use cases te kijken die door het fieldlab geadresseerd worden. Echter, in de verkennende gesprekken kon er nog geen voldoende concrete, breed gedragen use case in de sector geïdentificeerd worden.

In de US roadmap voor wind cybersecurity [20] wordt voor de inzet van testbeds ook aangegeven dat deze zich moeten ontwikkelen: In eerste instantie zouden de inspanningen gericht moeten zijn op bestaande, toegankelijke testbeds om kwetsbaarheden van bestaande wind technologie te beproeven. Deze kunnen op middellange termijn uitgebouwd worden naar sector-brede testbeds waarin ook potentieel nieuwe kwetsbaarheden onderzocht kunnen worden, wat een grotere investering vraagt en beter gezamenlijk opgepakt kan worden. Uiteindelijk moeten dergelijk testbeds uitgebouwd worden naar meer permanente, uitgebreide testbeds ten bate van de gehele wind supply chain.

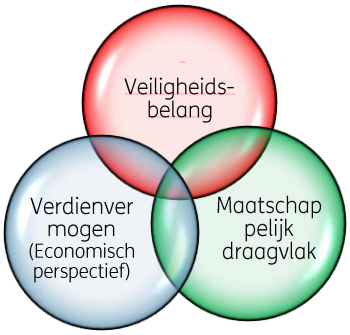
Aan de publieke kant toonden het Min BZK, NCSC en RDI interesse in samenwerking met de sector. Als leidraad voor de definitie van use cases in de markt zouden zij kunnen helpen om de risico’s goed in kaart te brengen. Echter, de mogelijkheden om informatie over specifieke dreigingen te delen zijn in verband met de vertrouwelijkheid daarvan zeer beperkt.

Samenvattend is er dus voorzichtig interesse in samenwerking vanuit zowel de private als de publieke kant, maar het is een uitdaging om binnen het diverse en versnipperde speelveld voldoende focus te creëren om duidelijke stappen te kunnen zetten.

3.5.2 FLECS selectie van mogelijke use-cases

Voor het concreet vormgeven van het fieldlab en het betrekken van relevante partijen bij onderzoek en innovatieontwikkeling, is het zoals boven omschreven noodzakelijk om focus te creëren. Dit kan gedaan worden door het definiëren van use-cases: representatieve voorbeelden van concrete probleemstellingen als startpunt voor onderzoeksactiviteiten. Deze kunnen vervolgens doelgericht gezamenlijk door de betrokken partijen geanalyseerd en aangepakt worden.

Motivatieperspectieven voor use cases
Het ontwikkelen van FLECS use cases kan vanuit verschillende perspectieven relevant zijn. In samenspraak met het ministerie EZK is geconstateerd dat een geschikte use case voor FLECS vanuit drie verschillende type belangen gemotiveerd zou moeten worden:



Veiligheidsbelang: mogelijke use cases kunnen geclassificeerd worden door de potentiële impact in te schatten waarbij kans en negatief effect van een specifieke cyberaanval gebalanceerd kan worden met preventie, detectie en mogelijke mitigatiemaatregelen. Het veiligheidsbelang komt voort vanuit de verplichting van marktpartijen & overheid, t.a.v. de leveringszekerheid, en vanuit de behoefte van de overheid, specifiek de veiligheidsdiensten en toezichthouders, om de continuïteit van vitale processen te waarborgen. Specifieke richtlijnen voor beoordeling van de nationale veiligheidsbelangen van use cases kunnen gevonden worden in [21].

Verdienvermogen / Economisch perspectief: use cases kunnen geclassificeerd worden naar behoefte van marktpartijen en de Nederlandse overheid om hun economische positie duurzaam te verdedigen/verbeteren. Bij de beoordeling hiervan speelt mee: (1) de potentiële marktomvang voor de use case en het aandeel daarin voor FLECS partners, (2) het innovatie-gedreven groeipotentieel waar (kennis opgebouwd in) FLECS aan kan bijdragen en (3) de niet-geldelijke positieverbetering die gerealiseerd kan worden (bijvoorbeeld vermindering van afhankelijkheid van buitenlandse leveranciers).

Maatschappelijk draagvlak en -belangen: cybersecurity voor hernieuwbare energie use cases dragen impliciet al direct bij aan het maatschappelijke doel van de energietransitie. Maar use cases kunnen ook op andere manieren bijdragen aan maatschappelijke belangen, zoals leveringszekerheid van elektriciteit voor elke burger, continuïteit van de digitale transitie (digitalisering vergt elektriciteit) en van andere kritieke infrastructuur die sterk afhankelijk is van de beschikbaarheid van elektriciteit. Verder heeft wind op zee voordelen ten aanzien van ruimtelijke ordening vraagstukken rond zonneparken en wind op land; maar dan dient de complexere beveiliging ervan wel op orde te zijn.

Genoemde use cases

Tijdens de gevoerde interviews zijn door marktpartijen de volgende windenergie-specifieke onderwerpen genoemd die uitgewerkt zouden kunnen worden tot use-cases:

- Fysieke veiligheid ten behoeve van digitale veiligheid (vermijden van fysieke toegang, Ninja-cables, etc.);
- Secure Networking wind op zee (green field) security by design voor o.a. IoT sensoriek.

Hiernaast zijn er algemene IT/OT convergentie-vraagstukken naar voren gekomen, waaronder:

- Maintenance & patching in legacy OT systemen;
- Algemene supply chain security windenergie (land of zee);
- big data toepassingen voor optimalisatie in industrial control systems;

Tenslotte is er in de interviews ook ter sprake gekomen dat voor de wind op zee sector ook algemene cryptografie-gerelateerde onderwerpen relevant zijn, zoals de ontwikkeling van een Public Key Infrastructuur (PKI) of post-quantum cryptografie migratie;

Selectie van use cases

Niet elk van de genoemde use-cases hebben een geschikte motivatie (vanuit veiligheid, economisch of maatschappelijk belang), of is relevant in de context van FLECS. Bijvoorbeeld, op het onderwerp post-quantum cryptografie en een algemene PKI wordt reeds uitgebreid onderzoek verricht en dit heeft momenteel geen specifieke aspecten die gerelateerd zijn aan hernieuwbare elektriciteitsopwekking. Verder is hiervoor geen breed draagvlak in de markt te herkennen. De legacy patching en maintenance problematiek is relevant voor de hele markt en zou daarmee een breed draagvlak kunnen hebben. Echter, de investering om ermee aan de slag te gaan lijkt voor marktpartijen ten opzichte van de voorziene baten op dit moment (nog) niet aantrekkelijk, de drempel is te hoog. Het maatschappelijke belang dat ermee gemoeid gaat is niet de primaire zorg van marktpartijen tenzij daar regelgeving voor wordt opgesteld. De genoemde verbetering van de fysieke veiligheid is niet direct een cybersecurity-gerelateerde uitdaging.

De tijdens de interviews genoemde onderwerpen van IT/OT convergentie, supply-chain security en secure networking lijken uitermate relevant voor de gehele Wind op Zee sector. Zij bieden in

principe een goede basis om in de toekomst op voort te bouwen en zodoende focus te creëren. De uitdaging is echter dat zij nog erg breed zijn en verder geconcretiseerd zouden moeten worden. Het blijkt dus lastig om vanuit de markt een duidelijke en concrete use case te definiëren. In enkele interviews is benoemd dat er om deze reden leiding vanuit de overheid wenselijk is.

4 Conclusies

Uit de interviews en analyse van het ecosysteem komt voort dat het Wind-op-Zee ecosysteem complex en divers is. De conclusies van de eerste **verkenning van het speelveld cybersecurity voor Wind op Zee** zijn als volgt:

1. Grootschalige windparken zijn over het algemeen structureel beveiligd, zowel fysiek als digitaal. Grote spelers tonen vaak een redelijk volwassenheidsniveau. Voor MKB partijen daarentegen zijn prioriteit en budgetten voor cybersecurity beperkt.
2. De Wind op Zee sector kan in de toekomst door de energietransitie en evolutie van het dreigingslandschap vaker doelwit van gerichte cyberaanvallen worden, en de mogelijke impact van uitval groeit. Daarom is er structureel betere beveiliging nodig.
3. Aan de technische kant zijn de belangrijkste cybersecurity uitdagingen voor de Wind op Zee sector het veilig maken van legacy technologie en de bekende IT cybersecurity concepten vertalen en toepassen op operationele technologie zoals windmolens.
4. Aan de organisatorisch-technische kant van cybersecurity in de Wind op Zee sector ligt de uitdaging vooral in de ketensamenwerking, standaardisatie en testen:
    - Er is i.v.m. een gesloten deur beleid een gebrek aan informatie-uitwisseling, samenwerking, normen/eisen en veiligheids-tests in de supply chain (waaronder toeleverende MKB partijen met beperktere cyber-expertise). Hierdoor is er over de supply-chain weinig zicht op de mate van beveiliging en op de verschillende risico's (kans en impact);
    - Door het missen van concrete eisen is het lastig voor de minder volwassen marktpartijen om te bepalen waar en op welke manier de eerste stappen te zetten zijn;
    - De markt wenst begeleiding en richting vanuit de overheid.
5. Op dit moment is er geen expliciete vraag vanuit de wind op zee markt naar technologie van cybersecurity technologie bedrijven. Daardoor is er (nog) geen specifiek aanbod. Indien een vraag vanuit de markt richting cybersecurity leveranciers gesteld wordt is te verwachten dat het aanbod zal volgen.

Met de gehouden interviews is er in de sector vervolgens een **behoefte aan praktische & pre-competitieve samenwerking op cybersecurity** geïdentificeerd. Uit deze verkenning wordt

geconcludeerd dat er binnen de sector en vanuit de overheid een drietal behoeftes bestaan, namelijk naar:

a. het delen van operationele informatie over huidige dreigingen en uitdagingen;
b. samenwerking in de vorm van experimenten en praktijktesten;
c. pre-competitieve samenwerking om het (toekomstige) elektriciteitsnet “by design” te beschermen tegen cyber-aanvallen.

Een inventarisatie van bestaande samenwerkingsverbanden in de vorm van ISACs of fieldlabs laat zien dat er al veel cybersecurity en energie gerelateerde initiatieven bestaan. Er is echter nog geen samenwerkingsverband *specifiek voor cybersecurity in de Wind op Zee sector* aangetroffen. Verder lijkt er op dit moment geen samenwerkingsvorm te bestaan waarin pre-competitieve samenwerking met een duidelijk toekomstperspectief plaatsvindt, bijvoorbeeld door de ontwikkeling van architectuurdesigns voor het toekomstige elektriciteitsnet (security-by-design).

De behoefte van de sector lijkt daarom op dit moment niet in zijn geheel door bestaande overlegorganen, samenwerkingsverbanden of initiatieven vervuld te worden. De vervulling van deze behoefte zou in PPS setting vormgegeven kunnen worden, waar op termijn ook fieldlab onderzoek verricht zou moeten worden naar cybersecurity use cases omtrent IT/OT convergentie, supply-chain, secure networking en kwetsbaarheden van WoZ technologie.

Verder blijkt uit de interviews dat op dit moment vooral concretere en meer “richtinggevende” wet- en regelgeving in de Wind op Zee sector, gemotiveerd vanuit het publieke belang, de meest effectieve manier lijkt om partijen in dit complexe ecosysteem te stimuleren voldoende cybersecurity in hun producten op te nemen. Het definiëren van concrete use cases vanuit de markt voor onderzoek en innovatie in een dergelijk fieldlab zal dan ook uitdagend blijven zolang de ketenverantwoordelijkheden niet scherp gedefinieerd zijn en er gewacht wordt op concrete, nationale en internationale wetgeving.

Met de aankomende vertaling van de NIS2 Directive, de voortdurende grote kavel-aanbestedingen op de Noordzee en steeds meer awareness over het belang van cybersecurity en ketenveiligheid lijken de omstandigheden gunstig om nu het momentum te creëren om en een dergelijke pre-competitieve samenwerking vorm te geven.

5 Verwijzingen

[1] [Online]. Available: https://www.tennet.eu/nl/nieuws/monitoring-leveringszekerheid-2022.

[2] [Online]. Available: https:\\www.nctv.nl\binaries\nctv\documenten\publicaties\2022\07\04\cybersecuritybeeld-nederland-2022\Cybersecuritybeeld+Nederland+2022.pdf.

[3] „Colonial Pipeline Ransomware Attack - Wikipedia," [Online]. Available: https://en.wikipedia.org/wiki/Colonial_Pipeline_ransomware_attack.

[4] [Online]. Available: https://www.wired.co.uk/article/ukrainian-power-station-cyber-attack.

[5] „Jaarverslag MIVD," [Online]. Available: www.rijksoverheid.nl/binaries/rijksoverheid/documenten/jaarverslagen/2023/04/19/openbaar-jaarverslag-2022-mivd/openbaar-jaarverslag-mivd-2022.pdf.

[6] 2. a. 2. Kamerbrief 'Staat van de Unie'. [Online].

[7] TNO 2022 R10712, „EZK Valorisatieketens: Waardenetwerk Cryptocommunicatie," TNO, [Online]. Available: https://publications.tno.nl/publication/34640009/T3lL6g/TNO-2022-R10712.pdf.

[8] „Rijksoverheid - Windenergie op zee," [Online]. Available: https://www.rijksoverheid.nl/onderwerpen/duurzame-energie/windenergie-op-zee.

[9] ENCS. [Online]. Available: encs.eu.

[10] T. E. |. ECHT, „Managementsamenvatting speelveldanalyse cybersecurity Wind op Zee," 25 04 2023. [Online]. Available: https://topsectorenergie.nl/documents/376/Speelveldanalyse_Cybersecurity_Wind_op_Zee_1.pdf.

[11] Rijksinspectie Digitale Infrastructuur (RDI), „Onderzoek storingsproblematiek en cyberveiligheid omvormers voor zonnepanelen," 2023. [Online]. Available: https://www.rdi.nl/documenten/rapporten/2023/05/30/onderzoek-storingsproblematiek-en-cyberveiligheid-omvormers-voor-zonnepanelen.

[12] T. Christiaan van den Berg, „Sectorale samenwerking voor betere cybersecurity rond omvormers," [Online]. Available: https://topsectorenergie.nl/nl/kennisbank/sectorale-samenwerking-voor-betere-cybersecurity-rond-omvormers/.

[13] TNO 2022 R10378, „Herstelvermogen binnen OT infrastructuren," NCSC, Den Haag, 2022.

[14] NCSC, „Samenwerking in een ISAC," [Online]. Available: https://www.ncsc.nl/onderwerpen/start-een-

samenwerking/zelf-een-samenwerking-starten/samenwerking-sector.

[15] NCSC, „NCSC Guide ISAC," [Online]. Available: https://english.ncsc.nl/get-to-work/publications/publications/2019/juli/02/ncsc-guide-isac.

[16] ENISA, „Information Sharing," [Online]. Available: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing.

[17] ENISA, „ISACs - cooperative models," [Online]. Available: https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models.

[18] N. -. DTC, „Overzicht van samenwerkingsverbanden," [Online]. Available: https://www.digitaltrustcenter.nl/overzicht-van-samenwerkingsverbanden.

[19] ISACs.eu, „European ISACs," [Online]. Available: https://www.isacs.eu/european-isacs.

[20] U.S. Department of Energy - Office of Energie Efficiency and Renewable Energy, „Roadmap for Wind Cyber security," 2020.

[21] Analistennetwerk Nationale Veiligheid, „Leidraad risicobeoordeling geïntegreerde risicoanalyse nationale veiligheid," RIVM, 2019.

[22] Ministerie Economische Zaken en Klimaat (DG Klimaat en Energie), „Nationaal Crisisplan Elektriciteit," 2021.

Bijlagen

A.1 Lijst van gesproken partijen

- OEMs:
  Siemens, Siemens Gamesa, Vestas
- Consultancies & bemiddelaars:
  Pondera, ECHT
- Samenwerkingsverbanden:
  Topsector Energie, TKI Wind op Zee, Grow, NWEA, Innovation Quarter, dcypher
- Energieleveranciers:
  Eneco, Shell
- Netbeheer:
  ENCS, TenneT, Stedin
- Cyber:
  Compumatica, Technolution, KPMG
- Overheidspartijen & veiligheidsdiensten:
  EZK K&E, EZG DE, NCSC, NBV, AT, RWS, NCTV, RDI
- Kennis:
  TU Delft, TNO intern (CST, ACE, SBA, Windenergie, ISP Business Development, ...)

ICT, Strategy & Policy

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

A.2 Afkortingenlijst

AIVD	Algemene Inlichtingen- en Veiligheidsdienst
AVR	Automated Vulnerability Research
BZK	Ministerie van Binnenlandse Zaken en Koninkrijkrelaties
DG	Directoraat Generaal
DTC	Digital Trust Centre
ENCS	European Network for Cybersecurity
EZK	Ministerie van Economische Zaken en Klimaat
FLECS	FieldLab Energie & CyberSecurity
ICS	Industrial Control Systems
IenW	Ministerie van Infrastructuur en Waterstaat
ISAC	Information Sharing and Analysis Centre
JenV	Ministerie van Justitie en Veiligheid
NBV	Nationaal Bureau voor Verbindingsbeveiliging
NCSC	Nationaal Cybersecurity Centrum
NCTV	Nationaal Coördinator Terrorismebestrijding en Veiligheid
OEM	Original Equipment Manufacturer
RDI	Rijksinspectie Digitale Infrastructuur (voormalig Agentschap Telecom)
SCADA	Supervisory Control and Data Acquisition
TKI	Topconsortium voor Kennis en Innovatie
TNO	Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek
TO2	Toegepast Onderzoek Organisatie
TSE	Topsector Energie
WoZ	Wind op Zee
WUR	Wageningen University of Research

ICT, Strategy & Policy

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