tki urban energy
topsector energie

Eindadvies Cyberzon

Een verkenning naar het verbeteren van de cyberweerbaarheid van de solarsector in Nederland

Christiaan van den Berg en Marc Koetse (TNO)

januari 2024

Inhoudsopgave

Voorwoord

Naast de energietransitie ontvouwt zich ook een digitale transitie waarbij de fysieke werels steeds vaker en verdergaand gekoppeld wordt met het virtuele. Deze twee transities zijn onlosmakelijk verbonden met elkaar. Om elektriciteit optimaler te gebruiken en beheren wordt steeds meer ICT- en meetapparatuur aan het systeem toegevoegd. Door de opkomst van het Internet of Things (IoT) en 5G is bovendien alles in sterke mate met elkaar verbonden. Steeds meer elektrische apparaten, zoals thuislaadpalen, warmtepompen en omvormers voor zonnepanelen, maken gebruik van IoT. Dit maakt het mogelijk voor apparaten om via een internetverbinding gegevens te verzamelen en uit te wisselen.

Deze vorm van digitalisering biedt zowel kansen als uitdagingen. Enerzijds wordt het mogelijk voor deze apparaten om hun omgeving te monitoren en actie te ondernemen op basis van de gegevens die ze verzamelen of ontvangen. Tegelijkertijd maken deze digitale netwerken de energiesector kwetsbaar voor cyberaanvallen. Een denkbaar scenario is dat de controle over de aansturing van apparaten (op grote schaal) wordt overgenomen en ze (gelijktijdig) worden aan- of uitgeschakeld. Voor individuele gebruikers is dat vervelend, zij lopen hierdoor mogelijk zonne-energie mis. Veel belangrijker is echter dat deze manipulatie het elektriciteitsnet kan destabiliseren, met mogelijke maatschappelijke en economische ontwrichting tot gevolg.

De Topsector Energie ziet cyberveiligheid en cyberweerbaarheid als kritische succesfactoren bij de opbouw van het duurzame digitale energiesysteem. In december 2022 startte de Topsector Energie samen met de Rijksdienst voor Ondernemend Nederland (RVO) drie kwartiermakerstrajecten. Het primaire doel was om de behoefte te onderzoeken van energiepartijen en te kijken hoe samenwerking vormgegeven kan worden zodat de energiesector digitaal minder kwetsbaar wordt. Drie kwartiermakers voerden een verkenning uit binnen verschillende deelsectoren: Hans Timmers (ECHT) naar de offshore windsector, Bruno van Hoek (Elaad) binnen laadsector en Christiaan van den Berg (TNO) voor de zonnestroomsector.

Met zijn verkenning heeft de kwartiermaker voor ZonPV een positieve beweging in gang gezet, mede gesteund door de urgentie vanuit aankomende EU-wetgeving en het nieuws over toenemende cyberdreigingen. De kwartiermaker heeft verkend op welke wijze samenwerking vormgegeven kan worden en gepoogd om concrete startpunten voor vervolg te verstrekken, zodat wij als opdrachtgevers maar vooral ook de sector zelf versneld kunnen komen tot impactvolle samenwerking rond het thema cybersecurity. Als uitkomst worden in deze rapportage een aantal analyses en conclusies gepresenteerd, inclusief het voorstel voor een integrale aanpak voor het verbeteren van de cyberweerbaarheid in de zonnestroomsector.

Het afgelopen jaar zijn nieuwe initiatieven gestart en bestaande initiatieven versterkt. In mei 2023 organiseerden Topsector Energie en RVO een kennissessie waar de resultaten zijn gepresenteerd aan stakeholders vanuit de overheid, netbeheerders en branche- en koepelorganisaties. Ook zijn de bevindingen gedeeld in een digitale sessie met partijen in de solarsector. De werkgroep cyberveiligheid van Holland Solar heeft de ambitie uitgesproken en eerste stappen gezet om door te groeien naar een Information Sharing and Analysis Centre (ISAC). TNO werkt aan een innovatieprojectvoorstel om onderzoek te doen naar een meer technologische (deel)oplossing voor het verbeteren van cyberweerbaarheid. En als Topsector Energie pakken we onze rol bij het stimuleren van verdere samenwerking voor het ontwikkelen en toepassen van kennis en innovaties voor betere cybersecurity in de duurzame energiesector.

Soe van Dijk
Programmacoördinator
Topsector Energie Digitalisering

Pim Vork
Innovatieanalist
Topsector Energie
TKI Urban Energy

Jesper Juffermans
Adviseur Energie innovatie
Rijksdienst voor Ondernemend Nederland

Samenvatting

Opdracht

Vanuit het programma Digitalisering van de Topsector Energie en RVO als opdrachtgevers werden drie kwartiermakerstrajecten parallel opgestart om de mogelijkheden te verkennen voor betere sectorale samenwerking en kennisdeling, Naast een traject gericht op *wind op zee* en op de *laadpaalinfrastructuur* werd ook een traject gericht op de omvormers van zonnepanelen. Aan Christiaan van den Berg (TNO) werd deze laatste kwartiermakersrol gevraagd in te vullen. Daarvan is dit rapport het resultaat.

Het primaire doel van de drie kwartiermakerstrajecten was om de behoefte te onderzoeken van de huidige en toekomstige spelers in deze deelsectoren en te kijken hoe samenwerking vormgegeven kan worden, zodat de energiesector digitaal minder kwetsbaar wordt.

Aanpak

Als aanpak is gekozen voor gesprekken met individuele organisaties, en enkele workshops. Deze gesprekken en workshops schoven in karakter op van verkennend naar synthetiserend en validerend. Met behulp van een online whiteboard werd in elk gesprek gebouwd aan een aantal canvassen rond *probleemanalyse*, *stakeholderveld*, *juridische context* en wat later in het traject ook *oplossingsrichtingen*. In de gesprekken werd op deze manier steeds doorgebouwd op de bijdragen van eerdere gesprekken.

Gaandeweg werd duidelijk dat een exclusieve focus op de omvormers te beperkt was, daarom werd in afstemming met de opdrachtgevers de focus verbreed naar aan het internet gekoppelde apparaten in PV-systemen.

Uiteindelijk zijn 45 personen gesproken van 30 verschillende organisaties: van marktpartijen uit de solarsector tot kennisinstellingen, overheidspartijen, brancheverenigingen, cybersecuritybedrijven en consultants.

De belangrijkste bevindingen en aanbevelingen van kwartiermaker zijn:

- Het risico op hacks van PV-systemen in Nederland is reëel. Het is bovendien aannemelijk dat het mogelijk is om verstoringen te veroorzaken in de elektriciteitsvoorziening met hacks van PV-systemen. Dit ondanks de beperkte beschikbaarheid van casuïstiek op dit moment. Er zijn verschillende zorgelijke trends, waardoor wordt ingeschat dat de risico's eerder groeiend dan afnemend zijn. Een nadere risico-analyse wordt aanbevolen.

- De solarsector kent een divers speelveld met partijen in verschillende maten van volwassenheid ten aanzien van cybersecurity. Ook de grootteverschillen van relevante spelers in dit licht valt op. Tevens is opgevallen dat de bereidheid om bij te dragen aan het verbeteren van de cybersecurity van de sector, en om daarin samen te werken groot is. Het is aanbevelenswaardig om de aangetroffen samenwerkingsbereidheid te benutten bij de vervolgstappen.

- Er komen veel verschillende verordeningen en wetten op de sector af de komende jaren vanuit de Nederlandse overheid en (met name) de Europese Commissie. Deze nieuwe cybersecurity-eisen komen erop neer dat steeds meer bedrijven en organisaties in de solarsector te maken krijgen met verplichte strengere beveiligingsmaatregelen om zich te beschermen tegen cyberaanvallen en datalekken.

- Tijdens het kwartiermakerstraject zijn veel partijen aangetroffen met voldoende bewustzijn ten aanzien van de cybersecurity-uitdaging van de sector, die zich bovendien bereid tonen om in samenwerkingen te komen tot vooruitgang. Er bestaan ook al diverse waardevolle initiatieven op het gebied van cybersecurity, waaruit blijkt dat samengewerkt wordt. Het betreft echter relatief kleine initiatieven, die ook afhankelijk lijken van individuen. Het is de uitdaging om de initiatieven te versterken door ze minder persoonsafhankelijk te maken, te verbinden aan elkaar en met additionele initiatieven, en door toe te werken naar een programmatische samenhang.

- De uitdaging om de cybersecurity in de solarsector structureel te verhogen vraagt om een integrale aanpak waarin diverse spelers samenwerken. In zo'n aanpak zouden de krachten gebundeld kunnen worden rond zes thema's. Allereerst rond het thema cybersecurity awareness: het vergroten van de kennis en van het bewustzijn rond cybersecurity. Ook lijkt het opportuun op korte termijn een samenwerking te starten, die meer zicht kan brengen in de kans en impact van de verschillende cyberrisico's. Met dit verbeterde zicht op de risico's kunnen cyberveilige werkwijzen, diensten en producten worden gevestigd middels standaarden en certificeringen. Ook kunnen rond onderzoek en ontwikkeling de krachten gebundeld worden om nieuwe technieken, producten, diensten en kennis beschikbaar te krijgen voor de sector. Rond Information sharing & analysis lijkt voldoende initieel enthousiasme aanwezig te zijn om een kleinschalige start te maken met het sectoraal uitwisselen van best practices en dreigingsinformatie. In een later stadium kan dan ook het gezamenlijk management van incidenten worden ontwikkeld.

Hoofdstuk 1

Cyberrisico's PV-systemen

1.1. Kleine (residentiële) versus grote (industriële) PV-installaties

Als startpunt voor dit hoofdstuk, wordt hieronder een schets gegeven van een tweetal 'archetypische' PV-systemen[1]. Het eerste systeem is een typisch residentieel systeem, en het tweede een typisch grootschalig systeem. Naast een beschrijving van het systeem wordt vooral aandacht gegeven aan eventuele connectie met het internet en welke schade zou kunnen worden toegebracht bij een eventuele cyberaanval.

1.1.1. Kleinschalige en residentiële PV-systemen

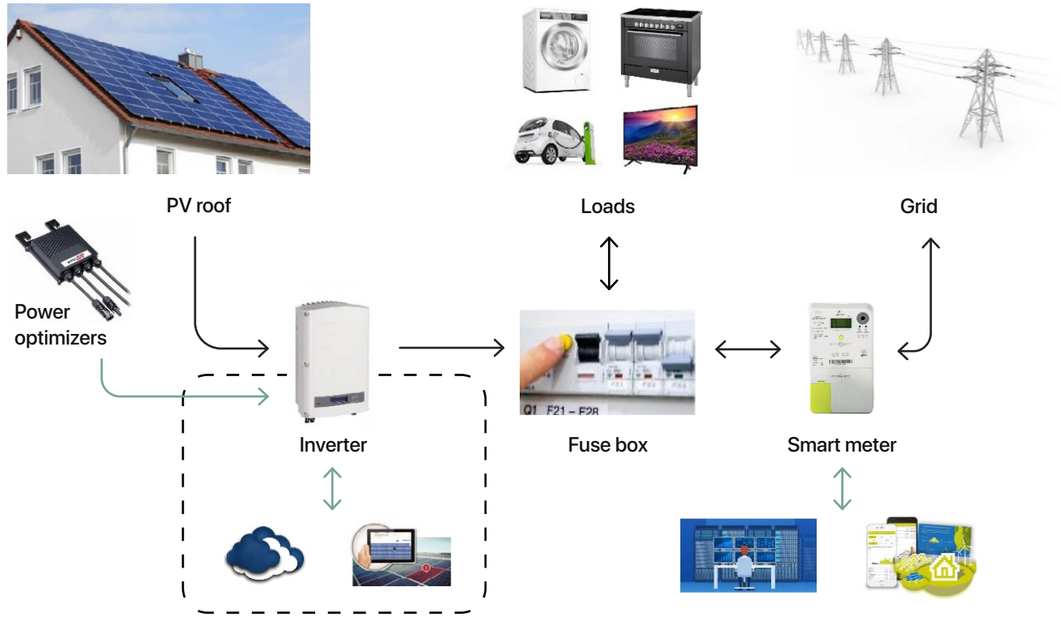
Kleinschalige en residentiële PV-systemen vormen een belangrijke component binnen het Nederlandse energielandschap. Omdat het een nogal gedistribueerde component is, met relatief kleine vermogens op verschillende locaties, lijkt de invloed van een eventuele hack of aanval op het totale energy systeem klein. Echter, als een specifiek type omvormer wordt gehackt of een grote hoeveelheid inlogcodes wordt buitgemaakt, kan een significant vermogen worden aangevallen, zoals aangetoond bij de Solar-Man hack[2].

Een schematische opbouw van een typisch residentieel of klein PV-systeem is weergegeven in figuur 1.1. Het bestaat uit PV-panelen, een omvormer en eventuele optimisers of micro-omvormers. De PV-panelen zijn of in een string verbonden met een string-omvormer of -minder frequent - individueel aangesloten met behulp van zogenaamde micro-omvormers. In sommige gevallen zijn de panelen voorzien van een optimiser, een apparaatje dat de panelen individueel optimaal regelt. Vervolgens is het geheel elektrisch verbonden met een aardlekschakelaar en een stop in de meterkast. Via de slimme meter wordt niet gebruikte elektriciteit teruggeleverd aan het net. Eventuele batterijen en laadpalen zijn niet opgenomen in dit schema.

In de meeste gevallen is de omvormer het aan het internet ('netgekoppelde') apparaat: deze is verbonden met een cloud-service en klantportaal (zie 1.1.3) van de fabrikant. Dit gebeurt veelal via het lokale netwerk van de gebruiker. Via de cloud-service levert de fabrikant services zoals monitoring en updates van de firmware. Dataverkeer is in essentie mogelijk in twee richtingen. Over het algemeen kan de gebruiker geen directe invloed op de werking van het systeem uitoefenen. Een installateur met een installateurs-account zou dat wel kunnen.

1.1.2. Middelgrote en grootschalige PV-systemen

Middelgrote PV-systemen op bijvoorbeeld de daken van distributiecentra, of grootschalige systemen in 'zonneweides' of 'zonneparken' produceren op piekvermogen een significante hoeveelheid elektriciteit die bij ongewenst afschakelen invloed kan hebben op de netstabiliteit. In opbouw is een middelgroot of grootschalig PV-systeem goed vergelijkbaar met een residentieel systeem. Belangrijke verschillen liggen met name in de schaal en de aanwezigheid van infrastructuur om een gridconnectie mogelijk te maken. In deze paragraaf ligt de focus op de PV-specifieke infrastructuur, maar het is belangrijk te onderkennen dat een aantal stations, met name na de schakelkast en transformator, in een grootschalig PV-systeem dezelfde risico's kennen als een klassiek elektriciteitssysteem.



Figuur 1.1: *Schematische weergave van een residentieel PV-systeem*

[1] *Een fotovoltaïsche (PV), of zonnestroominstallatie zet zonlicht om in elektriciteit*

[2] *Solar Magazine - Onderzoekers 'hacken' 42.000 Nederlandse installaties met zonnepanelen*

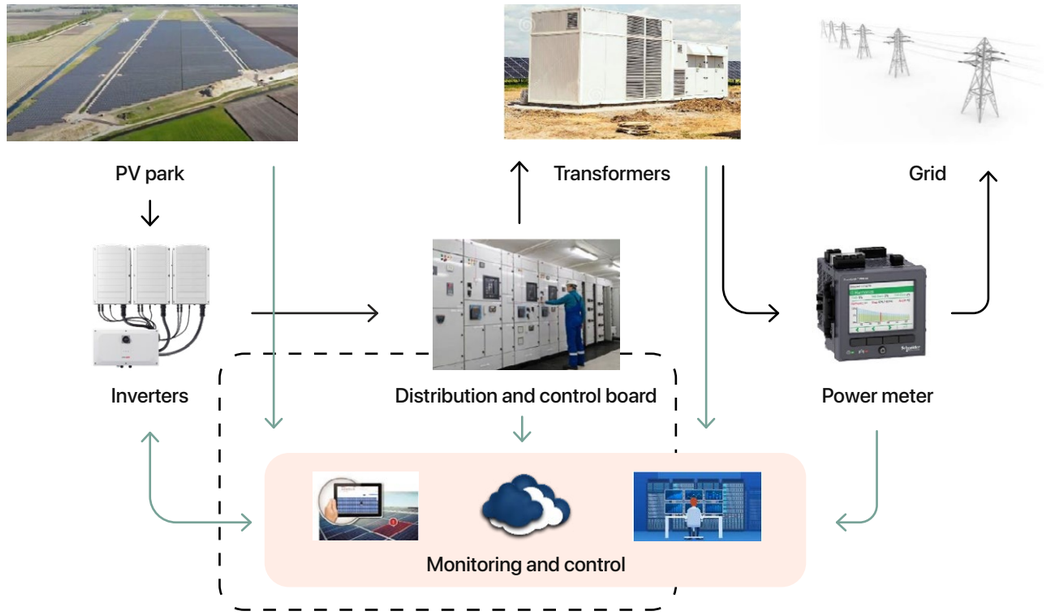
figuur 1.2 laat een (vereenvoudigde) schematische weergave van een zonnepark zien. De hoofdcomponenten van het PV-specifieke deel zijn de panelen, de string-omvormers en combiner-boxes. Afhankelijk van de situatie kan er wederom gekozen worden voor individuele micro-omvormers of string-omvormers. Daarnaast zijn er, zeker bij moderne parken, *monitoring and control devices* die het mogelijk maken voor stakeholders om het functioneren van het systeem te beïnvloeden. Dit soort apparatuur wordt wel *operationele technologie* genoemd (OT), die bestaat naast de bekende Informatietechnologie (IT) van bedrijfsautomatisering die al veel langer geassocieerd wordt met cyberrisico's.

Met name de omvormers en monitoring and control devices zijn via portalen en cloud-services te bereiken. Dit is van belang voor bijvoorbeeld een handelaar die dynamisch wil kunnen af- en opschakelen met de prijs die momentaan geboden wordt voor de opgewekte stroom. Zeker bij negatieve prijzen wil men de productie kunnen afschakelen op tijdelijk opslaan.

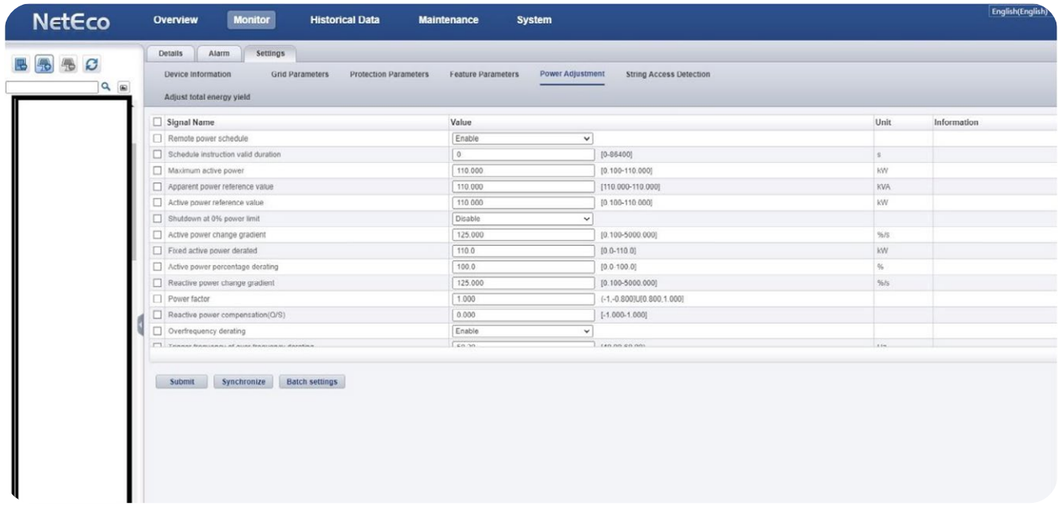
1.1.3. Klantportalen

Omvormers en *monitoring and control devices* worden doorgaans geleverd door de fabrikant met een klantportaal. Met deze klantportalen kunnen gebruikers instellingen wijzigen, en het vermogen regelen.

Naast de klantportalen van de fabrikanten zijn er ook derde partijen die portalen leveren waarmee bijvoorbeeld apparatuur van verschillende leveranciers kan worden bediend. Ter impressie hieronder een screenshot van een klantportaal van Huawei (NetEco) - figuur 1.3, en dat van een derde partij - figuur 1.4. Op het laatste screenshot is goed te zien hoe het vermogen van een PV-installatie wordt afgestemd op de actuele prijsniveaus voor stroomlevering.



Figuur 1.2: *Vereenvoudigde schematische weergave van een grootschalig PV-systeem*



Figuur 1.3: *Klantportaal NetEco*

Figuur 1.4: *Portaal derde partij*

1.2. Diverse aanvalsscenario's, diverse motieven

In de gesprekken met de sector, en met het bredere stakeholderveld, kwamen drie hoofdscenario's naar voren waarlangs een hack zou kunnen plaatsvinden in PV-systemen (figuur 1.5).

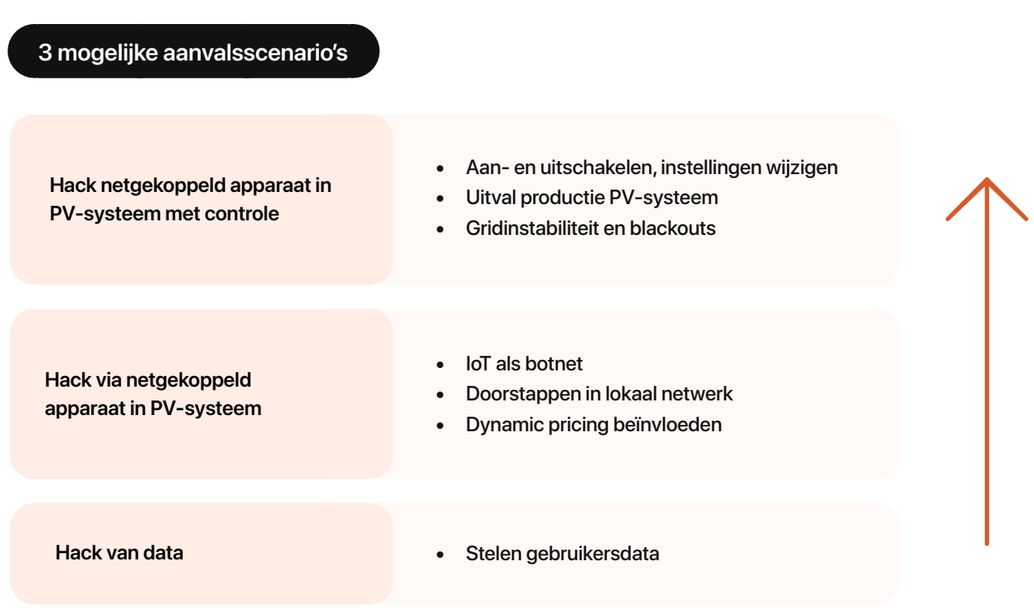
In het kwartiermakertraject is met name aandacht geweest voor de eerste twee scenario's, die het meest direct bedreigend zijn voor de leveringszekerheid van energie.

1.2.1. Hack van een netgekoppeld apparaat in een PV-systeem

Het eerste hoofdscenario betreft een hack van netgekoppelde apparaten, waarbij de hacker controle krijgt over de instellingen, en over het geleverde vermogen van een PV-systeem. Met deze controle kan een hacker vermogen afschakelen, en daarmee de stroomproductie frustreren. Dat kan directe gevolgen hebben voor bedrijfsprocessen die afhankelijk zijn van de lokale PV-installatie, zoals een laadstation voor bedrijfswagens, of een airco-installatie.

Als voldoende (cumulatief) vermogen wordt afgeschakeld, bestaat het risico van gridinstabiliteit, en zelfs black-outs in het elektriciteitssysteem. Dit scenario is zowel voorstelbaar voor de residentiële PV-systemen, als voor de middelgrote en grote PV-systemen.

Een belangrijke kwetsbaarheid bij netgekoppelde apparaten is het wachtwoordbeleid. Bij eerdergenoemde SolarMan-hack bleek het standaardwachtwoord van een type omvormer in veel gevallen niet gewijzigd te worden, waarmee het gemakkelijk was om een groot cumulatief vermogen in één keer te kunnen beïnvloeden. Een andere kwetsbaarheid ligt bij zogenaamde 'zero days': foutjes in de software, waardoor een hacker zich toegang kan verschaffen tot een systeem. Deze 'zero days' worden gedeeld of verkocht op zwarte markten op internet, en kunnen verholpen worden met een software update of 'patch'. In dat licht is het zorgelijk dat veel omvormers niet gedurende hun hele levensduur onderhouden worden, bijvoorbeeld omdat de fabrikanten niet meer actief zijn op de markt.



Figuur 1.5: *Hoofdscenario's aanvalsscenario's*

Een motief voor dergelijke aanval zou er een kunnen zijn van terrorisme, of een van een statelijke actor die economische schade wil veroorzaken. Een cybercrime-motief is echter ook mogelijk, waarbij een hacker bijvoorbeeld probeert ransomware[3] te plaatsen om daarmee losgeld te kunnen eisen.

1.2.2. Hack via netgekoppelde apparaten, maar zonder controle

Een tweede hoofdscenario betreft een hack via een netgekoppelde apparaat als een omvormer, maar dan zonder directe controle over de instellingen en het geproduceerde vermogen.

Ook zonder directe controle kan een hack vervelende gevolgen hebben, zoals de inzet van een netgekoppelde apparaten als onderdeel van een botnet[4] in een DDoS-aanval[5]. Of als een hacker via het initiële inbreekpunt weet over te stappen naar andere apparatuur in het netwerk van een PV-systeem. Bijvoorbeeld naar apparatuur die een batterijsysteem aanstuurt, of aangesloten laadinfrastructuur. Of naar een lokaal energiemanagement-systeem dat het samenspel van systemen regelt. Al deze apparatuur is in principe te ontregelen.

Het is bovendien voorstelbaar dat een hacker zou ingrijpen in de monitorings- en handelsapplicaties, waarmee verstoringen kunnen worden veroorzaakt. Steeds meer elektriciteitshandel wordt namelijk via 'dynamic pricing' geregeld, waarbij prijzen afhankelijk zijn van de momentane balans tussen vraag en aanbod. Voor deze mechanismes is het heel vervelend als de meetdata van het geproduceerde vermogen niet kloppen met de daadwerkelijke productie. Dan kan namelijk de lokale energiebalans verstoord worden, met gridinstabiliteit tot mogelijk gevolg. Dit scenario is vooral voorstelbaar de middelgrote en grote PV-systemen, maar ook in mindere mate voor de residentiële PV-systemen.

Ook bij dit hoofdscenario geldt dat een motief voor een dergelijke aanval een terroristische zou kunnen zijn, of een van een statelijke actor die economische schade wil veroorzaken. Een cybercrime-motief is echter ook mogelijk, waarbij een hacker bijvoorbeeld probeert ransomware te plaatsen om daarmee losgeld te kunnen eisen, of waarbij een hacker met voorkennis van een incident mogelijk geld kan verdienen aan de aan- en verkoop van energie.

1.2.3. Hack van data

Een laatste hoofdscenario betreft een hack via een netgekoppelde apparaat als een omvormer naar andere apparatuur in het PV-systeem, en via dit lokale OT-netwerk naar het aangesloten IT-netwerk. Het is voorstelbaar dat een hacker via deze weg persoonsgegevens zou kunnen stelen van gebruikers, of informatie over het energiegebruik. Zulke informatie kan geld waard zijn op de zwarte markten op internet. Dit scenario is vooral voorstelbaar bij de middelgrote en grote PV-systemen, maar ook in mindere mate voor de residentiële PV-systemen.

Op dit derde hoofdscenario is niet ingegaan in de kwartiermakersopdracht: de focus is komen te liggen op de eerste twee hoofdscenario's.

[3] *Gijzelingssoftware*

[4] *Netwerk van aan internet verbonden appraten die dankzij de installatie van kwaadaardige software gezamenlijk ingezet kunnen worden voor cybercriminaliteit – vaak zonder medeweten van eigenaren*

[5] *Distributed Denial of Service aanvallen zijn pogingen om een computer, computernetwerk of dienst niet of moeilijker bereikbaar te maken voor de bedoelde klanten door met meerdere computers tegelijk de aanval op hun doelwit uitvoeren.*

1.3. Conclusie: meer analyse nodig

Gedurende de kwartiermakersopdracht is duidelijk geworden dat het risico op verstoring van PV-systemen door cyberincidenten reëel is. Alhoewel er op dit moment nog weinig casuïstiek voorhanden is van daadwerkelijke aanvallen, zijn vrijwel alle geïnterviewden het erover eens dat de risico's bestaan, niet verwaarloosbaar zijn en dat de risico's bovendien eerder toenemen dan afnemen. Daarbij komen de volgende signalen naar voren:

- Het aandeel hernieuwbare energie in de nationale elektriciteitsproductie zal in de komende jaren sterk toenemen, tot zo'n 85% in 2030[6]. Daarvan is stroom uit PV-installaties een belangrijk onderdeel.
- De vraag naar elektriciteit zal sterk toenemen de komende jaren, onder andere voor mobiliteit, industriele productie en verwarming/koeling in de gebouwde omgeving.
- In toenemende mate worden PV-systemen geïntegreerd met andere systemen zoals laadinfrastructuren voor elektrische auto's EV, energiemanagementsystemen en batterijen.
- Er komen steeds meer verschillende netgekoppelde apparaten in PV-systemen terecht. Met name doordat klanten behoefte hebben aan 'curtailment' en diensten ten behoeve van het voorkomen van netcongestie. In een aantal gevallen zijn de netgekoppelde apparaten en platformen van relatief kleine spelers afkomstig, die (nog) te klein zijn voor een volwassen security-afdeling.
- De aanslag op de Nordstream 1 pijpleiding heeft aangetoond dat de West-Europese energievoorziening kwetsbaar is voor aanslagen, en dat bovendien partijen zijn die bereid zijn om deze kwetsbaarheid aan te grijpen.

Het is tevens duidelijk geworden, dat er onvoldoende zicht is op de verhouding tussen de beschreven risico's in termen van kans en impact. Dat maakt dat het op dit moment onduidelijk is of het bijvoorbeeld meer zin heeft om te investeren in het mitigeren van de risico's bij residentiële installaties, of juist in de middelgrote en grootschalige systemen. Als onderdeel van de integrale aanpak (Hoofdstuk 4) komt een nadere risicoanalyse dan ook naar voren.

[6] *Klimaat- en Energieverkenning (KEV) | PBL Planbureau voor de Leefomgeving*

Hoofdstuk 2

Speelveldanalyse

2.1. Divers speelveld, grote bereidheid tot samenwerken

Als onderdeel van zijn verkenning heeft de kwartiermaker een speelveldanalyse gemaakt in samenwerking met brancheverenigingen Holland Solar en TKI Urban Energy. Daarmee is een eerste beeld ontstaan van de verschillende rollen in de sector, de mate waarin en wijze waarop zij betrokken zijn bij de geïdentificeerde cyberrisico's en hun behoeften en belangen ten aanzien van (het verbeteren van) cyberweerbaarheid. Het doel was om de meest relevante actoren te bepalen bij vervolgacties richting het meer cyberweerbaar maken van de sector.

Uit de speelveldanalyse blijkt dat partijen in de solarsector veelal verschillende rollen vervullen. Hierdoor is het soms onduidelijk wie precies verantwoordelijk is voor welk deel van de waardeketen. Figuur 2.1 laat zien dat de eerste vijf rollen *direct* invloed hebben op het cyberrisico, terwijl rollen 6-9 meer in indirecte zin kunnen bijdragen aan het verminderen van de cyberrisico's. Een derde categorie rollen staat nog wat verder af van het directe cyberrisico.

De interviews geven een divers beeld van de actoren: van grote partijen die al lang in de energiewereld actief zijn, en vallen onder het 'vitale regime' van NCSC tot start-ups en scale-ups. De cybermaturiteit lijkt daaraan verbonden. De grotere spelers hebben vaak al functionarissen in dienst die zich bezighouden cyberveiligheid, terwijl de kleinere partijen andere prioriteiten of domweg niet de middelen hebben. De kleinere partijen werken ook vaak met eigen soft- en hardware, waar de grotere spelers deze vaak betrekken van OEMs en specialisten. Hierdoor wordt het 'aanvalsoppervlak' allengs breder dan alleen apparatuur van OEMs.

De geïnterviewde partijen geven aan het belangrijk te vinden om bij te dragen aan de verbetering van cyberveiligheid van PV-systemen. Ook blijkt er een grote bereidheid te bestaan ten aanzien van het onderling samenwerken aan het verbeteren van cyberveiligheid. Regelmatig werd de noodzaak daartoe uitgesproken.

Overzicht van de actoren en hun invloed op het cyberrisico van PV-systemen

• **Original Equipment Manufacturer (OEM)** • **Trader (oa Congestion Service Provider en Balance Service Providers)** • **Operation & maintenance (O&M)** • **Assetmanagement** • **Engineering, procurement & construction (EPC)**	Directe invloed
• **Projectontwikkelaar** • **IT-serviceprovider** • **Eigenaar** • **Netbeheerder (TSO / DSO)**	Indirecte invloed
• **Overheid – wetgever / handhaver / toezichthouder** • **Kennisinstelling**	Indirecte invloed

Figuur 2.1: *Overzicht van de actoren en hun invloed op het cyberrisico van PV-systemen*

Hoofdstuk 3

Wettelijke en juridische ontwikkelingen

3.1. Veel verschillende Europese richtlijnen en verordeningen

Op het gebied van privacybescherming en cyberveiligheid is er een brede range aan Europese *acts* (verordeningen) en *directives* (richtlijnen) in ontwikkeling, die de komende jaren zijn beslag zal krijgen voor de Nederlandse markt. Ten behoeve van de spelers in de solarsector is gepoogd om wat meer duidelijkheid te scheppen. Dat valt nog niet mee, omdat de details veelal nog niet bekend zijn: er wordt nog stevig over onderhandeld over de wetteksten.

3.2. Actuele verordeningen

3.2.1. NIS1 & Wet beveiliging netwerk- en informatiesystemen (Wbni)

Sinds 2018 bestaat de Nederlandse wet 'beveiliging netwerk- en informatiesystemen' (Wbni) en het bijbehorende Besluit beveiliging netwerk- en informatiesystemen (Bbni). De Wbni is de Nederlandse implementatie van de Europese Netwerk- en Informatiebeveiliging Richtlijn (bekend als de NIS-Richtlijn). De Rijksinspectie Digitale Infrastructuur is toezichthouder op deze wet.

De Wbni geldt voor aanbieders van een essentiële of vitale dienst of categorieën van zodanige aanbieders (ook als zij niet zijn aangewezen als 'aanbieders essentiële dienst' (AED) of 'andere aangewezen vitale aanbieder' (AAVA). Het betreft onder andere de netbeheerder van het landelijk hoogspanningsnet, de regionale netbeheerders en elektriciteitsbedrijven die installaties beheren met een vermogen van meer dan 100MW.

De wet verplicht diverse zaken: (1) er geldt een meldplicht voor incidenten; (2) het is verplicht om passende technische en organisatorische maatregelen te nemen om de risico's voor de beveiliging van netwerk- en informatiesystemen te beheersen; (3) het is verplicht om passende maatregelen te treffen om incidenten te voorkomen. Daarnaast hebben ze de plicht de gevolgen van dergelijke incidenten zo veel mogelijk te beperken. Daar staan ook rechten tegenover: (1) het recht op bijstand van het Nationaal Cyber Security Centrum (NCSC) bij het treffen van maatregelen om de continuïteit van hun diensten te waarborgen of te herstellen; (2) het recht op informatie en adviezen van het NCSC over dreigingen en incidenten met betrekking tot hun netwerk- en informatiesystemen.

3.2.2. Cyber Security Act (CSA)

Sinds 2019 geldt de Cyber Security Act (CSA): het Europese certificatiesysteem voor cyberveiligheid voor fabrikanten en leveranciers van ICT-producten, -diensten en –processen. Dit geldt ook voor omvormers die van buiten de EU komen. De verordening biedt een kader voor de certificering van producten, processen en diensten op het gebied van cyberveiligheid en moet zorgen voor certificeringsverplichtingen die voor alle lidstaten hetzelfde zijn. Fabrikanten en dienstverleners hoeven straks niet meer in elke lidstaat afzonderlijk een certificaat te behalen.

De Rijksinspectie voor de Digitale Infrastructuur houdt toezicht in de rol van National Cybersecurity Certification Authority (NCCA). De certificeringen van de CSA zijn vooralsnog niet verplicht, maar het ontstaan van verplichtingen in de nabije toekomst is zeer waarschijnlijk. In het Europese proces rond de NIS-richtlijn en de Radio Equipment Directive wordt gesproken over een bevoegdheid van de Europese Commissie om specifieke certificeringen of gebruik van specifieke gecertificeerde producten, diensten en processen verplicht te stellen. Op 31 december 2023 zal de Europese Commissie onder de CSA een evaluatie uitgevoerd hebben om eventuele verplichtingen te overwegen.

3.3. Korte- en middellange termijn

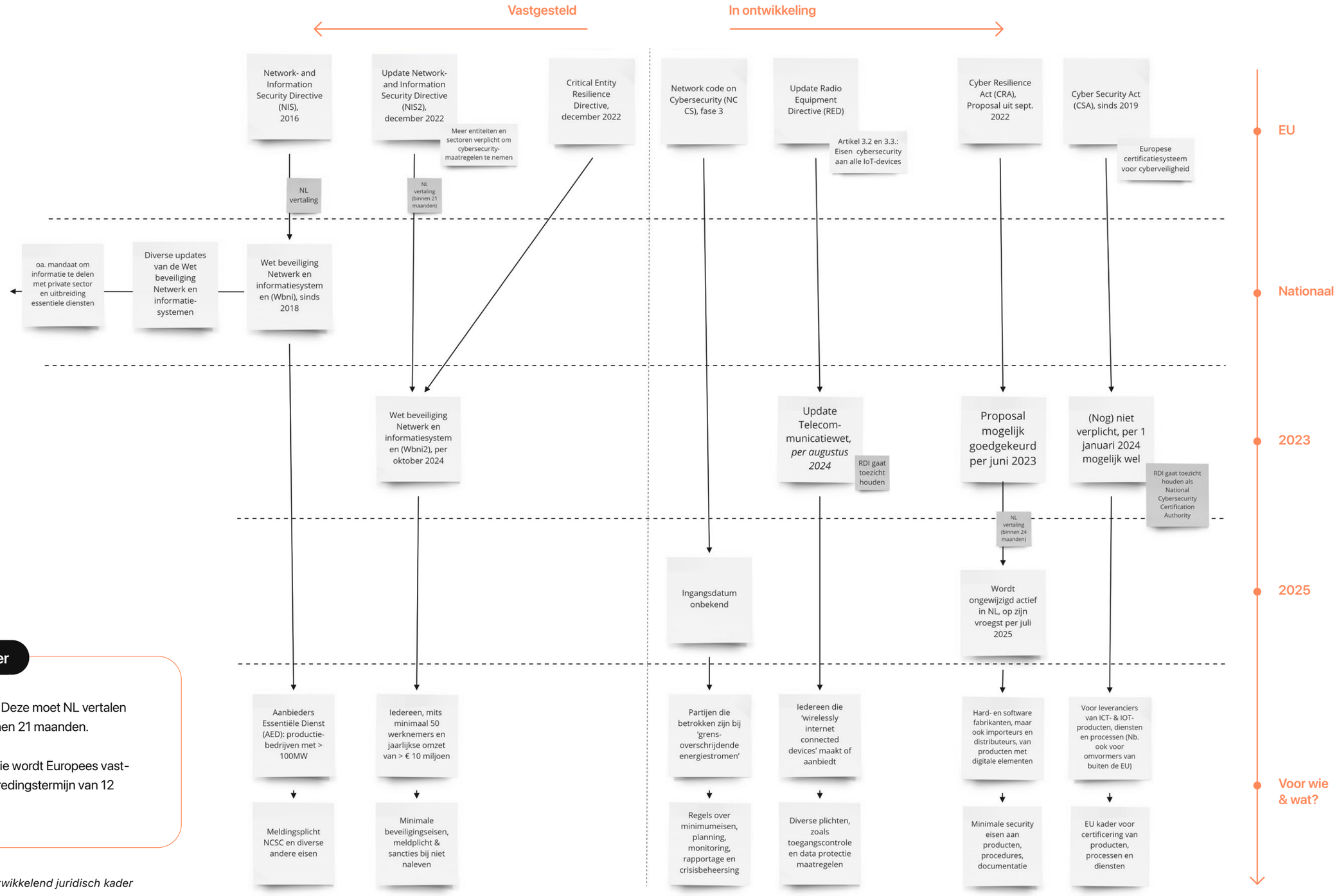
In aanvulling op het huidige wettelijke kader, wordt op Europees en nationaal niveau gewerkt aan diverse nieuwe verordeningen en richtlijnen, waarvan het meest relevant zijn: de NIS 2, de Network Code, een aanvulling op de Radio Equipment Directive , de Cyber Resilience Act, en de Cyber Security Act. In figuur 3.1 hieronder wordt gepoogd om de samenhang, en de belangrijkste elementen naar voren te brengen. Zie bijlage b voor de complete figuur, met daarin ook de NIS 2.

3.3.1. NIS 2-richtlijn (update van de Wbni)

De NIS 2-richtlijn beoogt het gemeenschappelijk niveau van cybersecurity in de Europese Unie verder te verhogen, mede wegens aanzienlijke implementatieverschillen tussen de lidstaten[9]. De NIS 2 zal van toepassing zijn, naast de vitale aanbieders die al vallen binnen de Wbni, op middelgrote en grote ondernemingen binnen de energiesector. Een voorwaarde is dat het bedrijf middelgroot moet zijn, wat gedefinieerd wordt als: minimaal 50 werknemers in dienst en een jaarlijkse omzet van meer dan € 10 miljoen.

Er worden meer uitgebreide en expliciete minimale beveiligingseisen gesteld waar elk bedrijf aan moet doen. Daarbij richt NIS 2 zich met een apart artikel over governance bovendien rechtstreeks tot het bestuur van de entiteiten: bestuursorganen dienen de cybersecuritymaatregelen goed te keuren, toe te zien op de uitvoering ervan en moeten bovendien aansprakelijk kunnen worden gehouden indien de entiteit zich niet aan de beveiligingsplicht houdt. Daarnaast schrijft NIS 2 voor dat bestuurders zich scholen: zij moeten dus een cybersecurityopleiding volgen. Tevens zijn ondernemingen onder de nieuwe richtlijn verplicht om cyberdreigingen in de keten aan te pakken en is er een meldplicht van cyberincidenten. Ook kunnen lidstaten

[9] *Cybersecurity in Europa. De herziene Netwerk- en Informatiebeveiligingsrichtlijn (NIS 2). Nynke Brouwer en Jurriaan van Mil.*



Juridisch kader

Directive = Richtlijn. Deze moet NL vertalen naar NL context binnen 21 maanden.

Act = verordening. Die wordt Europees vast-gesteld. Inwerkingstredingstermijn van 12 maanden.

Figuur 3.1: *Overzicht zich ontwikkelend juridisch kader*

eisen dat entiteiten gebruik maken van gecertificeerde producten of diensten in de zin van de CSA.

3.3.2. Richtlijn Radioapparatuur (RED) artikel 3.3

De Richtlijn Radioapparatuur 2014/53/EU (RED) van de Europese Commissie stelt een regelgevend kader vast voor radioapparatuur, met essentiële vereisten voor veiligheid en gezondheid, elektromagnetische compatibiliteit en radiospectrumefficiëntie. Artikel 3.3 van de richtlijn bevat apparaatvereisten met betrekking tot cyberbeveiliging en privacy. Op 12 januari 2022 is de verordening gepubliceerd, die de nalevingsvereisten voor dit artikel afdwingt. De verordening vereist cyberbeveiliging, privacy van persoonsgegevens en bescherming tegen fraude voor toepasselijke draadloze apparaten die op de EU-markt verkrijgbaar zijn. De verordening wordt verplicht op 1 augustus 2025. De RDI gaat in Nederland toezicht houden.

De vereisten zijn dat radioapparatuur (a) elementen bevat voor het bewaken en beheersen van netwerkverkeer, met inbegrip van de verzending van uitgaande gegevens; (b) is ontworpen om de effecten van voortdurende denial of service-aanvallen te beperken; (c) passende mechanismen heeft voor authenticatie en toegangscontrole; (d) opgeslagen, verzonden of anderszins verwerkte persoonsgegevens beschermt tegen onbedoelde of ongeoorloofde opslag, verwerking, toegang, openbaarmaking, ongeoorloofde vernietiging, verlies of wijziging of gebrek aan beschikbaarheid.

De verordening is relevant voor alle entiteiten die apparaten maken of aanbieden die draadloos met het internet verbonden zijn. Denk hierbij aan partijen die omvormers maken of aanbieden.

3.3.3. Cyber Resilience Act (CRA)

Met de Cyber Resilience Act (CRA) wordt beoogd dat producten met digitale elementen die in de EU op de markt worden gebracht veilig(er) zijn, dat fabrikanten verantwoordelijk blijven voor de cyberbeveiliging gedurende de hele levenscyclus van een product en dat consumenten de nodige bescherming genieten[10]. De CRA bevat cyberbeveiligingsbepalingen voor fabrikanten, ontwikkelaars en distributeurs van producten met digitale elementen.

Het voorstel is uit september 2022 en in het najaar van 2023 onderhandelen de lidstaten met het Europees Parlement over de definitieve wettekst. Naar verwachting treedt de CRA in 2027 in werking. De cybersecurity eisen uit de RED 3.3 zullen dan overgaan in de CRA.

De CRA zal van toepassing worden op producten met digitale elementen waarvan – kort gezegd – het beoogde gebruik een verbinding met een apparaat of netwerk omvat. Producten met digitale elementen zijn: 'elk software of hardware product en de oplossingen voor gegevensverwerking op afstand, met inbegrip van software- of hardwarecomponenten die afzonderlijk in de handel worden gebracht'. Het grootste deel van de verplichtingen uit de CRA richt zich tot fabrikanten. Daarnaast bevat de CRA ook bepalingen met verplichtingen voor importeurs en distributeurs.

Fabrikanten zullen een product met digitale elementen alleen in de handel mogen brengen, indien het is ontworpen, ontwikkeld en geproduceerd overeenkomstig basisvoorwaarden op het gebied van cyberbeveiliging. De cyberbeveiligingseisen waaraan fabrikanten zullen moeten voldoen, vallen in drie onderdelen uiteen:

- producten met digitale elementen moeten zodanig worden ontworpen, ontwikkeld en geproduceerd dat zij een passend niveau van cyberbeveiliging waarborgen op basis van de risico's;
- producten met digitale elementen worden geleverd zonder bekende kwetsbaarheden;
- op basis van een verplichte risicobeoordeling moeten, indien van toepassing, producten met digitale elementen voldoen aan een aantal verplichtingen, zoals: levering met een standaard beveiligde configuratie; de vertrouwelijkheid van opgeslagen, verzonden of anderszins verwerkte (persoons)gegevens, bijvoorbeeld door middel van encryptie; en de minimalisering van gebruikte (persoons)gegevens.

Naast cyberbeveiligingseisen zullen fabrikanten moeten voldoen aan eisen met betrekking tot de behandeling van kwetsbaarheden. Fabrikanten zullen bijvoorbeeld kwetsbaarheden moeten vaststellen en documenteren, beveiligingsupdates verstrekken voor kwetsbaarheden in verband met de risico's die zijn verbonden aan producten met digitale elementen, informatie verstrekken over verholpen kwetsbaarheden en ervoor zorgen dat beveiligingsupdates onverwijld en kosteloos worden verspreid, vergezeld van informatie over te nemen maatregelen voor gebruikers. Het is nog onduidelijk wie toezicht gaat houden, maar mogelijk gaat ook hier de RDI een rol spelen.

3.3.4. Network Code on Cybersecurity (NCCS)

De Netwerkcode Cybersecurity (NCCS) beoogt een Europese norm te stellen voor de cyberbeveiliging van grensoverschrijdende elektriciteitsstromen. Het omvat regels voor de beoordeling van cyberrisico's, gemeenschappelijke minimumvereisten, cyberbeveiligingscertificering van producten en diensten, monitoring, rapportage en crisisbeheer. Deze NCCS poogt een definitie te geven van de rollen en verantwoordelijkheden van de verschillende belanghebbenden voor elke activiteit.

Het omvat alle entiteiten die opwekking, transmissie, distributie, aggregatie, vraagrespons, energieopslag, levering of aankoop van elektriciteit, commerciële, technische of onderhoudsfuncties uitvoeren, ongeacht de omvang. Onduidelijk is of dit alleen partijen betreft die betrokken zijn bij grensoverschrijdende elektriciteitsstromen.

Het voorstel is in een afrondende fase, maar het is onduidelijk wat de ingangsdatum zal worden.

3.4. Conclusie: cybersecurity-eisen nemen toe voor de hele sector

De Europese Commissie ontwikkelt in de komende jaren nieuwe cybersecurity-eisen voor de lidstaten om de digitale veiligheid te verbeteren. Dit houdt in dat bedrijven en organisaties, ook in de energiesector, strengere beveiligingsmaatregelen moeten treffen om zich te beschermen tegen cyberaanvallen en datalekken.

Deze nieuwe richtlijnen vereisen dat de lidstaten een nationaal kader opzetten om te zorgen voor een hoger niveau van cyberbeveiliging. Daarnaast moeten bedrijven werkzaam in de energiesector technische en organisatorische maatregelen nemen om de risico's van cyberaanvallen te minimaliseren en de veiligheid van hun systemen te waarborgen.

Voor de energiesector betekent dit dat partijen meer moeten investeren in beveiliging van hun systemen en infrastructuren om zo de kritieke infrastructuur van Nederland te beschermen. Bovendien moeten zij snel reageren op incidenten en deze melden aan de relevante autoriteiten om de schade zoveel mogelijk te beperken.

[10] *Nynke Brouwer & Minke Reijneveld (2023). De ontwikkeling van cyberveiligheid in Europa. Voorstel voor de Cyber Resilience Act. Nederlands Juristenblad.*

Hoofdstuk 4

Integrale aanpak nodig

4.1. Bouwstenen integrale aanpak

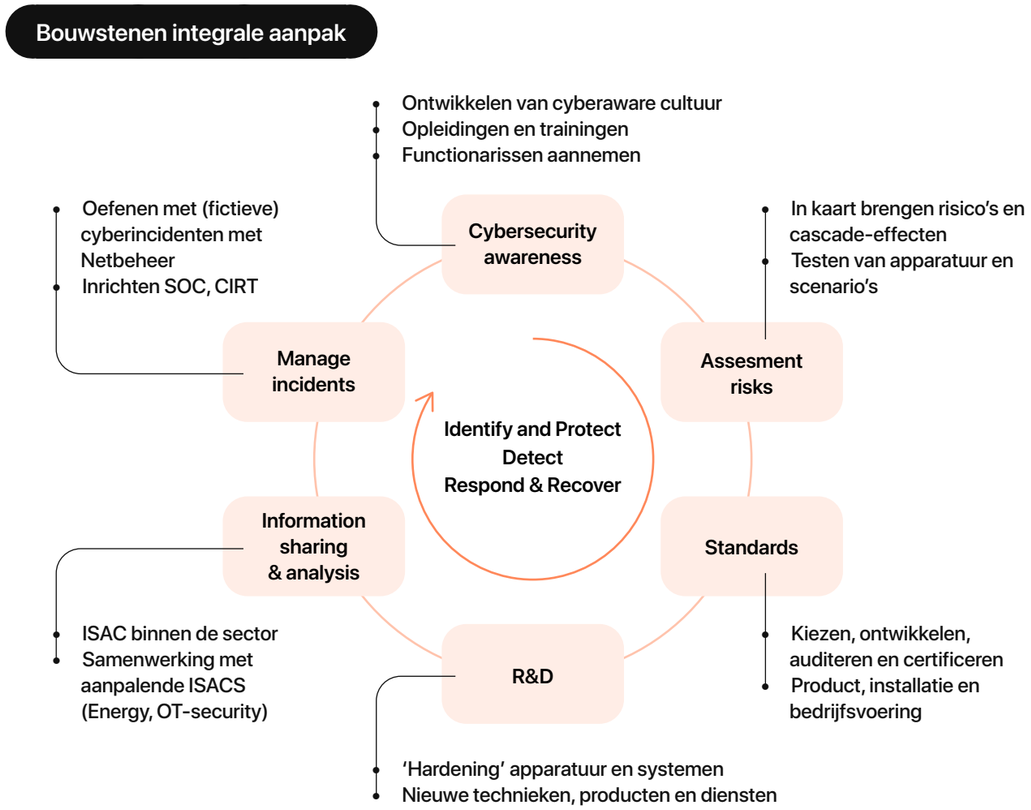
Tijdens de interviews zijn door diverse suggesties naar voren gekomen voor verbetering van de cybersecurity in de solarsector. Een analyse van deze suggesties leidde tot een logische clustering tot een integrale aanpak (figuur 4.1), die zich goed bleek te verhouden tot het NIST-framework[11] cybersecurity van het Amerikaanse National Institute of Standards and Technology. Vanuit het NIST-framework komen ook de vijf werkwoorden in het midden van de figuur, die bruikbaar zijn om het denkraam voor cybersecurity voldoende breed te krijgen. De woorden slaan op de verschillende fases waar maatregelen op gericht kunnen zijn. Dit toepassend op de cyberuitdagingen van de solarsector kan gedacht worden aan het *identificeren* van de te beschermen voorzieningen of assets. Zodat deze vervolgens met maatregelen kunnen worden *beschermd* tegen aanvallen. In de wetenschap dat 100% bescherming niet mogelijk zal blijken, is het ook verstandig om te investeren in detectie van aanvallen als deze zich voordoen, zodat erop *gereageerd* kan worden om schade te beperken. Na een aanval is het zaak om een PV-systeem veilig opnieuw online te brengen: *herstellen*.

4.1.1. Cybersecurity awareness

Het bewustzijn van cybersecurity is duidelijk groeiend in de solarsector. In de interviews gaven vrijwel alle gesproken partijen aan dat ze de cyberdreiging serieus nemen, en zich ontwikkelen richting een meer cyberweerbare organisatie.

[10] *Nynke Brouwer & Minke Reijneveld (2023). De ontwikkeling van cyberveiligheid in Europa. Voorstel voor de Cyber Resilience Act. Nederlands Juristenblad.*

[11] *Cybersecurity Framework | NIST*



Figuur 4.1: *Bouwstenen integrale aanpak, geïnspireerd op het NIST framework.*

Bestaande ontwikkelingen:

- Vermeldenswaardig is in dit kader het project 'Cyberweerbaarheid Electrische Installatiebedrijven' dat branchevereniging Techniek Nederland uitvoert samen met Cybersecuritybedrijven ThreadStone en Hudson Cybertec. In een tweejarig programma wordt gewerkt aan het verbeteren van de bewustwording, van het vakmanschap en van de kwaliteit van de installatiebedrijven met het oog op cybersecurity. Het ligt voor de hand om uitkomsten van dit project te vertalen naar trainingen toepassing in de solarsector, en deze breed te verspreiden.
- Branchevereniging Holland Solar heeft ook een belangrijk initiatief rond cybersecurity ontplooid: de oprichting van een werkgroep cybersecurity. Deze werkgroep, bestaande uit diverse organisaties als OEMs, O&M-partijen, projectontwikkelaars en assetmanagementpartijen, wil onder andere eenvoudig bruikbare checklists opstellen, en best practices beschrijven, waarmee branchegenoten de cybersecurity van hun installaties en systemen kunnen verbeteren. Diverse leden van de werkgroep toonden zich in individuele gesprekken bereid om bij te dragen aan het verbeteren van cybersecurity in de sector, en om daarin samen te werken met andere organisaties. De werkgroep lijkt een krachtige kern te zijn, waarmee de bewustwording in de sector versterkt kan worden.
- Solar Magazine tenslotte besteedde als vakblad al diverse malen aandacht aan het thema cybersecurity. Ook het kwartiermakerstraject werd tweemaal belicht in een publicatie.

Overzicht van de actoren en hun invloed op het cyberrisico van PV-systemen

	Wat gebeurt er al?	Aanbeveling?	Mogelijke coördinator	Mogelijke bijdragende organisaties
Cyber-security awareness	• Ontwikkeling trainingen installateurs Techniek Nederland • Artikelen vakbladen • Werkgroep Holland Solar	• Training en campagne specifiek voor Solar installateurs • Publicatie best practices en checklists (o.a. NIS2 basisbeveiligingseisen vertalen)	• Holland Solar	• Techniek Nederland, Solar Magazine, Digital Trust Center, onderwijsinstellingen, Rijksinspectie Digitale Infrastructuur
Assessment risks	• Onderzoek door RDI naar cyberrisico's IoT consumenten	• Risico's nader uitwerken: kans, effect, cascade-effecten • Verkennen mogelijkheid calls CS4NL te benutten • Apparatuur testen (nav standaarden)	• TNO	• Rijksinspectie Digitale Infrastructuur, TU Delft, Haagse Hogeschool, Netbeheer NL (werkgroep cybersecurity & crisismanagement), TKI Urban Energy, Cybersecuritybedrijven via Cyberveilig Nederland
Standards	• Diverse standaarden uit andere sectoren (mn telecom) • ISO27001	• Standaarden en normen kiezen en nader detailleren • Opbouwen certificeringen	• NEN	• Rijksinspectie Digitale Infrastructuur, Holland Solar, Techniek Nederland, Ministerie van EZK, Netbeheer NL (werkgroep cybersecurity & crisis-management)
R&D	• Data-diode • Innovatieprogramma CS4NL	• (Inherent) veilige producten zoals omvormers • Nieuwe wijzen van detecteren • Oplossingen voor oa installed base residentieel • Solar als 'use case' voor dcypher • Aandacht voor risico's van toenemende inzet van AI	• TKI Urban Energy	• OEMs, O&M-partijen, kennisinstellingen, dcypher
Information sharing	• ISAC Energy • ISAC OT	• Start met ISAC Solar NL, en verbindt deze met andere ISACs. Start klein en eenvoudig, en bouw langzaam uit • ISAC OEMs Europees	• Holland Solar	• Trader, O&M-partijen, Assetmanager, Digital Trust Center, Netbeheerders (TSO, DSO), • (+ OEMs)
Manage incidents	• Voor netbeheerders, grote OEMs en energie-bedrijven bestaan SOCs	• Ontwikkelen incident response plannen • Ontwikkelen oefening van een realistische cyberdreiging • Inrichten en delen CERT en SOC	• Netbeheer NL (werkgroep cybersecurity & crisis-management)	• Netbeheerders (TSO, DSO), 'vitale' energiebedrijven, Digital Trust Center, Rijksinspectie Digitale Infrastructuur

Figuur 4.2: *Mogelijke coördinatoren en bijdragende organisaties integrale aanpak*

Aanbevelingen:
De diverse initiatieven zijn te bekrachtigen door ze onderling te verbinden, en te versterken door een meerjarig plan te maken, waarin de diverse deelnemers bijdragen om reikwijdte en impact te vergroten richting de sector. Bijvoorbeeld met een campagne onder installateurs, waarin do's en don'ts op het gebied van cybersecurity onder de aandacht worden gebracht.

Logische actoren en vervolgstappen:
Naast de reeds beschreven partijen, lijkt het logisch om bijdragen te benutten van het Digital Trust Center en de Rijksinspectie Digitale Infrastructuur, en onderwijsinstellingen te betrekken die mensen opleiden voor de solarsector. Als coördinator voor deze bouwsteen zou mogelijk Holland Solar willen opstaan.

4.1.2. Assessment risks

Zoals beschreven in hoofdstuk 2, is het risico op verstoring van PV-systemen door cyberincidenten reëel. Alhoewel er op dit moment nog weinig casuïstiek voorhanden is van daadwerkelijke aanvallen, zijn vrijwel alle geïnterviewden het erover eens dat de risico's bestaan, niet verwaarloosbaar zijn en dat de risico's bovendien eerder toenemen dan afnemen. Het is tevens duidelijk geworden, dat er onvoldoende zicht is op de verhouding tussen de beschreven risico's in termen van kans en impact. Dat maakt dat het op dit moment onduidelijk is of het bijvoorbeeld meer zin heeft om te investeren in het mitigeren van de risico's bij residentiële installaties, of juist in de middelgrote en grootschalige systemen.

Bestaande ontwikkelingen:
In de gesprekken zijn diverse partijen geïdentificeerd die relevante aspecten onderzoeken van de cybersecurity uitdaging, zoals die voor de solarsector bestaat:

- Zo loopt er een onderzoek door RDI naar cyberrisico's van IoT[12]-apparaten bij consumenten thuis.
- De TU Delft pleegt onderzoek naar de kwetsbaarheden van het energienetwerk met het oog op cybersecurity in het 'Control room of the future'[13]

Aanbevelingen:
Ontwikkel een onderzoeksproject of -programma, dat de cyberdreiging nader verkent, en in perspectief plaatst. Maak van de gelegenheid gebruik om de diverse partijen met elkaar te verbinden: betrek zowel de solarsector, cybersecuritybedrijven, kennisinstellingen en overheid.

Als eerste aanzet voor onderzoeksvragen kan onderstaande worden gebruikt:

- Wat zijn voorstelbare aanvalsstrategieën van cybercriminelen, terroristen en statelijke actoren met betrekking tot de solarsector? Hier kan mogelijk een Red Teaming exercitie helpen.
- Waar bevinden zich de risicovolle legacy-systemen, die niet meer geüpdatet worden? Hoeveel zijn dat er? Waar zitten de grote vermogens?
- Wat zijn mogelijke cascade-effecten op de lokale energievoorziening, en verder in het netwerk (grid-instabiliteit en blackouts)?
- Hoeveel vermogen moet uitvallen om problemen te veroorzaken?
- Kwantificeer ordegroottes van kans, effect en cascade-effecten
- Verkennen mogelijkheid calls CS4NL te benutten.

Een ander perspectief op risico assessment dat genoemd werd in de gesprekken betreft het daadwerkelijk testen van apparatuur aan de hand van standaarden als die zijn vastgesteld (volgende bouwsteen). Er is behoefte in de markt aan een uitspraak over cyberveiligheid ten aanzien van specifieke apparatuur en dienstverleners. Op termijn zal er daarom ruimte zijn aan auditors en certificeringsorganisaties (zie ook 4.1.3 hieronder).

Logische actoren en vervolgstappen:
Diverse partijen hebben aangegeven bij te willen dragen aan een nadere risicoanalyse. Als eerste de kennisinstellingen TNO en de Haagse Hogeschool (lectoraat 'Network and Systems Engineering Cyber Security'). Ook lijkt het logisch om de TUDelft te betrekken. Verder hebben de RDI en de (werkgroep cybersecurity) van NetbeheerNL interesse getoond, net als de TKI Urban Energy. Passende cybersecuritybedrijven kunnen benaderd worden via CyberveiligNL.

Een logische vervolgstap kan de ontwikkeling zijn van een onderzoeksproject inspelend op de nieuwe calls van dcypher (CS4NL[14]). De eerste CS4NL TKI-call voor supply chain security lijkt al goed passend. Mogelijk kan deze activiteit door TNO gecoördineerd worden.

4.1.3. Standards

Veel partijen in de solarsector geven aan in de gesprekken dat het onduidelijk is hoe ze kunnen 'voldoen' aan de basisvereisten voor cybersecurity. Er is een grote behoefte aan standaarden die dermate concreet zijn, dat ze als 'checklists' kunnen worden afgevinkt. De verschillende beleidsmatige ontwikkelingen beschreven in hoofdstuk 4 dreigen uit te monden in een diverse set aan ambigue eisen, waar de sector beducht voor is.

Bestaande ontwikkelingen:

- Verschillende partijen verwijzen naar bruikbare standaarden uit andere sectoren, waaronder telecom. Met name de standaard ISO27001 (informatiebeveiliging) wordt genoemd als een bruikbaar startpunt.
- De werkgroep cybersecurity van Holland Solar beweegt met haar voornemen om een bruikbare checklist te maken richting een (sector)standaard.
- Verschillende partijen uit de vitale energie-infrastructuur hebben relevante kennis in huis, die gemobiliseerd kan worden voor de vaststelling van passende standaarden voor de solarsector. Onder andere de Nederlandse Energy ISAC, het Europese netwerk voor cybersecurity van de netbeheerders ENCS[15] en stichting Elaad zijn noemenswaardig in dit kader.

Aanbevelingen:
Het verdient een aanbeveling om een sectorstandaard aan te wijzen, of samen te stellen voor de eerste stappen richting meer volwassenheid ten aanzien van cybersecurity. Een eerste stap kan de opstelling zijn van een eenvoudige 'no regret' lijst, gesteund door de brancheverenigingen. Deze zou voldoende detail moeten bevatten om bruikbaar te zijn ook voor organisaties die nog niet hun eerste cybersecurity professional in dienst hebben, maar 'het erbij doen'.

Vervolgens kan dan gewerkt worden aan opvolgende niveaus van standaardisering, die idealiter in de wetgeving wordt vastgelegd. Daaruit kunnen dan certificerings- en auditeringsdiensten worden ontwikkeld.

Logische actoren en vervolgstappen:
Diverse partijen hebben aangegeven actief te (willen) zijn in het komen tot (sector)standaarden: brancheverenigingen Holland Solar en Techniek Nederland, RDI en de werkgroep cybersecurity van NetbeheerNL. Het ministerie van Economische Zaken en Klimaat is betrokken bij de Europese onderhandelingen over de wetteksten voor onder andere de NIS2.

Mogelijk kan de het Nederlands Normalisatie instituut NEN gevraagd worden om een commissie op te zetten om de benodigde standaarden te ontwikkelen met de geïnteresseerde partijen. Mogelijk kunnen partijen uit de vitale energie-infrastructuur betrokken worden via de Nederlandse Energy ISAC, en kunnen ENCS en stichting Elaad ook een bijdrage leveren.

4.1.4. R&D

Vanuit de gesprekken zijn een aantal suggesties en ontwikkelingen naar voren gekomen die onder de noemer 'research and development' passen:

Bestaande ontwikkelingen:

- Op het vlak van productontwikkeling gebeurt veel bij de OEMs, ook op het gebied van cybersecurity. Onder 'hardening' wordt het aanscherpen verstaan van apparatuur en platformen. Deze ontwikkeling zal met de komende wettelijke eisen vanuit de Europese Commissie verder worden gestimuleerd, wat zal leiden tot steeds veiliger producten en diensten.
- De cyberveiligheid van IoT-apparatuur is in de volle breedte een zorg. In dat licht zijn er nieuwe technieken in ontwikkeling voor bescherming, detectie en respons. Interessant is bijvoorbeeld de ontwikkeling

[12] *Internet of things*
[13] *TU Delft's Control Room of the Future makes power grid digitally resilient*
[14] *CS4NL · dcypher*
[15] *www.encs.eu*

van een data-diode[16], waarmee kan worden gegarandeerd dat dataverkeer maar in één richting plaatsvindt. Ook de toepassing van digital twins in IoT-devices is een interessante ontwikkeling: door het gedrag van bijvoorbeeld een omvormer steeds te vergelijken met een nauwkeurige digitale kopie van een normaal opererende omvormer, kunnen afwijkingen worden gedetecteerd[17].
- Het recent gelanceerde onderzoeksprogramma CS4NL (zie ook de aanbevelingen in paragraaf 4.1.2) biedt financiering voor onderzoek naar cybersecurity.

Aanbevelingen:
Oplossingen voor de cybersecurity-uitdagingen van IoT-apparatuur zal ook de weg naar de solarsector gaan vinden. Dit kan versneld worden door expliciet de verbinding te leggen met het cybersecurity-onderzoek en de solarsector als *use case* aan te bieden aan onderzoeksprojecten van universiteiten of onderzoeksinstellingen.

Onderzoeksonderwerpen die genoemd zijn in de gesprekken zijn:
- (Inherent) veilige producten zoals omvormers
- Nieuwe wijzen van detecteren van (voorbereidingen) op aanvallen
- Nieuwe oplossingen voor het 'retrofitten' van omvormers die niet meer geüpdatet worden (vooral in de residentiële setting, maar ook in de grootschaliger PV0systemen)
- Aandacht voor risico's van toenemende inzet van AI in energy managementsystemen

Logische actoren en vervolgstappen:
Voor de research-kant van R&D hebben zich met name de kennisinstellingen gemeld, waaronder de Haagse Hogeschool en TNO. Zeker ook de universiteiten hebben hier natuurlijk een bijdrage te leveren. De TKI Urban Energy en dcypher kunnen in het richten van de onderzoekslijnen en missies onderzoek en samenwerking rond cybersecurity van PV-systemen stimuleren.

Voor de *development*-kant van R&D zijn de OEMs en O&M-partijen primair aan zet, als het gaat om de 'hardening' en van hun producten en diensten.

Mogelijk kunnen de belangrijkste R&D-uitdagingen worden meegenomen in het onderzoeksproject dat zich zou kunnen vormen naar aanleiding van de aanbeveling uit paragraaf 4.1.2 Het definiëren van de onderzoeksuitdagingen lijkt een taak waarin de TKI Urban Energy voorop kan gaan.

4.1.5. Information Sharing

Bij de opdrachtverstrekking van het kwartiermakerstraject, is het concept van een Information Sharing and Analysis Centre (ISAC) al meegegeven. In deze overlegvorm over cybersecurity wisselen organisaties uit dezelfde sector gevoelige en vertrouwelijke informatie uit over incidenten, dreigingen, kwetsbaarheden en maatregelen. Door over de ervaringen te praten wordt van elkaar geleerd.

Bestaande ontwikkelingen:
- Er bestaan in Nederland voor diverse sectoren ISACs. Onder andere in de zorg, rail, voedingsmiddelenindustrie en telecom, en ook in het energiedomein. De Nederlandse overheid voert een stimulerend beleid om meer ISACs te laten ontstaan[18].
- In opdracht van het Digital Trust Center (DTC) voert TNO een onderzoek uit naar de bouwstenen voor een succesvolle ISAC. Gedurende het kwartiermakerstraject is met deze onderzoekers samengewerkt
- De Nederlandse Energy ISAC bestaat (met name) uit een vertegenwoordiging van netbeheerders en energiebedrijven en staat in verbinding met de Europese Energy ISAC. Een expliciete vertegenwoordiging van de solarsector zit nog niet aan tafel. Wel nemen grote energiebedrijven deel, die ook solar-activiteiten hebben.
- Er is ook een ISAC in oprichting dwars op de sectoren staat: de ISAC OT (Operationele Technologie).

Uitvoeringsvarianten integrale aanpak

Zonder enige vorm van coördinatie, zal een deel van bovenstaande activiteiten uit de bouwstenen zeker tot stand komen. Veel van de aanbevelingen zijn immers een doorvertaling van reeds ontplooide activiteiten. Echter, door enige vorm van coördinatie expliciet aan te brengen, kan verwacht worden dat meer voortgang kan worden bereikt in dezelfde tijd ten aanzien van de cyberweerbaarheid van de sector.

Zelforganisatie als minimale coördinatievorm

De minimale vorm van coördinatie die vanuit het kwartiermakerschap wordt aanbevolen, betreft die van 'zelforganisatie', waarbij elke bouwsteen door een eigen 'trekker' wordt gecoördineerd (zie tabel 5.1). Deze partij betrekt de andere organisaties, en organiseert een aantal keer per jaar een bijeenkomst.

In deze bijeenkomsten kan een jaarplan worden opgesteld, en kan de voortgang ten aanzien van dit jaarplan worden gemonitord. Ook kunnen in dit overleg gezamenlijk volgende stappen bepaald worden, en kunnen coalities gesloten worden voor specifieke activiteiten. Het voorzitterschap van deze afstemmings-overleggen kan door een vaste of roulerende partij worden ingevuld.

Aanbevolen: programmamanager

Als de integrale aanpak ondersteund wordt door een programmamanager kan naar verwachting een beter resultaat worden behaald. Deze persoon kan de trekkers van de bouwstenen ondersteunen, functioneren als voorzitter van de overleggen, verbinding leggen tussen bouwstenen, en achterblijvende onderdelen aanjagen. Ook kan deze persoon actief zoeken naar financiering en kansen om tot meer impact te komen en de totale aanpak representeren in bijeenkomsten. Voor financiering van zo'n rol kan gekeken worden naar de brancheorganisatie Holland Solar en naar de overheid omdat het niet alleen een sectorale uitdaging betreft maar ook een maatschappelijke. Ook netbeheerders kunnen mogelijk een bijdrage leveren aangezien het cyberweerbaar maken van de solarsector zeker ook in het belang van de netten is.

[16] *Factsheet Data Diode (securitydelta.nl)*
[17] *Digital Twin for Self-Security of Smart Inverters | IEEE Conference Publication | IEEE Xplore*
[18] *Samenwerking in een ISAC | Start een samenwerking | Nationaal Cyber Security Centrum (ncsc.nl)*

Aanbevelingen:
In de gesprekken tijdens het kwartiermakerstraject is vastgesteld dat er bij verschillende partijen interesse bestaat om deel te nemen. Er lijkt voldoende animo in de sector om kleinschalig te beginnen met de start van een ISAC voor de solarsector. Het lijkt vervolgens aanbevelingswaardig om verbindingen te leggen met andere ISACs rond gedistribueerde energie (wind, laadpaleninfrastructuur) en met de Energy ISAC.

Logische actoren en vervolgstappen:
Logische partijen om te betrekken zijn: Trader, O&M, Assetmanager, DTC, Netbeheerder (TSO / DSO) (+ OEM) en Holland Solar.

4.1.6. Manage incidents

De laatste bouwsteen betreft een set aan activiteiten die mogelijkerwijs wat verder in de toekomst kunnen worden opgepakt: het opbouwen en organiseren van capaciteiten om incidenten goed te kunnen afhandelen.

Bestaande ontwikkelingen:
In de 'vitale infrastructuur' zijn Cyber Emergency Response Teams (CERT's) en Security Operation Centres (SOC's) gemeengoed. Het betreft gespecialiseerde teams van professionals die continu digitale infrastructuren monitoren en klaarstaan om in te grijpen bij een incident. Netbeheerders, grote OEMs en energiebedrijven hebben dit soort arrangementen operationeel. Ook wordt er met een zekere regelmaat geoefend op incidenten in verschillende schaalniveaus. In de solarsector is hier vooralsnog geen sprake van.

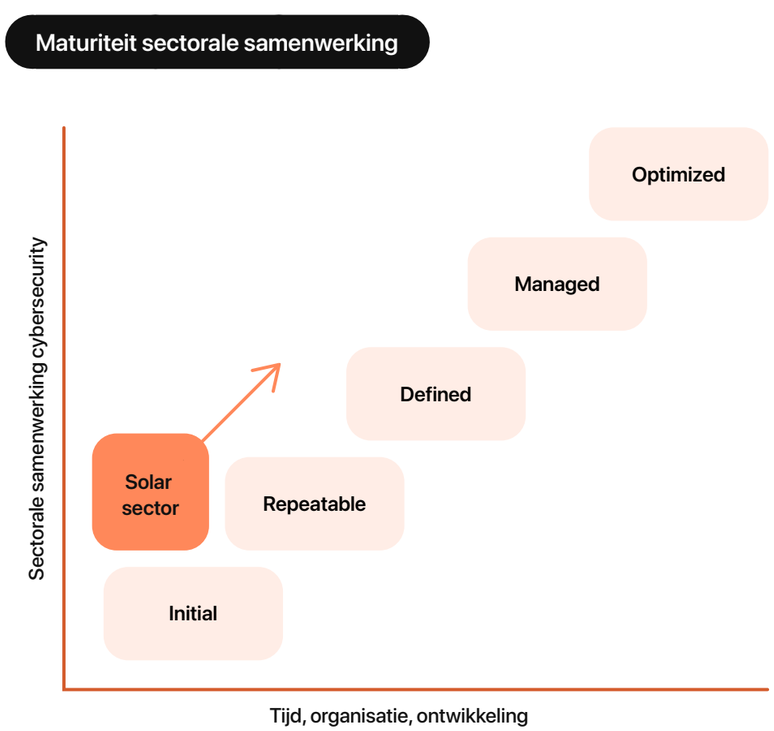
Aanbevelingen:
Het lijkt logisch om ook voor de solarsector toe te werken naar incident response plannen op organisatie- en sectorniveau. Zeker omdat er veel kleinere partijen een belangrijke rol spelen in de sector, lijkt het interessant om te gaan verkennen of dit soort dienstverlening niet centraal (en gedeeld) kan worden aangeboden.

Op termijn kan dan ook toegewerkt worden naar het gezamenlijk oefenen van een realistische cyberdreiging. Dit hangt dan ook samen met de bouwsteen Assessment Risks.

Logische actoren en vervolgstappen:
Het lijkt voor de hand te liggen dat partijen met bestaande SOC en CERT-infrastructuren de activiteiten uitbreiden naar de solarsector: Netbeheerders (TSO / DSO) en 'vitale' energiebedrijven kunnen hier vooropgaan, met ondersteuning van DTC en RDI. Als een Solar-ISAC is opgericht, lijkt het ook logisch deze te betrekken.

4.2. Conclusie: start gemaakt, nu samenwerking uitbouwen

Tijdens het kwartiermakerstraject zijn veel partijen aangetroffen met voldoende bewustzijn ten aanzien van de cybersecurity-uitdaging van de sector, die zich bovendien bereid tonen om in samenwerkingen te komen tot vooruitgang. De hierboven beschreven initiatieven tonen aan dat er ook al zeker samengewerkt wordt. Het betreft echter relatief kleine initiatieven, die ook afhankelijk lijken van individuen. Het is de uitdaging om de initiatieven te versterken door ze minder persoonsafhankelijk te maken, te verbinden aan elkaar en met additionele initiatieven, en door toe te werken naar een programmatische samenhang. Daarmee kan de volwassenheid van de sectorale samenwerking rond cybersecurity in de komende jaren verbeteren (figuur 4.3).



Figuur 4.3: *Maturiteit sectorale samenwerking – geïnspireerd op het NIST framework*

Meer lezen?

- Solar Builder | Solar inverter cyber security strategy that improves system monitoring
- Sunspec Alliance | Sunspec DER Cybersecurity videos
- Solar Industry | DOE NREL Seeking Cybersecurity Solutions for Renewable Energy
- Hack Talk | Hack the Grid
- Renewable Energy World | Taking on solar's cybersecurity challenges
- US Department of Energy | Solar Cybersecurity
- Digital Trust Center | Cyberweerbaarheid installatiebranche
- Digital Trust Center | Cyber Chain Resilience Consortium
- RDI | Onderzoek storingsproblematiek en cyberveiligheid omvormers voor zonnepanelen

Colofon

Het kwartiermakerschap cybersecurity & zonPV is uitgevoerd door Christiaan van den Berg (TNO) in opdracht van de RVO en Topsector Energie (programma Digitalisering en TKI Urban Energy). De rapportage is opgesteld door Christiaan van den Berg en Marc Koetse (TNO).

Redactie
Soe van Dijk (Topsector Energie)

Vormgeving
Vrije Stijl

Voor meer informatie over deze publicatie kun je contact opnemen met de Topsector Energie.

E-mail
info@tki-urbanenergy.nl
digitalisering@topsectorenergie.nl

Website
www.topsectorenergie.nl

Lees meer op onze website →