CyberZon

Een verkenning naar het verbeteren van de cyberweerbaarheid van de Solar-sector in Nederland

Christiaan van den Berg, Marc Koetse

Inhoudsopgave

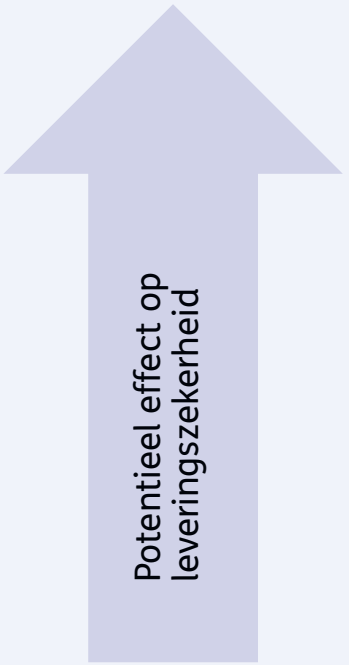
Aanleiding - kwartiermaken

- In opdracht* van RVO en Topsector Energie: onderzoek kansen voor samenwerking tbv verbeteren cybersecurity Solar-sector
- Activiteiten:
  - In kaart brengen van het actorlandschap
  - Gesprekken met zo'n 30 partijen
  - In kaart brengen dreigingsscenario's
  - In kaart brengen juridische context
  - Inventariseren behoeften, ideeën en initiatieven om de cyberweerbaarheid van de solarsector te verbeteren. Specifiek: *connected devices*

* https://www.topsectorenergie.nl/nieuws/verkenning-gestart-naar-samenwerking-cybersecurity-binnen-energiesector

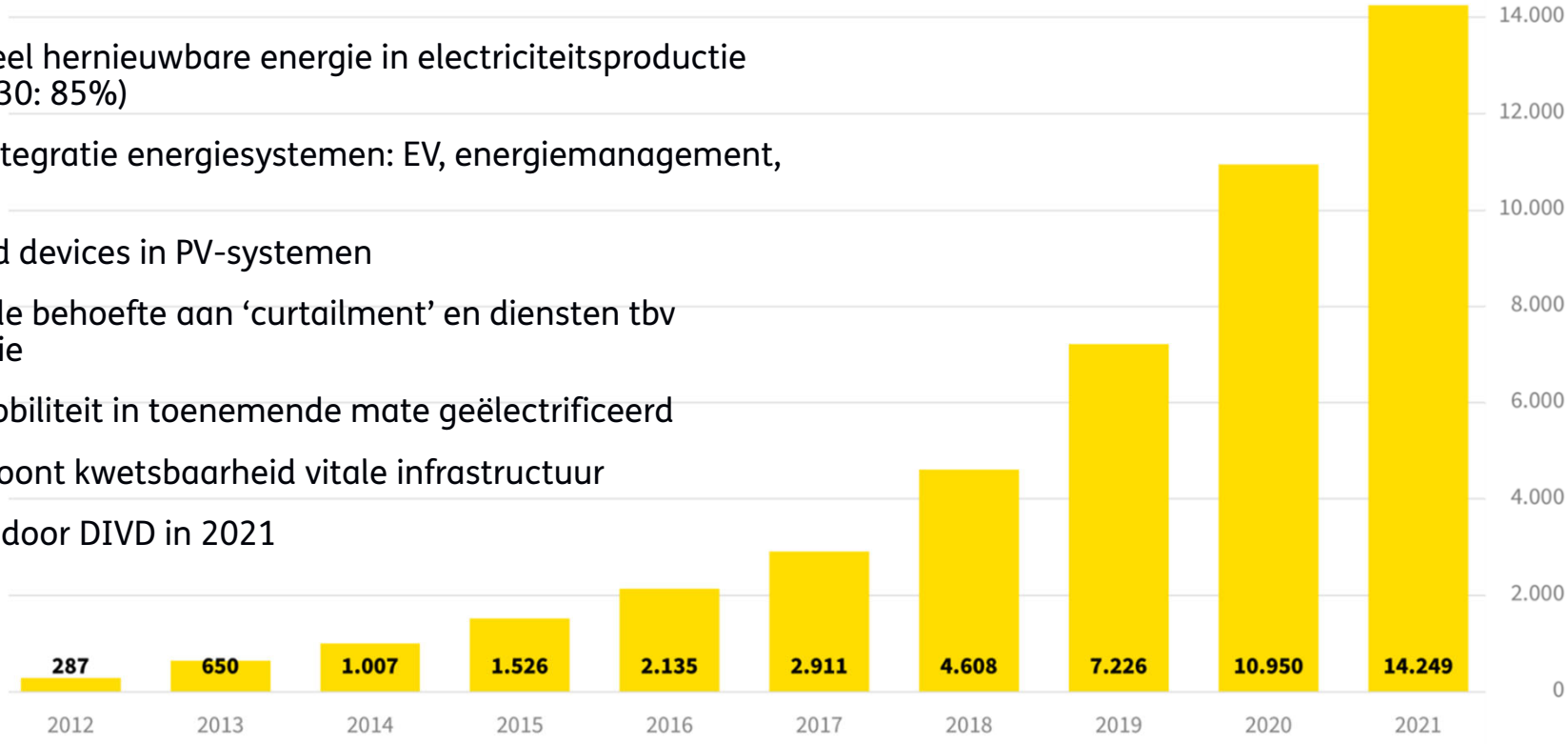
Cybersecurityrisico's PV-systemen

Hack connected device PV met controle	• Aan- en uitschakelen, instellingen wijzigen • Uitval productie PV-systeem • Gridinstabiliteit en blackouts
Hack via connected device PV	• IoT als botnet • Doorstappen in lokaal netwerk • Dynamic pricing beïnvloeden
Hack van data	• Stelen gebruikersdata



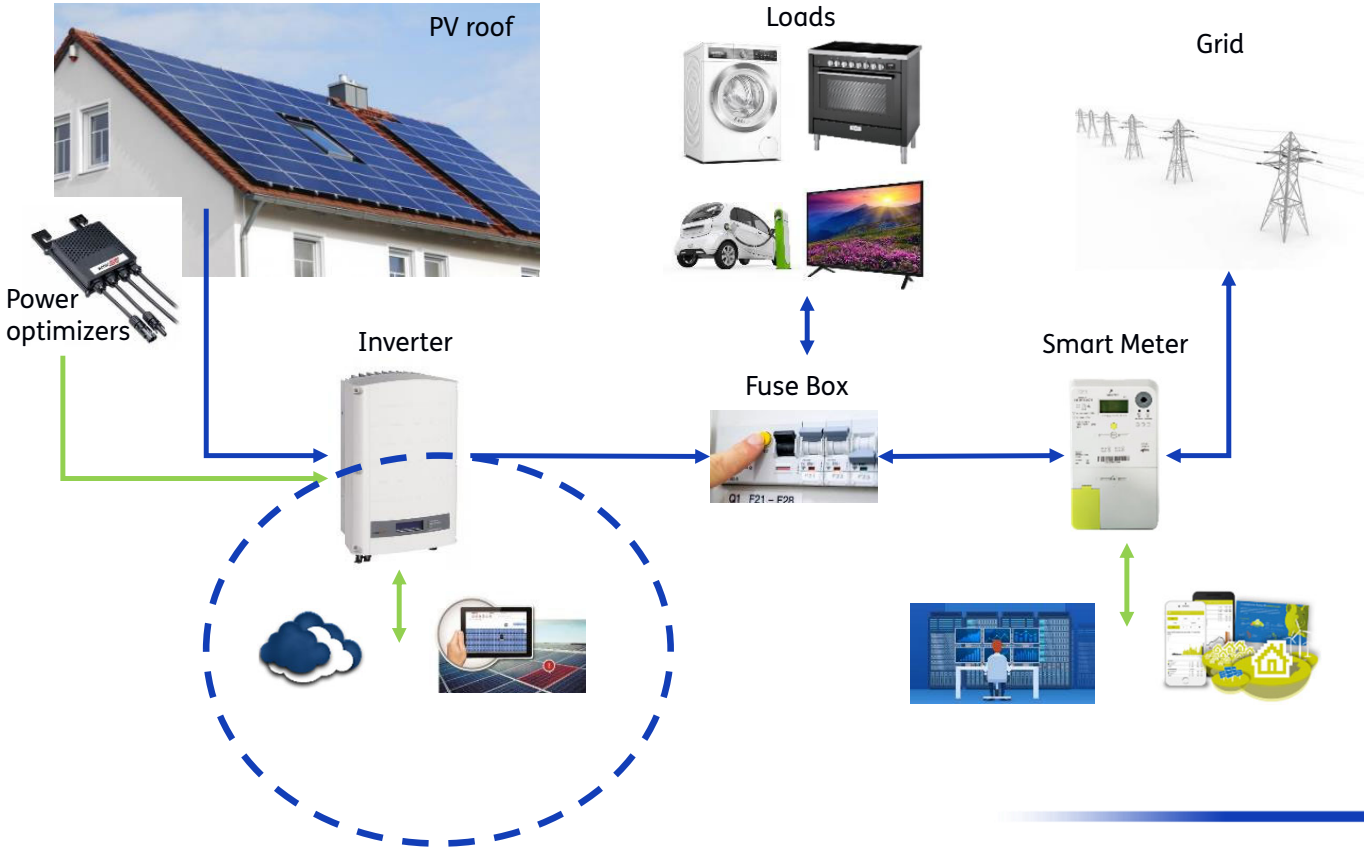
Signalen tot zorg

- Groeiend aandeel hernieuwbare energie in electriciteitsproductie (raming PBL 2030: 85%)
- Toenemende integratie energiesystemen: EV, energiemanagement, batterijen
- Meer connected devices in PV-systemen
  - Toenemende behoefte aan ‘curtailment’ en diensten tbv netcongestie
- Industrie en mobiliteit in toenemende mate geëlectrificeerd
- Nordstream 1 toont kwetsbaarheid vitale infrastructuur
- Solarman hack door DIVD in 2021

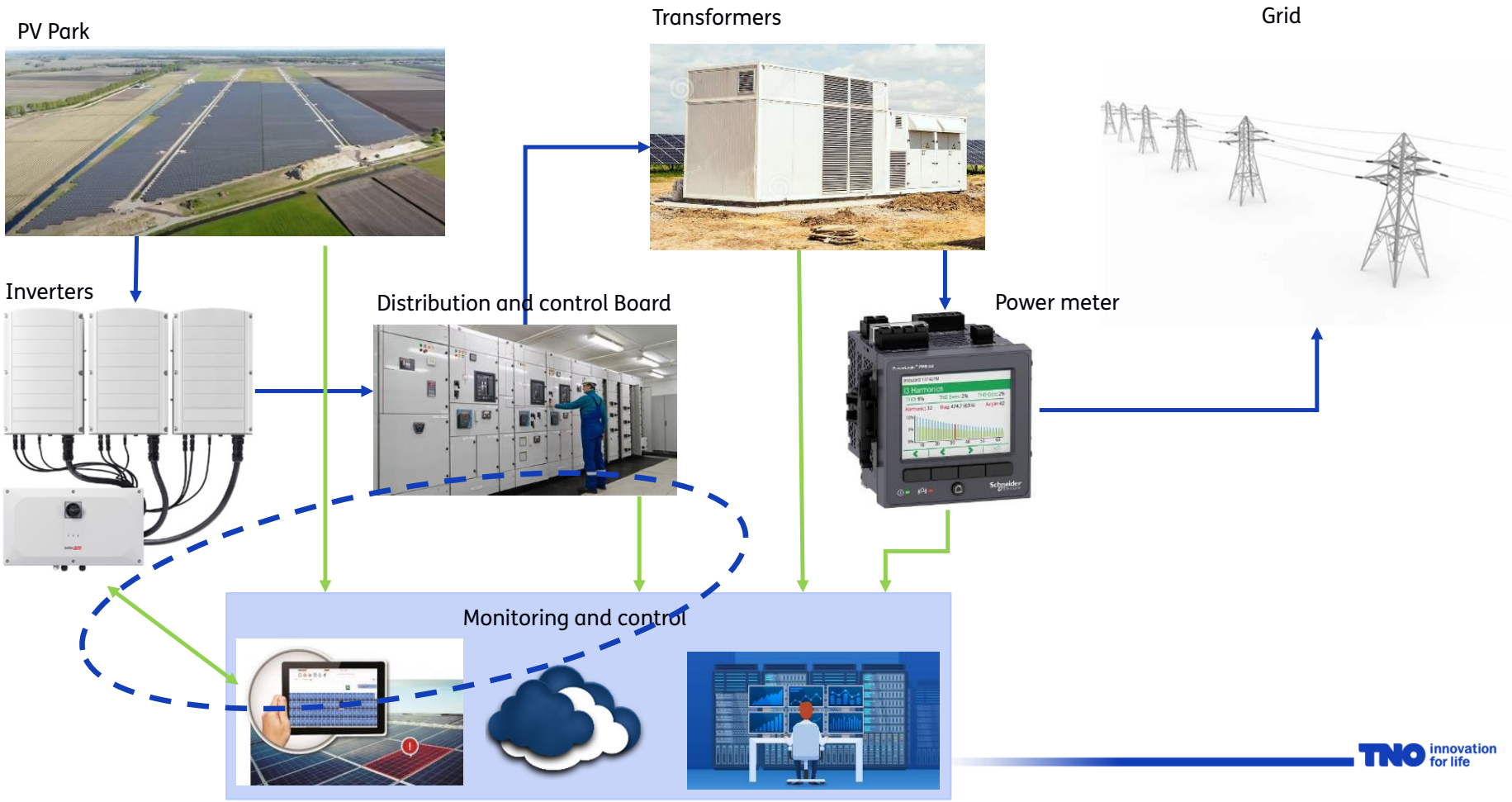


Cumulatief vermogen zonnepaneelinstallaties Nederland (MWP) - Solar Magazine

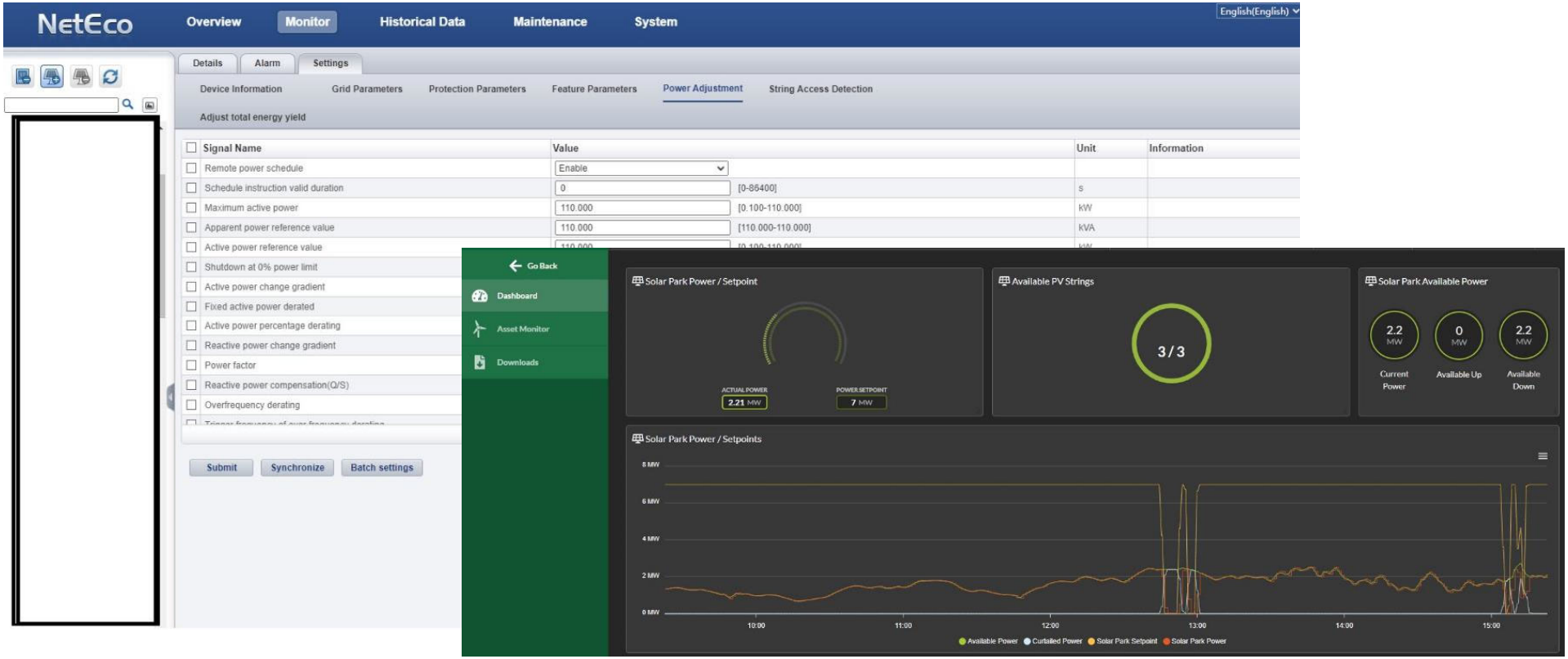
Impressie residentieel PV-systeem



Impressie grootschalig PV-systeem



Impressie portalen PV-systemen



Hack van PV-systemen kan grote gevolgen hebben

- Focus op leveringszekerheid: controle over aan/uit en instellingen van PV-systemen
- Niet alleen de omvormers
- Trend is: meer interconnectiviteit tussen systemen, meer connected devices in PV-systemen

- Risico op hacks bestaat, maar we weten niet precies hoe groot de risico's zijn (kans en impact)
- Specifiek legacy systemen zonder service vormen uitdaging
- Mogelijke cascade-effecten: lokale energievoorziening versus gridinstabiliteit en blackouts

Speelveldanalyse - rollen

• 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 • Netbeheerders (TSO / DSO)	Indirecte invloed
• Kennisinstelling • Overheid – wetgever / handhaver / toezichthouder	Indirecte invloed

Speelveldanalyse

- Spelers vervullen meerdere rollen
- ‘Aanvalsoppervlak’ breder dan omvormers (OEM’s)
- Zeer divers beeld van de actoren:
  - Grote en kleine partijen
  - Groot verschil in ‘maturiteit’ cybersecurity: vitale partijen al volwassen, andere partijen zetten eerste stappen
  - Diverse (jonge) spelers met eigen hard- en software

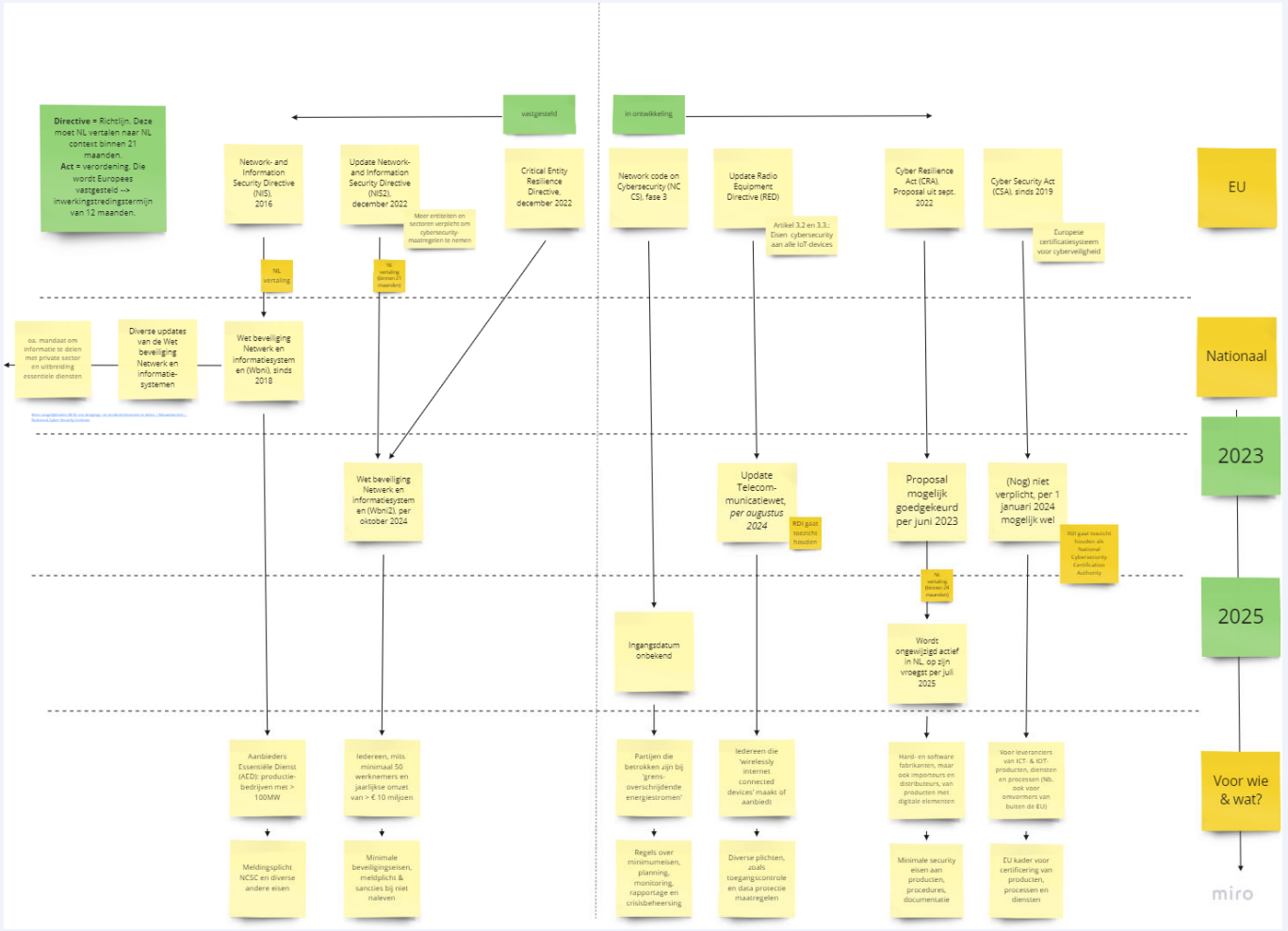
- Willingnes:
  - Grote bereidheid om bij te dragen aan verbeteren cybersecurity
  - Ook: grote bereidheidheid om samen te werken

  → **Benutten bereidheid: versterken samenwerking**

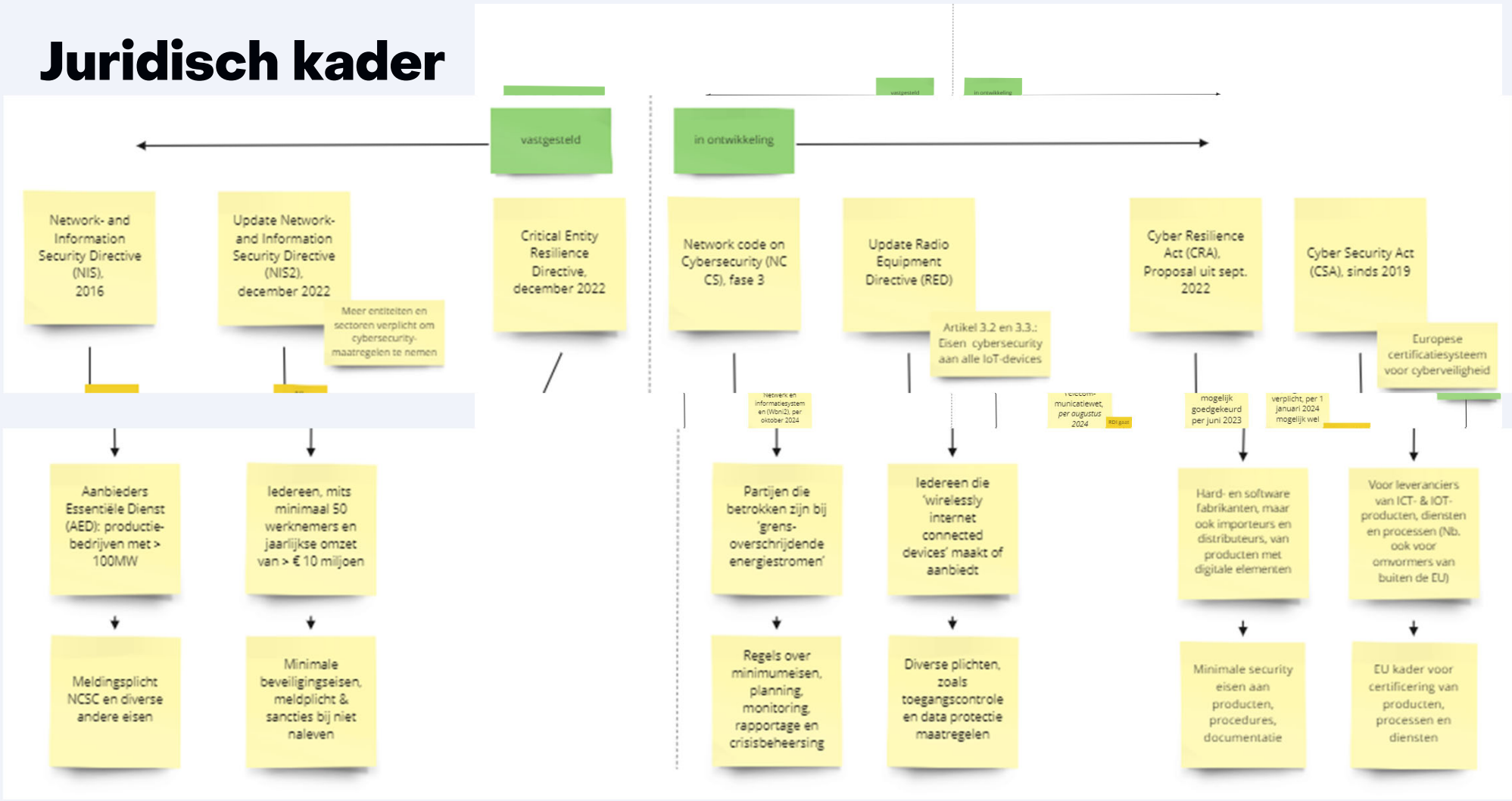
Juridisch kader

In de komende jaren richting 2025:

- Toenemende cybersecurity-eisen voor de sector vanuit mn EC
- Minimumeisen aan producten, werkwijzen, toegangscontrole en dataprotectie
- Meldingsplicht incidenten, zorgplicht richting klanten, aansprakelijkheid
- Toezicht wordt uitgebreid
- Zal leiden tot standaarden, audits en certificeringen

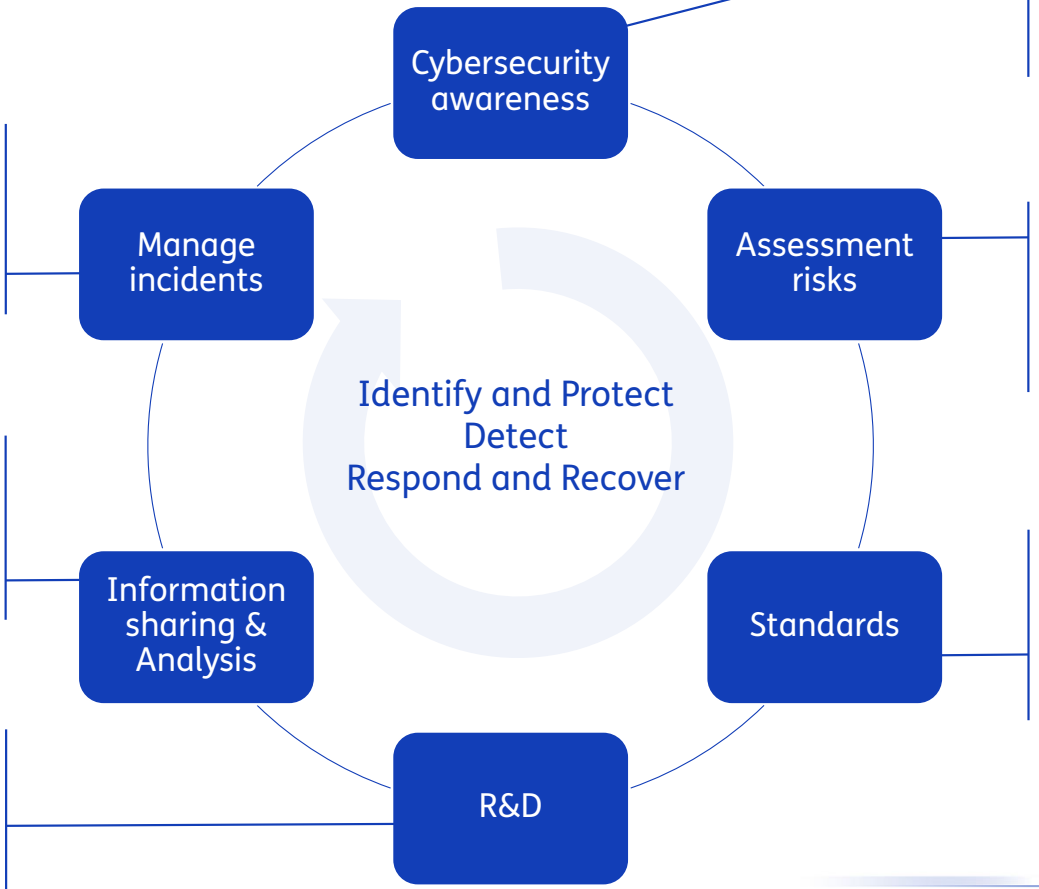


Juridisch kader



Naar een integrale aanpak

Geïnspireerd op het NIST framework



- Ontwikkelen van cyberaware cultuur
- Opleidingen en trainingen
- Functionarissen aannemen

- In kaart brengen risico's en cascade-effecten
- Testen van apparatuur en scenario's

- Kiezen, ontwikkelen, auditeren en certificeren
- Product, installatie en bedrijfsvoering

- 'Hardening' apparatuur en systemen
- Nieuwe technieken, producten en diensten

- ISAC binnen de sector
- Samenwerking met aanpalende ISACS (Energy, OT-security)

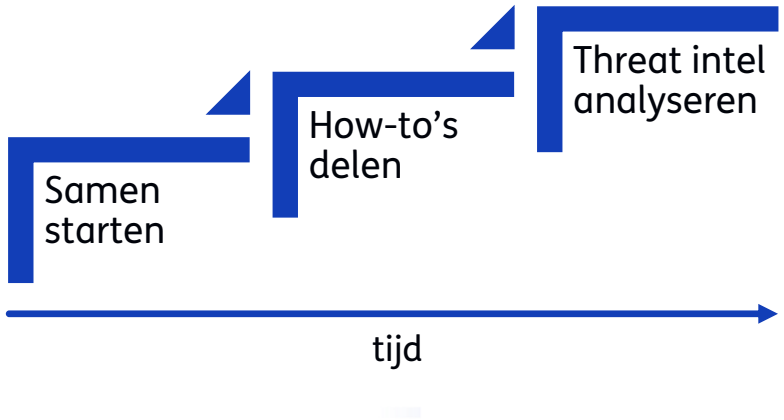
- Oefenen met (fictieve) cyberincidenten met Netbeheer
- Inrichten SOC, CIRT

Integrale aanpak nader uitgewerkt

	Wat gebeurt er al?	Aanbeveling	Wie
Cybersecurity awareness	• Ontwikkeling trainingen installateurs Techniek Nederland • Artikelen vakbladen • Werkgroep Holland Solar	• Training en campagne specifiek voor Solar installateurs • Publicatie best practices en check-lists (oa NIS2 basisbeveiligingseisen vertalen)	• Holland Solar, Techniek Nederland, Solar Magazine, DTC, onderwijsinstellingen
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)	• RDI, TNO, TUDelft, Haagse Hogeschool, (werkgroep cybersecurity) NetbeheerNL
Standards	• Diverse standaarden uit andere sectoren (mn telecom) • ISO27001	• Standaarden en normen kiezen en nader detailleren • Opbouwen certificeringen	• NEN, RDI, Holland Solar, Techniek Nederland, minEZK, (werkgroep cybersecurity) NetbeheerNL, ENCS
R&D	• Data-diode • Onderzoeksprogramma 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, 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	• Trader, O&M, Assetmanager, DTC, Netbeheerder (TSO / DSO) (+ OEM)
Manage incidents	• Voor netbeheerders, grote OEM's en energiebedrijven bestaan SOCs	• Ontwikkelen incident response plannen • Ontwikkelen oefening van een realistische cyberdreiging • Inrichten / delen CERT en SOC	• Netbeheerders (TSO / DSO), 'vitale' energiebedrijven, DTC

Kansen voor een ISAC-structuur

- Enthousiasme bij iig 5 gesproken partijen voor ‘peer-to-peer’ kennisdeling over cybersecurity. Verwachting is: er zijn er nog 2-4 te vinden.
  - Rond praktische tips & tricks
  - (Later) ook cyber threat intelligence samen analiseren
- Aandachtspunt: grote verschillen in maturiteit



Start gemaakt: samenwerking uitbouwen

Geïnspireerd op het NIST framework