

CyberZon

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

Christiaan van den Berg, Marc Koetse



Inhoudsopgave



1. Aanleiding
2. Cyberrisico's PV-systemen
3. Speelveldanalyse
4. Wettelijke en juridische ontwikkelingen
5. Integrale aanpak nader uitgewerkt
6. Uitgelicht: kansen voor een ISAC-structuur
7. Versterken structurele samenwerking

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

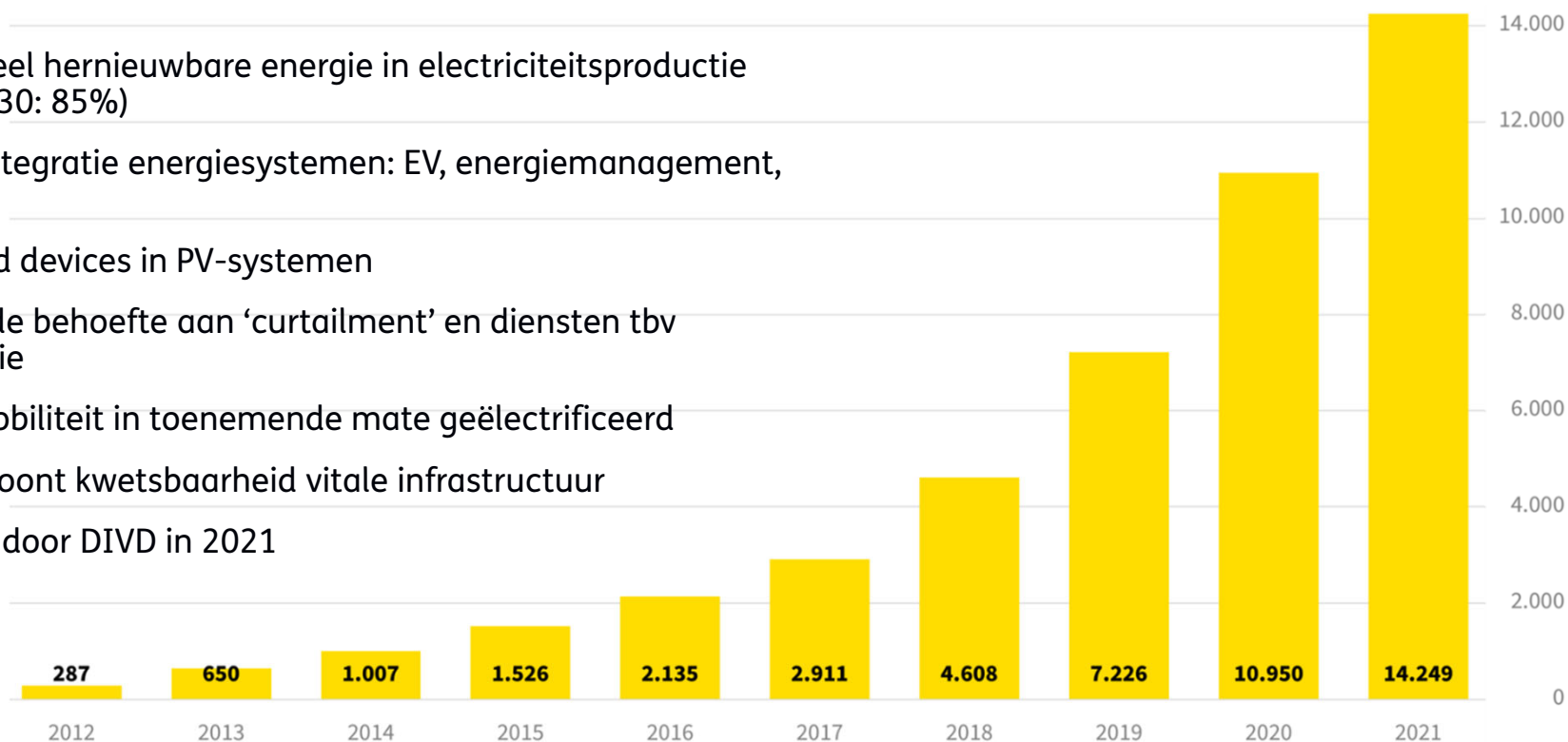
Hack van data

- Stelen gebruikersdata

Potentieel effect op leveringszekerheid

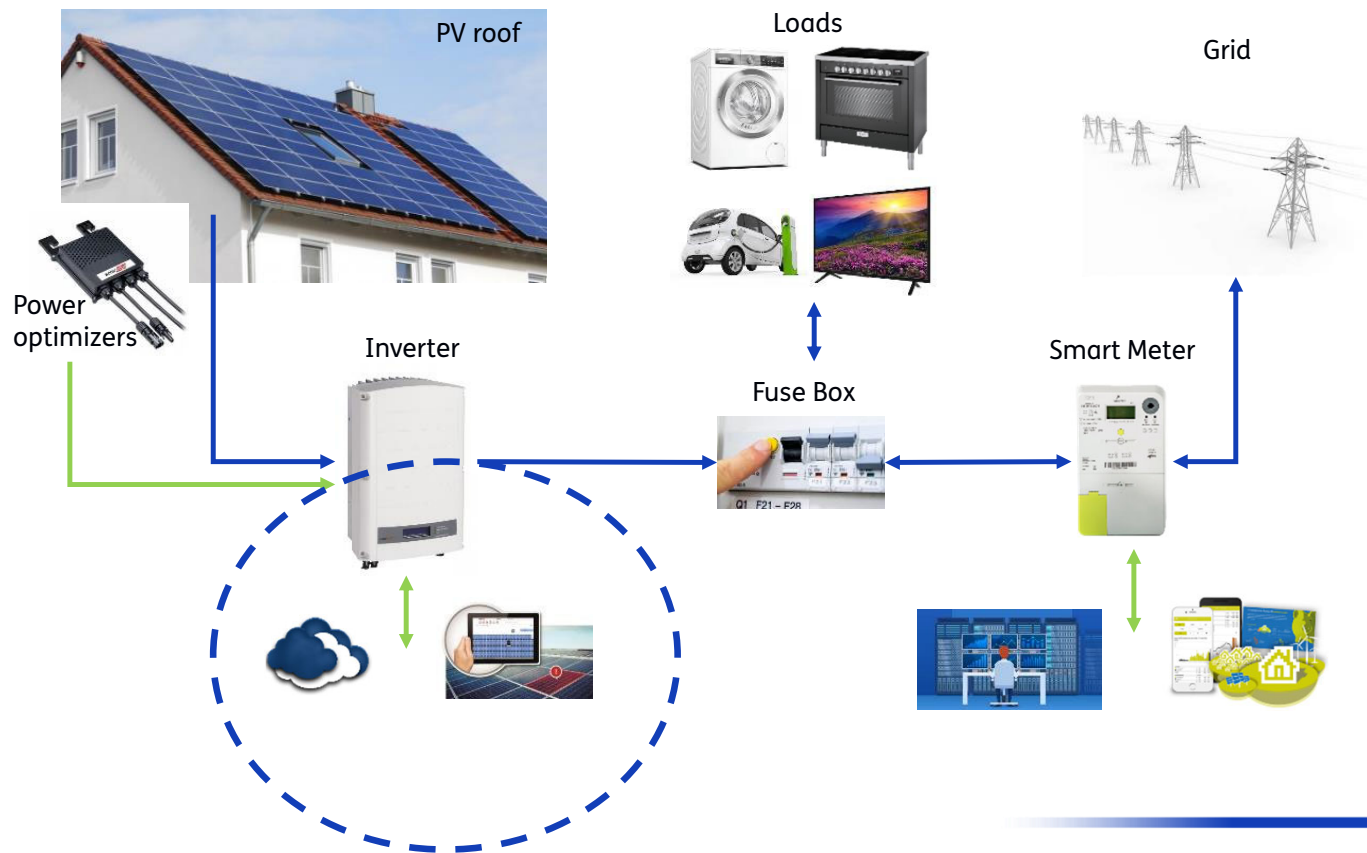
Signalen tot zorg

- 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

PV Park



Transformers



Grid



Inverters



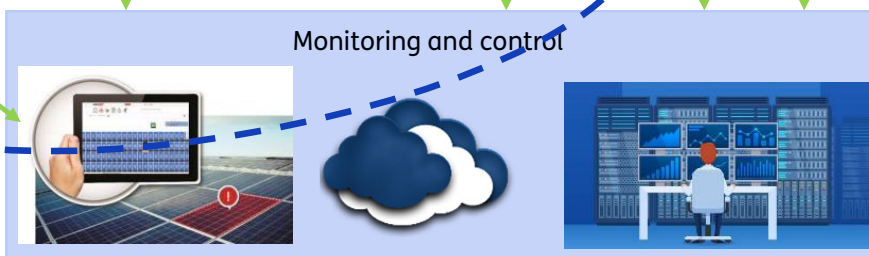
Distribution and control Board



Power meter



Monitoring and control



Impressie portalen PV-systemen

The screenshot displays the NetEco monitoring portal interface, which is divided into several sections:

- Navigation Bar:** Includes 'NetEco' logo, 'Overview', 'Monitor' (active), 'Historical Data', 'Maintenance', and 'System'. A language dropdown is set to 'English(English)'.
- Sub-headers:** 'Details', 'Alarm', and 'Settings' are visible, with 'Settings' being the active tab.
- Configuration Tabs:** 'Device Information', 'Grid Parameters', 'Protection Parameters', 'Feature Parameters', 'Power Adjustment' (active), and 'String Access Detection'.
- Configuration Table:** A table for adjusting total energy yield with columns for 'Signal Name', 'Value', 'Unit', and 'Information'.

Signal Name	Value	Unit	Information
Remote power schedule	Enable		
Schedule instruction valid duration	0	s	[0-86400]
Maximum active power	110.000	KW	[0.100-110.000]
Apparent power reference value	110.000	KVA	[110.000-110.000]
Active power reference value	110.000	KW	[0.100-110.000]
Shutdown at 0% power limit			
Active power change gradient			
Fixed active power derated			
Active power percentage derating			
Reactive power change gradient			
Power factor			
Reactive power compensation(Q/S)			
Overfrequency derating			
Tripping frequency of overfrequency derating			
- Left Sidebar:** A green sidebar with 'Go Back', 'Dashboard', 'Asset Monitor', and 'Downloads' options.
- Dashboard Widgets:**
 - 'Solar Park Power / Setpoint' showing 'ACTUAL POWER' at 2.21 MW and 'POWER SETPOINT' at 7 MW.
 - 'Available PV Strings' showing a gauge for 3/3 strings.
 - 'Solar Park Available Power' showing three gauges: 'Current Power' (2.2 MW), 'Available Up' (0 MW), and 'Available Down' (2.2 MW).
 - 'Solar Park Power / Setpoints' line chart showing power levels from 10:00 to 15:00. The chart includes data for Available Power, Curtailed Power, Solar Park Setpoint, and Solar Park Power.
- Buttons:** 'Submit', 'Synchronize', and 'Batch settings' are located at the bottom of the configuration section.

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

<ul style="list-style-type: none">• Original Equipment Manufacturer (OEM)• Trader (oa Congestion Service Provider en Balance Service Providers)• Operation & maintenance (O&M)• Assetmanagement• Engineering, procurement & construction (EPC)	Directe invloed
<ul style="list-style-type: none">• Projectontwikkelaar• IT-serviceprovider• Eigenaar• Netbeheerders (TSO / DSO)	Indirecte invloed
<ul style="list-style-type: none">• Kennisinstelling• Overheid – wetgever / handhaver / toezichthouder	Indirecte invloed

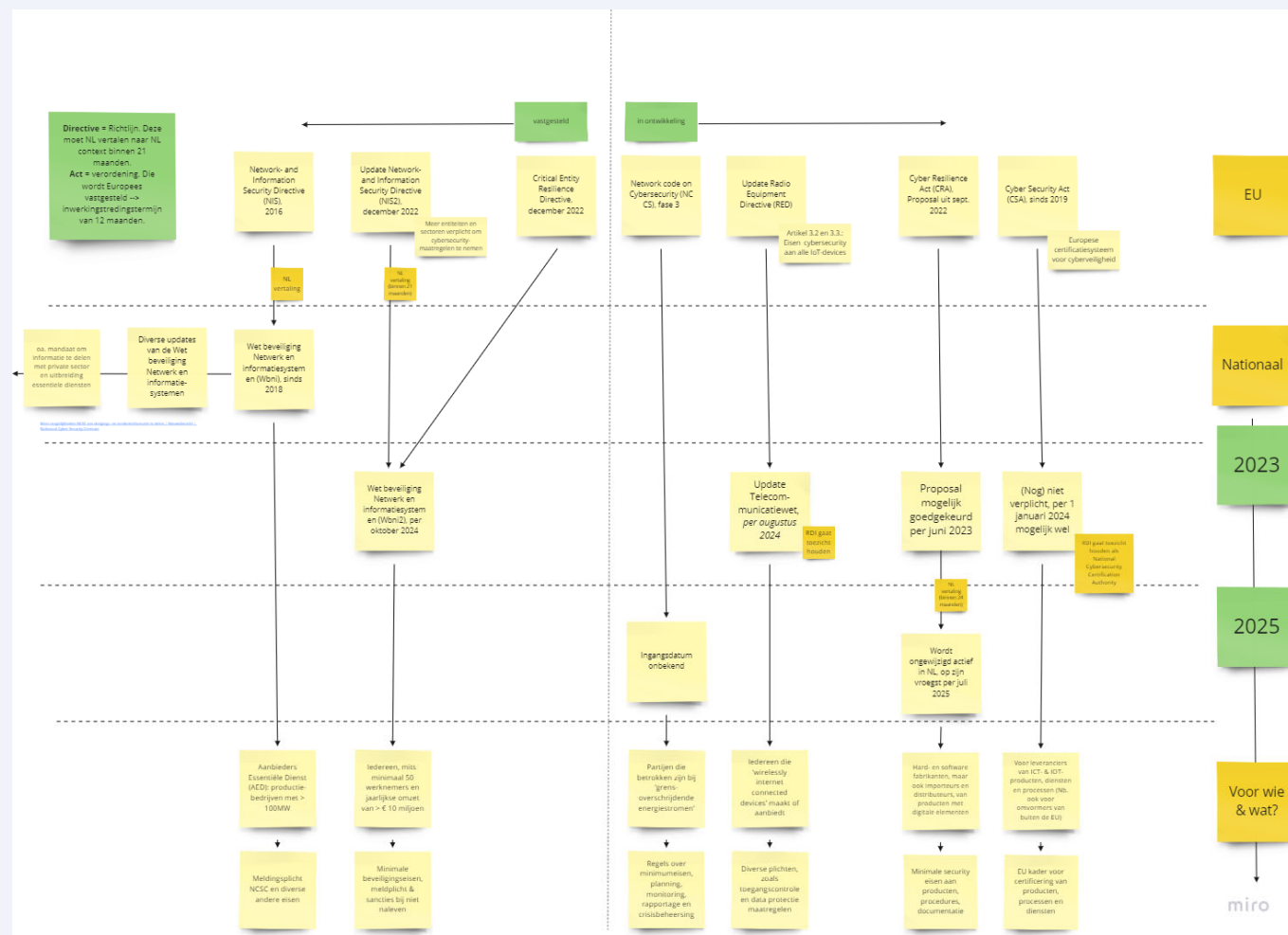
Speelveldanalyse

- 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 bereidheid om samen te werken
- **Benutten bereidheid: versterken samenwerking**

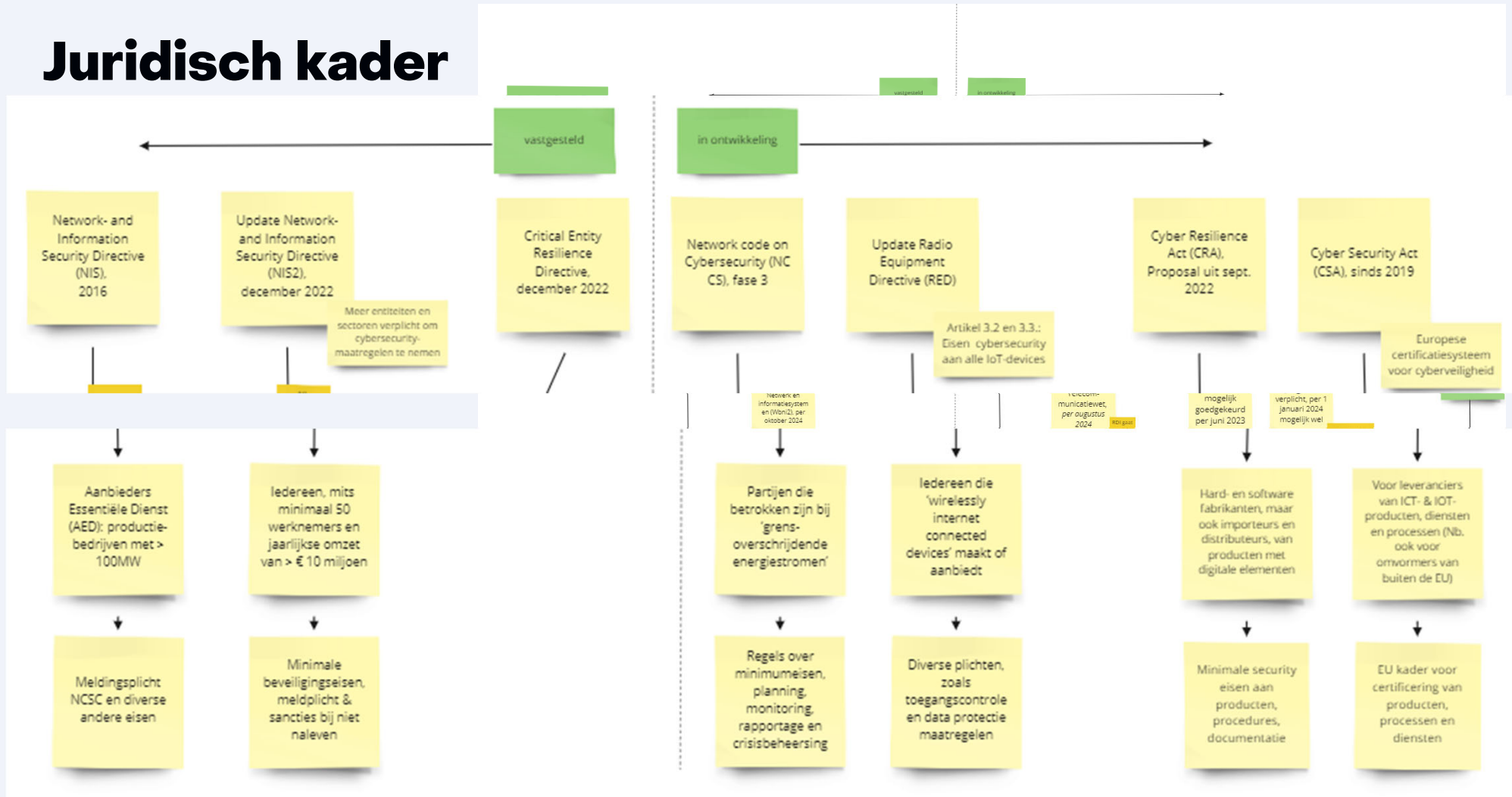
Juridisch kader

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

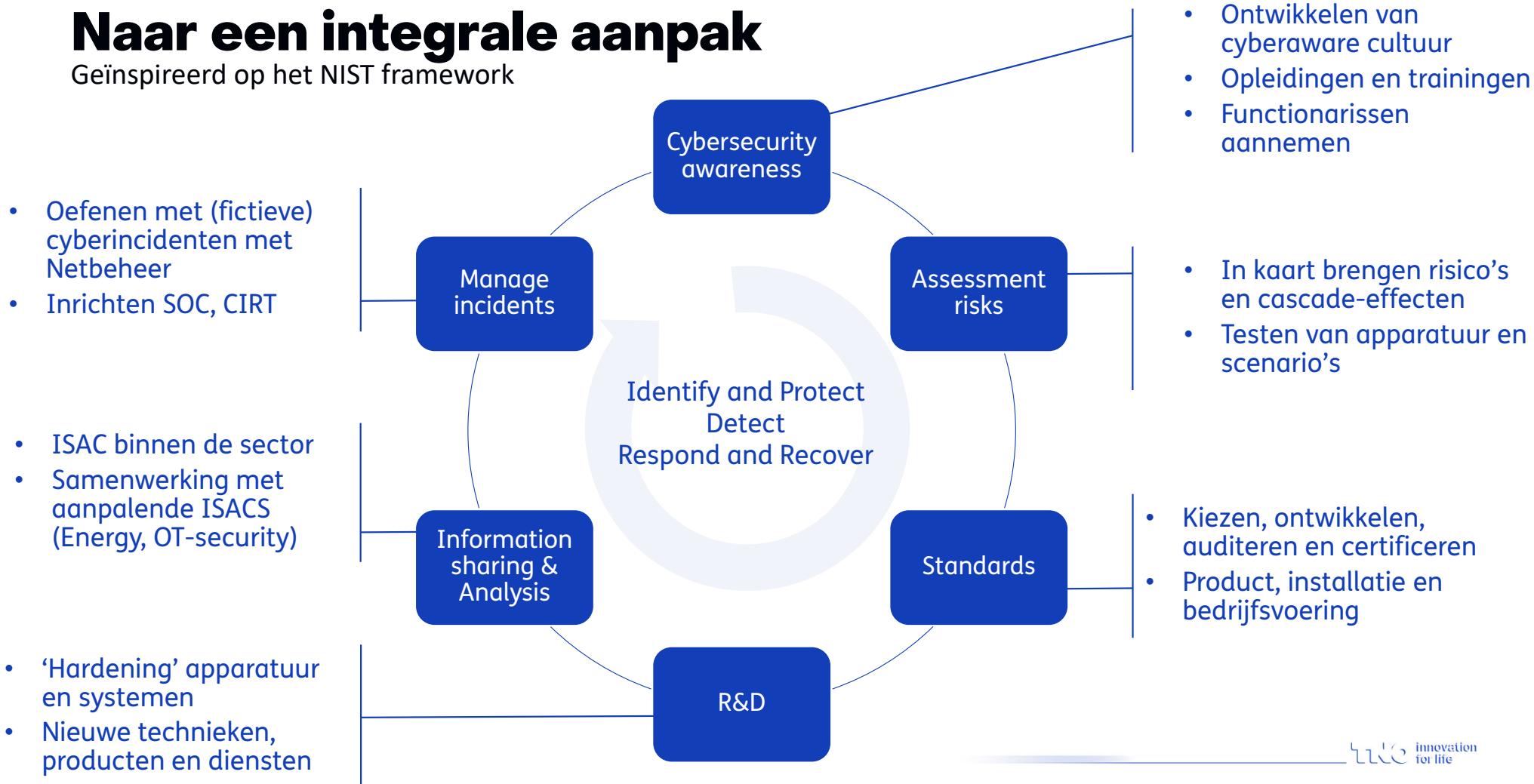


Juridisch kader



Naar een integrale aanpak

Geïnspireerd op het NIST framework

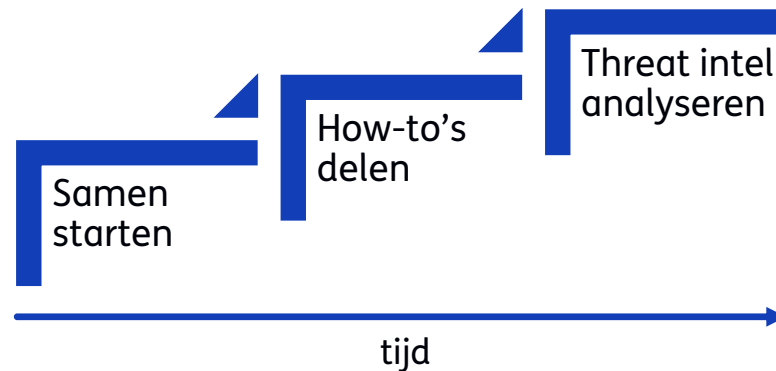


Integrale aanpak nader uitgewerkt

	Wat gebeurt er al?	Aanbeveling	Wie
Cybersecurity awareness	<ul style="list-style-type: none"> • Ontwikkeling trainingen installateurs Techniek Nederland • Artikelen vakbladen • Werkgroep Holland Solar 	<ul style="list-style-type: none"> • Training en campagne specifiek voor Solar installateurs • Publicatie best practices en check-lists (oa NIS2 basisbeveiligingseisen vertalen) 	<ul style="list-style-type: none"> • Holland Solar, Techniek Nederland, Solar Magazine, DTC, onderwijsinstellingen
Assessment risks	<ul style="list-style-type: none"> • Onderzoek door RDI naar cyberrisico's IoT consumenten 	<ul style="list-style-type: none"> • Risico's nader uitwerken: kans, effect, cascade-effecten • Verkennen mogelijkheid calls CS4NL te benutten • Apparatuur testen (nav standaarden) 	<ul style="list-style-type: none"> • RDI, TNO, TUDelft, Haagse Hogeschool, (werkgroep cybersecurity) NetbeheerNL
Standards	<ul style="list-style-type: none"> • Diverse standaarden uit andere sectoren (mn telecom) • ISO27001 	<ul style="list-style-type: none"> • Standaarden en normen kiezen en nader detailleren • Opbouwen certificeringen 	<ul style="list-style-type: none"> • NEN, RDI, Holland Solar, Techniek Nederland, minEZK, (werkgroep cybersecurity) NetbeheerNL, ENCS
R&D	<ul style="list-style-type: none"> • Data-diode • Onderzoeksprogramma CS4NL 	<ul style="list-style-type: none"> • (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 	<ul style="list-style-type: none"> • TKI, OEMS, O&M-partijen, kennisinstellingen, dcypher
Information sharing	<ul style="list-style-type: none"> • ISAC Energy • ISAC OT 	<ul style="list-style-type: none"> • Start met ISAC Solar NL, en verbindt deze met andere ISACs. Start klein en eenvoudig, en bouw langzaam uit • ISAC OEMs Europees 	<ul style="list-style-type: none"> • Trader, O&M, Assetmanager, DTC, Netbeheerder (TSO / DSO) (+ OEM)
Manage incidents	<ul style="list-style-type: none"> • Voor netbeheerders, grote OEM's en energiebedrijven bestaan SOCs 	<ul style="list-style-type: none"> • Ontwikkelen incident response plannen • Ontwikkelen oefening van een realistische cyberdreiging • Inrichten / delen CERT en SOC 	<ul style="list-style-type: none"> • 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 analyseren
- Aandachtspunt: grote verschillen in maturiteit



Start gemaakt: samenwerking uitbouwen

Geïnspireerd op het NIST framework

