Berenschot

EINDRAPPORT

Impact van cyber-security risico's op de nationale laadinfrastructuur

30 november 2021 | 65719 | Openbaar

EINDRAPPORT

Impact van cybersecurity risico's op de nationale laadinfrastructuur

30 november 2021 | 65719 | Openbaar

Auteurs:

MANAGEMENTSAMENVATTING

Conclusies en aanbevelingen

Inleiding: energietransitie en de nationale agenda laadinfrastructuur

De energietransitie is een grote uitdaging waar Nederland samen met de rest van de wereld voor een belangrijke opgave staat. Deze energietransitie betekent dat vele koolstof bevattende energiebronnen, zoals benzine, kolen, olie en gas worden vervangen door elektriciteit:

- Vervoer over de weg wordt aangedreven door elektriciteit;
- Woningen en bedrijven worden verwarmd door elektrische warmtepompen en restwarmte;
- Industriële processen en waterstofproductie worden aangedreven door elektriciteit.

De elektriciteit hiervoor wordt steeds meer opgewekt door zon en wind. Deze energiebronnen zijn duurzaam, maar niet altijd voorspelbaar en leveren vanuit het hele elektriciteitsnet. In de toekomst komt ook lokale elektriciteitsopslag middels onder andere batterijen in beeld.

In het klimaatakkoord van juni 2019 zijn de maatregelen van Nederland opgenomen. Daarin is opgenomen dat elektrische personenauto's rond 2025 concurrerend worden, de laadinfrastructuur voor elektrische voertuigen verder wordt uitgerold (inclusief eventuele netaanpassingen) en dat in 2030 alle nieuwe auto's emissieloos zijn. De Nationale Agenda Laadinfrastructuur is een meerjarige beleidsagenda die op basis hiervan is opgesteld.

Cyberveiligheid van laadpunten

In dit onderzoek hebben we de cybersecurity van de laadinfrastructuur onderzocht. Daarbij gold het richtjaar 2030. Naar de huidige verwachting zijn er dan geen 270.000, maar 1,8 miljoen laadpunten in Nederland en stijgt dit aantal in 2030 nog steeds sterk. Het totale gevraagde piekvermogen door laadpunten is dan twintigmaal zo hoog als nu. Nederland loopt momenteel voorop in de wereld voor het uitrollen van elektrisch rijden. Daarmee kan Nederland een belangrijke rol vervullen in het borgen van randvoorwaarden voor goed en veilig vervoer.

Naast de mogelijkheid voor inzet van laadinfrastructuur om in flexibiliteit te voorzien wanneer de stabiliteit van het elektriciteitsnet daarom vraagt, is er ook de keerzijde, namelijk dat plotselinge uitval of verstoringen in laadpatronen een zeer grote impact kunnen hebben op de mobiliteit van Nederland en de stabiliteit van het elektriciteitsnet.

Wij hebben vier scenario's geïdentificeerd waarin een typische cyberaanval tot substantiële verstoring leidt. Elk scenario heeft een eigen verloop en impact op de maatschappij. De vier scenario's zijn:

Scenario 1. Slimme aanval door Statelijke Actor

In dit scenario wordt ervan uitgegaan dat smart charging grotendeels in Nederland is ingevoerd. In dit scenario wordt het backoffice systeem van een Charge Point Operator aangevallen waarna, door manipulatie van smart charging mogelijkheden, de door dit backoffice systeem bestuurde laadpunten worden ingezet om het elektriciteitsnet van Nederland uit balans te brengen en tot een black-out te komen die mogelijk een paar dagen kan duren. Naar verwachting is dit in Nederland mogelijk vanaf een moment na het jaar 2025.

Scenario 2. Grote aanval van een Statelijke Actor

In dit scenario wordt de centrale informatieverstrekking aangevallen waarin de balans van het elektriciteitsnet via een status of via prijzen wordt doorgegeven, waarna plotseling het laden van aangesloten laadpunten kan worden gestopt. Indien het zo plotseling wegvallende vermogen groter is dan 3.000 MW is er een reëel risico op een black-out op nationaal niveau in Nederland. Naar verwachting is dit scenario mogelijk vanaf ongeveer het jaar 2027.

Door smart charging wordt het mogelijk meer laadpalen aan te sluiten op de netten ten opzichte van de situatie zonder smart charging. Daarmee wordt de belasting op de netten hoger en ook de gevoeligheid voor een black-out. Bij kleiner wegvallend vermogen op een geografisch geconcentreerd gebied kunnen op regionaal niveau verstoringen optreden. Bij regio's waar de netten al onder druk staan treedt een verstoring ook sneller op.

Op nationaal niveau verwachten we dat een black-out ten gevolge van een succesvolle aanval op één enkele grote Charge Point Operator pas enkele jaren na 2030 mogelijk is. Tegen die tijd zullen de toegenomen piekvermogens van laadpalen en elektrische auto's een dergelijke aanval ook eenvoudiger succesvol maken.

De effecten van scenario 1 en 2 zijn zeer ernstig en vergelijkbaar. De mobiliteit wordt flink aangetast. Bestel- en vrachtvervoer valt uit en hulpdiensten worden zwaar in de mobiliteit gestoord. Een black-out van het elektriciteitsnet kan het openbare leven volledig ontwrichten; ook internet, mobiele telefonie, TV, en alle van elektriciteit afhankelijke diensten vallen weg, mogelijk leidend tot rellen en doden.

Scenario 3: Gewone cyberaanval.

In dit scenario wordt bijvoorbeeld het backoffice systeem van een Charge Point Operator aangevallen door onder andere. ransomware, een scriptkiddie of anti-duurzaamheid terroristen. Daardoor valt het backoffice systeem van de Charge Point Operator uit en kunnen de beheerde laadpalen gedurende dagen of weken uitvallen. Dit kan ertoe leiden dat de klanten van die betreffende Charge Point Operator niet meer kunnen laden. Afhankelijk van de klanten van de Charge Point Operator kan dit betekenen dat Hulpdiensten of essentiële logistieke diensten deels kunnen uitvallen, of dat veel mensen in een bepaalde stad of regio niet naar hun werk kunnen omdat hun auto niet meer kan worden opgeladen.

Scenario 4: Privacy aanval

In dit scenario worden de klantdata van laadsessies gestolen en gepubliceerd of er wordt via een andere wijze misbruik van gemaakt. Dit kan gebeuren door statelijke actoren dan wel criminele organisaties. Het doel is geld verdienen dan wel het ondermijnen van vertrouwen. Er is geen direct effect op de mobiliteit of het elektriciteitsnet, maar het kan wel het vertrouwen in de nationale laadinfrastructuur ondermijnen en daarmee de verdere groei van elektrisch vervoer schaden.

Analyse en advies

De onderzochte scenario's zijn reëel en leveren in de toekomst een reëel risico op voor de mobiliteit van Nederland, de nationale laadinfrastructuur en de stabiliteit van het elektriciteitsnet. Een inschatting van de mogelijk negatieve economische impact van een dergelijk incident kan oplopen tot ongeveer 4 miljard euro per dag voor Nederland. De maatschappelijke impact van een stroomstoring is voor een groot deel afhankelijk van de tijdsduur. Maatschappelijke kosten die met storingen gepaard gaan variëren van het verlies van vrije tijd, tot mobiliteit, bedrijvigheid, en zelfs leven.

De risico's worden in de loop van de tijd ook groter; behalve dat het gebruik van laadpunten steeds verder stijgt zijn ook onverwachte keten- en cascade effecten te verwachten en de piekvermogens van elektrische voertuigen en laadpunten nemen steeds verder toe. Hoewel wij ons in dit onderzoek hebben beperkt tot Nederland, zijn de effecten waarschijnlijk groter doordat Charge Point Operators laadpunten in meerdere landen beheren, mobiliteit ook over grenzen heen gaat en het elektriciteitsnet op Europees niveau is gekoppeld. Ook kan een verstoring op een lager netvlak gevolgen hebben voor hogere netvlakken, zeker wanneer verstoringen elkaar opvolgen in gebieden waar de netten al onder druk staan.

De scenario's laten zien dat het cyberrisico vooral ligt in de backoffice systemen van Charge Point Operators en Smart Charging Service Providers. Er bestaat nu geen wet- en regelgeving voor de cybersecurity van deze backoffice systemen. Er bestaan weliswaar richtlijnen voor laadpunten zelf vanuit ElaadNL/ENCS die, omdat ze bij openbare aanbestedingen worden gevraagd, een duidelijke norm geven voor de laadpalen zelf, maar slechts deels voor de backoffice systemen. Overigens worden de door ElaadNL/ENCS opgestelde normen vooral toegepast bij aanbestedingen voor publieke laadpunten en nauwelijks bij de inkoop van private laadpunten (die 2/3 van de markt vormen).

Het ontbreken van deze wet- en regelgeving wordt door respondenten verklaard doordat het een nieuwe ontwikkeling betreft die vooral in de consumenten-sfeer wordt gezien. Maar doordat laadpunten vrijwel allemaal bestuurd worden vanuit een backoffice systeem heeft een dergelijk systeem een impact die vele malen groter kan zijn dan een grote elektriciteitsgenerator. Een grote elektriciteitsgenerator heeft wel normen en toezicht vanuit wet- en regelgeving op het gebied van cybersecurity.

Het is derhalve zeer gewenst dat een adequate cyberbeveiliging van de systemen van de nationale laadinfrastructuur middels wet- en regelgeving wordt geborgd. Aangezien het elektriciteitsnetwerk Europees is gekoppeld zou ook op Europees niveau moeten worden geagendeerd dat er een adequate beveiliging van de vitale systemen rond de laadinfrastructuur zal gaan worden geborgd.

Er zijn momenteel binnen Nederland meerdere bestaande wet- en regelgevingskaders die daarbij een startpunt kunnen vormen om de noodzakelijke wet- en regelgeving te gaan realiseren. Daarbij is het gewenst dat uiteindelijk wordt gekomen tot een situatie waarbij belangrijke partijen in de laadinfrastructuur van Nederland niet alleen een zorgplicht hebben om de cybersecurity van de systemen onder hun beheer te borgen, maar ook hiervoor onder toezicht komen te staan en incidenten moeten melden.

Ook is het gewenst dat er daarbij een segmentatie van backoffice systemen wordt doorgevoerd, zodat bij een geslaagde cyberaanval de impact beperkt kan blijven. Daarmee gaat het beter aansluiten bij wat er aan normen wordt gesteld bij reguliere balanshandhaving, die vereist dat bij uitval van een enkel element geen verstoring optreedt.

Inhoudsopgave

HOOFDSTUK 1

Introductie

1.1 Inleiding

Aan Berenschot is de volgende opdracht geformuleerd:
Geef de taakgroep cybersecurity van de werkgroep veiligheid van de Nationale agenda Infrastructuur inzicht in wat de risico's en impact zijn als de cybersecurity van de laadinfrastructuur niet goed is ingericht.

In ieder geval moeten risico's en impact voor de volgende stakeholders geduid worden:

- ***TSO***
- ***DSO's***
- ***CPO 's***
- ***EMSP's***
- ***EV-rijders***
- ***De maatschappij***

Dit onderzoek gaat in op deze opdracht.

1.2 Leeswijzer

In hoofdstuk 2 'Achtergrond en methodiek' bespreken we hoe we het onderzoek hebben uitgevoerd. In hoofdstuk 3 gaan we in op de opbouw van de laadinfrastructuur en de verwachte ontwikkelingen en prognoses in aantallen. In hoofdstuk 4 bespreken we het belang van de balans in het elektriciteitsnet. In hoofdstuk 5 gaan we in op de cybersecurity van laadpunten, waaronder de regelgeving. In hoofdstuk 6 identificeren we vier typische scenario's en de impact ervan op mobiliteit, de elektriciteitsvoorziening en de maatschappij.

In de bijlagen worden de interviews, en een lijst met afkortingen behandeld.

Wij hebben geprobeerd in dit rapport de soms technische aspecten rond elektriciteit en cybersecurity ook voor lezers, zonder de betreffende specifieke technische achtergrond, begrijpelijk te maken. Waar mogelijk zijn verwijzingen gemaakt naar de betreffende schriftelijke bronnen.

HOOFDSTUK 2

Achtergrond en methodiek

2.1 De uitdaging

Waar nu nog zo'n 270.000 laadpunten bestaan zal dit naar verwachting stijgen naar 1,8 miljoen laadpunten in 2030. Het gaat om een infrastructuur waarin vele partijen actief zijn met samenwerkende ICT-systemen. Daardoor zijn er meerdere cyberaanvalsvlakken voor aanval of verstoring mogelijk. De impact van een (gerichte) verstoring van de infrastructuur kan zeer groot zijn. Zowel stroomopwaarts (naar de DSO's en de TSO) als stroomafwaarts (via elektrische auto's naar mobiliteit en naar stilleggen van substantiële delen van het nationale vervoer naar het verstoren van andere vitale sectoren).

Het onderzoeken van risico's en impact vanuit cybersecurity van de laadinfrastructuur is een opgave met meerdere dimensies. Wij denken dat een goede analyse van de mogelijke risico's en impact van cybersecurity essentieel is om de awareness te vergroten en mogelijke problemen ten aanzien van elektrisch rijden en laadinfrastructuur tijdig te signaleren. Inzichten vanuit meerdere kennisgebieden zijn nodig voor een integraal beeld. Denk daarbij aan kennis van cybersecurity, de markt en de ICT-infrastructuur rond laadpunten, alsmede maatschappelijke gevolgen van uitval van elektriciteit, transport en andere vitale sectoren. Daarbij moet een open oog zijn voor ontwikkelingen die nu nog beperkt spelen maar in enkele jaren een substantiële bedreiging kunnen vormen. Prognoses richting 2030 zijn hierin leidend. De toekomst laat zich niet voorspellen, maar waar mogelijk en nodig maken wij gebruik van onderbouwde aannames om ook kwantitatieve inschattingen te kunnen geven.

In dit rapport brengen wij de risico's en impact voor de diverse stakeholders in beeld en geven daarnaast adviezen en handvatten om de verkregen inzichten verder te ontwikkelen in aanbevelingen en normstellingen.

2.2 Uitgangspunten voor dit onderzoek

- Er wordt uitgegaan van de situatie in 2030. Dat betekent onder andere geen 270.000 maar 1,8 miljoen laadpunten, concentratie, maar ook nieuwe toetreders op alle deelmarkten.
- Er wordt uitgegaan van de huidige situatie zonder aanvullende normering, regelgeving en maatregelen tussen nu en 2030.
- Er wordt uitgegaan van een verder ontwikkeld smart grid volgens de opzet van ECISS.
- Voor de ontwikkeling van de markt van laadpunten wordt uitgegaan van de huidige voorspellingen.
- Voor de regelgrenzen wordt gebruik gemaakt van de huidige normstellingen van de TSO en DSO's.
- Er wordt uitgegaan van de huidig bekende aanvalsvlakken en modi operandi van cyberactoren.
- Voor kansen van cyberaanvallen en mogelijkheden van aanvalsvlakken wordt uitgegaan van een expert oordeel. Daarbij wordt – conform de huidige werkelijkheid – ervan uitgegaan dat ondanks richtlijnen, zoals die van ElaadNL/ENCS, er toch mogelijkheden voor cyberintrusie overblijven. Genoemde richtlijnen van ElaadNL/ENCS worden bovendien slechts bij publieke aanbestedingen toegepast, terwijl private thuis- en werklaadpunten een groter volume vertegenwoordigen.
- Cyberaanvallen zijn actieve, moedwillige aanvallen op een ICT-systeem[1].

2.3 Methodiek

We hebben voor dit onderzoek een documentstudie gedaan en experts geïnterviewd. De documentstudie had als doel om een beter beeld te krijgen van de huidige kennis over cybersecurity van laadpunten. De documenten en informatie voor de studie is verkregen via deskresearch van openbare bronnen of toegestuurd door gesprekspartners. De gesprekspartners bestonden uit wetenschappelijke experts van technische universiteiten op het gebied van de laadinfrastructuur en elektriciteitsnetten en experts met relevantie functies werkzaam bij onder andere CPO's, eMSP's, TSO, DSO's, en leveranciers van laadpunten. Bovendien spraken we met vertegenwoordigers van de onderzoeksorganisaties ElaadNL en ENCS.

Tot slot is er ook een bijeenkomst geweest waarbij we met experts Marko Kruithof en Vincent Frijlink in gesprek zijn gegaan over de mogelijke cyberrisico's die we geconstateerd hebben op basis van de documentstudie en interviews. In de sessie zijn de risico's verder uitgediept en zijn er nog een aantal aanvullingen gedaan op de tot dan toe geformuleerde risico's.

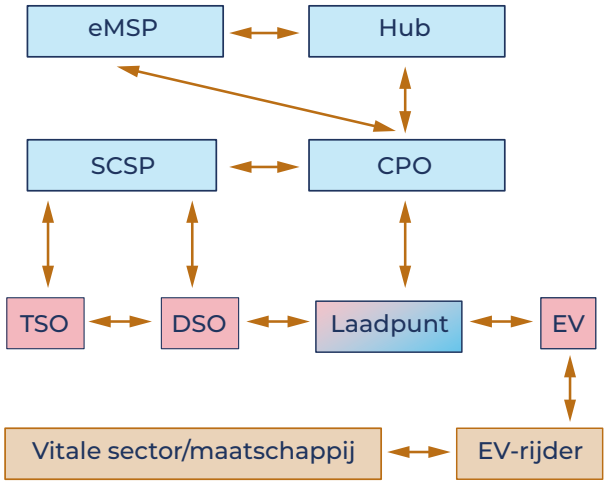
Op basis van de documentstudie, de informatie verkregen uit de interviews en de input van de expert bijeenkomst is het rapport opgesteld. Waar mogelijk is verwezen naar de bronnen van informatie.

HOOFDSTUK 3

Nationale laadinfrastructuur

Voordat we ingaan op de cyberrisico's van de nationale laadinfrastructuur, gaan we eerst in op de opbouw hiervan. Daarbij kijken we primair naar de *technische* opbouw en koppelingen. De eigendomsverhoudingen kunnen anders liggen: een laadpunt kan eigendom zijn van een particulier, maar zal veelal technisch door een CPO worden aangestuurd, die daartoe ook backoffice systemen en apps ter beschikking stelt, zeker als in 2030 smart charging de norm zal zijn.

3.1 Vereenvoudigde opbouw van de laadinfrastructuur



Figuur 1 **Vereenvoudigd schema opbouw laadinfrastructuur.**

Bovenstaand schema is te lezen als een introductie op de laadinfrastructuur. In paragraaf 5.2 (Systeemoverzicht laadinfrastructuur) wordt een meer compleet schema getoond.

Aangrijpingspunten voor cybersecurity liggen vooral in de *blauwe vlakken*: het laadpunt zelf en de ICT-infrastructuur van de Smart Charging Service Providers (SCSP's): de Charging Point Operators (CPO's) en de e-Mobility Service Providers (eMSP's). Deze bestaan zowel uit diverse applicaties als de koppelingen ervan, uitgevoerd met bijvoorbeeld OCPI. Het aantal is momenteel groot, zo zijn er nu al zo'n 50 eMSP's voor alle Nederlandse laadpunten. Een belangrijk aangrijpingspunt ligt voorts in de Smart Charging Service Providers (SCSP's).

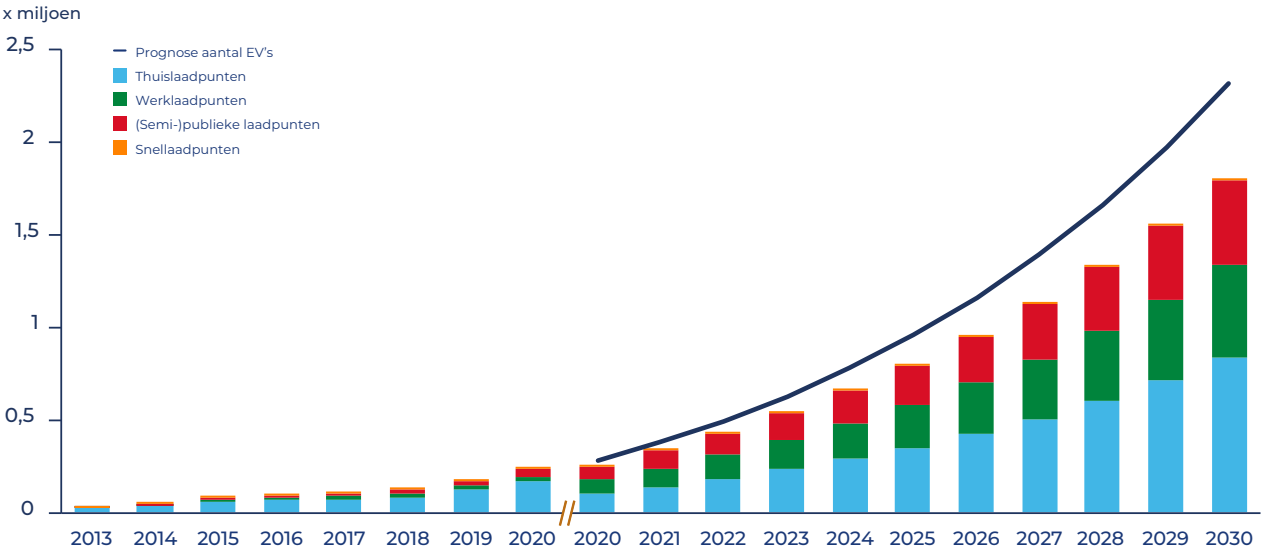
SCSP's besturen de opzet en werking van het zogenaamde 'smart grid', waarbij afname en teruggave van elektriciteit tussen laadpunten en het elektriciteitsnet worden bestuurd, ook op basis van pieken en dalen in het verbruik in het elektriciteitsnet zelf. Hubs worden ook wel Roaming Service Platform (RSP) genoemd en zorgen voor vooral financiële afhandeling van laadsessies tussen CPO's en eMSP's onderling.

De *rode vlakken* laten de levering van elektriciteit zien: van het hoogspanningsnet beheerd door de TSO TenneT via de midden- en laagspanning beheerd door de DSO's tot het fysieke laadpunt. Cyberverstoringen bij het laadpunt via de CPO of eMSP, of in de toekomst via de SCSP, kunnen in potentie grote verstoringen veroorzaken bij de DSO's en TSO. Essentieel daarbij zijn omvang en snelheid van de verstoring. Verstoringen op deze vlakken gaan tevens gepaard met mogelijk grote impact op de maatschappij. Daar wordt verder op ingegaan in paragraaf 6.

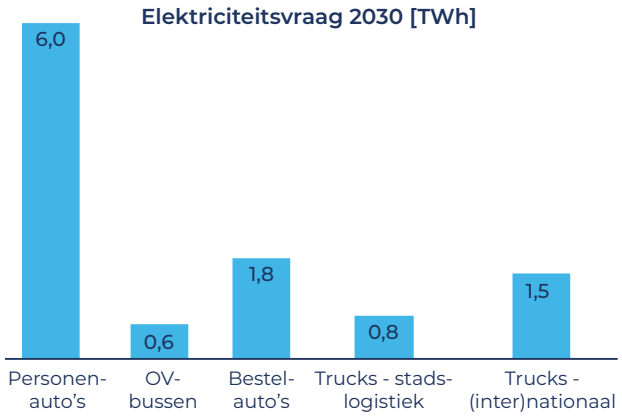
Bij de bepaling van de directe impact zijn de **oranje vlakken** relevant: het effect op de EV-rijder en de maatschappij met de nadruk op vitale sectoren zijn relevant. Ook verstoring van alleen deze vlakken kan een forse impact hebben op de maatschappij. Meer over de impactanalyse ook in paragraaf 6.

3.2 De verwachte groei van EV's en laadinfrastructuur richting 2030

Op basis van gegevens van onder andere ElaadNL hebben wij analyses gemaakt. In Figuur 2 wordt de prognose voor de elektriciteitsvraag in het jaar 2030 vanuit mobiliteit weergegeven, voor personenvoertuigen, OV, en vracht. De huidige vraag is ongeveer 2.000 GWh voor mobiliteit[2] (dit is inclusief treinen). In 2030 is de elektriciteitsvraag voor mobiliteit bijna 11.000 GWh (dit is ongeveer 9% van het totale landelijk gebruik), in het midden-scenario (exclusief treinen). Te zien is dat - naast personenvervoer - ook bestelvoertuigen en vrachtvervoer een aanzienlijke elektriciteitsvraag zullen hebben in 2030. De elektriciteitsvraag van OV-bussen is dan bijna maximaal, maar beslaat een relatief klein aandeel van de mobiliteitssector.



Figuur 3 **Aantal elektrische personenauto's en laadpunten. Historische ontwikkeling tot en met 2020: RVO 2021. Prognose 2020-2030: ElaadNL outlook 2021.**



Figuur 2 **Prognose elektriciteitsvraag per modaliteit in 2030 op basis van prognoses uit de verschillende ElaadNL outlooks voor aantallen in het midden-groei scenario en constant elektriciteitsverbruik per type voertuig.**

3.2.1 De ontwikkeling van elektrische personenauto's

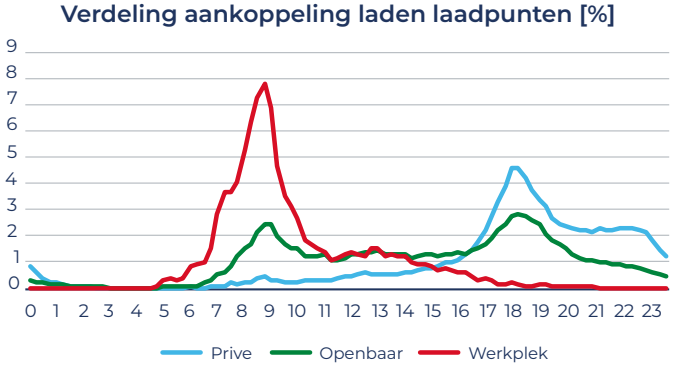
Het beleid van de Nederlandse regering is dat per 2030 alleen nog emissieloze personenauto's worden verkocht[3]. Ook internationaal worden dergelijke doelen gesteld: President Biden heeft gesteld dat in 2030 de helft van nieuwe auto's in de USA elektrisch moet zijn[4].

Naar verwachting zullen er in 2030 in Nederland 1,8 miljoen laadpunten[5] zijn, daarmee een verwachting volgende van ongeveer 2,3 miljoen EV's. In figuur 3 laten we de prognose richting 2030 van de aantallen elektrische personenauto's en verschillende laadpunten zien. De historische data sluiten niet precies aan op de prognose, zoals te zien aan de verschillen tussen de twee 2020 punten. Het aantal thuislaadpunten is historisch weergegeven op basis van een het percentage EV-rijders dat in 2020 heeft aangegeven thuis te laden[6], dat geeft naar schatting 169.000 private laadpunten[7]. Dit terwijl slechts ongeveer 30% van de huishoudens beschikt over een eigen oprit, en ongeveer 47-59% van de kilometers thuis worden geladen (getallen verschillen tussen de 2020 en 2021 enquête).

Daarbovenop wordt 16-23% thuis aan een publieke laadpaal geladen. Vermoedelijk zal het percentage private laadpunten richting de toekomst afnemen, omdat de groep met eigen oprit nu oververtegenwoordigd lijkt.

In figuur 2 is de historische ontwikkeling tot en met 2020 en de prognose tot het jaar 2030 weergegeven. Te zien is dat in 2030 het aantal laadpunten op 1,8 miljoen is geprognosticeerd, en het aantal EV's op ongeveer 2,3 miljoen.

In Figuur 4 wordt weergegeven hoe de aankoppelingen aan laadpunten zijn verdeeld op een doordeweekse dag, verdeeld over de verschillende typen laadpunten[12]. In aantallen kWh zou dit plaatje er anders uitzien omdat er niet evenveel van alle typen laadpunten zijn. Doordeweeks is de laadbehoefte het grootst. Thuis wordt er vooral ingeplugd rond 18:00 uur. Om overbelasting van het laagspanningsnet rond dit tijdstip te voorkomen zal op termijn smart charging (en een SCSP) nodig zijn.

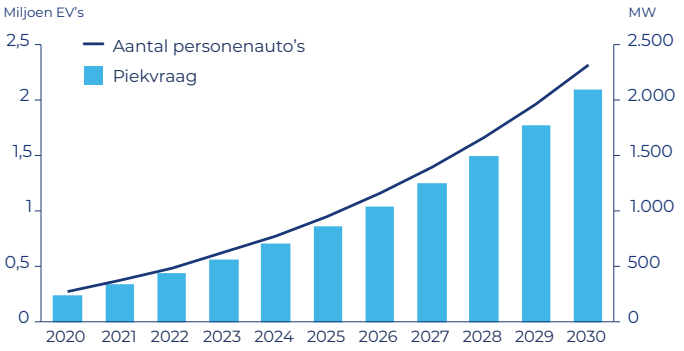


Figuur 4 **Aantal aankoppelingen (in percentages!) per verschillende type laadpunten. Het overgrote deel (~75%) van de behoefte wordt voorzien door thuislaadpunten. Daar is de piek in het aantal nieuwe koppelingen rond 18:00 uur. In absolute termen is de laadbehoefte in de avond het grootst, omdat het grootste deel van de laadbehoefte volgens het private profiel wordt ingevuld.**

Hoewel maar ongeveer 30% van de huishoudens een eigen oprit heeft, wordt in het jaar 2021 maar liefst 59% van de laadbehoefte thuis (privaat) ingevuld, waarvan 8% via het stopcontact en 51% via een thuislaadpunt. In 2020 was dat 47% (waarvan 7% via het stopcontact en 40% via een thuislaadpunt). De coronapandemie speelt een rol bij de grote verschillen tussen getallen uit 2020 en 2021. De ochtendpiek vindt met name plaats bij publieke laadpunten bij de werkplek. De avondpiek ligt nu voornamelijk bij thuislaadpunten maar in de toekomst zal de avondpiek steeds meer ook de publieke laadpunten betreffen.

De totale laadbehoefte voor personenauto's in 2030 is naar verwachting 6.000 GWh[13]. De verwachte ontwikkeling van de piekvraag[8] wordt weergegeven in Figuur 5. Daarin is te zien dat de piekvraag in 2030 rond de 2.000 MW zal liggen.

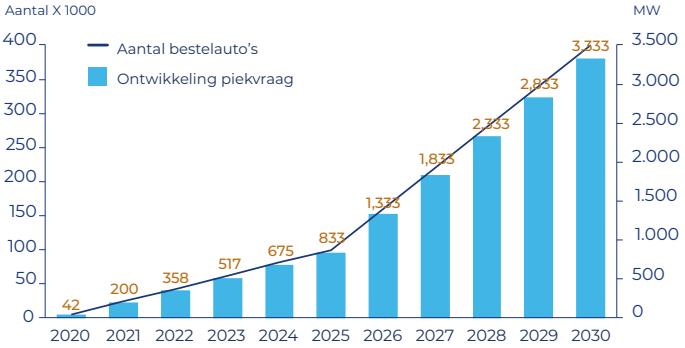
Bij al deze prognoses wordt nog geen rekening gehouden met smart charging. Om pieken te dempen zal smart charging in de toekomst nodig worden, maar vormt daarmee meteen een extra kwetsbaarheid als het smart charging door een cyberaanval wordt verstoord. Tijdens een piek is de kwetsbaarheid vaak het grootst. Een groot deel van de piekvraag in de avond wordt ingevuld bij private laadpunten. Zoals in Figuur 4 te zien is er ook een piek in de ochtend. Die piek wordt voor het grootste deel bij werklaadpunten ingevuld. Een inschatting op basis van de beschikbare data is dat de piekvraag in de ochtend ongeveer 35% zal zijn van de piekvraag in de avond. Daarmee is de piekvraag in de ochtend in 2030 naar verwachting rond de 700 MW . Het grote verschil met de avondpiek is dat hiervan het grootste deel via publieke laadpunten zal worden geladen.



Figuur 5 **Ontwikkeling piekvraag met het aantal personenauto EVs. De piekvraag vindt aan het begin van de avond plaats rond 19:00h.**

3.2.2 De ontwikkeling van bestelauto's en vrachtvervoer

Naast de groei van personenauto's zal ook de elektriciteitsvraag van bestelauto's en vrachtvervoer sterk groeien. De verwachte piekvraag van bestelauto's voor 2030 wordt gegeven in Figuur 6. Daarin is te zien dat – zonder smart charging, de piekvraag van bestelauto's naar verwachting zal groeien naar 3.300 MW in 2030. De piekvraag van bestelauto's en vrachtvervoer vindt min of meer gelijktijdig plaats met de avondpiek van de elektrische personenauto's. Dit is gebaseerd op een inschatting van ElaadNL[14], en geëxtrapoleerd op basis van de groei in aantallen elektrische bestelauto's naar 2030. Alhoewel het aantal bestelauto's en vrachtvervoer beduidend kleiner is dan het aantal personenauto's, is de piekvraag hoog. Dat wordt veroorzaakt doordat het verbruik van bestelauto's relatief hoog is, en de piekvraag sterker is geconcentreerd naar de avondpiek. Met smart charging kan de piekvraag dalen naar 40% van de piekvraag zonder smart charging, ofwel 1.300 MW. Hiervan zal naar verwachting 50% gebruik maken van private en publieke laadpunten rondom het woonadres, en de rest van laadpunten bij het bedrijf.



Figuur 6 **Prognose groei aantal elektrische bestelauto's[16] en bijbehorende piekvraag, zonder smart charging en zonder grote verhoging capaciteit laadpunten (interpolatie tussen 2020, 2025, en 2030).**

Ook elektrisch vrachtvervoer (buiten bestelauto's) zal naar verwachting sterk groeien[3]. Het laadprofiel zal anders zijn dan bij personen- en bestelauto's, en er zal meer tussendoor met snelladers worden geladen. Bij laadpunten voor vrachtvervoer wordt uitgegaan van gemiddeld een 50 kW aansluiting (voor een 'gewoon' laadpunt) tot gemiddeld 650 kW voor een snellader (bij verzorgingsplaatsen of speciale truck-snellaadlocaties)[3]. Het verwachte piekvermogen van vrachtvervoer in 2030 ligt rond de 800 MW en groeit richting 2035 sterk door naar 2.900 MW[3].

3.2.3 Ontwikkeling van piekvermogen en aangekoppeld vermogen van personenauto's en bestelauto's

Als we de ontwikkeling van het verwachte gevraagde piekvermogen in de vorige twee paragrafen samenvoegen, dan komen we tot de volgende totalen. Daarin gaan we in op zowel het verwachte gevraagde piekvermogen in het jaar 2020, het referentiejaar 2030, en op het jaar 2025. Daarbovenop komt nog het vermogen voor vrachtvervoer, zoals gesteld in de prognose van ElaadNL[3]. Dit leidt tot de volgende tabel.

	Piekvermogen (MW)			
Jaar	Personen-auto's	Bestel-auto's	Vracht-vervoer	Totaal
2020	250	40		290
2025	860	830	90	1800
2030	2.100	3.300	840	6.300

Tabel 1. **Piekvermogen totaal per jaar,**

Dit totaal piekvermogen van 6.300 MW in 2030 is iets minder dan een derde van het huidige maximaal landelijk vermogen van ongeveer 21.000 MW.

Qua vermogen (hoeveelheid energie per seconde) zitten er flinke verschillen tussen bestaande laadpunten. Bij een 1-fase aansluiting, een typisch thuislaadpunt, is dat rond de 3,7 kW en bij een typische 3x25A 3-fase aansluiting is dat, vanwege elektrotechnische eisen, 11 kW. Op die vermogens wordt momenteel het meeste geladen. De meeste sessies laden met ongeveer 3,7 kW[9].

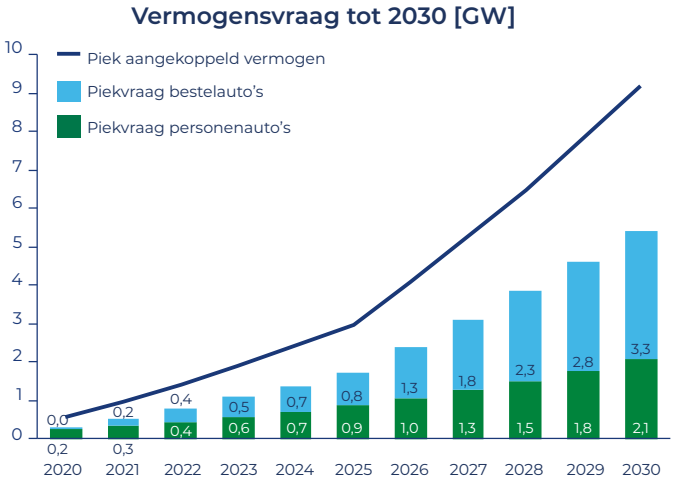
In 2018 was dat in meer dan 70% van de gevallen, en in 2020 nog bij ongeveer 35% van de laadsessies aan publieke laadpunten. Bij de publieke laadpunten wordt 11 kW op dit moment het meest toegepast, dat was in 2020 goed voor ongeveer 30% van de laadsessies. Alle nieuwe modellen van elektrische auto's hebben een 3-fase lader aan boord. Dat was voorheen soms nog een 1-fase lader, maar hier lijkt van afgestapt te zijn. Slechts 5% van de sessies vindt op hoger vermogen plaats, maar ook 5% op lager vermogen.

Momenteel worden er vooral 11 kW laadpunten bijgeplaatst. De prognose voor aantal laadpunten in 2030 in de laatste ElaadNL outlook[10] is 1,8 miljoen. Bij een gemiddeld maximaal vermogen van 11 kW[11] per laadpunt gaat dat om een opgesteld vermogen van 18700 MW in 2030. Dat betekent niet dat er tegelijkertijd dat vermogen zal worden geladen, want niet elk laadpunt zal bezet zijn en niet elke ingeplugde auto heeft een maximale laadbehoefte.

Uit een nadere studie van de data van een deel van de publieke laadpunten in het Randstedelijk gebied en noordwesten van Nederland[12] blijkt dat er per sessie gemiddeld 14-20 kWh wordt geladen. In 2020 werd er (ten tijde van de coronapandemie) 70 GWh geladen door 280.000 EV rijders, bij 11.000 publieke laadpunten tijdens 4,3 miljoen sessies. Per EV-rijder zijn dat gemiddeld ruim 15 sessies bij een specifiek laadpunt van ~16 kWh in het jaar. Per laadpunt werd er gemiddeld ruim 6.000 kWh geladen. In 2019 was het gemiddelde vermogen per publieke laadpunt 5,1 kW. Dat zal sindsdien wat zijn gestegen, doordat er meer met 3-fasen wordt geladen (dat geeft 11 kW). Bij 7 kW betekent dat dat een laadsessie ruim 2 uur duurt. In 80% van de gevallen staat een auto 6 uur aan een laadpunt, en gemiddeld 8 uur voor alle laadsessies, inclusief de uitschieters aan de onder- en bovenkant. Bij laadpunten op het werk is de laadduur 5,5 uur voor 80% van de gevallen, met een gemiddelde van 6,6 uur. Thuis staan de auto's het langst verbonden, met 10,3 uur voor 80% van de gevallen, en een gemiddelde van 12 uur. Daarvan wordt naar verwachting ongeveer 25% actief benut. 75% van de kilometers wordt thuis geladen. Naar verwachting daalt dat percentage naar de toekomst, omdat de oververtegenwoordiging van huishoudens met een eigen oprit naar verwachting zal verminderen. Er zijn forse verschillen tussen de regio's. Het gebruik van een laadpunt varieert van 4.881 kWh/jaar in SGZH (18 gemeenten in de provincie Zuid-Holland) tot 8.356 kWh/jaar in Utrecht.

Het vermogen aan accu's van personenauto's dat op een moment tegelijkertijd is aangekoppeld kan worden afgeleid uit de laadprofielen en de benuttingsgraad. De benuttingsgraad van laadpunten (de mate waarin een laadpunt feitelijk een EV laadt) varieert flink, maar is tussen de 25-40%, voor publieke en private laadinfrastructuur. De benuttingsgraad zal gemiddeld hoger zijn tijdens de piekvraag. Wat de benuttingsgraad tijdens de avondpiekvraag is, is niet precies bekend. Als we aannemen dat de benuttingsgraad in de piek wat hoger dan gemiddeld is schatten we die in op 50%. Het piekvermogen dat wordt gevraagd is dan rond de 2.000 MW. Het totaal aan aangekoppelde vermogen van personenauto's is dan, inclusief de auto's die niet actief aan het laden zijn, circa 4.000 MW.

Daarbovenop komt het aangekoppeld vermogen van bestelauto's, dit vermogen schatten we ook in op basis van de piekvraag, we nemen aan dat dat 150% is van de piekvraag. De piekvraag van bestelauto's in de avond is ingeschat op 3.300 MW. Bij de aanname dat het aangekoppeld vermogen daar 150% is, geeft een aangekoppeld vermogen van bestelauto's 5.000 MW. Van personenauto's en bestelauto's gezamenlijk is dat dan 4.000+5.000 =9.000 MW. Deze hebben eenzelfde vraagprofiel in de avond. Al in 2025 wordt, bij dezelfde aannames, een aangekoppeld vermogen van 3.000 MW bereikt voor personenauto's en bestelauto's gezamenlijk, wat gelijk is aan de regelgrens van het Europese net.



Figuur 7 **Inschatting ontwikkeling aangekoppeld vermogen personenauto's en bestelauto's tijdens de avondpiek (voor bestelauto's alleen ingevuld met bekende prognoses).**

Voor de mogelijke impact en het risico van een cyberaanval van type 2 (zie hoofdstuk 6) is vooral de piekvraag van belang omdat dit laat zien hoe groot het direct snel te beïnvloeden vermogen is als een cyberaanval plaatsvindt tijdens piekuren.

3.2.4 Verschillende aansluittypes

In onderstaande tabel is te zien dat er een verscheidenheid van aansluittypes is per netbeheerder. Hierin zijn de kleinverbruik aansluitingen weergegeven, maar de grootverbruik aansluitingen (vanaf 3x80A) zijn niet opgenomen. Ook zijn de verhoudingen tussen de verschillende aansluittypen verschillend per netbeheerder.

De aansluitingen voor de eerste drie rijen (1x25A, 3x25A en 1x35A) zijn aansluitingen met het basistarief, daarboven moeten consumenten meer betalen voor de vaste jaarlijkse netwerkkosten. Daarom kiezen maar 3,4% van de consumenten voor een andere, meestal zwaardere aansluiting. Met 1x35A is maximaal 8KW te leveren, met 3x25A maximaal 17 kW. Zo valt te zien dat met deze tariefstructuur een laadcapaciteit van 22 kW voor zeer weinig consumenten mogelijk is.

Knelpunten worden verwacht bij de aansluitingen bij bedrijventerreinen, met name voor transportbedrijven met meerdere elektrische vrachtwagens. Een deel van de bestelauto's laadt op private laadpunten. Met name in de randstad is er grotere vraag naar publieke laadpunten voor bestelauto's, vanwege gebrek aan eigen terrein of oprit met laadmogelijkheden. Het aantal laadpunten groeit hard vanaf 2025. Bestelauto's maken veel kilometers en zullen relatief vaak moeten laden, maar ten opzichte van personenauto's is het aantal benodigde laadpunten nog beperkt.

Aansluittype	Min. laadtijd 50kwh	Enexis	Liander	Stedin	Totaal	Aandeel
1*25A	13 uur	531.906	1.126.192	152.151	**1.810.249**	**21,9%**
3*25A	4½ uur	823.655	1.097.822	323.397	**2.244.874**	**27,2%**
1*35A	7 uur	1.088.888	1.215.387	1.617.748	**3.922.023**	**47,5%**
Rest		191.586	20.866	69.990	**282.442**	**3,4%**
Totaal		**2.636.035**	**3.460.267**	**2.163.286**	**8.259.588**	**100%**

Figuur 8. **Verdeling aansluittypes per netbeheerder.**

3.2.5 Toenemende laadvermogens en smart charging

De ontwikkeling van laadpunten naar gaat in de richting van een situatie waarin thuislaadpunten over het algemeen 11 kW maximaal aankunnen[13]. Voor laadpunten onderweg is een ontwikkeling zichtbaar, waarbij de vermogens voor snelladen gebaseerd zijn op gelijkspanning (DC) en steeds hoger worden, op korte termijn tot 350 kW voor personenauto's[14]. Er wordt nu vanuit het CharIN consortium (die ook de in Europa veel gebruikte CCS 'stekker' heeft ontwikkeld) gewerkt aan een laadpunt en een stekker voor vrachtwagens van 4.500 kW[15].

Door Entso-e, de vereniging van TSO's in Europa wordt gepleit voor snelle actie bij het uitrollen van laadpunten met de mogelijkheid van smart charging, zodat deze later niet hoeven te worden vervangen. Daarbij is het vanuit het Europese elektriciteitsnet gewenst dat afname en teruglevering van elektriciteit kan worden afgestemd op balans van het net en de productie van zon en wind. Smart charging kan daarmee een rol spelen in het handhaven van de balans op het elektriciteitsnet, en is daarmee uitermate belangrijk voor de energietransitie. Voordat het 'smart grid' van de grond kan komen moeten er nog een aantal hordes worden genomen:

- Het moet duidelijk worden hoe de voordelen van 'smart charging' ook bij de EV-rijder terecht kunnen komen[16].
- De Europese standaard voor charging: de combined charging system standard (CCS) zal verder moeten zijn ontwikkeld inclusief de publicatie van de ISO-standard 15118-20, zodat ook volledig Vehicle to Grid smart charging mogelijk is en kan worden ingebouwd in EV's, laadpunten en SCSP's. Naar verwachting kan dit in of na het jaar 2025 zijn gerealiseerd [17] [18]. Rond deze tijd zal het toepassen van smart charging steeds meer essentieel worden om de laadinfrastructuur mogelijk te maken binnen de huidige infrastructuur van de TSO en de DSO's zonder aanzienlijke verzwaringen.
- Er moet duidelijk worden onder welke condities de diverse data die nodig zijn voor een smart grid worden uitgewisseld. Niet alleen de technische standaarden, maar ook het eigenaarschap en de waarde ervan, alsmede de privacy en veiligheid van de data.

"As EVs will be increasingly integrated in the energy system, security from cyber-attacks will also represent a key issue, so as to avoid data being intentionally manipulated to generate negative impacts on the system balance. Moreover, control systems of EV-charging should be designed in such a manner that data failure or manipulation does not lead to a substantial change in system balance (cyber-resilience) and emergency situations are properly managed (e. g. restoration after black-outs)."
ENTSO-E Position Paper - Electric Vehicle Integration into Power Grids, 31 march 2021.

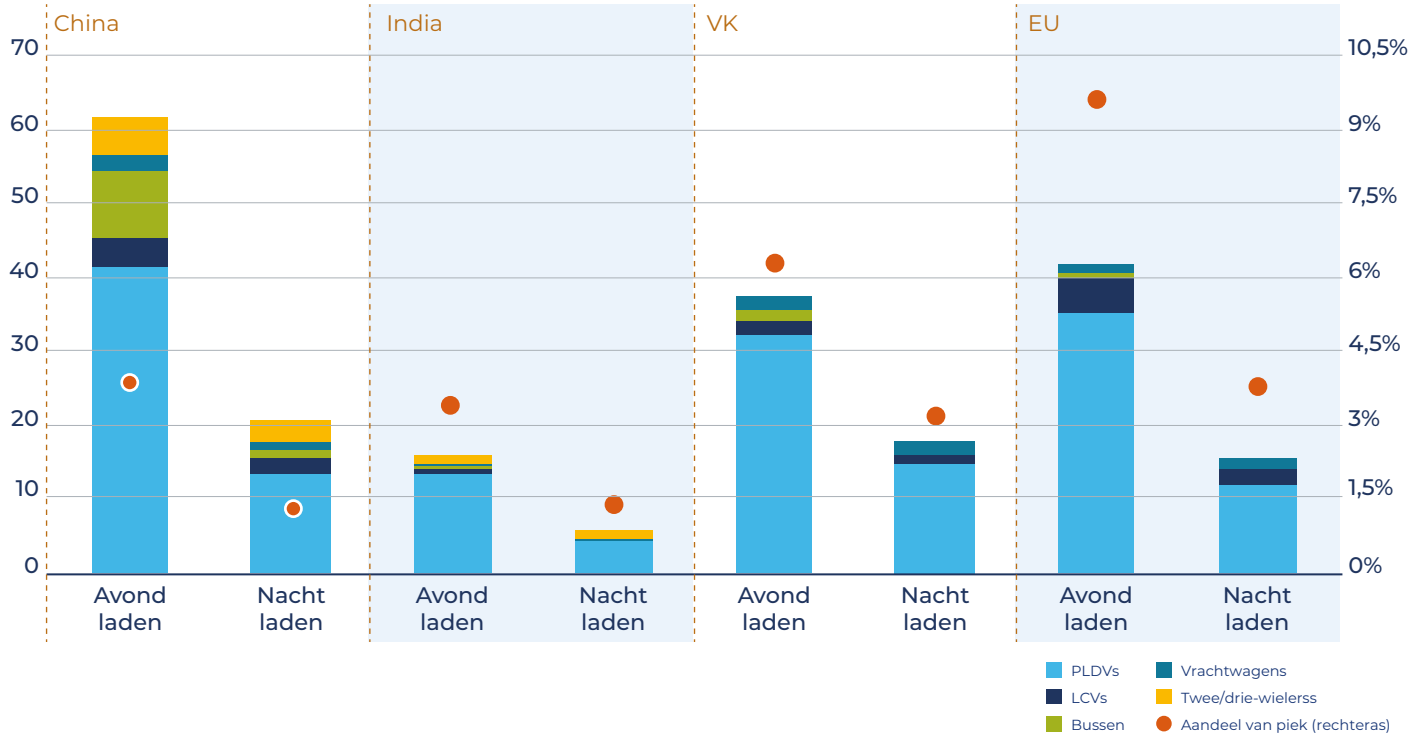
Het is duidelijk dat smart charging nodig zal zijn om ook in 2030 een stabiel elektriciteitsnet in Europa te krijgen. In een position paper van de Europese TSO's: Entso-e wordt gesteld dat TSO's hier een belangrijke rol in hebben en dat een ongecontroleerd laadproces 'significante uitdagingen' zal geven aan het elektriciteitsnetwerk[19]. En dat door smart charging de piek 's avonds tussen 16:00 uur en 22:00 uur kan worden verminderd en uitgesteld naar de nacht en middag, wanneer prijzen ook lager zijn[20].

Voor smart charging zijn natuurlijk ook SCSP-partijen nodig om de laadpunten 'smart' te laten worden en rekening te laten houden met de balans in het net. Er zijn verschillende partijen die zich opmaken om in de toekomst de rol van SCSP te gaan spelen: autofabrikanten, energieleveranciers, CPO's en eMSP's. De tijd zal leren welke partijen in welke mate en in welke combinatie de SCSP-rol zullen gaan vervullen.

3.3 Wereldwijde verwachtingen

3.3.1 Piekbelasting door EV's

De verwachting van het Internationaal Energie Agentschap is dat in het jaar 2030 9,6% van de piekbelasting in de avond in de Europese Unie afkomstig is van het laden van elektrische auto's in het *sustainable development scenario*, waarbij uit wordt gegaan van niet bestuurde charging [21]. (In Nederland is dit percentage in 2030 hoger en meer rond de 30% doordat de adoptie van elektrisch rijden in Nederland hoger is dan het gemiddelde van Europa).



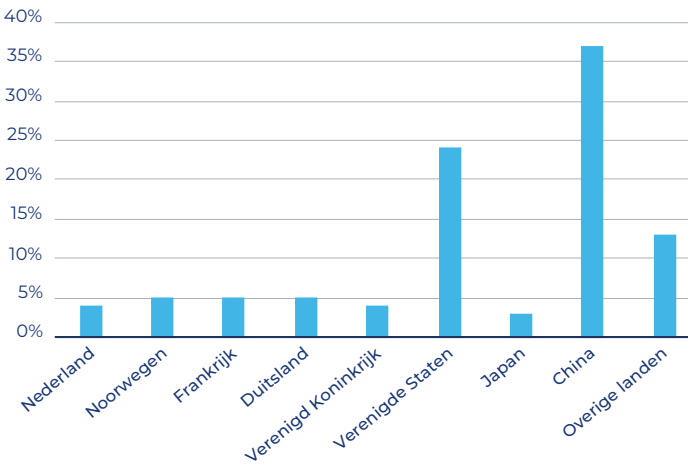
Figuur 9. **Belasting door EV's per werelddeel in 2030 met percentage piekbelasting (oranje bollen).**

3.3.2 Batterijen

De batterijen welke worden gebruikt in elektrische auto's zullen zich ook steeds verder ontwikkelen. Dat heeft ook invloed op de kosten aangezien de batterij ongeveer 35-45% van de kosten van een elektrische auto bedragen[22]. Batterijen zijn tussen 2010 en 2020 al bijna 90% goedkoper geworden[23]. Daarbij worden voortdurend nieuwe technieken ontwikkeld leidend tot grotere batterijen met lagere kosten, hogere prestaties en minder gebruik van schaarse metalen[24]. Daarbij kan aan de bovenkant van de markt al de eerste 30% van de accu worden snel geladen met gelijkspanning en een vermogen van 250 KW[25]. Er wordt verwacht dat per 2030 de ontwikkeling van de huidige Li-ion technologie een eindpunt zal hebben bereikt, waarbij EV's gemiddeld 350- 400 km kunnen rijden op één volle batterij van 70-80 kWh.

3.3.3 Aantal private laadpunten per land

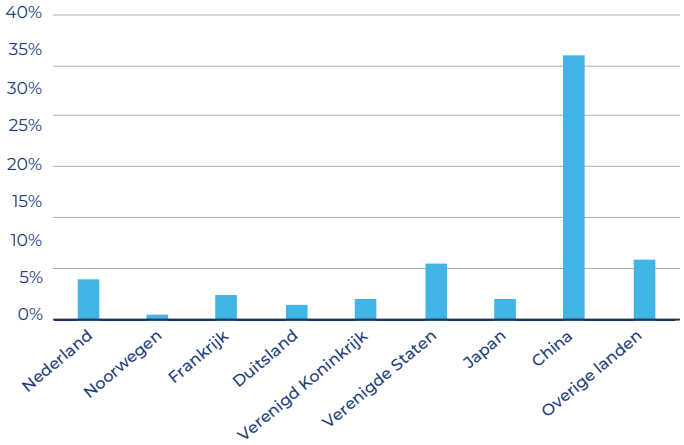
Het aantal laadpunten in Nederland is relatief hoog: in 2019 was dit 4% van het aantal private laadpunten wereldwijd[26]. Het aantal is gebaseerd op een inschatting, gegeven het percentage van EV-rijders dat heeft aangegeven thuis te kunnen laden[9].



Figuur 10. **EV langzame laadpunten per land in 2019.**

3.3.4 Publieke laadpunten

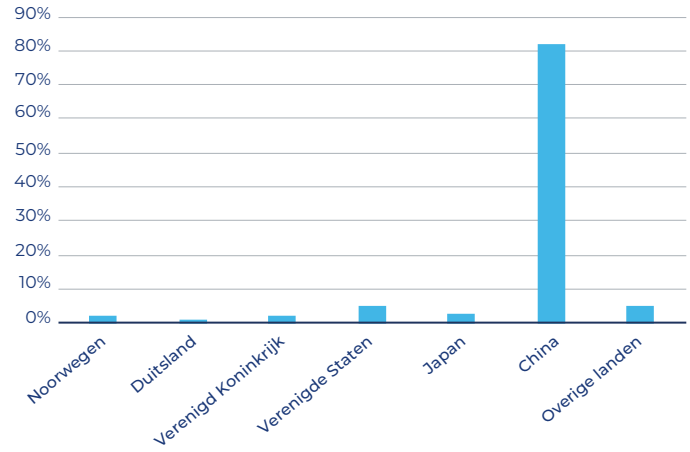
Nederland heeft relatief veel publieke laadpunten: 8% van het aantal publieke langzame laadpunten wereldwijd.[27]



Figuur 11. **Publieke langzame laadpunten per land in 2019.**

3.3.5 Snellaadpunten

Nederland heeft daarentegen relatief weinig snellaadpunten[28]: Het belang daarvan zal naar verwachting richting het jaar 2030 toenemen, zeker gezien de mogelijkheden van moderne EV's om te laden met een capaciteit rond of boven de 250 kW[29]. Extrapolatie van verwachtingen laat globaal een vervijfvoudiging van het aantal snelladers in 2030 zien. De snelladers worden vooral neergezet door autofabrikanten, zelfstandige en brandstof exploitanten, en restaurants en autoverkopers[30].



Figuur 12. **Publieke snelle laadpunten per land in 2019.**

3.3.6 Aanbieders van laadpunten en CPO's

Er zijn een beperkt aantal CPO's en laadpaalfabrikanten in Nederland actief.

Grotere laadpaalfabrikanten zijn onder andere:

- Alfen
- ChargePoint (USA)
- Ecotap
- Enovates (software en hardware voor laadpunten)
- EV Hub
- EVBox (onderdeel van het Franse energiebedrijf Engie)
- Ratio
- Schneider
- Webasto

Grotere CPO's zijn onder andere[31]:

- Allego
- BP met Volkswagen
- Eneco e-Mobility
- Engie
- FastNed
- Shell Recharge (incl. Newmotion en Ubricity)
- Vattenfall

HOOFDSTUK 4

De stabiliteit van het elektriciteitsnet

Om te berekenen hoe belangrijk een ongeplande verstoring van de nationale laadinfrastructuur is voor het elektriciteitsnet (door bijvoorbeeld een cyberaanval) gaan we in deze paragraaf in op de regelgrenzen van het elektriciteitsnet.

4.1 Inleiding: de balans in het elektriciteitsnet

Het Nederlandse (en het Europese) elektriciteitsnet moet permanent 'in balans' zijn voor een ongestoorde levering. 'In balans' betekent dat er op elk moment evenveel elektriciteitsvermogen wordt geleverd als dat er wordt gebruikt. Dat is niet eenvoudig: zo ligt tegenwoordig de piek 's avonds voor het slapen gaan en is er midden op de dag een dip. Zo varieert zowel het verbruik als de productie op een dag tussen de 5.000 en 21.000 MW [32].

In Nederland wordt die *balans* bewaakt door de TSO TenneT, die via diverse soorten contracten per kwartier met elektriciteitsproducenten ervoor zorgt dat er op elk moment van de dag evenveel elektriciteit wordt geproduceerd als er wordt verbruikt. Dat doet de TSO TenneT door goed te letten op de *frequentie* van het elektriciteitsnet. Als het elektriciteitsnet in balans is, is de frequentie precies 50 Hz: de stroom gaat 50 keer per seconde heen en weer. Als die frequentie onder de 50 Hz komt, betekent dat, dat er te weinig stroom wordt geleverd (de generatoren kunnen het tempo niet bijhouden), als de frequentie boven de 50 Hz komt wordt er te veel stroom geproduceerd.

Technisch is het Nederlandse elektriciteitsnet verbonden met de landen om ons heen tot het Europese elektriciteitsnet. Als er in Nederland te veel of te weinig elektriciteit wordt geproduceerd kan er stroom worden geëxporteerd of geïmporteerd naar het buitenland. Alle TSO's van Europa bewaken zo gezamenlijk de balans in hun verbonden en synchrone elektriciteitsnetten. De TSO's van Europa hebben zich daartoe verenigd in de Entso-e organisatie die in juridische documenten precieze afspraken maakt over de verplichtingen van alle TSO leden.

4.2 Regelgrenzen in het kader van dit onderzoek

Om de impact te duiden van verstoringen in de Nederlandse laadinfrastructuur wegens cyberaanvallen, hebben wij ook gekeken naar de keteneffecten stroomopwaarts: de impact op het Nederlandse elektriciteitsnet.

De verwachting van het Internationaal Energie Agentschap is dat in het jaar 2030 In Europa ongeveer 9,6% van de piekbelasting in de avond afkomstig is van het laden van elektrische auto's[33]. Als we dit getal als maatstaf aanhouden dan is de verwachting dat een dergelijke omvang naar verwachting goed is op te vangen in 2030 als we kijken naar het reguliere verbruik over de dag. Maar als we kijken naar de piekvermogens die we zelf berekenen (6.300 MW in 2030), dan kan dit rond één derde van het totale piek vermogen van Nederland zijn. Het verschil is te verklaren door relatief meer elektrische auto's in Nederland dan in Europa als totaal. Dit laat zien dat de uitdaging van de Nationale Laadinfrastructuur aanzienlijk is.

Als we ook gaan kijken naar de mogelijke impact van cyberaanvallen moeten we ook gaan kijken naar mogelijke verstoringen in een periode van seconden en minuten. We noemen drie voorbeelden om dit te illustreren.

1. Het eerste voorbeeld betreft de beperkingen die voortkomen uit de beperkte transportcapaciteit van het Europese net. Uit de recente separatie van het Europese elektriciteitsnetwerk op 8 januari 2021 blijkt dat een storing zich in slechts 43 seconden kan verspreiden van het initiële uitvallen van een hoogspanningslijn in Kroatië tot het separeren van het eerst nog aaneengesloten Europese elektriciteitsnetwerk in twee delen[34]. Door het uitvallen van één hoogspanningslijn worden de hoogspanningslijnen ernaast ook zwaarder belast, die vervolgens ook uitvallen, et cetera.

2. Na de separatie was er een tekort aan vermogen van 6.300 MW in het Noordwestelijke deel en een teveel aan vermogen van 6.300 MW In het zuidwestelijke deel. Door onder andere afschakelen van grote verbruikers in Italië en Frankrijk en het loskoppelen van een centrale in Turkije kon het effect worden beperkt en konden na een uur de twee delen weer met elkaar worden verbonden.

Figuur 13. **Splitsing Europese elektriciteitsnetwerk in twee delen op 8 januari 2021.**

Dit voorbeeld laat zien dat ook de transportcapaciteit een beperkende factor kan vormen. Dit geldt op Europese schaal maar ook binnen Nederland. Door zogenaamde 'congestie-management' kan TenneT binnen Nederland transport-problemen in het hoogspanningsnet oplossen, bijvoorbeeld door de aanvoer van elektriciteit in het ene deel van Nederland te verlagen en elders te verhogen, zodat de behoefte aan transportcapaciteit wordt verminderd.

3. Een tweede voorbeeld van de snelheid waarmee een storing kan optreden is de uitval van elektriciteit op 9 augustus 2019 rond Little Barford in Engeland. Na een blikseminslag in een transmissielijn volgde er een cascade van uitval van generatoren en windturbines totdat na 76 seconden bij een uitval van 1.700 MW een minimum frequentie van 48,8 Hz was bereikt. Daarop werd, zoals in dergelijke situaties gepland, stroom naar klanten afgeschakeld, zodat 1,1 miljoen klanten zonder stroom kwamen te zitten. De frequentie was mede daardoor na 5 minuten weer op 50 Hz gebracht[35], maar de klanten zaten tussen de 15 en 45 minuten zonder stroom.

4. Dat statelijke actoren in staat zijn om een elektriciteits-netwerk aan te vallen blijkt uit het voorbeeld van de aanvallen op DSO's in Oekraïne op 23 december 2015. In een gecoördineerde en lang voorbereide cyberaanval werden drie DSO's aangevallen, waarbij de besturing van het elektriciteitsnet met de SCADA-besturingssystemen door de aanvallers werd overgenomen. Daardoor werden dertig 35 kV en 100kV onderstations 3 uur afgeschakeld waardoor 225.000 klanten zonder elektriciteit kwamen te zitten. [36] [37]

Wij zullen ons in dit onderzoek voor de impact op het elektriciteitsnet derhalve primair richten op de mogelijke impact van cyberverstoringen op ***snelle*** verstoringen van de elektriciteitsvraag (of -aanbod) door laadpunten, omdat deze verreweg de grootste potentiële impact kunnen hebben.

4.3 Beheersing van snelle verstoringen in het elektriciteitsnet

Voor snelle verstoringen in het elektriciteitsnet in Nederland heeft de TSO TenneT de beschikking over drie soorten van tevoren gecontracteerd snel beschikbaar vermogen[38]:

1. Het Primaire reservevermogen (Frequency Containment Reserve (FCR)). Dit wordt binnen enkele seconden automatisch geactiveerd en moet volledig kunnen leveren in 30 seconden en dit vasthouden gedurende 15 minuten. Bij een afwijking van 0,2 Hz van de 50 Hz wordt dit maximaal gebruikt.
   De FCR van Nederland wordt samen met de TSO's van Oostenrijk, België, Duitsland, Westelijk Denemarken, Frankrijk, Slovenië, en Zwitserland op een dagelijkse veiling voor de volgende dag ingekocht. De FCR van Nederland moet binnen Nederland worden geleverd, met maximaal voor het over de grens te leveren vermogen. De FCR van de Nederlandse TSO: TenneT is voor het jaar 2021 vastgesteld op 114 MW.

2. Het Regelvermogen (automatic Frequency Restoration Reserve (aFRR)). Dit kan door de TSO worden geactiveerd en moet het gecontracteerde vermogen kunnen leveren binnen 15 minuten met 7% stijging per minuut. De aFRR van de Nederlandse TSO: TenneT is voor de tweede helft van het jaar 2021 vastgesteld op 290 MW zowel op als neer.

3. Daarnaast heeft TenneT de beschikking over de 'Manual Frequency Restoration Reserves directly activated' (mFRRda). Voor de tweede helft van 2021 is deze bepaald op 1015 MW opwaarts en 760 MW neerwaarts. Deze wordt manueel afgeroepen bij incidenten.

Nederland is echter ook onderdeel van het Europese elektriciteitsnetwerk hetgeen wordt beheerd door de TSO's, die leden zijn van de Europese vereniging ENTSO-e. De frequentie wordt zo dicht mogelijk in de buurt van 50 Hz gehouden: een overschrijding van meer dan 0,2 Hz wordt als kritisch beschouwd[39]. Het in de praktijk snel beschikbare vermogen wordt bepaald per 15 minuten en is verschillend per dag.

De TSO TenneT gaat uit van een uit van een maximaal referentie incident van 3.000 MW, zowel naar beneden als naar boven [40].

Als we dat in beschouwing nemen, zouden we eigenlijk ook het effect van een gelijktijdige cyberverstoring in Europa moeten meenemen, want systemen van CPO's, eMSP's en SCSP's zijn veelal grensoverschrijdend. Een cyberincident zal zich ook over grenzen heen kunnen manifesteren.

Naar verwachting zal de behoefte van Nederland aan elektriciteit in 2030 ongeveer 140.000 GWh zijn, een stijging van ongeveer 30% ten opzichte van 2020[3]. Door de verduurzaming van de energieopwekking zal de variatie aan elektriciteitsopwekking toenemen. Zo zal in 2030 naar verwachting de capaciteit van offshore windenergie zijn gestegen naar 20.000 MW[41].

Een andere beperking ligt in de hoeveelheid internationale cross-border connecties vanuit Nederland[42]: In totaal gaat het hier om ongeveer 9 interconnectoren met een totale capaciteit van ongeveer 21.000 MW. De belasting hiervan is wisselend, dan weer de ene, dan weer de andere kant op. Soms is de som van het vermogen van een transfer tussen twee landen boven de 3.000 MW[43].

4.4 Een fragiel en te krap bemeten distributienet

Door de energietransitie wordt het elektriciteitsnet zowel belangrijker als instabieler. Dat komt doordat zowel levering als verbruik decentraler wordt met minder invloed van de nationale TSO. Als er in 2030 1,8 miljoen laadpunten zijn en mensen bij thuiskomst hun auto aansluiten aan het laadpunt en stroom gaan vragen wordt in de toekomst het verbruik op het piekmoment 's avonds rond 18:00 uur versterkt. De uitdaging voor de balans voor het elektriciteitsnet wordt ook groter omdat de toevoer van elektriciteit ook steeds meer afhankelijk is van duurzame bronnen die afhankelijk zijn van het weer. Zo zal in 2030 naar verwachting de totale capaciteit van windenergie in Nederland met een omvang van 18.300 MW dicht bij het piek elektrisch verbruik van Nederland liggen[44]. Maar er zullen natuurlijk ook dagen zijn dat het windstil is en er weinig zon is en er toch elektriciteit moet worden geleverd.

De huidige omvang van het distributienetwerk voor elektriciteit is bij lange na niet genoeg om de energietransitie mogelijk te maken. Dat leidt nu ook al tot knelpunten, schaarste en een situatie waarin consumenten de komende jaren langer moeten wachten tot hun laadpaal aangesloten wordt[45]. De DSO Alliander meldt dat er straks in 2050 2,5 tot 6 keer zo veel vraag zal zijn naar stroom dan er nu capaciteit beschikbaar is[46]. Dat komt voor een belangrijk deel in een stad als Amsterdam door een sterke stijging van laadpalen, in combinatie met bijvoorbeeld de levering van stroom door zonnepanelen en extra behoefte aan stroom door nieuwe bedrijven en datacenters. Dat kan deels worden opgelost door kabels die nu 'in reserve' worden gehouden voor het geval er een storing in een andere kabel optreedt, óók in te zetten, maar daarmee leidt een storing in een kabel ook veel sneller tot een verstoring van de energielevering aan burgers en bedrijven.

De kans dat een storing leidt tot uitval wordt vergroot als transportcapaciteit die voorheen in reserve werd gehouden om in te zetten bij storingen, wordt ingezet voor regulier transport. Op 2 juli 2020 is door de Autoriteit Consument en Markt besloten dat dit is toegestaan aan de TSO TenneT voor een gedeelte van haar net in Noord-Nederland: de storingsreserve mag worden ingezet voor regulier transport van duurzame stroom, in het belang van de energietransitie[47]. Daarmee is voor dit deel van het net de 'N-1 redundantie' niet meer van toepassing.

Ook verschuift de levering van energie van grote generatoren naar een veelheid van decentrale opwekking van verschillende soorten duurzame energie waarvan het vermogen zeer wisselend kan zijn. In Nederland zijn dat voornamelijk:

- zonnepanelen; en
- windturbines.

Het verbruik van elektriciteit wordt vergroot doordat fossiele energiebronnen worden vervangen door elektrische energie:

- industrie;
- verwarming;
- vervoer.

Deze drie extra behoeften aan elektrische energie zijn verschillend over de dag maar onder normale omstandigheden wel redelijk te voorspellen. Ze maken de afhankelijkheid van elektriciteit natuurlijk wel nog groter dan deze al was. Als smart charging nodig gaat worden om binnen de capaciteit van het elektriciteitsnetwerk te blijven, creëert dit een extra kwetsbaarheid indien de smart charging wordt uitgeschakeld of niet meer goed werkt.

Ook kunnen er extra maatregelen nodig zijn om de netstabiliteit te borgen indien de productie van elektriciteit vrijwel geheel door hernieuwbare bronnen plaatsvindt. Denk aan blindvermogen. Wij gaan hier in het kader van dit onderzoek niet verder op in.

Daarnaast worden cyberrisico's vergroot doordat er een veelheid van consumentenapparaten via het internet aan een backoffice systeem ligt dat aan en uit kan schakelen en waarmee een substantiële vermogens-vraag of -aanbod kan worden gerealiseerd.

Denk aan:
- laadpunten;
- slimme thermostaten en Home Energy Management Systemen (zoals TOON);
- warmtepompen;
- zonnepanelen;
- wasmachines;
- ovens; en
- batterijen voor lokale opslag van elektriciteit.

4.5 Impact van de laadinfrastructuur op de elektriciteitsnetten

De toename aan regelbaar en relatief flexibel vraagvermogen, geeft grote mogelijkheden om in de toekomst te helpen de netten stabiel te houden. Als bijvoorbeeld smart charging wordt toegepast, wordt de piekvraag verminderd, en de elektriciteitsvraag uitgesmeerd over een grotere tijdsduur. Daarmee kan er meer vermogen worden aangesloten op de elektriciteitsnetten. Dat slimme en regelbare vermogen heeft echter ook een keerzijde, wanneer het regelbaar vermogen plotseling ingezet wordt op een manier die tegengesteld werkt aan wat nodig is om de netbalans te handhaven. Als er in de toekomst wordt uitgegaan van smart charging en dit opeens niet zou werken, zou de piekvraag in de avond opeens veel hoger zijn dan mét smart charging het geval zou zijn. Wanneer de netten daar niet meer op berekend zijn en veel voller zitten dan met zo een piekvraag kan worden voorzien, kan dit tot verstoringen leiden. In onderstaande analyse bekijken we wat de capaciteit is die het elektriciteitsnet typisch aankan, en hoe de groei van laadinfrastructuur daaraan relateert.

4.5.1 Nationaal tot internationaal

Het hoogspanningsnet is een 380 kV netwerk en kan typisch 2.000–2.500 MW vermogen transporteren. Eerder noemden we al dat TenneT als onderdeel van Entso-e uitgaat van snel schakelbaar noodvermogen van 3.000 MW. Dit vermogen moet snel kunnen worden bij- en afgeschakeld om de netbalans te waarborgen. Wanneer de laadinfrastructuur over enkele jaren is ingeregeld om met smart charging binnen de technische grenzen van het elektriciteitsnet te blijven, kan door het plotseling op- of afschakelen van het laadvermogen of door het uitzetten van smart charging bij een cyberaanval een black-out op nationaal of zelfs internationaal niveau worden veroorzaakt.

Bij niet toepassen van smart charging en enkel een plotseling uitval van daadwerkelijke stroomvraag van ladende personenauto's en bestelauto's, wordt een piekvraag van 3.000 MW volgens onze prognose rond 2027 bereikt. Het uitvallen van alle laadinfrastructuur tegelijk zou dan voor instabiliteit op het net kunnen zorgen. Wanneer levering van slechts één CPO uitvalt, is het slechts een percentage daarvan dat overeenkomt met hetgeen door een CPO wordt bediend. De dreiging van een nationale black-out door uitval van 1 CPO vindt waarschijnlijk pas in de periode na 2030 plaats.

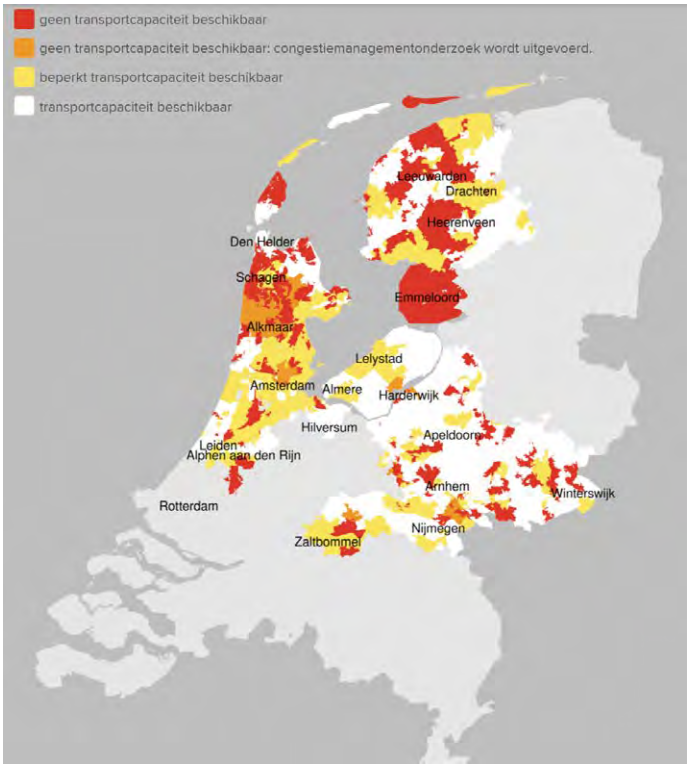
Bij smart charging van personenauto's en bestelauto's en bediening van alle CPO's tegelijk kan het vermogen van 3.000 MW eerder worden bereikt: namelijk wanneer het totaal op enig moment aangekoppeld vermogen de 3.000 MW bereikt. In paragraaf 3.2.5 hebben we beredeneerd dat dit vermogen al in 2025 wordt bereikt. Door alle voertuigen tegelijkertijd te laten terugladen kan het volledige aangekoppeld vermogen worden aangesproken voor een plotseling aanbod. Door alle voertuigen tegelijkertijd te laten laden kan ditzelfde vermogen worden aangesproken als plotselinge vraag. De dreiging voor de nationale netstabiliteit bij slimme besturing van álle personenauto's en bestelauto's is dus volgens onze prognoses al rond 2025. Zwaarder vrachtvervoer draagt bij aan de belasting maar is niet apart bekeken omdat deze naar verwachting ook een ander laadpatroon kent.

Verwachtingen van mogelijkheden voor smart charging worden gesteld op of na 2025. Het maximaal aangekoppeld volume is dan naar verwachting dus al 3.000 MW. Het is zaak om voor de tijd na te denken over de cybersecurity aspecten, zodat het onmogelijk is om op een manier alles tegelijkertijd te kunnen bedienen via één 'knop'. Bij de netbeheerders is segmentatie van regelvermogen standaard, om een vergelijkbare veiligheid in te bouwen. Toenemend vermogen van smart infrastructuur naast laadpunten, zoals slimme energiesystemen thuis, wasmachines, ovens, of warmtepompen, maken het extra dringend om over cyberveiligheidsnormen na te denken.

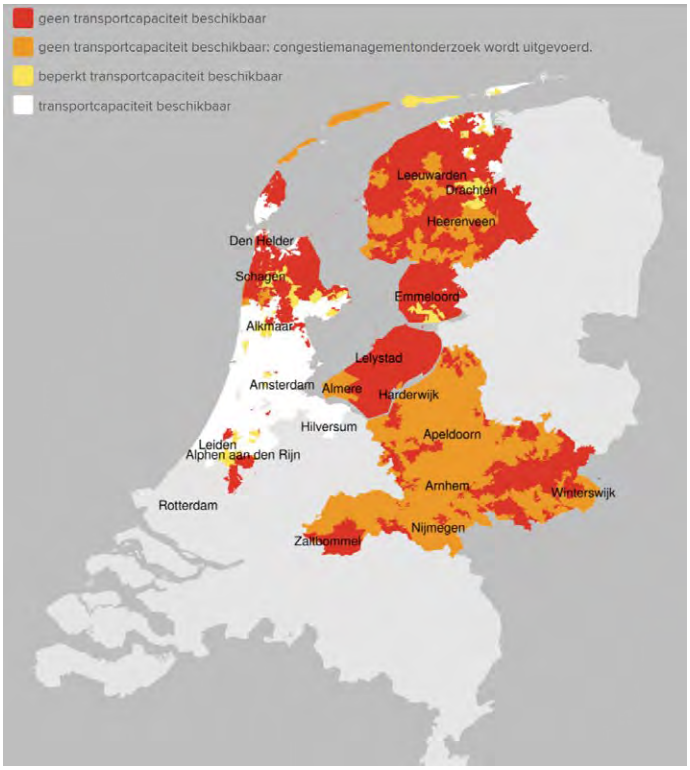
Regionaal en lokaal

Transportnetten op 150 kV hebben een transportcapaciteit van typisch 250-400 MW. Onder de transportnetten hangen de middenspanningsnetten van het distributienet, die de spanning verdelen over de lagere netvlakken. De distributienetten hebben een spanningsniveau van 10 – 20 - 50 kV, en daaronder zitten nog laagspanningsnetten op 400/230 V. Transformatorstations koppelen de verschillende spanningsniveaus van de netten. Een huishouden met een 3x25 Ampère aansluiting, heeft een maximaal totaal vermogen van 17 kW. De capaciteit van de transformatorstations tussen het middenspannings- en laagspanningsniveau zijn rond de 0,2-1 MW, en van middenspanning naar het 150 kV net rond de 100 MW. De transformatoren tussen transportnet (380 kV) en een koppelnet hebben veelal een vermogen groter dan 500 MW.

Op dit moment zijn er al meerdere plaatsen in Nederland waar congestie optreedt op de lagere netvlakken. Figuur 10 en figuur 11 illustreren dit middels een voorbeeld van de Liander netvlakken waar door de netbeheerder op dit moment al knelpunten worden ervaren bij afname en opwek voor grootverbruikersaansluitingen. De grootste knelpunten zijn het resultaat van de groei in aanbod van hernieuwbare elektriciteit, wat op lage netvlakken wordt ingevoerd en waar de netten niet op zijn berekend. Netverzwaringen duren lang en vergen planning, waardoor niet meer overal aansluiting kan worden verzorgd. Bij verstoringen op zwaar belaste netvlakken treden problemen eerder op dan wanneer ruime capaciteit beschikbaar is. Door slimme aansturing, zoals bij smart charging, kan de piekbelasting worden verlaagd en daarmee ruimte worden gecreëerd om meer aansluitingen te realiseren. De keerzijde is dat de druk op de netten daarmee wordt verhoogd.



Figuur 14. **Overzicht beschikbaarheid transportcapaciteit voor extra afname grootverbruik Liander . Bron: Liander.**



Figuur 15. **Overzicht beschikbaarheid transportcapaciteit voor extra aanbod grootverbruik Liander. Bron: Liander.**

Effecten van plotseling af- of opschakelen van laadvermogen van EVs, kan op de regionale netten al eerder impact hebben dan op het 380 kV net het geval is. De distributie van netten en aansluitingen varieert sterk door het land heen. Daarmee zullen sommige regio's gevoeliger zijn voor disrupties dan andere. Als de capaciteit maar net genoeg is voor de huidige situatie zal een verstoring makkelijker kunnen optreden. Het systeem staat dan al onder druk.

Ter illustratie: 100 MW, wat ongeveer de capaciteit is van een onderstation dat het distributienet met het 150 kV net verbindt, heeft ruimte voor 9.000 laadpalen van 11 kW, als die tegelijkertijd afnemen, mits er verder geen andere elektriciteitsvraag is bij dat station. Bij kleinere stations, van 20 MW, is die ruimte er slechts voor minder dan 2.000 laadpalen. Bij een disruptie van dat aantal laadpalen worden de grenzen van een onderstation al bereikt. Daarnaast is de impact afhankelijk van of een verstoring eenmalig of herhaaldelijk voorkomt. Op het moment dat er regionaal 25-100 MW actief wordt verstoord kunnen er al problemen met leveringszekerheid op regionaal niveau plaatsvinden.

De huidige concessies voor publieke laadpunten overschrijden de 1.000 laadpalen, ofwel de capaciteit van kleinere stations. In 2018 was er een concessie voor 4.500 publieke laadpalen, verdeeld over twee provincies en 43 gemeentes[48]. Een samenwerking tussen Rotterdam en 30 andere Zuid-Hollandse gemeenten beoogt het aantal publieke laadpunten uit te breiden met 7.000 in de komende 5 jaar. In gemeente Utrecht worden er via een concessie de komende 4 jaar 1.600 publieke laadpunten bijgeplaatst. Het is afhankelijk van de grootte van het gebied en configuratie van de netten wanneer daadwerkelijk grenzen van transport of transformatoren wordt bereikt. Op het moment dat smart charging noodzakelijk wordt om aansluiting te garanderen kun je ervan uitgaan dat bij plotselinge uitval van de mogelijkheid tot smart charging er problemen zullen optreden.

HOOFDSTUK 5

Cybersecurity van laadpunten

In dit hoofdstuk gaan we in op de cybersecurity van laadpunten.

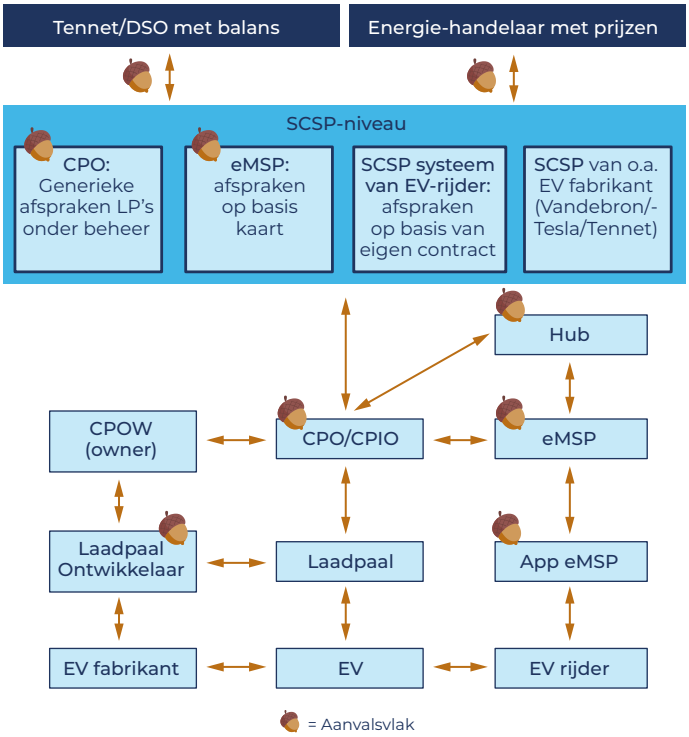
5.1 Inleiding

Achtereenvolgens gaan we daarbij in op:

- Een systeemoverzicht laadinfrastructuur: Welke elementen zijn er gezien vanuit het oogpunt van cybersecurity in de laadinfrastructuur?
- De regelgeving en normstellingen in de huidige situatie: Welke wetten en regelgeving bestaan er nu voor de laadinfrastructuur?
- De vulnerabiliteit in laadinfrastructuur: we gaan in algemene zin in op enkele achtergronden van de vulnerabiliteit van de nationale laadinfrastructuur, en geven enkele voorbeelden.
- Tot slot geven we een kort overzicht van de typische fasen in een cyberaanval.

5.2 Systeemoverzicht laadinfrastructuur

In onderstaand schema geven wij een vereenvoudigd overzicht van de elementen van de laadinfrastructuur met daarin aangegeven wat de belangrijkste cyberaanvalsvlakken zijn.



Figuur 16. **Vereenvoudigd overzicht laadinfrastructuur met cyberaanvalsvlakken.**

Per element geven wij hieronder een korte toelichting.

- EV = Electric Vehicle: dit is de elektrische auto die moet worden opgeladen. Een aanval op één auto is vervelend maar alleen bedreigend voor het systeem als zo andere elementen kunnen worden aangevallen.
- **EV-rijder:** de berijder van de auto.
- **EV-fabrikant**: deze kan een aanvalsvlak vormen en zo door bijvoorbeeld een besmette update ervoor zorgen dat een EV besmet raakt met malware.
- Laadpunt: deze kan één of meerdere EV's laden. Een cyber-aanval hierop is alleen gevaarlijk als van hieruit andere elementen kunnen worden aangevallen.
- De laadpunt ontwikkelaar kan een cyberaanvalsvlak vormen: als de updates[49] van de software malware bevatten kunnen vele laadpunten worden besmet. Daarmee is eventueel ook de in de software van het laadpunt opgenomen 'generieke' software een cyberaanvalsvlak.
- De CPO/CPIO (Charge Point (Infrastructure) Operator heeft veelal een backoffice systeem waarmee vele laad-punten worden beheerd. Dit is een belangrijk aanvalsvlak.
- De CPOW (Charge Point Owner, oftewel eigenaar van het laadpunt) kan een particulier zijn, een gemeente, een eigenaar van een parkeergarage, etc. Veelal hebben ze geen gegevensuitwisseling met laadpunten en hebben daarom geen cyberaanvalsvlak[50].
- De eMSP (eMobility Service Provider) levert kaarten, soms een App en financiële services, zodat EV-rijders bij publieke laadpunten kunnen opladen en later daarvoor een rekening krijgen. Zij vormen een cyberaanvalsvlak, omdat zij namen en laadgegevens van klanten kennen, die privacygevoelig zijn.
- De App van de eMSP kan een functie hebben als identificatie en ook om het laden te beïnvloeden en laadgegevens te zien. Daarmee is het een cyberaanvalsvlak voor het laadgedrag en voor privacy.
- De roaming Hub geeft door van de eMSP naar de CPO welke kaarten geldig zijn, en van de CPO naar de eMSP welke ladin-gen zijn uitgevoerd. Omdat hier geen directe persoonsgegevens worden uitgewisseld is het een beperkt cyberaanvalsvlak.
- Het SCSP-niveau kan nog op meerdere wijzen in de toekomst worden ingevuld. Vaak vanuit een bestaande partij in de laadinfrastructuur.
- De meeste ervan vormen een cyberaanvalsvlak omdat middels stuursignalen laden kan worden verminderd of in de toekomst ook kan worden ontladen via V2G (Vehicle to grid).
- TenneT en DSO kennen de balans op nationaal en lager niveau. De informatieverstrekking aan het SCSP-niveau is een cyberaanvalsvlak aangezien manipulatie hiervan het laadgedrag van vele CPO's (plotseling) kan laten veranderen.
- Energiehandelaar met prijzen is een speler waarvan wij verwachten dat deze bij een smart grid zal opkomen en gebaseerd op contracten per dag per 15 minuten prijzen kan bieden aan EV-rijders, eMSP's en CPO's. Manipulatie van deze gegevens kan tot een plotseling veranderd laadgedrag leiden en daarmee een cyberaanvalsvlak creëren.

Voor het daadwerkelijk gevraagde vermogen is het belangrijk te beseffen dat vele elementen uit dit schema het gevraagde vermogen kunnen afknijpen. Dat begint met de EV: de oplaadstatus van de accu en beperkingen vanuit de oplaadsoftware kunnen ervoor zorgen dat er minder hard dan het maximum wordt opgeladen. De laadpaal zelf kan het te leveren vermogen beperken, zeker als het laadpunt minder dan het maximum kan leveren, door bv. beperkingen vanuit de elektriciteitsaansluiting of beperkingen door meerdere laadsessies. De CPO/CPIO kan de oplaadsnelheid van de aangesloten laadpunten beperken, bijvoorbeeld vanuit overwegingen van inkoopprijzen of beperkingen vanuit de maximale capaciteit van meerdere laadpunten. De SCSP kan vanuit vele overwegingen, waaronder actuele prijs en balans, de aangesloten CPO's en laadpunten een signaal geven om minder te laden. TenneT en de Energiehandelaar met prijzen geven informatie aan de SCSP op basis waarvan deze kan sturen op minder laden dan het maximum.

5.3 Regelgeving en normstellingen in de huidige situatie

Momenteel bestaan er eigenlijk geen wettelijke normen voor de cybersecurity van laadpunten en de achterliggende infrastructuur.

Wel bestaan er een aantal regels en normen of startpunten om deze in de toekomst te ontwikkelen. Wij noemen de volgende:

5.3.1 Security requirements for procuring EV charging stations van ENCS en ElaadNL

De ***'Security requirements for procuring EV charging stations' van ENCS en ElaadNL***[51]. Hoewel deze richtlijn niet formeel afgedwongen wordt, wordt deze sinds 2017 veel voorgeschreven bij openbare aanbestedingen voor concessies voor publieke laadpunten in Nederlandse gemeenten en provincies[52]. Daardoor wordt deze norm door CPO's en laadpuntfabrikanten beschouwd als een *de facto* norm waar ze aan zouden moeten kunnen voldoen.

In deze eisen zijn cybersecurity eisen opgenomen ten aanzien van het laadpunt zelf:

a. Authenticatie en autorisatie voor gebruikers en systemen.
b. Cryptografische sleutels.
c. Openmaken en logging van security gebeurtenissen.
d. Op afstand updaten van firmware.
e. Beperken van kwetsbaarheden met 'hardening'.
f. Bescherming van de communicatie via een WAN.
g. Ontwikkelproces van de software van het laadpunt.

Het is voor laadpuntfabrikanten eenvoudiger om één of enkele types laadpunten op de markt te brengen. Doordat ze moeten voldoen aan deze security eisen en Nederland op dit moment een belangrijke markt is voor laadpunten, wordt dit wel als een standaard gezien.

Dit betekent niet dat alle op de markt aangeboden laadpunten hier ook geheel aan voldoen. Bij testen van de feitelijke eigenschappen wil nog wel eens blijken dat aanpassingen nodig zijn. Het is onduidelijk of deze eisen ook altijd geheel worden toegepast bij private laadpunten, die het grootste aandeel vormen. Ook kan in het beheer of de feitelijke levering door sommige leveranciers worden gekozen voor een lagere cybersecurity, omdat dit bijvoorbeeld eenvoudiger is in het beheer en daarmee kostenbesparend is.

Daarnaast geeft deze norm wel security eisen aan het laadpunt zelf, maar beperkt en alleen indirect aan het backoffice systeem ('CSMS') dat het laadpunt beheert en kan aansturen.

Er zijn nog veel laadpunten die de lagere versie 1.6 van het OCCP-protocol gebruiken, waarbij ook beveiliging van de verbinding middels alleen username en password kan plaatvinden zonder certificaten aan de zijde van het laadpunt en van het backoffice systeem.

5.3.2 NIS directive en Wbni

Momenteel maken laadpunten geen onderdeel uit van de vitale infrastructuur en vallen daarmee ook niet onder de Wbni: de Wet beveiliging netwerk – en informatiesystemen[53]. Aanbieders die hieronder vallen moeten passende technische en organisatorische maatregelen treffen om hun ICT-systemen te beveiligen en hebben daarnaast een meldplicht. Indien laadpunten of de backoffice systemen ervan als vitaal zouden worden aangemerkt zouden ze moeten gaan voldoen aan de zorg-, meld en toezichtsplicht die daarbij hoort. De Wbni is een Nederlandse invulling van de 'NIS directive' van de Europese Unie [54] en wordt mogelijk in de komende jaren aangepast.

5.3.3 Nationale Cybersecurity Agenda

De Nationale Cybersecurity Agenda (NCSA) [55] is in 2018 uitgekomen en omvat 7 ambities. Deze NCSA is in 2021 geëvalueerd en op 11 juni 2021 aan de Tweede Kamer aangeboden door de minister van Justitie en Veiligheid. Op 28 juni 2021 is, door de minister van Justitie en Veiligheid, het Cybersecuritybeeld Nederland aangeboden aan de Tweede Kamer en tegelijkertijd geïnformeerd over de voortgang van de Nederlandse Cybersecurity Agenda. Op basis van de aanbevelingen uit de evaluatie kunnen belangrijke leerpunten worden geïdentificeerd. Een besluit over de opvolging van de Nationale Cybersecurity Strategie zal moeten worden genomen door het volgende kabinet.

5.3.4 EU cybersecurity certification framework

Op Europees niveau is het 'EU cybersecurity certification framework' in ontwikkeling. Dit moet een basis gaan bieden voor 'EU-brede certificatie schema's'. Zo'n certificatie schema behelst welke categorieën van producten of diensten erdoor worden beschreven, welke cybersecurity vereisten zoals standaarden of technische specificaties er bestaan, hoe wordt geëvalueerd en het beoogde niveau van beveiliging dat ermee wordt bereikt[56]. Daarbij is ENISA, de EU-agency for cybersecurity, betrokken die op basis van de EU-cybersecurity Act een aantal mandaten heeft gekregen op het gebied van cybersecurity[57]. Een dergelijk schema zou in de toekomst mogelijk een basis kunnen vormen van een EU-brede cyberbeveiligingsstandaard voor laadpunten.

5.3.5 CE-normen

Daarnaast bestaan er de CE-normen, welke betrekking hebben op de elektrische eisen aan het laadpunt, net zoals die gelden voor broodroosters of andere elektrische apparaten. Laadpunten worden veelal geassembleerd uit componenten die voldoen aan de CE-normen, echter dit betreft vooral normen op het gebied van elektrotechniek en fysieke veiligheid.

5.3.6 Radio Equipment Directive

Het Radio Equipment Directive is een directive van de EU en geldt sinds 2017 voor radioapparatuur dat wordt verkocht binnen de EU. Het zou betrekking kunnen gaan hebben op onder andere de communicatie, privacy en fraudepreventie van laadpalen met het backoffice systeem van een CPO.

5.3.7 Framework guideline on sector-specific rules for cybersecurity aspects of cross-border electricity flows

Ook zouden laadpunten of de backoffice systemen van bijvoorbeeld CPO's mogelijk onderwerp kunnen gaan uitmaken van het 'Framework guideline on sector-specific rules for cybersecurity aspects of cross-border electricity flows' van ACER, de European Union Agency for the Cooperation of Energy regulators. Ze maken er geen expliciet onderdeel van uit, maar zouden er in de toekomst wel onder kunnen gaan vallen. Het is mogelijk dat ze dan deel uitmaken van de Entiteiten in tabel 1, zoals een 'electricity digital market platform' of 'critical service provider' waarvoor de regels uit dit framework zullen gaan gelden[58]. Dit framework is in juli 2021 aangeboden aan de Europese commissie en zal binnen 12 maanden worden uitgewerkt tot een voorstel voor een network code.

5.3.8 Richtlijn energieprestatie van gebouwen

In de EU-richtlijn 2018/844 van 30 mei 2018 tot wijziging van Richtlijn 2010/31/EU betreffende de energieprestatie van gebouwen en Richtlijn 2012/27/EU betreffende energie-efficiëntie worden in artikel 8 eisen opgenomen over laadpunten, waaronder de eis dat in gebouwen met meer dan 10 parkeerplaatsen infrastructuur voor leidingen wordt aangelegd voor minimaal één op de 5 parkeerplaatsen in gebouwen niet geschikt voor bewoning en voor elke parkeerplaats in gebouwen wel geschikt voor bewoning. Er worden echter geen functionele of security eisen aan verbonden.

5.3.9 Overige directives en regulations

Daarnaast bestaan er diverse andere directives en regulations vanuit de Europese unie met raakvlakken naar laadpunten, maar dit zijn veelal beperkte of geen cybersecurity bepalingen[59]:

- Trans-European Network for Transport (TEN-T) Regulation review;
- Alternative Fuels Infrastructure Directive (gepubliceerd in 2021; deze krijgt de status van 'Regulation');
- CO_2 Emissions for cars and vans performance standards;
- Clean vehicles directive;
- Sustainable and smart mobility strategy;
- Renewable energy directive II 2018/2001/EU (nieuwe versie in 2021 verwacht);
- Energy eficiency directie (EU) 2018/2002 ;
- The European Green Deal ;
- 2030 Climate target.

5.3.10 Regels aan laadpunten vanuit Verenigd Koninkrijk

In het Verenigd Koninkrijk wordt gewerkt aan beveiliging van het smart charging systeem. Wellicht kan dit ook binnen de EU inspireren.

Er is in het Verenigd Koninkrijk onderkend dat cyberrisico's bestaan en dat het hacken van controlesystemen van laadpunten de stabiliteit van het elektriciteitssysteem bedreigen als grote aantallen laadpunten tegelijk kunnen worden gemanipuleerd[60]. In het Verenigd Koninkrijk zijn 90-100 leveranciers actief, deze hebben 800 modellen laadpunten laten goedkeuren en de top-drie laadpaalproducenten hebben marktaandeel zien zakken van 95% in 2014 tot 70% in 2020. Daarbij is gekozen voor de volgende beleidskeuzen[61]:

a. Alle private laadpunten moeten 'smart' zijn, dat betekent dat ze ook moeten kunnen terugleveren aan het eigen huis of het net, zonder V2G nu al verplicht te maken.
b. Alle laadpunten moeten gedurende de set-up standaard zijn ingesteld om niet op te laden tijdens piektijden (8:00 uur tot 11:00 uur en 16:00 uur tot 22:00 uur op werkdagen).
c. Alle laadpunten moeten een willekeurige vertraging hebben om te starten met laden (zodat niet bijvoorbeeld alle laadpunten om 22:00 uur exact beginnen met laden, want dan zou er een nieuwe plotselinge piekbelasting ontstaan).
d. Alle laadpunten moeten in ieder geval al voldoen aan de minimale eisen van de Internet Of Things cybersecurity standaard ETSI EN 303 645[1]. Deze eisen gaan gelden vanaf de herfst van 2022.

5.4 Vulnerabiliteit in laadinfrastructuur

Doel van het onderzoek is om te onderzoeken wat de cybersecurity aspecten zijn van de nationale laadinfrastructuur in 2030.

5.4.1 Toenemende belang cyberveiligheid

Door verschillende instanties wordt gewezen op het toenemende belang van cyberveiligheid.

In het Cyber Security Beeld Nederland 2021 (CSBN 2021) van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) dat in samenwerking met het Nationaal Cyber Security Centrum (NCSC) is opgesteld, wordt gesteld dat de dreiging op cyber gebied zich steeds verder ontwikkelt, en de dreiging vanuit statelijke actoren zich steeds mee vermengt met de dreiging vanuit cybercriminelen. Daarbij is ransomware een solide verdienmodel voor cybercriminelen geworden. Voorbereidingshandelingen voor sabotage vormen een risico voor de nationale veiligheid.

In juli 2021 werd ook door Angeline van Dijk, directeur van het Agentschap Telecom, gewaarschuwd dat de overgang naar een duurzame energievoorziening het Nederlandse stroomnetwerk kwetsbaarder voor hackers kan maken. In het bijzonder werden daarbij zonnepanelen en laadpunten genoemd. Vooral als software om deze aan te sturen wordt aangevallen is er een probleem[62]. In het rapport 'Cybersecurity risico's voor het elektriciteitsnet in het licht van de energietransitie' van het Agentschap Telecom wordt opgemerkt:

- dat men bezig is om overbelasting bij smart charging te voorkomen door eisen te stellen, maar dat het lastig is om eisen te stellen richting consumenten;
- dat een grootschalige hack van laadpunten, de backoffice ervan of van de autofabrikant een zeer hoge ranking krijgt vooral wegens de gemiddelde kans en een hoge maatschappelijke impact;en
- dat de producent te klein is om onder huidige toezichtregime te vallen waardoor geen zicht is op cybersecurityrisico's [63].

1 Deze standaard geeft een basis aan van regels voor consumenten Internet of Things apparaten, maar verwacht verdere uitwerking in andere standaarden.

5.4.2 Analyse ICT-cyberaanvalsvlakken laadpunten

Bij de uitwerking van de gevoeligheidsanalyse onderscheiden wij twee verschillende aspecten: laterale vulnerabiliteit en keteneffecten. Beide aspecten zullen we onderzoeken.

5.4.3 Laterale vulnerabiliteit

Laterale cyber vulnerabiliteit komt voor als een bepaald onderdeel van een software netwerk is gecompromitteerd, dat daarna eenvoudig ook andere onderdelen van dit software netwerk kunnen worden aangevallen. Een voorbeeld was een deel van de NotPetya malware, die de malware zelfstandig verspreidde naar andere computers in hetzelfde netwerk. Voor laadpunten kan laterale vulnerabiliteit zich manifesteren indien bijvoorbeeld een SCSP zich technisch in hetzelfde netwerk bevindt als de CPO's waarmee de SCSP communiceert.

5.4.3.1 Voorbeelden laterale vulnerabiliteit laadpunten

Recent is duidelijk geworden dat de cybersecurity van laadpunten te wensen overlaat. Door onderzoekers konden meerdere typen laadpunten worden gehackt. Sommige laadpunten waren ook in opzet eigenlijk niet veilig doordat ze gebruik maakten van technieken die niet veilig te krijgen zijn. De onderzoekers konden zo een laadpunt overnemen, toegang krijgen tot het Wi-Fi netwerk, of toegang krijgen tot het backoffice systeem door via de API toegang te krijgen[64]. Of door de firmware te updaten. Het waren ook niet de kleinste: één leverancier had 2,9 miljoen apparaten in beheer. Sommige leveranciers reageerden snel en andere pas nadat een journalist ging informeren[65]. Er wordt in dit onderzoek ook gesteld dat door in backoffice systemen in te breken en vele laadpunten afwisselend aan en uit te zetten het elektriciteitsnet kan worden gedestabiliseerd waardoor black-outs kunnen ontstaan[67].

De kwetsbaarheid van de laadinfrastructuur voor cyberaanvallen zou natuurlijk aanzienlijk worden verminderd indien een laadpunt in het geheel niet zou worden gekoppeld aan een backoffice systeem van een CPO. Wij verwachten niet dat substantieel plaats zal gaan vinden om de volgende redenen:

- De tendens is juist dat devices steeds meer via internet aan backoffice systemen worden gekoppeld.
- Om (het door vele partijen gewenste) smart charging mogelijk te maken zal een laadpunt gekoppeld moeten worden aan een backoffice systeem die de actuele situatie en prijzen van het elektriciteitsnet kent.

5.4.4 Verticale vulnerabiliteit: Keteneffecten en maatschappelijke impact stroomstoring

Keteneffecten doen zich voor indien uitval van de ene component leidt tot uitval van de andere component. Dit kan bijvoorbeeld plaatsvinden indien uitval van een eMSP het gebruik van een CPO belemmert. Maar ook stroomopwaarts: bij plotselinge op- of afschakeling door CPO's kan de TSO of DSO in problemen komen. En ook stroomafwaarts: bij uitval van laadpunten valt vervoer uit waardoor diverse (vitale) sectoren in problemen komen. Zie als voorbeeld de files in de Rotterdamse haven na het uitvallen van de containerterminal van Maersk of de beperkte levering door tankstations na de ransomware aanval op Colonial Pipeline in mei 2021.

Maatschappelijke kosten bij uitval zitten in de volgende verschillende factoren:

- Verlies bedrijvigheid
- Mobiliteitsverlies (deels kan dit later worden 'ingehaald' maar deels ook niet)
- Uitval van nooddiensten
- Vastzittende liften
- Uitval 112 alarmlijnen
- Uitval van koelkasten
- Uitval van verwarming
- Mensenlevens

In deze studie doen we geen uitgebreide Maatschappelijke Kosten Baten Analyse van mogelijke stroomuitval, maar wel zijn er kengetallen te geven aan de hand van een paar historische situaties.

In een studie in 2003 werden de maatschappelijke kosten van een storing overdag in de Randstad geraamd op 72 miljoen euro per uur[66], zijnde een veelvoud van de niet geleverde stroom wat slechts ging om 1,6 miljoen euro[67]. Verschillen tussen sectoren bleken sterk, met de omvang van verloren vrije tijd voor huishoudens die vergelijkbaar was met de productieverliezen van bedrijven. Daarbinnen was de schade in de dienstensector groter dan in de industrie.

Een steeds groter aandeel van de energiebehoefte wordt afhankelijk van elektriciteit. Denk aan mobiliteit, warmte-voorziening, en dienstverlenende werkzaamheden. Bij de stroomuitval in 2017 in Amsterdam zaten 360.000 huis-houdens vanaf 4:00 uur 's nachts zonder stroom, lag het treinverkeer stil, viel de stadsverwarming uit en zaten 20.000 huishoudens zonder verwarming. Rond 9:00 uur was de stroomstoring helemaal verholpen, maar het duurde langer om ook de warmtevoorzieningen weer helemaal op te starten en afgekoeld water voor stadsverwarming op de juiste temperatuur te krijgen. De economische schade werd geschat op 20-30 miljoen euro.

Toekomstige effecten zullen bij langere storingen ook zwaarder wegen op diensten die afhankelijk zijn van elektriciteit, zoals mobiliteit van hulpdiensten. Als brandweer, politie, of ambulance niet meer kunnen uitrukken vanwege lege accu's kan noodhulp niet worden geboden waar nodig. Bij langere stroomstoringen stijgen de kosten navenant.

Ook onverwachte en onbedoelde cascade-effecten kunnen de impact van een storing in mobiliteit en elektriciteitsvoorziening groter maken dan in eerste instantie voorzien. Als voorbeeld: als (een deel van) een ziekenhuis ondanks noodvoorzieningen toch geen verwarming meer heeft, wordt de brandweer opgeroepen. Maar na het helpen bij het verplaatsen van patiënten kan ook batterij van de brandweerwagen uitgeput zijn waardoor niet meer naar een brand kan worden gereden. Et cetera.

In §3.2 is een inschatting gemaakt van de hoeveelheid vermogen die kan worden bestuurd via laadpunten op verschillende tijdstippen van de dag.

5.5 Fasen cyberaanval

Een cyberaanval verloopt in fasen. Deze fasen bestaan globaal uit[68]:

1. **Initieel toegang verkrijgen**
   Dit kan plaatvinden door bijvoorbeeld het proberen van passwords, het sturen van een phishing mail met een besmet document met daarin malware, of het aanvallen van een niet goed gepatchte website met een bekende kwetsbaarheid, et cetera. Het resultaat is dat de hacker 'binnen' is.

2. **Consolidatie en voorbereiding**
   De hacker verkrijgt steeds meer privileges, beweegt zich 'lateraal' door het netwerk, verstopt zich en zorgt dat hij op meerdere manieren toegang kan verkrijgen. Hij kan veelal echter geen toegang krijgen tot andere netwerken als deze zijn afgescheiden van het netwerk waar de hacker al binnen is.

3. **Toeslaan**
   De hacker slaat toe. Hij haalt data uit het netwerk naar buiten, versleutelt gegevens middels ransomware, maakt systemen kapot, et cetera. Bij laadpalen kan hij bijvoorbeeld een laadpaal met besmette firmware updaten, waardoor smart charging niet meer werkt, of de besturing door de hacker kan worden overgenomen, of een monteur langs elke laadpaal moet om te herstellen, et cetera.

HOOFDSTUK 6

Impact gepaard gaande met cyber-security risico van laadinfrastructuur

6.1 Inleiding

Dit hoofdstuk gaat in op de maatschappelijke impact en keteneffecten van vier verschillende scenario's voor een cyberaanval. Deze werden met behulp van experts geïdentificeerd, en in dit hoofdstuk gegroepeerd zodat er vier globale scenario's konden worden geïdentificeerd. Per scenario analyseren wij de impact.

Het gaat hier conform de uitgangspunten om moedwillige aanvallen. Daarnaast zijn er vanuit informatieveiligheid natuurlijk ook andere verstoringen denkbaar, denk bijvoorbeeld aan storingen in internet, elektriciteit of telefonie; slecht werkende software of smart charging algoritmes, et cetera.

6.2 Overzicht scenario's

Wij identificeerden de volgende vier scenario's. Elk scenario is gebaseerd op een typische cyberdreiging. Van elke cyberaanval is de cyberaanval met de meeste impact beschreven als typische aanval. Er zijn natuurlijk van de vier beschreven scenario's met aanvallen variaties te bedenken met minder impact: denk aan een aanval op een kleinere speler, een aanval niet tijdens piekuren, een minder goed uitgevoerde aanval, et cetera.

Voor elk scenario geven wij aan: de belangrijkste cyberdreigingen die wij hebben geïdentificeerd, met motivatie, de methode met de actor, het gebruikte aanvalsvlak of functie, en de belangrijkste aanvullende maatregelen.

Per scenario geven wij de impact aan, alsmede een berekening van het jaar wanneer dit scenario over de regelgrenzen heen zal gaan.

6.3 Scenario 1: **Slimme aanval door Statelijke Actor**

Scenario	Motivatie	Methode met actor	Aanvalsvlak/functie	Belangrijke maatregelen
1	Disruptie NL samenleving	APT (Advanced Persistant Attack)	Backoffice grote CPO's (gebruik makend evt. van OCCP en OCPI protocollen	• Segmentatie • Bescherming software development • Authenticatie en Autorisatie • Hardening CPO's en SCSP's • Intrusie detectie, patching, logging

Bij een aanval volgens scenario 1 wordt de backoffice van een grote CPO gehackt. Van daaruit worden alle aangesloten laadpunten ingezet voor een aanval op het elektriciteitsnet. Daarbij wordt gebruik gemaakt van de mogelijkheden van smart charging. In dit scenario komt ook naar voren dat als voor de stabiliteit van het elektriciteitsnetwerk wordt vertrouwd op smart charging om de piekvraag te verminderen, dit ook een extra kwetsbaarheid introduceert als smart charging bewust door een kwaadwillende tegengesteld aan de bedoeling wordt ingezet om het elektriciteitsnetwerk te destabiliseren. Dit is in mindere mate ook van toepassing op het tweede en derde scenario.

Actor	Statelijke Actor
Motivatie	Disruptie samenleving
Aanpak	Aanval op één of meerdere backoffice systemen van laadpunten. In het bijzonder backoffice systemen van een CPO of SCSP. Daarbij wordt gebruik gemaakt van manipulatie van mogelijkheden van smart charging
Impact TSO	Mogelijk een black-out van Nederland en afschakeling van Nederland uit het Europese netwerk, en mogelijk een black-out van Europa, zeker als de CPO ook in meerdere andere landen actief is
Impact DSO	Lokale verstoringen en black-outs, ook vanuit TSO
Impact CPO	Verstoorde werking aangevallen CPO, bij uitval elektriciteitsnetwerk uiteraard ook uitval laadinfrastructuur overige CPO's
Impact eMSP	Geen
Impact nationale laadinfrastructuur	Uitvallen nationale laadinfrastructuur. Ook doden te verwachten als elektrische hulpverleningsvoertuigen niet meer inzetbaar zijn: ambulances, politie, et cetera
Impact mobiliteit Nederland	Uitval mobiliteit gedurende black-out na het opraken van accu's van EV's.
Mogelijk bereikt in welk jaar	Vanaf 2025. Hierbij gaan we uit van aanval op één CPO

6.4 Scenario 2: **Grote aanval door Statelijke Actor**

Scenario	Motivatie	Methode met actor	Aanvalsvlak/functie	Belangrijke maatregelen
2	Disruptie NL samenleving	APT	Communicatie TenneT en elektriciteits-marktpartijen met SCSP's	• Encryptie communicatie stuursignalen en marktprijzen. • Tweezijdige authenticatie, segmentatie, beveiliging autorisatie
2	Disruptie NL samenleving	APT	Backoffice grote CPO's of EV fabrikant, ook OCCP en OCPI-protocollen Niet tweezijdige TLS Verspreiden Trojan via upgrade software laadpunten	• Authenticatie en autorisatie hardening CPO's en SCSP's • Intrusie detectie, patching, logging

Bij een aanval volgens scenario 2 wordt a) het stuursignaal vanuit TenneT met de netbalans of daarop gebaseerde prijzen gehackt, dan wel b) wordt een zeer centrale SCSP gehackt. Van daaruit worden alle aangestuurde laadpunten ingezet voor een aanval op het elektriciteitsnet. Daarbij wordt plotseling het laden via laadpunten onderbroken. Naar verwachting levert dit een verstoring van de netbalans indien het plotseling afgeschakelde vermogen groter is dan 3.000 MW.

Wij hebben 3.000 MW genomen als maatstaf omdat 3.000 MW wordt beschouwd als maatgevende referentie incident voor frequentieverstoring in het Europese Entso-e verband. In Nederland wordt een incident van 1.300 MW beschouwd als een incident dat de TSO zelf kan herstellen, maar omdat het Nederlandse net gekoppeld is aan het Europese zal een verstoring tot 3.000 MW naar verwachting geen werkelijk probleem opleveren. Ook een incident boven de 3.000 MW zou, afhankelijk van de omstandigheden op dat moment (bijvoorbeeld meerdere generatoren, welke actief zijn met een lage belasting) wellicht kunnen worden opgevangen. Wij zijn in dit rapport uitgegaan van bestaande en bekende regelgrenzen.

Een dergelijke aanval is natuurlijk ook mogelijk op één enkele grote CPO, maar omdat dan alleen de laadpunten van die CPO kunnen worden getroffen, zal het effect kleiner zijn. Als het bijvoorbeeld een CPO is die 20% van de laadpunten van Nederland beheerst, zal het maar om 20% van het piekvermogen zijn. Uitgaande van een piekvermogen voor persoonlijke EV's van 2.000 MW en een piekvermogen voor bestelauto's van 3.000 MW In het jaar 2030, is het effect maar 20% van 5.000 MW is 1.000 MW. Het kan dan van de locatie afhangen of dit tot directe problemen leidt op regionaal of nationaal niveau, of dat het door het elektriciteitsnet geabsorbeerd kan worden. In het bijzonder in stedelijke gebieden is de belasting van het elektriciteitsnetwerk dichter bij de maximale belasting en is de kwetsbaarheid dus hoger. Pas na 2030 zal een dergelijke aanval op één CPO tot een black-out leiden.

Actor	Statelijke Actor
Motivatie	Disruptie samenleving
Aanpak	Aanval op één of meerdere backoffice systemen laadpunten. Vooral CPO, SCSP of sturing vanuit TSO. Zodanig dat er meer dan 3000 MW in Nederland wordt afgeschakeld
Impact TSO	Mogelijk een black-out van Nederland en afschakeling van Nederland uit het Europese netwerk.
Impact DSO	Lokale verstoringen en black-outs, ook vanuit TSO
Impact eMSP	Geen
Impact nationale laadinfrastructuur	Uitvallen nationale laadinfrastructuur
Impact mobiliteit Nederland	Ook doden te verwachten als elektrische hulpverleningsvoertuigen niet meer inzetbaar zijn: ambulances, politie, etc.
Bereikt in welk jaar	Na het jaar 2027 indien een verbinding met TenneT of een centrale energieleverancier wordt aangevallen. Waarschijnlijk na het jaar 2030 indien een enkele grote CPO wordt aangevallen

Hoe groter de black-out, hoe langer deze meestal zal duren. Bij een landelijke black-out zijn de gevolgen significant. De duur zal ongeveer 8 uur zijn. Als de schaal nog groter is dan nationaal kan het nog langer duren. Boven de 8 uur is onbekend wat de gevolgen zijn. Zeker in het licht van toenemende afhankelijkheid van elektriciteit voor de voorziening van mobiliteit, maar ook warmte, telecommunicatie en IT.

Actor	Diverse actoren: scriptkiddie, antiduurzaamheid terroristen, criminele organisatie
Motivatie	Geld verdienen of uitproberen of een punt maken.
Aanpak	Aanval op één backoffice systemen laadpunten. Zodanig dat één CPO uitvalt.
Impact CPO	Uitvallen backoffice systeem van één CPO. Financiële schade (doordat een monteur naar elk laadpunt moet worden gestuurd) en imagoschade.
Impact eMSP	Waarschijnlijk beperkt; mogelijk financiële schade.
Impact DSO en TSO	Lokale verstoringen en brownouts of black-outs, ook vanuit TSO
Impact nationale laadinfrastructuur	Uitvallen laadpunten van één CPO. Mogelijk na enkele dagen weer live. Indien echter door de cyberaanval ook de firmware van laadpalen is gecompromitteerd, kan het weken duren voordat alle laadpalen langs zijn gegaan en handmatig zijn hersteld. Indien bepaalde essentiële diensten of een geografisch gebied sterk afhankelijk zijn van de getroffen CPO kan dit substantiële verstoring opleveren.
Impact mobiliteit Nederland	Minder beschikbaarheid publieke laadpunten. Een aantal private klanten kan niet meer thuis laden. Als het gaat om laadpunten met een hoge laadsnelheid: economische schade laadpleinen en bedrijven die overdag afhankelijk zijn van snelladers zoals bestelauto's, bevoorrading supermarkten.

6.5 Scenario 3: **'Gewone cyberaanval'**

Scenario	Motivatie	Methode met actor	Aanvalsvlak/functie	Belangrijke maatregelen
3	Financieel gewin	Criminele organisatie met ransomware	Technisch systeem onder SCSP of CPO systeem	Goede niet vanuit backoffice direct benaderbare back-up Intrusie detectie Adequate authenticatie
3	Bijvoorbeeld anti-duurzaamheid terroristen	DDOS	Toegang servers CPO's, eMSP's. Supply chain aanval door besmetting van door CPO gebruikte generieke software.	DDOS wasstraat inrichten CPO en eMSP
3	Uitproberen of boosheid	Onvoorspelbaar of scriptkiddie	Website, API van CPO	Basis op orde: autorisatie, authenticatie, patches
3	Maatschappelijk verstoring kleinere schaal	Gevangenen transport, ME, politie, brandweer, ambulance	Geografische informatie, CDR's veranderen	Idem.
3	Energieprijs op de beurs beïnvloeden door handelaren of Statelijke Actors	Flinke hack en van tevoren posities innemen		Idem.
3	Financieel gewin	Afromen van geldstromen, middelgrote actor	Hub, grote klap of kleine beetjes	Controle van geldstromen, authenticatie van juistheid uitgewisselde informatie.
3	Pech	APT	Ontsnapte Trojan met zero-Day	Segmentatie.

6.6 Scenario 4: **Privacy aanval**

Scenario	Motivatie	Methode met actor	Aanvalsvlak/functie	Belangrijke maatregelen
4	Vertrouwen in laadinfrastructuur aantasten of financieel gewin of spionage/voorbereiden aanval, spionage tussen partijen	Criminele organisatie of APT met semi-politieke doelen	Stelen CDR's (laaddata met privacy gegevens)	eMSP's : encryptie database CDR;'s, authenticatie, autorisatie Segmentatie Encryptie berichten

Actor	Vooral criminele organisaties, danwel Statelijke Actors met semi-politieke doelen.
Motivatie	Geld verdienen of vertrouwen in mobiliteit infrastructuur ondermijnen.
Aanpak	Vooral stelen van laadgegevens of gegevens van kaarthouders.
Impact CPO	Uitvallen backoffice systeem van één CPO.
Impact eMSP	Gegevens van klanten liggen op straat. Dalend vertrouwen.
Impact TSO	Geen
Impact DSO	Geen
Impact nationale laadinfrastructuur	Vermindering vertrouwen, dit leidt ook tot vertraging energietransitie.
Impact mobiliteit Nederland	Geen

Per scenario geven wij de impact aan, alsmede een berekening van het jaar wanneer dit scenario over de regelgrenzen heen zal gaan.

6.7 Kosten van een black-out in Nederland

Zoals hiervoor in dit hoofdstuk beschreven zijn er meerdere cyberaanvallen die het risico in zich dragen mogelijk tot een black-out te kunnen leiden. Een black-out in Nederland wordt veelal gedefinieerd als een situatie waarin meer dan 50% van de elektriciteitsvoorziening is uitgevallen. Gelukkig is dit in Nederland tot op heden niet voorgekomen. Daarom is er ook geen ervaring mee en statistiek hierover.

Hoe groter de black-out, hoe langer deze zal duren. Wij zijn uitgegaan van een black-out van 24 uur. In 2003 werden kosten van een stroomstoring overdag in de Randstad geraamd in de orde grootte van 72 miljoen euro per uur[70]. De kosten, en waar deze neerslaan, is mede afhankelijk van het tijdstip. Bij een storing overdag zijn er productieverliezen bij bedrijven, kan het moeilijk zijn om thuis te komen, en is er met name in de dienstensector grote impact.

De werkelijke kosten en schade kunnen natuurlijk anders uitvallen dan hieronder ruw berekend, onder andere door:

- een kortere duur van de black-out doordat de TSO en DSO's er in slagen om de storing sneller dan één dag op te lossen;
- een langere duur van de black-out doordat er nu nog onvoorziene cascade effecten optreden;
- een langere duur van de black-out doordat tijdens de herstelwerkzaamheden de cyberaanvallen doorgaan;
- de kosten voor geheel Nederland kunnen hoger uitvallen doordat de afhankelijkheid van elektriciteit in 2030 veel groter zal zijn dan de omvang zoals die in 2003 ten tijde van het opstellen van de schadepost van 72 miljoen bekend was.
- Zo komen wij tot een inschatting van de kosten van een black-out van 24 uur in Nederland[73], zoals weergegeven in Tabel 2.

Kosten schade één uur geen elektriciteit Randstad	72	Miljoen euro
Duur storing in uren	24	Uur
Totale schade gedurende Black-out	1.728	Miljoen euro
Omrekenfactor naar Nederland	2,2	
Totale schade Nederland gedurende black-out	3.736	Miljoen euro

Tabel 2. **Ingeschatte kosten van een landelijke black-out van 24 uur in Nederland.**

Een cyberaanval in Nederland kan ook effect hebben in andere landen. Ofwel doordat de cyberaanval ook laadpunten in andere landen treft, omdat bijvoorbeeld de aangevallen partij in meerdere landen actief is, en/of doordat een storing in de elektriciteitsvoorziening in Neerland ook doorwerkt naar andere Europese landen.

Bijlagen

BIJLAGE 1

Interviews

Er zijn interviews uitgevoerd met experts werkzaam bij de volgende partijen.

- Allego
- Agentschap Telecom
- ElaadNL
- ENCS
- eViolin
- Engie
- Enovates
- MultiTankcard
- Stedin
- TenneT
- Transport en Logistiek Nederland
- TU Delft
- TU Eindhoven

BIJLAGE 2

Lijst met afkortingen

aFRR	Automatic Frequency Restoration Reserve. Dit is het 'Regelvermogen'. Dit wordt aangestuurd door de TSO TenneT en kan na activatie binnen 15 minuten volledig worden ingezet.
CPO	Charge Point Operator
DDoS	distributed-denial-of-service
ENCS	European Network for Cyber Security. A non-profit member organization that brings together critical infrastructure owners and security experts to deploy secure European critical energy grids69.
ENTSO-E	European Network of Transmission System Operators for Electricity. Sinds 1 juli 2009 verantwoordelijk voor alle operationele taken van de TSO's in Europa.
eMSP	e-Mobility Service Provider
EV	Electric Vehicle
mFRR	Manual Frequency Restoration Reserve. Dit is het 'Reservevermogen'(mFRRsa) en 'Noodvermogen' (mFRRda). Dit vermogen kan door TSO worden ingezet bij langduriger onbalansen in het elektriciteitsnet om de aFRR weer 'vrij te spelen' zodat dit weer kan worden ingezet indien nodig.
OCPI	Open Charge Point Interface
OCPP	Open Charge Point Protocol
SCSP	Smart Charging Service Provider
SCADA	Supervisory Control And Data Acquisition
FCR	Frequency Containment Reserve. Dit is het 'Primair reservevermogen'. Dit vermogen kan binnen enkele seconden worden aangesproken en levert het volledig gecontracteerde vermogen binnen 30 seconden.

BIJLAGE 3

Referenties

Eindnoten

1 Deze definitie is met opzet beperkt van opzet. Hij is ook anders dan de definities in het Cybersecurity woordenboek van de Cybersecurity alliantie (https://www.cybersecurityalliantie.nl/documenten/publicaties/2019/09/30/cybersecurity-woordenboek) . Daarin is "Aanval' beschreven als "Actie waarbij iemand met opzet de beveiliging probeert uit te schakelen of te omzeilen om in een digitaal systeem te komen" , en is "Cyberaanval" beschreven als: "Een gerichte aanval in of via cyberspace. Doelwitten kunnen zijn: personen, groepen, bedrijven en organisaties, overheden, andere landen".
2 Klimaat- en Energieverkenning, PBL, 2020.
3 Klimaatakkoord, Den Haag, 28 juni 2019, p.50. Recharging economies: The EV-battery manufacturing outlook for Europe, McKinsey, p.3, mei 2019.
4 'Helft van Nieuwe auto's in VS moet vanaf 2E030 elektrisch zijn', NRC, 6 augustus 2021.
5 Zie ook het Klimaatakkoord, Den Haag, 28 juni 2019. Hierin is het aantal verwachte laadpunten geschat op 1,7 miljoen in 2030 (in de laatste ElaadNL prognose is dit 1,8 miljoen).
6 Nationaal laadonderzoek, ElaadNL, 2020. https:/www.elaad.nl/uploads/files/Rapport_Nationaal_Laadonderzoek_2020.pdf.
7 Jaaroverzicht Elektrisch rijden op (de) weg, RVO, 2020
8 Using electric vehicles as flexible resource in power systems: A case study in the Netherlands. A. Beltramo, A. Julea, N. Refa, Y. Drossinos, C. Thiel, and S. Quoilin. IEEE, 2017.
9 Elaad.nl Open datasets for electric mobility research, update april 2020.
10 ElaanNL outlook 'Elektrisch rijden in stroomversnelling', 1 november 2021. Online: https://www.elaad.nl/uploads/files/2021Q3_Elaad_Outlook_Personenautos_2050.pdf.
11 ElaadNL outlook 'Elektrisch op bestelling', 2020. Online: https://www.elaad.nl/uploads/files/20Q2_ElaadNL_Outlook_E-bestelvoertuigen_V1.0.pdf
12 Trends gebruik laadinfrastructuur, EV data, 3 september 2021, https://evdata.irias.nl/data?lang=nl.
13 Electric Vehicle integration into power grids, Entso-e position paper, entso-e, 31 maart 2021.
14 Electric Vehicle integration into power grids, Entso-e position paper, entso-e, 31 maart 2021, p.19.
15 Megawatt Charging System (MCS), Charin, 8 mei 2021, www.charin.global/technology/mcs/.
16 Electric Vehicle integration into power grids, Entso-e position paper, entso-e, 31 maart 2021, p.28 & p.29
17 https://www.charin.global/news/vehicle-to-grid-v2g-charin-bundles-200-companies-that-make-the-energy-system-and-electric-cars-co2-friendlier-and-cheaper/ .
18 The road to bidirectional CCS electric car charging, Bryce Gaton, 21 juli 2021, Online: https://thedriven.io/2020/07/21/the-road-to-bidirectional-ccs-electric-car-charging/
19 Electric Vehicle integration into power grids, Entso-e position paper, entso-e, 31 maart 2021.
20 Electric Vehicle integration into power grids, Entso-e position paper, entso-e, 31 maart 2021, p.29.
21 IEA, Contribution of electric vehicles to hourly peak demand by country and region in the evening and night charging cases in the Sustainable Development Scenario, 2030, IEA, Paris https://www.iea.org/data-and-statistics/charts/contribution-of-electric-vehicles-to-hourly-peak-demand-by-country-and-region-in-the-evening-and-night-charging-cases-in-the-sustainable-development-scenario-2030 .
22 Recharging economies: The EV-battey manufacturing outlook for Europe, McKinsey, p.3, mei 2019.
23 Elektrisch rijden wordt steeds goedkoper, nu.nl, 14 augustus 2021.
24 Tesla's 4680 battery cell is 'brilliant' according to industry experts, Iqtidar Ali, 4 oktober 2020, https://evannex.com/blogs/news/tesla-s-4680-cell-is-a-stroke-of-genius-sandy-munro.
25 Tesla model S Plaid fast charging result amaze: analysis, Mark Kane, 28 juli 2021, https://insideevs.com/news/515641/tesla-models-plaid-charging-analysis/ .
26 IEA, Private electric vehicle slow chargers by country, 2019, IEA, Paris https://www.iea.org/data-and-statistics/charts/private-electric-vehicle-slow-chargers-by-country-2019.
27 IEA, Publicly accessible electric vehicle slow chargers by country, 2019, IEA, Paris https://www.iea.org/data-and-statistics/charts/publicly-accessible-electric-vehicle-slow-chargers-by-country-2019 .
28 IEA, Publicly accessible electric vehicle fast chargers by country, 2019, IEA, Paris https://www.iea.org/data-and-statistics/charts/publicly-accessible-electric-vehicle-fast-chargers-by-country-2019 .
29 https://insideevs.com/news/515641/tesla-models-plaid-charging-analysis/
30 Snel, sneller, snelst, De ontwikkeling van snelladers in Nederland t/m 2025. Extrapolatie van het middenscenario komt ui op 8500 snelladers in 2030.
31 Zie bv. Dans om de laadpaalmarkt nog maar net begonnen, NRC, 20 april 2021.
32 https://www.tennet.eu/nl/elektriciteitsmarkt/data-dashboard/belasting/.
33 IEA, Contribution of electric vehicles to hourly peak demand by country and region in the evening and night charging cases in the Sustainable Development Scenario, 2030, IEA, Paris https://www.iea.org/data-and-statistics/charts/contribution-of-electric-vehicles-to-hourly-peak-demand-by-country-and-region-in-the-evening-and-night-charging-cases-in-the-sustainable-development-scenario-2030 .
34 System separation in the Continental Europe Synchronous Area on 8 January 2021 – 2nd update, Entso-e, 26 januari 2021, https://www.entsoe.eu/news/2021/01/26/system-separation-in-the-continental-europe-synchronous-area-on-8-january-2021-2nd-update/ . Start of events at 14:04:25.9 and separation of network completed at 14:05:08.6.
35 Technical Report on the events op 9 August 2019, ESO, 6 september 2019, 'National Grid ESO LFDD 09/08/2019 Incident Report', 37 pages, retrieved 23 june 2021 from www.nationalgrideso.com.
36 Can Cyber Attacks cause a blackout? b, A. Stefanov, TU Delft, 31 maart 2021.
37 Analysis of the cyber attack on the Ukrainian power grid, Defense use case, E-ISAC, 16 maart, 2016,
38 Dutch ancillary sevices, Tennet, retrieved from www.tennet.eu/electricity-market/dutch-acillary-services.html on 18 august 2021.
39 De grootste oplawaai in ruim tien jaar, www.hoogspanningsnet.com/tag/netfrequentie/. Opgehaald 15 juni 2021.
40 Dutch Ancillary Services, Tennet, "This means that an outage of 1000 MW anywhere in the synchronous area, should result in a Dutch FCR contribution of 37 MW. Since reference incident is 3000 MW in total" "https://www.tennet.eu/electricity-market/dutch-ancillary-services/: .
41 https://www.tennet.eu/electricity-market/transparency-pages/ ; "By 2030, the originally planned capacity of 15 gigawatts of offshore wind energy will increase to 20 GW."
42 https://www.tennet.eu/our-grid/international-connections/about-international-connections/ retrieved on 23 june 2021.
43 Bv. Op 15 augustus 2021 was de totale import m.b.v. interconnectoren uit Duitsland naar Nederland 3598 MW tussen 03:15 en 03:30 uur.
44 Review of wind generation within adequacy calculations and capacity markets for different power systems, L. Söder et al., Renewable and sustainable energy reviews 119 (2020) 109540, 22 november 2019.
45 https://www.liander.nl/nieuws/2021/06/24/knelpunten-op-het-elektriciteitsnet-amsterdam.
46 Alliander: 'Stad is hard op weg naar een stroominfarct', Het Parool, 3 augustus 2019, https://www.parool.nl/nieuws/netwerkbedrijf-alliander-stad-is-hard-op-weg-naar-een-stroominfarct~b74c497c/ .
47 Kenmerk ACM/UIT/534445, Zaaknummer ACM/19/036613, Besluit van de Autoriteit Consument en Markt op grond van artikel 37a van de Elektriciteitswet 1998, betreffende de ontheffingsaanvraag TenneT codebepalingen enkelvoudige storingsreserve, Autoriteit Consument en Markt, 2 juli 2020.
48 Gelderland en Overijssel gebruiken gezamenlijke inkoopkracht voor inkoop publieke laadpunten, Piano expertisecentrum aanbesteden, 2019.
49 Dit vindt niet bij alle CPO's plaats omdat updates soms niet goed lukken en storingen veroorzaken hetgeen een rit van een monteur vergt hetgeen kostenverhogend is.
50 Wel zou een cyber aanval op electriciteitsmeters of Home Electricity Management Systems ervoor kunnen zorgen dat de stuursignalen die deze afgeven in het geval van smart charging worden gecompromitteerd waardoor (ook) de laadpunten ongewenst gedrag kunnen gaan vertonen.
51 Security Requirements for procuring EV charging stations (https://encs.eu/encs-document/security-requirements-for-procuring-ev-charging-stations/, EV-301-2019, version 2.0, 24 december 2019.
52 ElaadNL: Niewe Eisen voor cybersecurity voor laadpalen het het eerst toegepast. 1 december 2016. https://www.elaad.nl/nieuwe-eisen-voor-cybersecurity-laadpalen-voor-het-eerst-toegepast/.
53 Beantwoording kamervragen welke zin gesteld door de het lid Renco Dijkstra (VVD) over het bericht 'Elektrische auto's duurder in onderhoud dan brandstofauto's, 22 januari 2021, brief van de Staatssecretaris van infrastructuur en waterstaat S. van Veldhoven – Ven der Meer aan de voorzitter van de Tweede Kamer der Staten-Generaal.
54 DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, Europese Unie, 19 juli 2016.
55 https://www.ncsc.nl/documenten/publicaties/2019/mei/01/nederlandse-cybersecurity-agenda .
56 'The EU cybersecurity framework', Euopse commissie, https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework, opgehaald op 2 augustus 2021.
57 The EU Cybersecurity Act, Europese commissie, https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act, opgehaald op 2 augustus 2021.12
58 'Framework guideline on sector-specific rules for cybersecurity aspects of cross-border electricity flows. ACER, 22 juli 2021.
59 Electric Vehicle integration into power grids, Entso-e position paper, entso-e, 31 maart 2021.
60 The Electric Vehicles (Smart Charge Ponts) Regulations 2021, Impact Assessment, 2021,
61 Smart Charging Consultation – Government Response, UK Government, July 2021.
62 'Hackers kunnen stroomnet saboteren via zonnepaneel en laadpaal', NOS, 12 juli 2021.
63 Riskid Cyber security risico's voor het elektricteitstnet in het licht van de energietransitie, Agentschap Telecom, 2021, p.77 en p.119.
64 Smart car chargers. Plug-n-play for hackers?, PenTestPartners, augustus 2021, https://www.pentestpartners.com/security-blog/smart-car-chargers-plug-n-play-for-hackers/.
65 Home car chargers owners urged to install updates, Dan Simons, BBC Click, 3 augustus 2021, www.bbc.com/news/technology-58011014.
66 "Gansch het radarwerk staat stil." De kosten van Stroomstoringen, C. Bijvoet, m. de Nooij, C. Koopmans, SEO, UvA, 2003, p.67.
67 Bij de DSO Enexis wordt voor een reguliere consumentenaansluiting de eerste 4 uur geen compensatievergoeding gerekend, voor de volgende 4 uur 35 euro, en voor elke 4 uur erna 20 euro. Deze 20 euro per 4 uur vertaald zich naar 8 cent per minuut. https://www.enexis.nl/consument/storingen-en-onderhoud/storingen/compensatievergoeding-na-storing . Dit bedrag is niet gelijk aan de maatschappelijke schade.
68 Lifecycle of a ransomware incident, CertNZ, 2021.
69 ENCS and ElaadNL, Security Requirements for procuring EV charging stations (https://encs.eu/encs-document/security-requirements-for-procuring-ev-charging-stations/).

Berenschot

‘WIJ ZIJN BERENSCHOT, GRONDLEGGER VAN VOORUITGANG’

Wij zien een Nederland dat altijd in ontwikkeling is. Zowel sociaal als organisatorisch verandert er veel. Al meer dan 80 jaar volgen wij deze ontwikkelingen op de voet en werken we aan een vooruitstrevende samenleving. Daarbij staan we voor duurzaam advies en de implementatie hiervan. Altijd gericht op vooruitgang én echt iets kunnen betekenen voor mensen, organisaties en de maatschappij.

Alles wat we doen, is onderzocht, onderbouwd en vanuit meerdere invalshoeken bekeken. In ons advies zijn we hard op de inhoud, maar houden rekening met de menselijke maat. Onze adviseurs doen er alles aan om complexe vraagstukken om te zetten naar praktische oplossingen waar u iets mee kan. Wij geven advies en bieden digitale oplossingen waarbij we ons focussen op:

- Toekomst van werk en organisatie
- Energietransitie
- Toekomst van zorg
- Transformatie van openbaar bestuur

Berenschot Groep B.V.

Van Deventerlaan 31-51, 3528 AG Utrecht

Postbus 8039, 3503 RA Utrecht

030 2 916 916

www.berenschot.nl