Conferentie over digitalisering van de stroomvoorziening: weten we wel genoeg van de risico's?

De Haagse Studio Dudok vormde op 24 april 2018 het decor van een conferentie over een actueel en complex onderwerp: de gevolgen van de digitalisering voor de betrouwbaarheid van onze stroomvoorziening. De bijeenkomst was georganiseerd door de Raad voor de leefomgeving en infrastructuur (Rli), naar aanleiding van het Rli-advies 'Stroomvoorziening onder digitale spanning'. Deskundigen op het gebied van cybersecurity, telecom, elektriciteit en waterveiligheid discussieerden in verschillende rondes met elkaar en met de zaal. Een verslag van een onderhoudende avond in 'DWDD-setting', met interessante gespreksdeelnemers.

De conferentie wordt geopend door tafelvoorzitter **Annemieke Nijhof** van de Rli, met aan haar zijde tafeldame **Birgitta Westgren**, directeur Energiemarkt en Innovatie bij het ministerie van Economische Zaken en Klimaat (EZK).

Annemieke Nijhof, raadslid Rli, geeft toelichting over advies 'Stroomvoorziening onder digitale spanning'

Nijhof geeft om te beginnen een schets van het advies van de Rli. Een 'dun' adviesje, aldus Nijhof, en dat komt doordat we eigenlijk nog maar weinig weten over de gevolgen die de digitalisering heeft voor onze stroomvoorziening. Wel voelt de Rli de urgentie om het onderwerp te agenderen. Want al hebben we het nog niet zo door, we zitten in het oog van een orkaan van transities en er gaat ontzettend veel veranderen. We gaan steeds meer elektriciteit gebruiken en die zal steeds vaker op een duurzame manier decentraal worden opgewekt door lokale windmolens en zonnepanelen.

Ook hoe we elektriciteit *gebruiken* wordt steeds complexer: de afname van stroom wordt meer en meer gestuurd door ingebouwde algoritmes die via internetverbindingen bepalen wat bijvoorbeeld een goed moment is voor het opladen van de accu van je auto. Als er veel stroomaanbod is, bijvoorbeeld doordat het dagenlang waait, laad je je accu op tegen een lagere prijs.
De digitalisering biedt dus veel mogelijkheden voor het optimaliseren van vraag en aanbod. Maar we worden tegelijkertijd wel kwetsbaarder. Onze afhankelijkheid van de besturing van de digitale systemen in onze apparatuur neemt toe. En doordat die besturing via internetverbindingen verloopt, is er het risico van *hacking*. We hebben her en der in de wereld kunnen zien dat moedwillige verstoring van digitale systemen tot grootschalige stroomuitval kan leiden. Maar ons elektriciteitsnet wordt vooral ook steeds kwetsbaarder door de geautomatiseerde systemen zélf: die kunnen onvoorzien gedrag vertonen. Als bijvoorbeeld zonnepanelen of elektrische auto's allemaal tegelijk een software-update krijgen waar een fout in zit, kan dat grote consequenties hebben voor de stabiliteit van het netwerk.

"Eigenlijk heeft niemand echt goed zicht op het totale systeem, op de samenhang der dingen"

Doordat de digitalisering overal in het systeem zit (aan de producentenkant, transportkant én de gebruikerskant) kan het systeem op al die punten 'van de leg' raken. Wij hebben in ons onderzoek vastgesteld, aldus Nijhof, dat eigenlijk niemand echt goed zicht heeft op het totale systeem, op de samenhang der dingen en hoe dat gaat veranderen. We weten er weinig van en rennen achter de feiten aan. Dat is een zorgelijke constatering. En daarom heeft de Rli geadviseerd: zorg dat je de kennis die er al is van het elektriciteitssysteem, *verbindt* met de kennis over digitalisering. Dat je daar iets voor institutionaliseert. En ook, omdat het een internationaal vraagstuk is: wacht niet op iets wat uit Brussel komt, maar zoek zelf Europese samenwerking.

Hoe is het advies gevallen bij het ministerie van EZK? "We waren er erg blij mee," laat tafeldame Birgitta Westgren weten. Het departement herkent het probleem: hebben we het elektriciteits-systeem wel voldoende in beeld en onder controle? En gaat dat ooit nog wel lukken? We zullen de risico's moeten gaan inventariseren, aldus Westgren. Wat haar betreft is de centrale vraag van de avond: hoe waarborgen we, gegeven de complexiteit die decentrale energieopwekking met zich meebrengt, de betrouwbaarheid en veiligheid van onze energievoorziening?

Als eerste tafelgast schuift **Raymond Kleijmeer** aan, cyberdeskundige bij de Nederlandsche Bank. Wat is zijn grootste zorg als het gaat om de betrouwbaarheid van het Nederlandse betalings-verkeer? Dat de pinautomaten uitvallen bij een grootschalige stroomstoring? Nee, dat is niet waar hij van wakker ligt. De *worst case*-scenario's waar financiële instellingen en centrale banken zich zorgen over maken hebben te maken met hackers en cybercrime – zeker wanneer er statelijke actoren bij betrokken zijn. Zulke systeemrisico's, stelt Kleijmeer, kunnen een grote impact hebben; als je ze niet snel oplost vliegen ze de hele wereld over. Voor de financiële sector betekent het risico van cyberaanvallen niet alleen dat we preventief muren moeten optrekken, maar ook dat we in staat moeten zijn om binnen twee uur een systeem weer werkend te krijgen; de zogenoemde *resumption time* is kort, omdat je moet voorkomen dat een probleem zich voortzet in andere tijdzones. De centrale banken in Europa hebben daarvoor richtlijnen opgesteld voor financiële instellingen.

"Wij zijn van een defensieve blik overgeschakeld naar 'denken als een aanvaller'"

Gevraagd naar zijn inschatting van de huidige veiligheid van het betalingsverkeer, geeft Kleijmeer een bemoedigend antwoord: hij slaapt de laatste tijd geruster dan een paar jaar terug. En dat komt, aldus Kleijmeer, doordat we er nu actief mee bezig zijn en dieper in de systemen maatregelen treffen. We hebben nu beter zicht op het probleem, we doorzien hoe hackers werken. Een belangrijke paradigmaverschuiving is voor DNB geweest: overschakelen van een defensieve blik naar 'denken als een aanvaller'. We hebben bijvoorbeeld, vertelt Kleijmeer, ethische hackers ingehuurd om aanvallen na te bootsen. Het probleem én de oplossing worden dan heel concreet. Je leert daar heel veel van. Er komt een plan uit met maatregelen om je beveiliging te verbeteren. Het gaat uiteindelijk om *security by design.* Je moet niet pas achteraf gaan nadenken over je veiligheid en veerkracht, maar al in de ontwerpfase van je systemen. En dat is iets waar ook de elektriciteitssector wereldwijd naar zou moeten streven.
In zijn bijdrage verwijst Kleijmeer naar een guidance: http://www.bis.org/cpmi/publ/d146.pdf en spreekt hij over redteaming, daarover is hier meer te vinden: https://www.dnb.nl/nieuws/nieuwsoverzicht-en-archief/nieuws-2017/dnb365801.jsp

In de tweede tafelronde buigen vijf gasten zich over de vraag: weten we straks nog wel hoe de ingewikkelde digitaal aangestuurde systemen voor elektriciteit en telecom precies werken? In het Rli-advies wordt gesignaleerd dat de overheid onvoldoende kennis heeft op dit terrein. De vraag is dan: welke kennis is nodig en waar halen we die vandaan? Birgitta Westgren legt om te beginnen de vraag op tafel: zijn er wellicht lessen te trekken uit de bankensector?
Volgens **Maarten Abbenhuis**, senior manager system operations van TenneT, zijn die er zeker. Het gaat vooral om de gevoeligheid voor aanvallen van buitenaf. We zijn in Nederland al een tijd bezig met veiligheidssystemen, met *security by design* als belangrijk uitgangspunt. En bij zowel energieproducenten als netwerkbeheerders wordt getraind op protectie en herstel. Maar: door de ontwikkelingen in het elektriciteitssysteem is een grotere kwetsbaarheid ontstaan en die delen we met heel veel landen. We hebben dus ons 'aanvalsoppervlak' vergroot. Daar moeten we goed over nadenken, aldus Abbenhuis.

"Grote storingen hoeven technisch gezien eigenlijk niet te gebeuren"

Volgens **Pallas Agterberg**, directeur Strategie bij Alliander, hoeven grote stroomstoringen in Nederland technisch gezien eigenlijk niet te gebeuren. Juist als we niet langer een centrale stroomproductie hebben, kun je bij een storing het probleem veel beter lokaal houden. De decentrale energieopwekking biedt wat dat betreft juist nieuwe mogelijkheden. Door de *compartimentering* die je kunt toepassen kun je het probleem verkleinen en zo je veerkracht vergroten. Maar dit is de technische kant van het verhaal. De vraag is wel: wie gaat dit praktisch realiseren?
Peter Spijkerman, directeur-hoofdinspecteur bij het Agentschap Telecom, belicht de digitaliseringsrisico's in relatie tot de telecomsector. Ook in de telecommunicatie speelt een publiek belang mee: denk bijvoorbeeld aan situaties waarin het mobiele netwerk uitvalt en het noodnummer 112 onbereikbaar is. Opmerkelijk is de secondenlange stilte die Spijkerman laat vallen na een cruciale vraag van voorzitter Annemieke Nijhof: zijn marktpartijen in de telecomsector bereid om op dit punt hun kennis te delen? Spijkerman moet toegeven: daar zijn ze nog niet aan toe. Ze zijn zelf nog aan het zoeken naar wat de afhankelijkheid van het wifi-netwerk betekent en wat eraan is te doen.
Remko Bos, directeur Energie bij de Autoriteit Consument en Markt (ACM) vertelt dat het toezicht op de energiesector sinds 2015 bewust scherper is gericht op de veiligheidsissues in de digitale processen. Er moet bij de netbeheerders op het gebied van digitale veiligheid nog het nodige gebeuren als het gaat om bewustwording (awareness), maar de ACM ziet daar wel een positieve ontwikkeling. De ACM is netbeheerders nadrukkelijk gaan vragen: maken jullie wel risicoanalyses? Laat ons zien hoe jullie de risico's indammen. En wat leren jullie van incidenten, en welke acties verbind je eraan? De ACM signaleert twee dingen: (1) de samenwerking tussen netbeheerders bij kennisuitwisseling en het zoeken naar oplossingen kan beter, en (2) het bewustzijn van wat er nodig is voor goede informatiebeveiliging moet nog verder groeien. Er is veel meer onderlinge kennisuitwisseling nodig om de sector in beweging te krijgen (tussen netbeheerders, maar ook met andere betrokken partijen in de keten). De *sense of urgency* om hiermee aan de slag te gaan groeit overigens wel. En het ACM-toezicht draagt daar volgens Bos ook aan bij . Het thema van digitale veiligheid bij spelers in energie wordt ook door CEER (Council of European Energy Regulators) nadrukkelijk opgepakt, bijvoorbeeld waar het gaat om kennisuitwisseling tussen toezichthouders. In meer generieke zin wijst Bos op het belang van een Europese aanpak op het vlak van digitale veiligheid: er komt in Nederland binnenkort nieuwe cybersecuritywetgeving, gebaseerd op Europese regelgeving. Daarnaast wordt er in Europa nagedacht over nieuwe regels om cascade-effecten te beperken. Ten slotte wijst Bos op bedreigingen van buitenaf: daarbij zou ook gekeken moeten worden naar potentieel onveilige – bijvoorbeeld uit China afkomstige - apparatuur en software aan de gebruikerskant van de markt. Mogelijk zou het invoeren van Europese certificeringsnormen op dit vlak soelaas kunnen bieden.
Frans Rooijers, directeur van onderzoeksbureau CE Delft, brengt een nieuw aspect in de discussie door te wijzen op de neiging van netbeheerders om veel aandacht te geven aan het besparende effect van een gedigitaliseerde elektriciteitsvoorziening ('smart grid'). Allerlei slimme schakelapparaatjes worden gehypet, aldus Rooijers, met als argument dat daarmee het verbruik van de klant kan worden 'gestuurd', zodat de netkosten omlaag gaan. Terwijl de impact die de digitalisering op het net zelf heeft, het probleem van de zware netbelasting als er massaal wordt aan- en uitgeschakeld, te weinig aandacht krijgt. Daar zit volgens hem een lacune.

Gespreksleider Annemieke Nijhof nodigt even later **Luc Kohsiek** aan tafel, dijkgraaf van het hoogheemraadschap Hollands Noorderkwartier. Hoe ver is men in de waterveiligheidssector als het gaat om digitalisering? Nou, geeft Kohsiek direct aan, tot hilariteit van de zaal: niet ver. En hij denkt ook niet dat dat gauw gaat gebeuren. In elk geval niet wanneer we het hebben over waterveiligheid.

"Wij vertrouwen die elektriciteit niet, dat is heel simpel"

Volgens de dijkgraaf wordt er vooral geïnvesteerd in het vasthouden van kennis waarmee het bewakingspersoneel ook 'met de hand' noodscenario's kan uitvoeren om de pompen goed aan te zetten. Die pompen werken natuurlijk wel op elektriciteit, maar als die uitvalt, zijn er aggregaten die dat overnemen, aldus Kohsiek. "Want wij vertrouwen die elektriciteit niet, dat is heel simpel."
En, vervolgt de dijkgraaf, dit principe hanteren we niet alleen bij polders en kleine gemalen.
De stormvloedkering in de Oosterschelde werkt op exact dezelfde manier. Ook die kan gewoon met de hand worden bediend en werkt ook met noodaggregaten. Het zou uiterst onverstandig zijn als we dat digitaal zouden doen.
Is de les die we hieruit moeten trekken dat we het elektriciteitssysteem niet hadden moeten digitaliseren? Nee, zo ver wil Kohsiek niet gaan. Het gaat hem alleen om de waterveiligheid. Omdat daarbij mensenlevens in gevaar kunnen komen. "Ik ben absoluut voor moderne techniek, maar waar het mensenlevens raakt, moet je extra voorzichtig zijn."
Pallas Agterberg geeft vanuit de zaal de dijkgraaf gelijk: "Eigenlijk wordt in de elektriciteitswereld dezelfde redeneertrant gevolgd. Hoogspannings-, middenspannings- en laagspanningsnetten kunnen in geval van nood allemaal lokaal handmatig worden bediend."
En hoe zit het met de *kennis* over het systeem? Het watersysteem is, in tegenstelling tot het complexe elektriciteitssysteem, behoorlijk goed in beeld gebracht. Rijkswaterstaat en de waterschappen hebben veel ervaringskennis opgebouwd en vastgehouden. Maar de klimaatverandering is in de waterwereld dominant geworden. Ze heeft nieuwe kennisvergaring nodig gemaakt. Er zijn nu scenariostudies opgesteld voor de watersector, die vér vooruit denken: naar de situatie over 30, 50, 100 jaar. In de waterwereld wordt die kennis *onafhankelijk* door een aantal instituten bij elkaar geharkt. Dat is een groot goed, benadrukt Kohsiek.


Annemieke Nijhof in gesprek met tafelgasten

In de volgende gespreksronde mag een vijftal nieuwe gasten aanschuiven, om elk vanuit hun eigen achtergrond hun licht te laten schijnen op het derde thema van de avond: hoe komen we tot een onafhankelijke kennisinfrastructuur over de kwetsbaarheden van digitalisering?
John Post, programmadirecteur Digitalisering bij de Topsector Energie, werpt de vraag op waarom een kennisinfrastructuur eigenlijk 'onafhankelijk' zou moeten zijn. Opvallend vindt hij ook dat mensen die het over zo'n kennisinfrastructuur hebben, altijd de universiteiten in gedachten hebben. Dat zijn vaak toch opleidingen die geen binding hebben met wat er in de praktijk gebeurt. Terwijl we een tekort hebben aan praktijkmensen: installateurs, mensen die bijvoorbeeld warmtepompen kunnen installeren. Als je die binding verliest, hebben we als maatschappij een probleem, aldus Post. Je moet investeren in mensen om de energietransitie mogelijk te maken.
Richard Beekhuis, directeur Sustainable Energy bij TNO, brengt een vergelijkbaar punt ter tafel: er is volgens hem een spanningsveld ontstaan tussen enerzijds elektrotechnici die IT gaan gebruiken en anderzijds informatici die iets voor het energiesysteem gaan doen. Die laatsten zijn doorgaans bezig het bedenken van ingewikkelde ICT-oplossingen en applicaties die eigenlijk in de echte wereld niet gaan werken. Want eindgebruikers hebben geen kennis van zaken. Daar zit een probleem, aldus Beekhuis: de praktische invalshoek ontbreekt nogal eens in de oplossingen die door informatici worden bedacht voor het energiesysteem.

"Als het van levensbelang is moet het niet digitaal zijn – daar geloof ik niet in"

Jaya Baloo, Chief Information Security Officer bij KPN, signaleert dat er tot nu toe wordt gesproken over de afzonderlijke sectoren: water, telecom en energie. Wat nog niet aan de orde is gesteld, zijn de intersectorale afhankelijkheden. We ontwerpen allemaal afzonderlijke scenario's voor dingen die kunnen gebeuren. Maar we vergeten dat in de praktijk in elk scenario iedereen elkaar nodig heeft. Immers: energie functioneert niet zonder telecom. En als we het dan over het

noodnummer 112 hebben: dat is een levenskritiek systeem, maar volledig gedigitaliseerd. "Als het van levensbelang is moet het niet digitaal zijn" – daar gelooft Baloo dan ook niet in. Uiteindelijk wordt alles digitaal. We moeten de onderlinge afhankelijkheden in kaart brengen, dáár gaat het om, vindt Baloo. Wat hebben we allemaal en hoe is het met elkaar verbonden? Zo kun je cascade-effecten in kaart brengen. Die kennis heb je nodig om systemen veilig te kunnen maken.
Martin Scheepers, directeur Energy Transition Studies bij ECN, heeft vooral zorgen over de snelheid die we in Nederland maken met de ontwikkeling naar een volledig duurzaam energiesysteem. Het duurzaamheidsdoel van 70% duurzame elektriciteit moet al in 2030 zijn gerealiseerd. Al die stroom, en we hebben het dan echt over tientallen gigawatt, komt dan dus van wind en zon. Dat betekent dat in korte tijd enorme veranderingen tot stand worden gebracht – want in diezelfde tijd draaien we ook nog de gaskraan dicht, zodat de elektriciteitsvraag nog extra zal toenemen. Uiteraard is er IT nodig om het allemaal te laten werken. Maar mijn grote zorg, aldus Scheepers, zit hem in de vraag: kunnen we het allemaal wel betrouwbaar houden? Lopen we niet het risico dat we uitkomen op een systeem dat uiteindelijk minder betrouwbaar is dan wat we nu hebben, met alle maatschappelijke problemen van dien?
Walter Ruijgrok, manager Markets & Environment bij Energie-Nederland, heeft eveneens zorgen. Hij signaleert dat er bij de ontwikkeling naar een gedigitaliseerd elektriciteitssysteem allerlei nieuwe actoren actief zijn: onbekende spelers of spelers uit een andere branche dan die van de netbeheerders en de energieproducenten. In de wereld van digitalisering worden de processen dus niet door de bekende spelers gestuurd. Willen we veiligheid introduceren en oplossingen voor risico's bedenken, dan moeten we die andere spelers er wél bij hebben. Want zonder hen gaat het niet gebeuren. Dat is best een hoofdbreker, aldus Ruijgrok.

Gespreksleider Annemieke Nijhof stelt vast: er is dus samenwerking nodig, zowel tussen de traditionele sectoren onderling als met nieuwe partijen, voor het bij elkaar brengen van kennis. Zij vraagt Jaya Baloo: wat is er nodig om dat voor elkaar te krijgen, wie zou daarin een stimulerende, faciliterende rol moeten vervullen? Baloo geeft aan: in de VS was het de federale overheid die heeft gezorgd voor een structuur waarin de kennisuitwisseling tussen de sectoren kon plaatsvinden. Annemieke Nijhof noteert tot besluit van deze gespreksronde dat er een besef bij de afzonderlijke actoren moet ontstaan dat het de moeite waard is om kennis te delen met concurrerende partijen. Dat is een voorwaarde voor succes.

Het laatste deel van de avond is gewijd aan enkele *politieke* aspecten rond de digitalisering van de stroomvoorziening. Is digitalisering van de stroomvoorziening eigenlijk wel een politieke kwestie? D66-Kamerlid **Rob Jetten** vindt van wel. Al tekent hij aan: we weten in de Tweede Kamer eigenlijk niet veel van de risico's van digitalisering. Ook in de commissie Economische Zaken en Klimaat zijn we er amper mee bezig tot op heden. Dus het Rli-rapport is meer dan welkom. Kwesties die tot nu toe in de Kamer op tafel liggen zijn veeleer: hoe zorgen we ervoor dat iedereen de komende tien-vijftien jaar groene energie kan krijgen? En: hoe zorgen we ervoor dat die energie betaalbaar blijft? Want veel mensen hebben moeite om elke maand de energierekening te betalen.
Tegelijkertijd vindt Jetten het wel belangrijk dat de 'klimaattafels' die minister Wiebes heeft ingesteld om de ambities op het gebied van energie en klimaat sectorgewijs waar te maken, onderling *verbinding* gaan zoeken. Immers, alles hangt met elkaar samen. Als het gaat om de mobiliteitstafel bijvoorbeeld: daar komt aan de orde dat we massaal elektrisch willen gaan rijden. Dat levert een energievraag op die je deels moet oplossen in de gebouwde omgeving, waar we die auto's weer gaan opladen. En die gebouwde omgeving levert weer een energieopgave op voor de energietafel. Dus het gaat alleen maar lukken als we verbindingen tussen de tafels weten te leggen.
Jetten roept de Rli en de aanwezigen op: help ons, de politici, om de kansen en bedreigingen van de digitalisering goed te zien. Zodat wij de juiste kaders kunnen scheppen voor de nodige innovatie. En belangrijk is bijvoorbeeld ook de vraag: moeten wij netverzwaring faciliteren of juist niet?

"Het idee dat je niet goed weet hoe het energiesysteem werkt, is ongemakkelijk"

Michel van Eeten, behalve hoogleraar aan de TU Delft ook lid van de Cybersecurityraad, stelt vast: de politiek bepaalt waar de politiek over gaat. Maar het publiek belang van de energievoorziening, en dus ook van het elektriciteitssysteem, is natuurlijk heel groot. Daar hoef je niemand van te overtuigen. Dus dat behoort tot de kerntaken van de overheid. Maar het idee dat je niet goed weet hoe het elektriciteitssysteem werkt, is ongemakkelijk, ook voor de overheid. We begrijpen niet hoe het werkt, en toch werkt het – net als internet. Het ongemakkelijke eraan is dat je er als politiek niet gemakkelijk grip op krijgt. Anders dan bijvoorbeeld de belastingwetgeving, waar je als politiek gewoon kunt besluiten om iets af te schaffen – bijvoorbeeld de dividendbelasting.
De ontwikkelingen in de energiemarkt van de afgelopen tien jaar hebben de situatie nog diffuser gemaakt dan zij al was. De overheid heeft steeds minder grip op wat daar allemaal gebeurt. "Het energiesysteem is meer gaan lijken op internet en dat is eigenlijk een lappendeken en een bende, waar we soms bij wijze van spreken met ducttape dingen weer aan elkaar plakken, en het soms lukt om dingen goed en grondig te regelen. Ook dan zien we dat IT-ers graag nét afwijken van afspraken en specificaties,," aldus Van Eeten. Dus we moeten de tering naar de nering zetten: soms moeten we stroomuitval accepteren. Het zal ook niet lukken de elektriciteitssector van hogerhand ingrijpend aan te passen. Omdat ons netbeheer nu eenmaal regionaal is geregeld, zal dat niet gaan.

Wat waren, alles overziend, de belangrijkste bevindingen die de avond heeft opgeleverd? Annemieke Nijhof sluit de conferentie af met een aantal rode draden:

- Van de toelichting van DNB hebben we geleerd dat er een paradigmaverandering nodig is: van 'alles buiten de muur houden' (defensief) naar een combinatie van 'defensie en preventie' en het inbouwen van veerkracht in het systeem door bijvoorbeeld het actief testen van systemen door ethische hackers. Maar de kunst om gezamenlijk vér vooruit te denken en dreigingsanalyses te maken, hebben nog niet alle vitale sectoren onder de knie.
- Ook hebben we vastgesteld dat door de decentralisatie, het toelaten van een groot aantal partijen tot het elektriciteitssysteem en door de digitalisering, het 'aanvalsoppervlak' in de elektriciteitsvoorziening sterk wordt vergroot – een probleem dat we onder ogen moeten zien.
- Een andere les is wellicht dat complexe systemen per definitie niet zijn te overzien en begrijpen: dit is iets waar we mee moeten leren leven. Dat neemt niet weg dat er behoefte is aan kennis over 'de keten': het doordenken van de impact van digitalisering en de raakvlakken daarbij tussen sectoren.
- Een belangrijk issue is deze avond ook gebleken: hoe verbinden we de bestaande spelers met nieuwe spelers? Hoe open is de cultuur om kennis te delen? Duidelijk is dat de overheid als systeemverantwoordelijke de rol heeft om partijen bij elkaar te brengen, maar kan dit niet zonder bereidwilligheid van de sectoren om mee te doen.
- En *last but not least* is duidelijk geworden: het onderwerp 'digitalisering van de stroom-voorziening' moet op de kennisagenda van de klimaattafel komen.

Met deze conclusies kwam een eind aan een inspirerende en vruchtbare conferentie.

Advies 'Stroomvoorziening onder digital spanning'

Verslag: Saskia van As / Tekstbureau van As