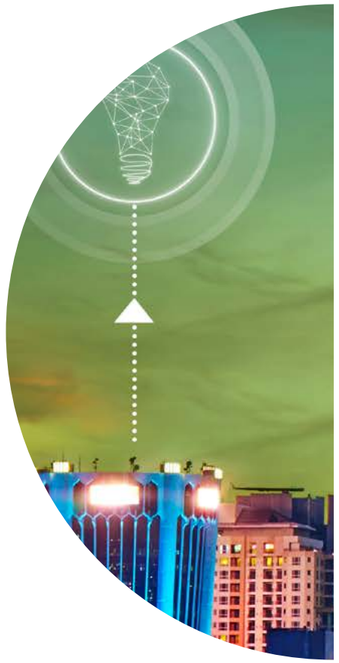
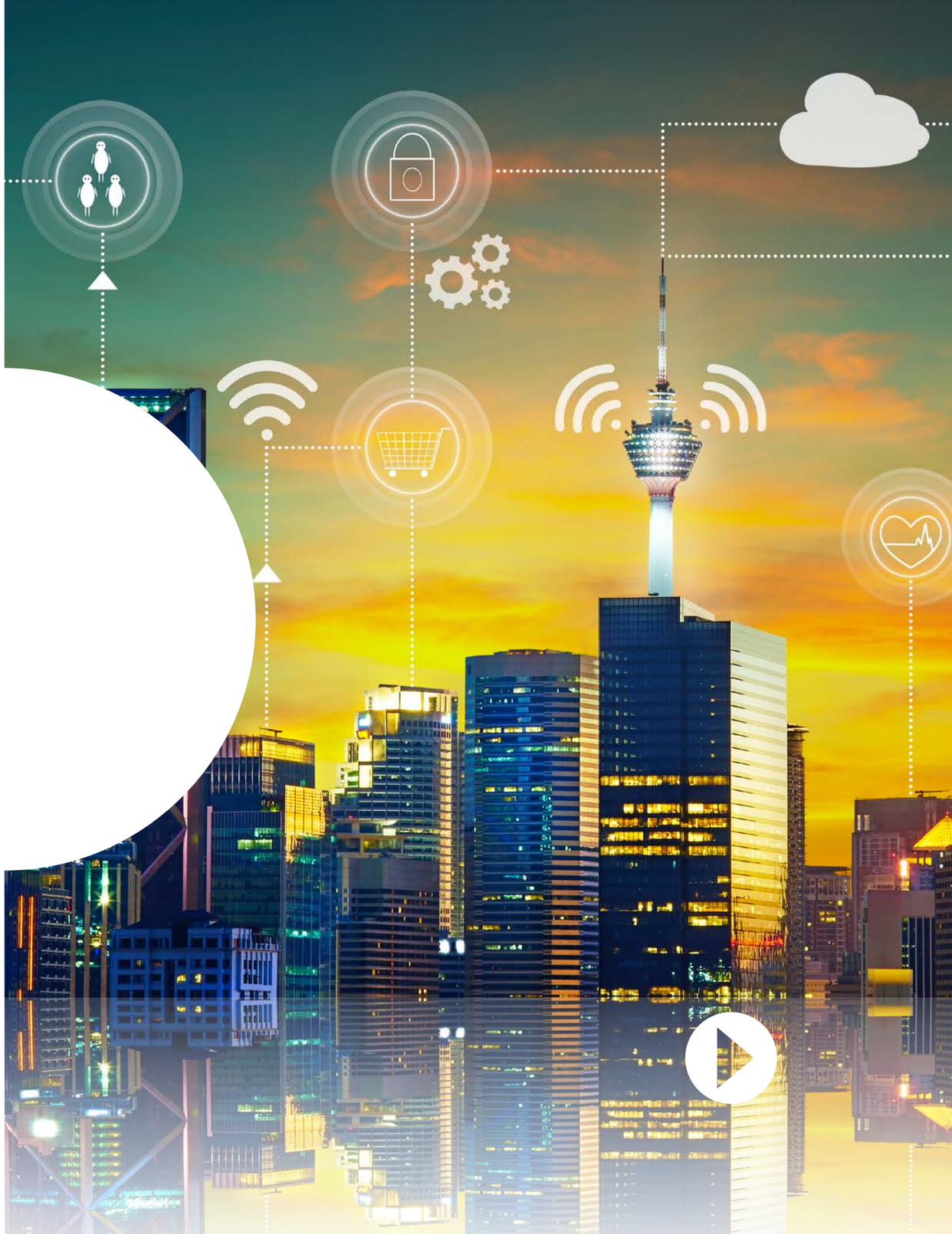
STROOMVOORZIENING ONDER DIGITALE SPANNING

FEBRUARI 2018





Raad
voor de leefomgeving
en infrastructuur

Raad voor de leefomgeving en infrastructuur

De Raad voor de leefomgeving en infrastructuur (Rli) is het strategische adviescollege voor regering en parlement op het brede domein van duurzame ontwikkeling van de leefomgeving en infrastructuur. De raad is onafhankelijk en adviseert gevraagd en ongevraagd over langetermijnvraagstukken. Met een integrale benadering en advisering op strategisch niveau wil de raad bijdragen aan de verdieping en verbreding van het politiek en maatschappelijk debat en aan de kwaliteit van de besluitvorming.

Samenstelling Rli

Ir. J.J. (Jan Jaap) de Graeff (voorzitter)

Ir. M. (Marjolein) Demmers MBA

Prof. dr. P. (Pieter) Hooimeijer

Prof. mr. N.S.J. (Niels) Koeman

Drs. J. (Jeroen) Kok

Ir. A.G. (Annemieke) Nijhof MBA

Drs. E. (Ellen) Peper

Drs. K.J. (Krijn) Poppe

Dr. J.C. (Co) Verdaas

Junior raadsleden

S.P. (Sybren) Bosch MSc

M.W.B. (Mart) Lubben MSc

I.Y.R. (Ingrid) Odegard MSc

Algemeen secretaris

Dr. R. (Ron) Hillebrand

Raad voor de leefomgeving en infrastructuur

Bezuidenhoutseweg 30

Postbus 20906

2500 EX Den Haag

info@rli.nl

www.rli.nl

INHOUD

VOORWOORD 4

SAMENVATTING 5

1 INLEIDING 7
1.1 Context 8
1.2 Vraagstelling 8
1.3 Leeswijzer 9

2 INGRIJPENDE VERANDERINGEN IN ELEKTRICITEITSSYSTEEM 10
2.1 Actuele ontwikkelingen 11
2.2 Centrale rol voor digitale technologie 12

3 NIEUWE KWETSBAARHEDEN 14
3.1 Fouten bij softwareontwerp 16
3.2 Onvoorzien ‘gedrag’ van autonome digitale systemen 16
3.3 Moedwillige verstoring 17
3.4 Internationale dimensie digitale kwetsbaarheden 18

4 AANBEVELINGEN 20
4.1 Onderzoek gevolgen van digitalisering voor betrouwbaarheid stroomvoorziening 21
4.2 Neem ‘no-regret’-maatregelen die digitale kwetsbaarheden indammen 22
4.3 Investeer structureel in een onafhankelijke kennisinfrastructuur 23
4.4 Zoek samenwerking met Europese partners om kwetsbaarheden aan te pakken 23

LITERATUUR 24

BIJLAGEN 26
Totstandkoming advies 26
Overzicht publicaties 29

VOORWOORD

Het advies *Stroomvoorziening onder digitale spanning* is voortgekomen uit een verzoek van de regering om te adviseren over de betrouwbaarheid van 'vitale processen'. De vraag die aan de Raad voor de leefomgeving en infrastructuur (Rli) werd voorgelegd was of er generieke lessen zijn te trekken uit de manier waarop in ons land uiteenlopende vitale processen zijn ontworpen.

In de eerste, verkennende fase van het adviestraject heeft de Rli zich verdiept in drie vitale processen: de elektriciteitsvoorziening, de telecommunicatie en het waterbeheer (de waterketen en het watersysteem). Al snel werd duidelijk dat de huidige organisatie en vormgeving van deze processen sterk verschillen als gevolg van uiteenlopende ontstaansgeschiedenissen. Ook het tempo waarin de processen veranderen en de omvang van de investeringen die de komende jaren zijn voorzien, zijn zeer verschillend. De Rli concludeerde hieruit dat algemene lessen over het ontwerp van vitale processen al snel erg algemeen zouden worden.
Duidelijk werd in de verkennende fase echter ook dat in alle bestudeerde vitale processen sprake is van een voortschrijdende digitalisering en dat het inzicht in de gevolgen hiervan nog veel witte vlekken kent. Daarbij vormt de wederzijdse afhankelijkheid van digitalisering en elektriciteit een grote uitdaging, want voor de toekomst geldt: zonder digitalisering geen stroomvoorziening, zonder stroomvoorziening geen digitalisering. Die rode draad bleek een goed uitgangspunt om het advies nader toe te spitsen en te concretiseren.

In het vervolg van dit adviestraject heeft de Rli zich verdiept in de veranderingen in het 'ecosysteem' van de elektriciteitsvoorziening als gevolg van digitalisering. Wat zijn hiervan de gevolgen voor de betrouwbaarheid van de stroomvoorziening?

SAMENVATTING

De Nederlandse stroomvoorziening raakt steeds meer verweven met digitale technologie. Geavanceerde software en algoritmes bepalen in toenemende mate de levering, het transport en de distributie van stroom. Deze ontwikkeling doet zich voor in een elektriciteitssysteem dat ook op andere fronten (met name de stroomproductie en het stroomgebruik) al sterk in verandering is: doordat er meer gebruik wordt gemaakt van duurzame energiebronnen, doordat bedrijven en burgers vaker zelf stroom opwekken en doordat de stroomopwekking afhankelijker wordt van weersomstandigheden.

De Rli analyseert in dit advies de kwetsbaarheden die in het elektriciteitssysteem ontstaan door het voortgaande proces van digitalisering. Het gaat daarbij om méér dan alleen de dreiging van moedwillige verstoring van de stroomvoorziening door cybercriminaliteit. Het gaat bijvoorbeeld ook om de potentiële gevolgen van softwareontwerpfouten en van onvoorzien 'gedrag' van autonome systemen die de stroomvoorziening in toenemende mate reguleren. De analyse die de Rli heeft gemaakt van deze en andere kwetsbaarheden maakt duidelijk dat de digitalisering van het elektriciteitssysteem nieuwe risico's met zich meebrengt voor de betrouwbaarheid waar onze stroomvoorziening om bekend staat.

Er is van overheidswege – gelukkig – steeds meer aandacht voor cybersecurity. Maar de Rli signaleert dat er nog onvoldoende zicht is op andere kwetsbaarheden die de digitalisering met zich meebrengt, terwijl de maatschappelijke impact daarvan groot kan zijn. Ook signaleert de Rli dat de aandacht van de overheid voor de digitale kwetsbaarheden zich vooral richt op de netwerken, die in publieke handen zijn. De stabiliteit van het totale elektriciteitssysteem wordt echter met name ondergraven vanuit de onderdelen die níet in publiek eigendom zijn.

De Rli doet in het licht van het bovenstaande vier aanbevelingen:

1. De overheid zou de mogelijke gevolgen van de digitalisering van het elektriciteitssysteem voor de betrouwbaarheid van de stroomvoorziening moeten onderkennen en onderzoeken.
2. Vooruitlopend op dit onderzoek zou de overheid 'no-regret'-maatregelen moeten nemen die digitale kwetsbaarheden indammen. De Rli denkt aan prikkels die partijen aanzetten om preventieve maatregelen te nemen en waarborgen dat actuele inzichten over veilig ontwerp en updaten van digitale systemen in standaarden worden vastgelegd.
3. De overheid zou structureel moeten investeren in een infrastructuur voor gezamenlijke kennisvergaring (*joint fact finding*), waarin behalve publieke ook marktpartijen hun kennis delen over de kwetsbaarheden van digitalisering. Deze bundeling van deskundigheid is nodig om onafhankelijke kennis in te kunnen zetten voor een stroomvoorziening waarin de publieke belangen structureel worden behartigd.
4. De overheid zou Europese samenwerking moeten zoeken om de kwetsbaarheid van de gedigitaliseerde stroomvoorziening aan te pakken, zowel in onderzoek, via productveiligheidseisen en via Europese netcodes.

1

INLEIDING

1.1 Context

Het belang van een betrouwbare stroomvoorziening is groot: verstoring of uitval van de stroomvoorziening kan leiden tot ongevallen met persoonlijke, materiële en/of financiële schade. Bij langdurige uitval kan bovendien maatschappelijke onrust ontstaan en (als gevolg daarvan) onveiligheid.

Om een betrouwbare, veilige, betaalbare en schone stroomvoorziening te kunnen blijven waarborgen moeten de levering, het transport en de distributie van elektriciteit goed zijn geregeld. De Nederlandse overheid heeft de verantwoordelijkheid voor deze processen in de jaren negentig van de vorige eeuw bij wet[1] deels in private handen gelegd en deels in publieke handen. Private energiebedrijven verzorgen sindsdien de opwekking, handel en levering van stroom. Publieke netbeheerders verzorgen het transport en de distributie van stroom via de elektriciteitsnetwerken. Energiebedrijven en netbeheerders dragen op deze manier bij aan het inlossen van de belofte van de overheid aan de samenleving dat zij zal zorgen voor een veilige, betrouwbare en betaalbare stroomvoorziening.[2]

De overstap naar het gebruik van 'schone' stroom verandert de komende tijd de stroomvoorziening ingrijpend en gaat gepaard met digitalisering. Om deze transitie in goede banen te leiden heeft de minister van Economische Zaken en Klimaat onlangs de wetgevingsagenda energietransitie (Tweede Kamer, 2017a) en zijn aanpak voor een Klimaat- en Energieakkoord gepresenteerd (Tweede Kamer, 2017b). Daarnaast worden met de nieuwe Cybersecuritywet en de Wet gegevensverwerking en meldplicht cybersecurity (Wgmc) gedigitaliseerde systemen waaronder het elektriciteitssysteem beter beschermd tegen moedwillige verstoring. Tegelijkertijd wordt gewerkt aan het in beeld brengen en verminderen van onderlinge afhankelijkheden van vitale processen, waaronder de elektriciteitsvoorziening en de telecommunicatie.[3]
De Rli onderschrijft het belang van deze overheidsinzet maar signaleert dat daarbij een bredere blik ontbreekt. Zo'n bredere blik is wél van belang, want de risico's die de digitalisering van het elektriciteitssysteem met zich meebrengt voor de betrouwbaarheid van de stroomvoorziening beperken zich niet tot cybercriminaliteit. Ook anderen hebben aandacht gevraagd voor de digitalisering van het elektriciteitssysteem, zoals het Planbureau voor de Leefomgeving (Hollander et al., 2017), het Internationaal Energie Agentschap (EIA, 2017) en de Cyber Security Raad (CSR, 2017).

1.2 Vraagstelling

Centraal in dit advies staat de vraag of de overheid haar belofte aan de samenleving om te zorgen voor een schone maar ook veilige, betrouwbare en betaalbare stroomvoorziening gestand kan blijven doen nu de digitalisering van het elektriciteitssysteem de komende jaren een nieuwe fase in gaat. Welke risico's brengen de veranderingen met zich mee voor de

1 Dit is vastgelegd in de Elektriciteitswet 1998.
2 Memorie van Toelichting bij de Gas- en Elektriciteitswet 1998 (Tweede Kamer 25 621, vergaderjaar 1997-1998).
3 Met de Cybersecuritywet en de Wgmc implementeert Nederland de Europese richtlijn netwerk- en informatiebeveiliging (NIB) (2016/1148).

betrouwbaarheid van onze stroomvoorziening? En zijn deze risico's wel in voldoende mate afgedekt?[4]

1.3 Leeswijzer

Hoofdstuk 2 van dit advies beschrijft de veranderingen in de stroomvoorziening die zich in de nabije toekomst gaan voltrekken. Vervolgens gaat dit advies in hoofdstuk 3 in op de kwetsbaarheden die de digitalisering met zich meebrengen. Tot slot volgen in hoofdstuk 4 aanbevelingen om deze kwetsbaarheden beter in beeld te krijgen en de gevolgen ervan te beperken.

4 In het kader van dit advies heeft de Rli met een groot aantal personen gesproken. Zie de bijlagen voor een overzicht van geraadpleegde personen en de samenstelling van de commissie en raad.

2

INGRIJPENDE VERANDERINGEN IN ELEKTRICITEITS-SYSTEEM

Ons elektriciteitssysteem verandert de komende jaren ingrijpend als gevolg van een aantal ontwikkelingen. De Rli bespreekt hieronder eerst een viertal van deze ontwikkelingen en gaat vervolgens in op de verandering die in dit advies centraal staat: de digitalisering van het elektriciteitssysteem zelf.

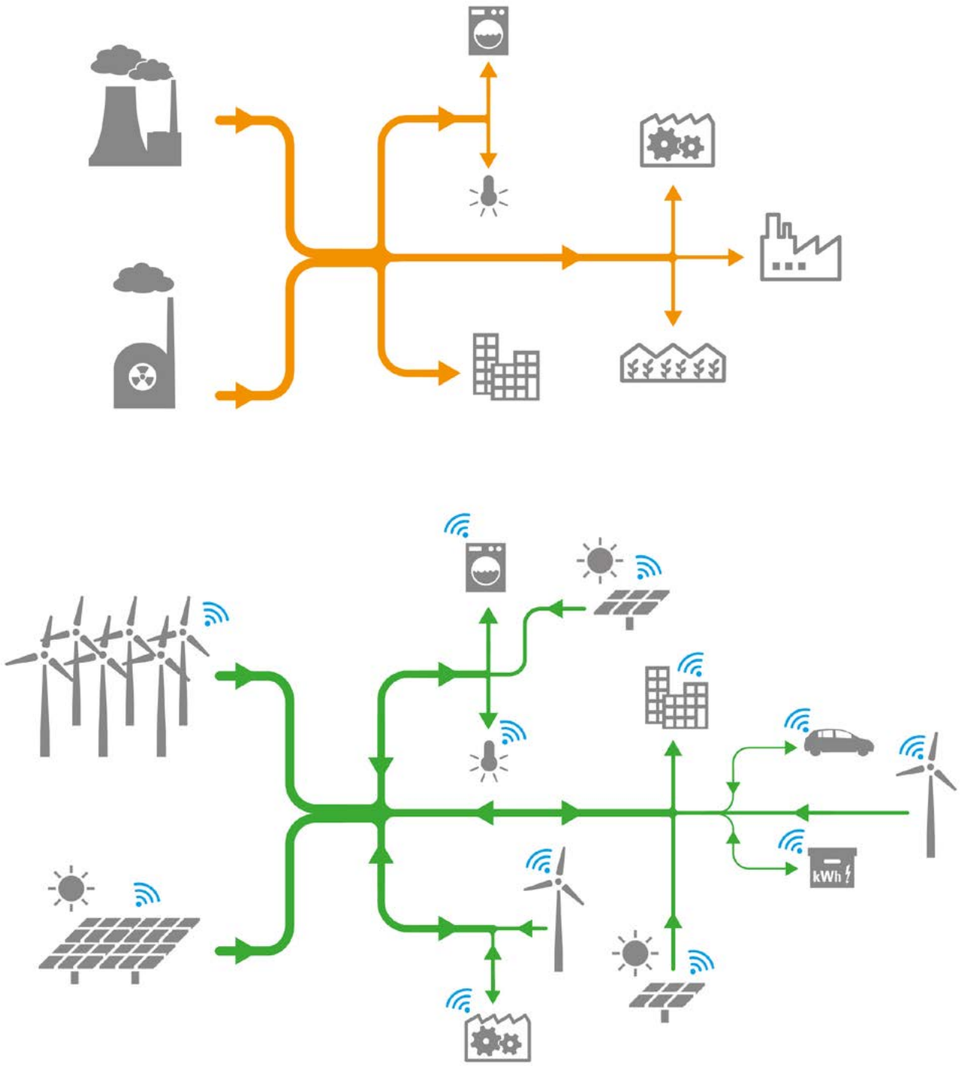
2.1 Actuele ontwikkelingen

Verschillende ontwikkelingen, die deels al zijn ingezet, hebben grote invloed op ons elektriciteitssysteem. Zonder uitputtend te willen zijn:

- *Elektriciteit gaat een veel groter deel van onze energiebehoefte vervullen*, doordat we afscheid nemen van olie en aardgas. Daarmee worden meer functies afhankelijk van elektriciteit (ECN et al., 2017). Op den duur zullen behalve auto's ook het zware transport, de luchtvaart en de zware industrie moeten overschakelen op niet-fossiele energiebronnen. Het verbruik van elektriciteit zal logischerwijs sterk toenemen. Voor Nederland wordt een verdubbeling van het elektriciteitsverbruik in 2050 verwacht.
- *Steeds meer elektriciteit wordt opgewekt uit hernieuwbare bronnen*, bijvoorbeeld met behulp van zonnepanelen, windturbines en/of warmtekrachtkoppelingsinstallaties. De verwachting is dat het aandeel duurzaam opgewekte elektriciteit sterk gaat groeien: van 8% in 2015 naar 44% in 2023 en 80% in 2050 (Sijm et al., 2017). De beleidsdoelstelling is zelfs om te komen tot 100% duurzaam opgewekte elektriciteit in 2050. Deze ontwikkeling leidt ertoe dat elektriciteit met veel meer verschillende installaties zal worden opgewekt dan nu. Tegelijk zal het onze internationale afhankelijkheid van de aanvoer van steenkool, aardolie en aardgas verminderen.
- *De elektriciteitsmarkt wordt minder overzichtelijk*, doordat nieuwe partijen toetreden die bovendien vaak meer rollen tegelijk vervullen. Behalve energiebedrijven plaatsen ook andere bedrijven en burgers zonnepanelen, windturbines en/of warmtekrachtkoppelingsinstallaties. Zo worden zij producent en consument tegelijk. Deze partijen zullen hun vraag naar en aanbod van elektriciteit gaan afstemmen op prijsschommelingen in de markt. Deze afstemming van vraag en aanbod in de stroommarkt zal vaak worden begeleid door makelaars (in het jargon 'aggregatoren' genoemd).
- *De afstemming van vraag en aanbod van elektriciteit wordt een ingewikkelder opgave* naarmate er meer stroom wordt opgewekt met zon en wind. De stroomproductie wordt immers afhankelijker van de weersomstandigheden: veel of weinig zon, veel of weinig wind. Ook het bewaken van de balans op het netwerk wordt daarmee complexer.[5] Om vraag en aanbod snel te kunnen laten reageren op wisselende omstandigheden zijn verschillende oplossingen denkbaar die kunnen bijdragen aan leveringszekerheid en betaalbaarheid van de stroomvoorziening. Op dit moment is nog niet duidelijk welke het best passend zijn binnen de Nederlandse context.

5 Voor een veilige en betrouwbare stroomvoorziening is een stabiel net cruciaal. Om deze stabiliteit te waarborgen moeten vraag naar en aanbod van stroom permanent met elkaar in balans worden gehouden. Deze balans wordt bewaakt door de landelijke netbeheerder (TenneT).

Figuur 1: De stroomopwekking verandert ingrijpend



Van centrale opwekking van elektriciteit naar een gedigitaliseerde stroomvoorziening waarin energieproducenten, bedrijven en burgers duurzame energie opwekken en alle onderdelen met elkaar communiceren.

2.2 Centrale rol voor digitale technologie

Digitale technologie gaat in de elektriciteitsvoorziening een centralere rol spelen. Dit zal de hiervoor geschetste veranderingen vergemakkelijken. Digitale technologie maakt bijvoorbeeld snelle aanpassing aan variaties in vraag en aanbod van elektriciteit mogelijk. Daarbij kunnen behalve grote bedrijven ook burgers en kleinere bedrijven worden betrokken. Op digitale platforms zullen vraag en aanbod van alle deelnemers op elkaar worden afgestemd.

Digitale technologie zorgt ervoor dat steeds meer gebruik wordt gemaakt van stroomopwekkende apparatuur, meetinrichtingen, opslagfaciliteiten en gebruiksapparatuur die via geautomatiseerde processen met elkaar communiceren.[6] Deze apparaten zullen voortdurend met elkaar in verbinding staan via geavanceerde software en voorgeprogrammeerde regels (algoritmes). Het gebruik en het aanbod van elektriciteit worden op die manier automatisch afgestemd op prijsschommelingen. Overtollige elektriciteit wordt opgeslagen in bijvoorbeeld thuisaccu's of de elektrische auto, of doorgeleverd aan de buren. (Preventief) onderhoud kan worden geoptimaliseerd op basis van monitoring. Mogelijk worden hiervoor in de toekomst ook zelflerende systemen gebruikt.

In het gedigitaliseerde elektriciteitssysteem zal een sleutelrol weggelegd zijn voor zogenoemde schakelpunten. Daarin worden tal van gegevens geanalyseerd en aan elkaar gekoppeld, zoals informatie over hoeveelheden opgewekte en gebruikte stroom, over prijsschommelingen, over gebruikspatronen

6 Dit wordt ook wel het 'internet der dingen' genoemd, in het Engels afgekort tot IoT (Internet of Things).

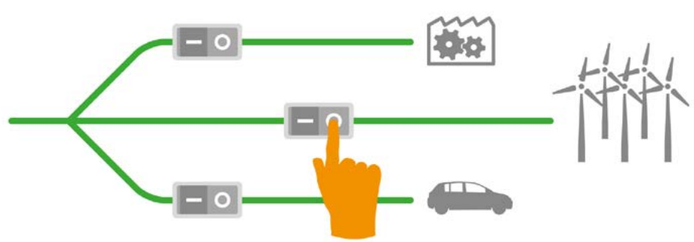
en over afgesloten contracten voor levering en afname van stroom. Schakelpunten zijn in staat om op basis van deze informatie apparaten te besturen: ze reguleren hun stroomverbruik, -productie en -levering.[7]

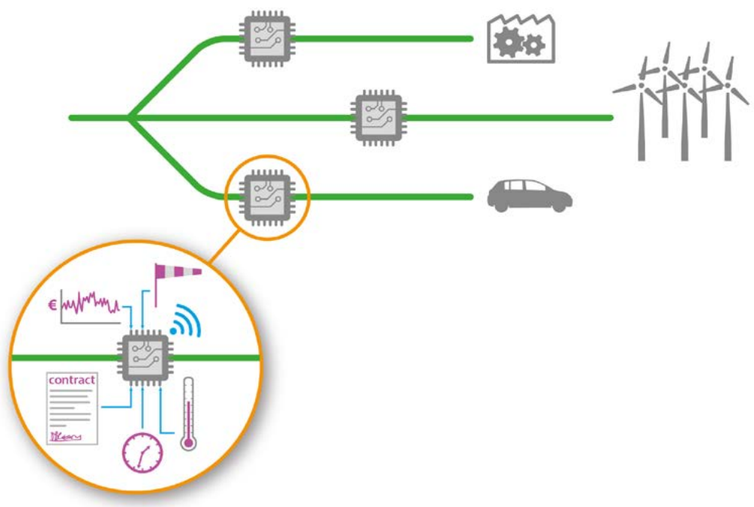
Schakelpunten zullen er in vele soorten en maten zijn. Soms zullen ze zijn ingebouwd in apparatuur, in andere gevallen zal het gaan om virtuele schakelpunten. Ze kunnen de meest uiteenlopende apparatuur met elkaar verbinden. In de industrie zullen schakelpunten de kracht- en warmtevraag van procesinstallaties registreren en sturen. In woningen zullen ze deze rol vervullen voor uiteenlopende huishoudelijke apparaten zoals thermostaten, koelkasten, zonnepanelen en warmtepompen. Ook windmolen- en zonne-energieparken zullen door een schakelpunt worden aangestuurd. Laadpalen voor (vracht)auto's zullen door een schakelpunt aan elkaar worden gekoppeld om het laden te optimaliseren. Vele combinaties zijn denkbaar.

De digitale techniek in de schakelpunten maakt het in al deze toepassingen mogelijk om op afstand data uit te lezen en processen real time en autonoom bij te sturen. De onderliggende software in de schakelpunten kan op afstand worden geüpdatet.

Met de hier geschetste ontwikkelingen ontstaat een gedigitaliseerd elektriciteitssysteem[8] waarin besluiten over opslag, levering en gebruik worden genomen door middel van voorgeprogrammeerde of zelflerende technologie, zowel binnen Nederland als in de ons omringende landen. Dit brengt behalve veel voordelen ook een groot nadeel met zich mee: de stroomvoorziening wordt afhankelijk van kwetsbare digitale voorzieningen. En dat heeft gevolgen voor de betrouwbaarheid – gevolgen die bovendien niet bij de landsgrenzen ophouden.

Figuur 2: Het verschil tussen analoge en digitale schakelpunten





Analoge schakelpunten worden handmatig bediend. Digitale schakelpunten bedienen apparaten op basis van informatie over bijvoorbeeld hoeveelheden opgewekte en verbruikte stroom, prijzen, gebruikspatronen en weersverwachting.

7 Schakelpunten moeten niet worden verward met allocatiepunten. Die laatste zijn virtuele punten waar de overdracht van stroom vanaf het net naar een individuele elektriciteitsaansluiting plaatsvindt.
8 Een gedigitaliseerde elektriciteitsvoorziening wordt ook wel smart grid genoemd.

3

NIEUWE KWETSBAARHEDEN

De digitalisering van het elektriciteitssysteem brengt nieuwe kwetsbaarheden met zich mee voor de elektriciteitsvoorziening. Er kunnen zich problemen voordoen in de digitaal aangestuurde apparatuur voor bijvoorbeeld stroomopwekking of -opslag, in de netwerken en/of in de complexe digitale processen die de communicatie daartussen verzorgen. En doordat de onderdelen van de stroomvoorziening steeds meer met elkaar verweven raken, kan één probleem diverse vervolgproblemen veroorzaken en uiteindelijk tot uitval van de stroomvoorziening leiden.

Uitval van de stroomvoorziening kan verstrekkende maatschappelijke gevolgen hebben, zo hebben incidenten in het verleden laten zien. Een recent voorbeeld is de stroomstoring in Amsterdam van januari 2017. De storingen op de netten van TenneT en Alliander waren na twee respectievelijk vijf uur opgelost. Maar de gevolgen waren groot en hielden lang aan (zie kader).

Stroomstoring in Amsterdam: urenlange chaos

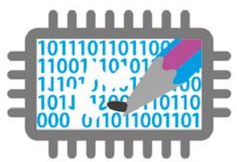
De stroomstoring in delen van Amsterdam, Zaandam en Landsmeer was volgens de plaatselijke netbeheerder het gevolg van problemen in een hoogspanningsverdeelstation. Ruim 360 duizend huishoudens zaten urenlang zonder elektriciteit. De storing veroorzaakte grote problemen, onder andere in de communicatiestructuur: het mobiele netwerk viel uit, de wifi functioneerde niet meer en zelfs het noodnummer 112 was voor burgers onbereikbaar. Ook nadat de stroomvoorziening weer was hervat hielden de problemen aan. Er was de hele dag chaos op het spoor tot ver buiten de Randstad, er ontstonden lange files, de schappen in sommige supermarkten bleven leeg. In het Slotervaartziekenhuis kon de hele dag niet worden geopereerd (Bouma, 2017; Stokmans & Logtenberg, 2017).

In de toekomst kunnen de gevolgen van dit soort incidenten nog groter worden, doordat er dan meer maatschappelijke functies afhankelijk zullen zijn van elektriciteit. Dit kan leiden tot maatschappelijke ontwrichting. Bij uitval van de elektriciteitsvoorziening kunnen behalve mobiele communicatie en internet ook het totale vervoer en delen van de industrie stilvallen, met alle economische gevolgen van dien. Bovendien kunnen mensen langdurig in de kou komen te zitten, wat slachtoffers met zich kan meebrengen. Grootschalige stroomstoringen kunnen daarnaast het functioneren van de openbare orde belemmeren en het vertrouwen van burgers in elkaar en in de overheid aantasten, bijvoorbeeld wanneer er spanningen ontstaan als gevolg van voedselschaarste of ongelijke toegang tot nood(stroom) voorzieningen.

Diverse partijen hebben de afgelopen tijd aandacht gevraagd voor kwetsbaarheden die samenhangen met de digitalisering van de stroomvoorziening. Zo zijn er publicaties geweest van het Planbureau voor de Leefomgeving (Hollander et al., 2017), de Cyber Security Raad (CSR, 2017) en het Internationaal Energieagentschap (IEA, 2017). De Rli constateert dat in deze publicaties de verschillende typen kwetsbaarheden onvoldoende worden onderscheiden en in samenhang worden bezien. Hieronder worden daarom de drie belangrijkste kwetsbaarheden in het gedigitaliseerde

systeem geschetst, de gevolgen ervan voor de betrouwbaarheid van de stroomvoorziening en de internationale dimensie daarvan. Voor de voorbeelden die worden aangehaald geldt dat deze allemaal hebben geleid tot maatregelen om herhaling te voorkomen.

3.1 Fouten bij softwareontwerp

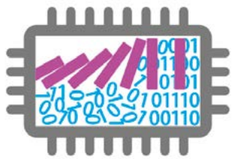


De processen in energiecentrales en elektriciteitsnetten worden aangestuurd door steeds complexere programmatuur. Hierdoor neemt de kans op uitval als gevolg van programmeerfouten toe (Next Generation Infrastructures, 2017). Het blijkt lastig te voorspellen hoe onderdelen van het elektriciteitssysteem op de invoeging van een nieuw software-element zullen reageren. Dat er fouten sluipen in het ontwerp van software is dan ook bijna niet te vermijden. Dit soort fouten kunnen systeemstoringen tot gevolg hebben (zie kader). Ook software-updates kunnen systeemstoringen veroorzaken.

Softwarefout: grote black-out in VS en Canada

Een softwarefout leidde op 14 augustus 2003 tot een grote black-out in de Verenigde Staten (VS) en Canada. De softwarefout veroorzaakte een onopgemerkte overbelasting. Door deze overbelasting viel een reeks van verbindingen uit, waarna grote delen van het productievermogen automatisch werden uitgeschakeld. Als gevolg hiervan kwamen zo'n 55 miljoen inwoners in delen van de VS en Canada zonder stroom te zitten. Ook in Nederland en de ons omringende landen wordt in de stroomvoorziening nog veel gebruik gemaakt van (erg) oude systemen (die in de jaren '70 en '80 zijn geïnstalleerd).

3.2 Onvoorzien 'gedrag' van autonome digitale systemen

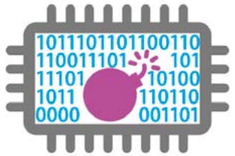


Verstoringen van de stroomvoorziening kunnen zich ook voordoen als gevolg van onbedoeld en onvoorzien 'gedrag' van autonome digitale systemen. In steeds meer apparatuur worden systemen ingebouwd waarmee de energieproductie van bijvoorbeeld zonnepanelen of de energieopslag van een thuisbatterij automatisch wordt afgestemd op de energieprijs. Waar mensen in een vrije markt zeer divers reageren op vergelijkbare prijsprikkels, zullen dit soort autonome systemen mogelijk veel uniformer reageren. Dit kan onvoorziene cumulatieve gevolgen hebben en de energievoorziening ontregelen.

Voorgeprogrammeerde Duitse energie-installaties hebben onvoorziene gevolgen

In Duitsland is in veel omvormers van wind- en zonne-installaties een algoritme geprogrammeerd om instabiliteit op het net te voorkomen. Het algoritme zorgt bij een bepaalde afwijking van de vaste netfrequentie van 50 Hz voor automatische beëindiging van de stroomlevering aan het net, waarbij ervoor wordt gezorgd dat niet alle apparaten precies op hetzelfde moment afkoppelen.

3.3 Moedwillige verstoring



Uitval van de stroomvoorziening kan ook het gevolg zijn van moedwillige verstoring door kwaadwillenden. Het gedigitaliseerde elektriciteitssysteem is kwetsbaar voor dergelijke verstoringen doordat tal van onderdelen in verbinding staan met internet. De windmolens van elektriciteitscentrales bijvoorbeeld, worden op afstand bestuurd via een internetverbinding. En ook het updaten van de software in de digitale systemen van dergelijke apparatuur gebeurt via internetverbindingen.

De *motieven* voor moedwillige verstoring van de stroomvoorziening kunnen variëren. Bij individuele hackers gaat het vaak om een virtuele vorm van baldadigheid, al dan niet met een activistische bedoeling (het blootleggen van zwaktes bij grote bedrijven). Bij georganiseerde cybercriminaliteit is de sabotage veeleer gericht op ontwrichting van de samenleving, al dan niet met eigen gewin als achterliggend motief. Wanneer dergelijke criminelen van staatswege worden aangestuurd zijn er doorgaans ook politiek-strategische motieven in het spel.
De gebruikte *methodes* bij moedwillige verstoringen zijn divers. Soms wordt de communicatie verstoord met zogenaamde Distributed Denial of Service-aanvallen (DDoS-aanvallen), waarbij websites of systemen worden overbelast en platgelegd. In andere gevallen wordt er malware (bewust kwaadaardige of schadelijke software) geplaatst in besturingssystemen.

Ook het *doelwit* van moedwillige verstoringen varieert. Aanvallen kunnen zich richten op hardware of juist op software. Er kan worden ingebroken in netwerken of juist in de daarmee verbonden apparatuur. Alle onderdelen van het elektriciteitssysteem, inclusief de toeleveringskanalen, zijn in principe kwetsbaar voor verstoring (Nationaal Coördinator Terrorismebestrijding en Veiligheid, 2017; Verhagen, 2016).

Cyberaanvallen op elektriciteitscentrales in Oekraïne

Op 23 december 2015 werden 700.000 mensen in de Ivano-Frankivsk-regio in Oekraïne getroffen door een stroomstoring van enkele uren. Een jaar later, op 17 december 2016, vond opnieuw een stroomstoring plaats in een deel van Kiev. Beide storingen waren het gevolg van cyberaanvallen, die volgens onderzoekers van een beveiligingsbedrijf aan elkaar waren gerelateerd.
In 2015 kwamen de aanvallers het besturingscentrum binnen via een 'Trojaans paard', waarna ze malware hebben achtergelaten. In 2016 ging het vermoedelijk om aanvallers die al een half jaar 'binnen' waren en die periode gebruikten om het systeem te leren kennen, zich toegang te verschaffen tot deelsystemen en verschillende tests uit te voeren om vervolgens een aanval te organiseren.
De aanvallen in Oekraïne worden door internationale experts gezien als de eerste voorbeelden waarbij kwaadwillenden de elektriciteitsvoorziening afsluiten voor grote groepen gebruikers.

3.4 Internationale dimensie digitale kwetsbaarheden

Doordat de stroomvoorziening van veel Europese landen met elkaar verknoopt is geraakt, vormen kwetsbaarheden in het elektriciteitssysteem van het ene land ook een risico voor het elektriciteitssysteem in andere landen. Het voorkomen van overbelasting van netwerken vergt dus een goede internationale afstemming van vraag en aanbod. Wanneer daar iets misgaat, zijn de gevolgen direct merkbaar, ook over de grens (zie kader).

Coördinatiefout stroomtransport Noordwest-Europa

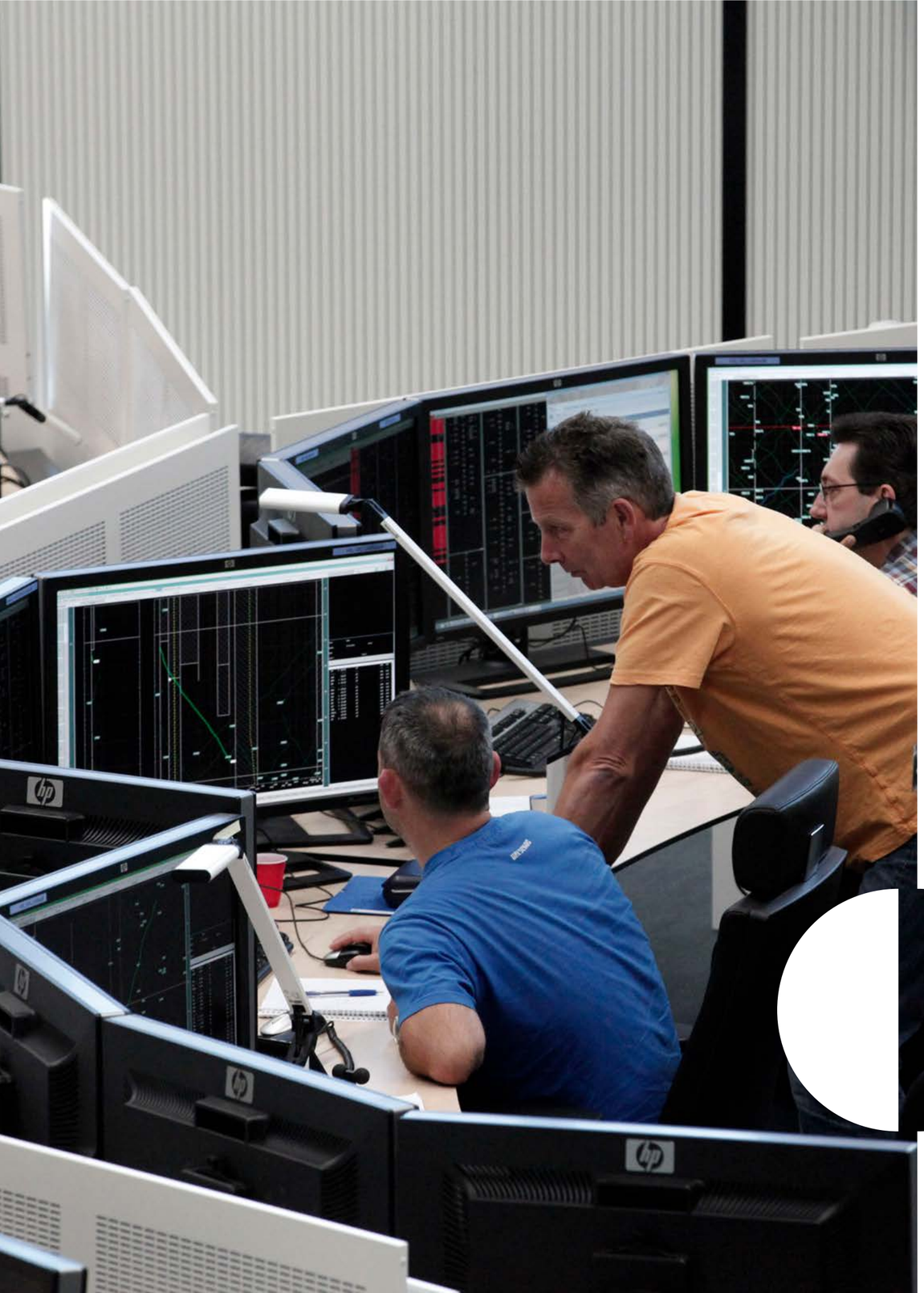
Op zaterdag 4 november 2006 werd kort na 22 uur 's avonds een grote Europese black-out in gang gezet door een schakelhandeling in het Duitse hoogspanningsnet. Netbeheerder E.ON.Netz had een hoogspanningslijn buiten bedrijf gesteld. Deze afschakeling vond plaats op verzoek van een scheepswerf en was nodig om een cruiseschip te kunnen laten passeren. Op zichzelf was de afschakeling goed voorbereid en weken van tevoren internationaal afgestemd. Een dag voordat het zover was kreeg de netbeheerder echter het verzoek van de scheepswerf om de afschakeling ruim drie uur te vervroegen. De netbeheerder stemde hierin toe nadat netberekeningen hadden uitgewezen dat dit niet tot onveilige netsituaties zou leiden. De naburige netbeheerders (TenneT en RWE TSO) werden hiervan echter niet op de hoogte gesteld, zodat zij hier niet op konden anticiperen.
Het gevolg was een kettingreactie van overbelaste verbindingen die in diverse West-Europese landen automatisch werden uitgeschakeld. Ruim 15 miljoen inwoners kregen daardoor te maken met een stroomonderbreking. Frankrijk, Italië, Spanje en Portugal kregen de grootste klappen te verwerken. In Nederland bleven de gevolgen van de stroomstoring naar verhouding beperkt. Alleen een aantal gemeenten in Zuid- en Oost-Nederland werd getroffen.

De digitalisering dringt door in verschillende onderdelen van het elektriciteitssysteem in Europa en de gevolgen daarvan voor de betrouwbaarheid van de stroomvoorziening zijn nog moeilijk te overzien. Wel is duidelijk dat het beperken van de genoemde nieuwe kwetsbaarheden in ieder geval ook een internationale aanpak vereist. Het fysieke elektriciteitssysteem binnen de Europese grenzen wordt immers meer en meer wereldwijd verbonden met het virtuele digitale netwerk.

Er zijn verschillende internationale ontwerpstandaarden die zich richten op elementen van een betrouwbare stroomvoorziening. Een voorbeeld zijn de standaarden voor industriële automatisering en besturingssystemen in de ISA/IEC-serie en de internationale normen voor het ontwerp van ICT-systemen (met daarin drie elementen: continuïteit, vertrouwelijkheid en integriteit[9]). Het is evenwel de vraag of deze bestaande standaarden wel gericht zijn op de volle breedte van veilige en betrouwbare digitale systemen. Normen voor ontwerp en onderhoud van consumentenapparatuur, transportmiddelen, systemen voor productie, opslag en transport van energie houden vaak onvoldoende rekening met het feit dat deze

9 Deze termen worden ook gebruikt in de Memorie van Toelichting bij de Cybersecuritywet. Internationaal gebruikt men de termen *availability*, *confidentiality* en *integrity*.

apparatuur in verbinding staat met het elektriciteitssysteem en dat dit consequenties kan hebben voor de betrouwbaarheid van de stroomvoorziening. Het is daarnaast de vraag of de bestaande standaarden ook andere digitale kwetsbaarheden dan alleen cybersecurity bestrijken. De Rli acht het werken met standaarden nuttig maar merkt op dat dit in het licht van de digitalisering onvoldoende is. Het tempo waarin standaarden en procedures worden ontwikkeld kan zich niet meten met de snelheid waarmee digitale veranderingen worden doorgevoerd.



4

AANBEVELINGEN

De uitgangspositie van Nederland in de verandering van het elektriciteitssysteem is goed. Onze huidige stroomvoorziening kent een grote betrouwbaarheid en wordt tegen relatief lage kosten gerealiseerd (ECN et al., 2016). Dit betekent dat de belofte van de overheid aan de samenleving dat zij zal zorgen voor een veilige, betrouwbare en betaalbare stroomvoorziening, op dit moment wordt waargemaakt.

De voortschrijdende digitalisering van de stroomvoorziening brengt echter nieuwe kwetsbaarheden met zich mee, die breder zijn dan alleen de dreiging van moedwillige verstoring door cybercriminelen. De kwetsbaarheden betreffen ook de gevolgen van eventuele softwareontwerpfouten en van onvoorzien gedrag van autonome systemen. Digitalisering vindt bovendien plaats in alle onderdelen van de stroomvoorziening, waardoor de stabiliteit van het totale systeem niet meer alleen via het netbeheer kan worden gewaarborgd. De levering, het transport en de distributie van elektriciteit kunnen door digitale risico's in het geding komen.

De Rli constateert dat een *integrale* benadering van de digitale kwetsbaarheden nodig is, waarbij op alle onderdelen van het elektriciteitssysteem in ogenschouw worden genomen. Dat betekent de overheid niet alleen moet kijken naar de onderdelen die in publiek eigendom zijn (de netbeheerders), maar ook daarbuiten. Daarvoor is extra expertise nodig van partijen die van buiten de elektriciteitssector afkomstig zijn en beschikken over kennis van de risico's rond digitalisering die zich niet beperkt tot cybersecurity. De belangrijkste zorg van de Rli is dat betrokken partijen aangeven dat er nog weinig zicht is op de gevolgen die deze digitalisering heeft voor de betrouwbaarheid van de elektriciteitsvoorziening. Daardoor is nu nog geen zorgvuldig oordeel mogelijk of de huidige instrumenten die de betrouwbaarheid moeten waarborgen, ook in de toekomst adequaat zijn. Daarom doet de Rli de rijksoverheid vier aanbevelingen.

4.1 Onderzoek gevolgen van digitalisering voor betrouwbaarheid stroomvoorziening

De Rli adviseert de rijksoverheid een onderzoeksprogramma te starten in nauwe samenwerking met partijen uit de elektriciteitssector, de ICT-sector en de telecommunicatie, om de kwetsbaarheden rond de gedigitaliseerde stroomvoorziening in samenhang te kunnen bekijken. Dit in het licht van de voorzienbare groei van het elektriciteitsverbruik in alle sectoren van de samenleving. De hoofdvraag waarop het onderzoeksprogramma zich zou moeten richten is: wat zijn de mogelijke gevolgen van de kwetsbaarheden die samenhangen met de digitalisering van het elektriciteitssysteem voor de betrouwbaarheid van de stroomvoorziening?

De in dit advies in kaart gebrachte kwetsbaarheden zullen in ieder geval in het onderzoeksprogramma moeten worden betrokken, te weten kwetsbaarheden veroorzaakt door:

- fouten in het ontwerp van software;
- onvoorzien of ongewenst gedrag van geautomatiseerde digitale systemen; en
- moedwillige verstoringen.

De Rli heeft een gezamenlijk onderzoeksprogramma voor ogen waarin zowel kennis over energiesystemen als over digitalisering is

vertegenwoordigd. De Rli denkt aan inbreng vanuit de wetenschap, kennisinstituten, netbeheerders, grote en kleine stroomproducenten, telecompartijen, toeleveranciers van digitale systemen, toezichthouders en departementen.

De vervolgvraag is of in het licht van de nieuwe kwetsbaarheden de huidige regelgeving en de afbakening van verantwoordelijkheden nog adequaat zijn en of alle partijen voldoende zijn toegerust om hun rol te vervullen. Denk bij dit laatste aan het wettelijke instrumentarium van de netbeheerders, de regels voor energieproducenten, de richtlijnen voor dienstverleners (zoals aanbieders van digitale platforms) en de standaarden voor apparatuur. Kwesties die hierbij aan de orde kunnen komen zijn:

- *crisismanagement bij stroomuitval*: is in de protocollen voor situaties waarin de elektriciteit op grote schaal uitvalt voldoende rekening gehouden met het digitale karakter van de stroomvoorziening?
- *eisen aan digitale schakelpunten*: moeten in het ontwerp van de digitale systemen voorzorgsmaatregelen worden ingebouwd om in crisissituaties het verbruik, de productie en de levering van stroom te kunnen reguleren via noodbesturing (waarbij alle door burgers en bedrijven geproduceerde en opgeslagen stroom via noodbesturing kan worden ingezet voor gemeenschappelijke belangen)?
- *verantwoordelijkheidsverdeling bij aanpak van verstoringen*: is helder vastgelegd wie welke rol vervult wanneer gehackte consumentenapparatuur de stroomvoorziening in bredere zin in gevaar kan brengen?

4.2 Neem 'no-regret'-maatregelen die digitale kwetsbaarheden indammen

Vooruitlopend op de uitkomsten van het bovengenoemde onderzoeksprogramma meent de Rli dat de overheid nu al enkele concrete 'no regret'-maatregelen kan starten:

- Uitbreiden van de bestaande *financiële of juridische prikkels* die partijen ertoe aanzetten om preventieve maatregelen te nemen tegen ontwerpfouten in software, onvoorzien geautomatiseerd gedrag en moedwillige verstoring. Te denken valt aan aansprakelijkstelling, inperking van toegang tot de energiemarkt en/of boetes bij nalatigheid.
- Waarborgen dat actuele inzichten over veilig ontwerp van digitale systemen die verbonden zijn met het elektriciteitsnet in *algemene standaarden*, zoals de netcodes, worden vastgelegd. Voor zover het gaat om apparatuur of installaties die vallen onder Europese productveiligheidsregels zal dit ook op Europees niveau moeten worden geregeld. Daarbij moet ook worden nagegaan of periodieke tests van de systemen op onvoorzien gedrag kunnen bijdragen aan het beperken van de kwetsbaarheid.
- Verkennen van mogelijkheden voor het *veiliger uitvoeren van softwareupdates*, binnen of in aanvulling op internationale standaarden hiervoor.

4.3 Investeer structureel in een onafhankelijke kennisinfrastructuur

De Rli adviseert de rijksoverheid om met alle betrokken partijen in de elektriciteitssector een gezamenlijke infrastructuur op te bouwen voor het vergaren van kennis over de kwetsbaarheden van digitalisering in de stroomvoorziening. Een kwalitatief goede en gezaghebbende kennisinfrastructuur is van belang om de ontwikkelingen in de stroomvoorziening, die elkaar in hoog tempo opvolgen, in goede banen te leiden. De infrastructuur moet gezamenlijke kennisvergaring (*joint fact finding*) faciliteren, waarin behalve publieke partijen ook marktpartijen binnen de elektriciteitssector hun kennis delen over de kwetsbaarheden van digitalisering. Ook afspraken over een meldplicht bij cyberaanvallen en cyberkwetsbaarheden moeten onderdeel vormen van de gezamenlijke kennisvergaring. Op die manier kan consensus worden bereikt over de maatregelen die moeten worden genomen om de kwetsbaarheden die het gevolg zijn van de van digitalisering van het elektriciteitssysteem, te beperken.
De Rli ziet hier een analogie met het VN-Klimaatpanel IPCC[10] en het kennisinstituut Deltares. Ook in deze gremia worden wetenschappelijke inzichten ontwikkeld en ontsloten en worden verschillen van inzicht met elkaar geconfronteerd.

4.4 Zoek samenwerking met Europese partners om kwetsbaarheden aan te pakken

De nationale elektriciteitsnetwerken in Europa en de daarmee verweven digitale systemen zijn verregaand met elkaar verbonden. Daarmee is er een belang om op Europees niveau samen te werken bij de aanpak van de kwetsbaarheden in de gedigitaliseerde stroomvoorziening. Het gaat dan zowel om het hiervoor besproken onderzoeksprogramma als om concrete richtlijnen voor producten. De Rli doet de rijksoverheid in dit licht de volgende aanbevelingen:

- Zorg ervoor dat in het nationale onderzoeksprogramma over kwetsbaarheden van digitalisering in de elektriciteitsvoorziening wordt samengewerkt met Europese partners.
- Onderzoek of er kan worden aangesloten bij Europese productveiligheidseisen voor apparaten die digitaal worden gestuurd en die van invloed kunnen zijn op de elektriciteitsvoorziening.
- Onderzoek of het gewenst is om in nieuwe Europese netcodes door verwijzing naar internationale normen de veiligheid bij software-updates in procedures te waarborgen.

10 IPCC: Intergovernmental Panel on Climate Change.

LITERATUUR

Bouma, K. (2017). 'Wat zijn de gevolgen van de stroomstoring die Amsterdam platlegde?' *Volkskrant*, 17 januari 2017.

Cyber Security Raad (2017). *Naar een veilig verbonden digitale samenleving: advies inzake de cybersecurity van het Internet of Things (IoT).* Den Haag.

ECN, Planbureau voor de Leefomgeving, Centraal Bureau voor de Statistiek & Rijksdienst voor Ondernemend Nederland (2017). *Nationale energieverkenning 2017*. Amsterdam/Petten: Energieonderzoek Centrum Nederland.

ECN, Energie-Nederland & Netbeheer Nederland (2016). *Energietrends 2016.* Petten.

Hollander, G. de, Vonk, M., Snellen, D. & Huitzing, H. (2017). *Mobiliteit en elektriciteit in het digitale tijdperk: publieke waarden onder spanning.* Den Haag: PBL.

International Energy Agency (2017). *World Energy Oulook 2017*. Paris.

Munnichs, G., Kouw, M. & Kool, L. (2017). *Een nooit gelopen race: over cyberdreigingen en versterking van weerbaarheid*. Den Haag: Rathenau Instituut.

Nationaal Coördinator Terrorismebestrijding en Veiligheid (2017). *Cybersecuritybeeld Nederland*. Den Haag.

Next Generation Infrastructures (2017). 'Gezocht: manager van de infrastructuur der infrastructuren'. *NGinfraMagazine*, 15 november 2017, 24-27.

Sijm, J., Gockel, P. (Alliander), Hout, M. van, Özdemir, Ö., Stralen, J. van, Smekens, K., Welle, A. van der, Joode, J. de, Westering, W. van & Musterd, M. (2017). *Demand and supply of flexibility in the power system of the Netherlands, 2015-2050: summary report of the FLEXNET project.* Arnhem: Alliander & Energieonderzoek Centrum Nederland.

Stokmans, D. & Logtenberg, H. (2017). ‘Hoe één verroest draadje de halve Randstad platlegt’. *NRC*, 7 juli 2017.

Tweede Kamer (2017a). *Duurzame ontwikkeling en beleid. Brief van de minister van Economische Zaken en Klimaat aan de Tweede Kamer van 11 december 2017*. Vergaderjaar 2016-2017, 30196, nr. 566.

Tweede Kamer (2017b). *Kabinetsaanpak Klimaatbeleid. Brief van de minister van Economische Zaken en Klimaat aan de Tweede Kamer van 8 december 2017.* Vergaderjaar 2017-2018, 32813, nr. 157.

Verhagen, H. (2016). *De economische en maatschappelijke noodzaak van meer cybersecurity: Nederland digitaal droge voeten*. Den Haag: Cyber Security Raad.

BIJLAGEN

TOTSTANDKOMING ADVIES

Raadscommissie

Prof. mr. N.S.J. Koeman, raadslid Rli

M.W.B. Lubben MSc, junior-raadslid Rli

Ir. A.G. Nijhof MBA, raadslid Rli en commissievoorzitter

Prof. dr. ir. M.R. van Steen, extern commissielid (wetenschappelijk directeur onderzoeksinstituut CTIT TU, Twente)

Drs. R. Wit, extern commissielid (directeur Corporate Strategy Eneco)

Projectteam

Ir. Y.M. Oostendorp, projectmedewerker

C.I.A. de Vries BC, projectassistent

Dr. B. Waterhout, projectmedewerker

Ir. D.K. Wielenga, projectleider

Geraadpleegde deskundigen en instanties

Deelnemers expertmeeting 18 en 19 september 2017

Erwin Bleumink, algemeen directeur, SURFNET

Pieter Bloemen, adviseur strategie en kennis, Staf Deltacommissaris

Aad Correljé, associate professor Economics of Infrastructures, TU Delft

Hugo Gastkemper, directeur, RIONED
Pieter van Gelder, hoogleraar Safety Science, TU Delft
Leendert Gooijer, senior wetenschappelijk medewerker en coördinator Nationale Veiligheid, RIVM
Jaap van den Herik, professor Informatica en Recht, Universiteit Leiden
Luc Kohsiek, dijkgraaf, hoogheemraadschap Noorderkwartier
Annette Ottolini, algemeen directeur, Evides Waterbedrijf
Abobakr Rassa, Corporate Strategy, Alliander
Theo van Ruijven, onderzoeker & adviseur Bescherming Vitale Infrastructuur, TNO
Monique Sweep, directeur, Deltawind

Deelnemers bijeenkomst op 7 december 2017
Herbert Bos, hoogleraar systeem- en netwerkbeveiliging, Vrije Universiteit Amsterdam
Annelies Huygen, TNO en hoogleraar ordening energiemarkten, Universiteit van Amsterdam
Machiel Mulder, hoogleraar regulering energiemarkten, Rijksuniversiteit Groningen
Hans-Peter Oskam, Manager Regulering en Marktfacilitering, Netbeheer Nederland
Frans Rooijers, directeur, CE Delft
Walter Ruijgrok, programmamanager Productie, Milieu en Klimaat, Energie-Nederland
Jos Sijm, senior researcher International Energy and Climate Issues, ECN

Geraadpleegde personen
Maarten Abbenhuis, senior Manager System Operations, TenneT
Pallas Agterberg, directeur strategie, Alliander
Erwin Bleumink, directeur, SURFnet
Frans Brom, secretaris raad en directeur bureau, WRR
Alan Croes, senior manager Corporate Asset Owner, TenneT
Michel van Eeten, onderzoeker in cybersecurity, TU Delft
Sabine Gielens, stuurgroepsecretaris Beveiliging & Crisismanagement, Vewin
Leendert Gooijer, senior wetenschappelijk medewerker en coördinator Nationale Veiligheid, RIVM
Hans Grünfeld, algemeen directeur, VEMW
Rudi Hakvoort, D-Cision, Zwolle
Sebastiaan Hers, senior onderzoeker/adviseur, CE Delft
Anke van Houten, beleidsmedewerker Deltaprogramma / crisisbeheersing, Unie van Waterschappen
Bart Jacobs, hoogleraar Digitale Veiligheid, Radboud Universiteit Nijmegen
Frank Jansen, senior adviseur business continuity, KPN
Wendy Kloeg, divisiemanager klant- en bedrijfsondersteuning, Dunea
Paul Koutstaal, program manager Energy Markets, ECN
Matthijs Kouw, researcher, Rathenau Instituut
Tom van der Lee, lid Tweede Kamer
Eric Luiijf, adviseur, TNO
Nicole Mallens, secretaris, VNO-NCW
Jos Meeuwsen, D-Cision, Zwolle
Geert Munnichs, themacoördinator, Rathenau Instituut
Annette Ottolini, algemeen directeur, Evides Waterbedrijf

Angela Puts, assetmanager, Dunea
Johan Rambi, Corporate Privacy & Security adviseur, Alliander N.V.
Nils Rosmuller, lector Transportveiligheid, Instituut voor Fysieke Veiligheid
Arno Rutte, lid Tweede Kamer
Jos Sijm, senior researcher International Energy and Climate Issues, ECN
Ben Voorhorst, Chief Operational Officer (COO), TenneT
Margot Weijnen, hoogleraar Process and Energy systems engineering, TU Delft en raadslid WRR
Annemarie Zielstra, directeur Cyber Security & Resilience, TNO

Geraadpleegde personen ministeries
Nel Aland, Hoofd Generieke Veiligheid, Nationaal Coördinator Terrorismebestrijding en Veiligheid
Esther van Beurden, afdelingshoofd directie analyse en strategie, Nationaal Coördinator Terrorismebestrijding en Veiligheid
Gijsbert Borgman, senior beleidsadviseur, ministerie van Infrastructuur en Milieu
Hidde Brugmans, beleidsondersteuner, ministerie van Economische Zaken
Maaike Daanen, senior beleidsmedewerker, ministerie van Economische Zaken
Bob Ent, senior beleidsmedewerker, ministerie van Economische Zaken
Saskia Ferf Jentink, senior, beleidsmedewerker, ministerie van Infrastructuur en Milieu
Sandor Gaastra, directeur-generaal Energie, Telecom en Mededinging, ministerie van Economische Zaken
Paul Gelton, directeur Veiligheidsregio's & Crisisbeheersing, Nationaal Coördinator Terrorismebestrijding en Veiligheid
Annemarieke Grinwis, senior beleidsmedewerker, ministerie van Infrastructuur en Milieu
Daniël de Groot, senior beleidsmedewerker, ministerie van Infrastructuur en Milieu
Peter Heij, directeur-generaal Water en Bodem, ministerie van Infrastructuur en Milieu
Dick Jung, manager, ministerie van Infrastructuur en Milieu
Maarten van Kesteren, medewerker, ministerie van Economische Zaken
Ronald van der Luit, medewerker, ministerie van Economische Zaken
Martin Lok, coördinerend beleidsmedewerker, ministerie van Economische Zaken
Inge Quist, coördinerend beleidsmedewerker, Nationaal Coördinator Terrorismebestrijding en Veiligheid
Dick Schoof, directeur-generaal, Nationaal Coördinator Terrorismebestrijding en Veiligheid
Hannah van Vorselen, rijkstrainee, ministerie van Economische Zaken

Reviewers
Herbert Bos, hoogleraar systeem- en netwerkbeveiliging, Vrije Universiteit Amsterdam
Han Slootweg, deeltijdhoogleraar Smart Grids aan de faculteit Elektrotechniek, Technische Universiteit Eindhoven
Paulien Herder, hoogleraar Engineering Systems Design in Energy, TU Delft

Onderzoek
D-Cision heeft in opdracht van de Rli een aantal internationale incidenten rond stroomvoorziening geanalyseerd op oorzaken en gevolgen.

OVERZICHT PUBLICATIES

2017

Brede blik op erfgoed, over de wisselwerking tussen erfgoed en transities in de leefomgeving. December 2017 (Rli 2017/03)

Energietransitie en leefomgeving: kennisnotitie. December 2017 (Rli 2017)

Grond voor Gebiedsontwikkeling. Instrumenten voor grondbeleid in een energieke samenleving. Juni 2017 (Rli 2017/02)

Technologie op waarde schatten. Een handreiking. Januari 2017 (Rli 2017/01)

2016

Dichterbij en sneller: kansen voor betere bereikbaarheid in stedelijke regio's. December 2016 (Rli 2016/05)

International Scan 2016. Emerging Issues in an International Context. November 2016 (Rli/EEAC)

Verbindend landschap. November 2016 (2016/04)

Opgaven voor duurzame ontwikkeling: hoofdlijnen uit vier jaar advisering door de Raad voor de leefomgeving en infrastructuur. Juli 2016 (2016/03)

Mainports voorbij. Juli 2016 (Rli 2016/02)

Systeemverantwoordelijkheid in de fysieke leefomgeving. Mei 2016 (Rli 2016/01)

2015

Vernieuwing omgevingsrecht: maak de ambities waar. December 2015 (Rli 2015/07)

Rijk zonder CO_2: naar een duurzame energievoorziening in 2050. September 2015 (Rli 2015/06)

Ruimte voor de regio in Europees beleid. September 2015 (Rli 2015/05)

Wonen in verandering, over flexibilisering en regionalisering in het woonbeleid. Juni 2015 (Rli 2015/04)

Stelselherziening omgevingsrecht. Mei 2015 (Rli 2015/03)

Circulaire economie: van wens naar uitvoering. Juni 2015 (Rli 2015/02)

Verkenning technologische innovaties in de leefomgeving. Januari 2015 (Rli 2015/01)

2014

Vrijkomend rijksvastgoed, over maatschappelijke doelen en geld. December 2014 (Rli 2014/07)

Risico's gewaardeerd, naar een transparant en adaptief risicobeleid. Juni 2014 (Rli 2014/06)

Milieuschade verhalen, advies financiële zekerheidstelling milieuschade Brzo- en IPPC4-bedrijven. Juni 2014 (Rli 2014/05)

Internationale verkenning 2014. Signalen: de opkomende vraagstukken uit het internationale veld. Mei 2014 (Rli 2014)

De toekomst van de stad, de kracht van nieuwe verbindingen. April 2014 (Rli 2014/04)

Kwaliteit zonder groei, over de toekomst van de leefomgeving. April 2014 (Rli 2014/03)

Doen en laten, effectiever milieubeleid door mensenkennis. Maart 2014 (Rli 2014/02)

Langer zelfstandig, een gedeelde opgave van wonen, zorg en welzijn. Januari 2014 (Rli 2014/01)

2013

Duurzame keuzes bij de toepassing van het Europese landbouwbeleid in Nederland. Oktober 2013 (Rli 2013/06)

Sturen op samenhang, governance in de metropolitane regio Schiphol/ Amsterdam. September 2013 (Rli 2013/05)

Veiligheid bij Brzo-bedrijven, verantwoordelijkheid en daadkracht. Juni 2013 (Rli 2013/04)

Nederlandse logistiek 2040, designed to last. Juni 2013 (Rli 2013/03)

Onbeperkt houdbaar, naar een robuust natuurbeleid. Mei 2013 (Rli 2013/02)

Ruimte voor duurzame landbouw. Maart 2013 (Rli 2013/01)

2012

Keep Moving, Towards Sustainable Mobility. Edited by Bert van Wee. Oktober 2012 (Rli/EEAC)

Colofon

Tekstredactie
Saskia van As, Tekstkantoor Van As

Fotoverantwoording
Cover: Jamesteohart / Shutterstock
Pagina 5: spainter_vfx / Shutterstock
Pagina 7: Thomas Boelaars Creative
Pagina 10: Flip Franssen / Hollandse Hoogte
Pagina 14: Robin Utrecht / Hollandse Hoogte
Pagina 20: Jan Lankveld / Hollandse Hoogte

Infographics
Slimme Financiering

Grafisch ontwerp
Jenneke Drupsteen Grafische vormgeving

Publicatie Rli 2018/01
Februari 2018

Vertaling
Dit advies is vertaald in het Engels en te downloaden via www.rli.nl

ISBN 978-90-8513-049-9
NUR 740