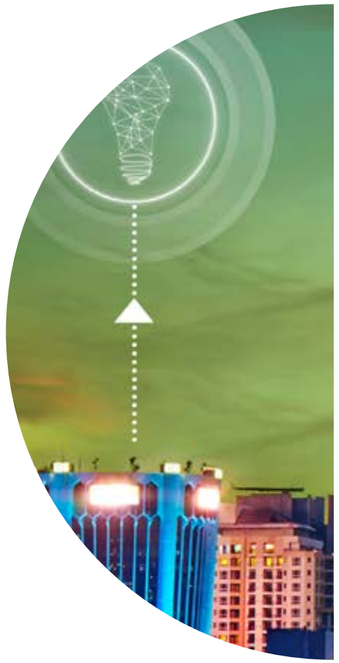
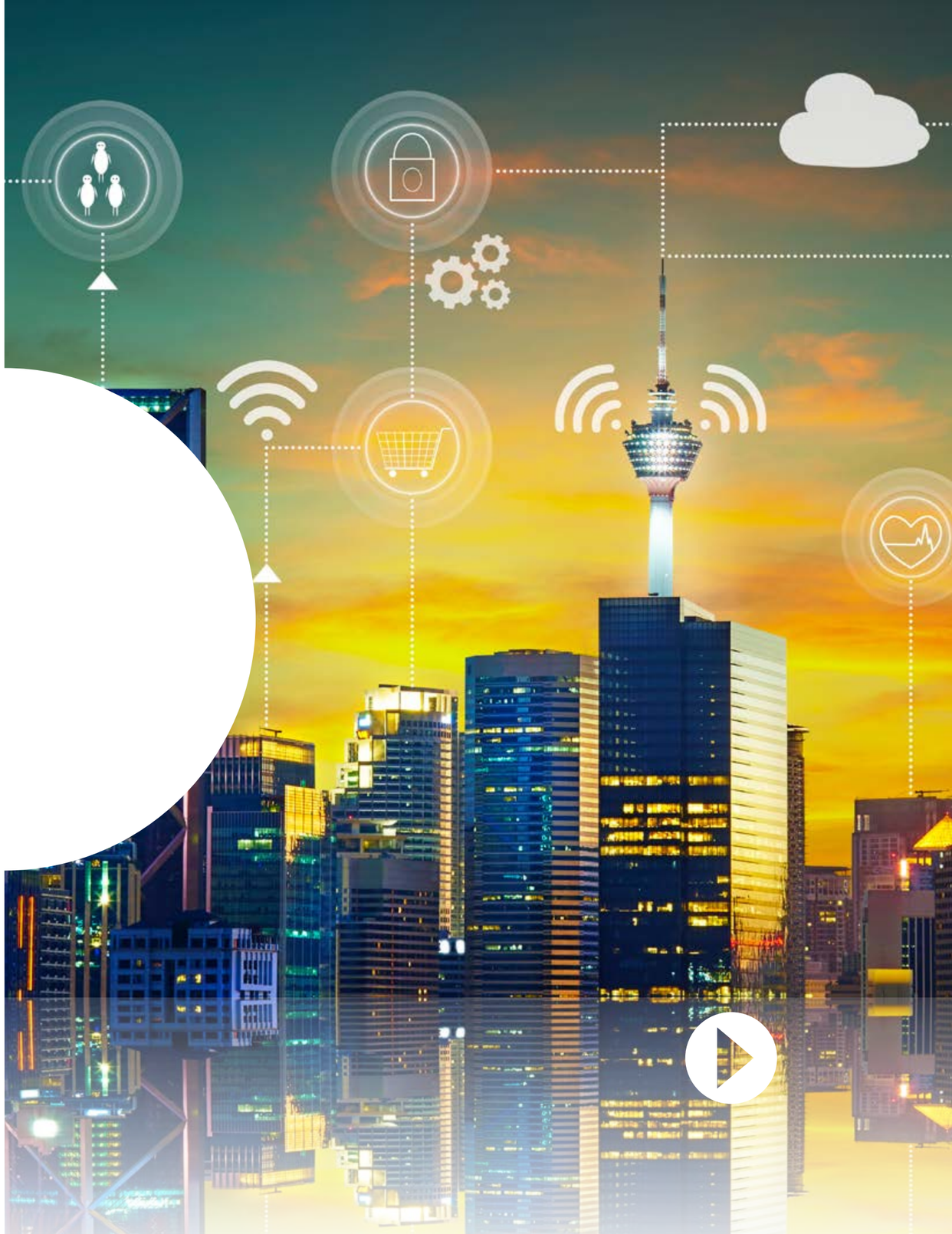
ELECTRICITY PROVISION IN THE FACE OF ONGOING DIGITALISATION

FEBRUARY 2018





Council
for the Environment
and Infrastructure

About the Council for the Environment and Infrastructure

The Council for the Environment and Infrastructure (*Raad voor de leefomgeving en infrastructuur*, Rli) advises the Dutch government and Parliament on strategic issues concerning the sustainable development of the living and working environment. The Council is independent, and offers solicited and unsolicited advice on long-term issues of strategic importance to the Netherlands. Through its integrated approach and strategic advice, the Council strives to provide greater depth and breadth to the political and social debate, and to improve the quality of decision-making processes.

The Council for the Environment and Infrastructure (Rli)

Bezuidenhoutseweg 30

P.O. Box 20906

2500 EX The Hague

the Netherlands

info@rli.nl

www.rli.nl

CONTENT

FOREWORD

The Council for the Environment and Infrastructure (*Raad voor de leefomgeving en infrastructuur, Rli, hereinafter also referred to as the "Council"*) has produced this advisory report in response to the Dutch government's request for advice about the reliability and continuity of the nation's 'critical infrastructures'. The Council was asked to determine whether there are any general lessons to be learned from the way in which the various critical infrastructures in the Netherlands have been designed.

During the initial exploratory phase, the Council examined three such critical infrastructures: the electricity production and distribution system, the telecommunication infrastructure, and water management (the water chain and the water supply system). It quickly became apparent that the current organisation and design of these infrastructures show marked differences, having been created at different times and under different circumstances. The rate at which these infrastructures are developing and the value of investments planned for the coming years are also dissimilar. The Council therefore concluded that any general lessons with regard to the design of critical infrastructures would inevitably be extremely abstract in nature.

It also became clear in the exploratory phase that all the critical infrastructures examined are subject to ongoing digitalisation, the implications of which are not yet fully understood. The mutual dependency between Information and Communication Technology (ICT) and the electricity system represents an interesting challenge. Without ICT there can be no electricity system, and without electricity there can be no ICT. This prompted the decision to narrow the scope of this advisory report and to focus on the digitalisation of electricity provision.

During the remainder of the advisory process, the Council examined developments within the 'ecosystem' of the generation, transmission and distribution of electricity, most notably those which are further to ongoing digitalisation. How will increasing reliance on digital technology affect the reliability and continuity of electricity provision?

SUMMARY

The Netherlands' electricity system is increasingly reliant on digital technology. Important decisions concerning generation, transmission and distribution are now made with the help of advanced software and algorithms. This development is one feature of an electricity system which is changing in many other respects. Generation increasingly makes use of sustainable, renewable energy sources. It is now more common for companies and individuals to produce their own electricity. In some cases, the ability to do so is dependent on weather conditions.

In this advisory report, the Council analyses the vulnerabilities which may be introduced to the current electricity system by the ongoing penetration of digital technology. Our analysis confirms that the digitalisation of the system does indeed raise new risks in terms of the reliability and continuity of electricity provision. The Council concludes that these new risks are not yet sufficiently understood, while their societal impact could be significant.

Fortunately, the government is devoting increasing attention to cybersecurity. However, the Council notes that there is insufficient insight into other possible vulnerabilities associated with digitalisation, even though they may have a significant impact on society. The Council has also observed that the government is mainly focused on digital vulnerabilities affecting publicly owned networks. However, the stability of the electricity system as a whole is particularly threatened by vulnerabilities in elements that are not publicly owned.

The Council therefore makes four recommendations:

1. The government must identify, examine and analyse the potential consequences of the digitalisation of the electricity system in terms of the reliability and continuity of supply.
2. Even before the results of this analysis are known, the government should implement 'no regret' measures to mitigate or prevent any vulnerabilities caused by ongoing digitalisation. Here, the Council suggests incentives which will encourage stakeholders to take preventive measures and to incorporate current knowledge about the secure design and updating of digital systems into a set of clear standards.
3. The government should create an infrastructure to support joint fact finding (knowledge development). Public sector authorities, grid operators and the market parties within the electricity sector should be encouraged to share their knowledge about the potential vulnerabilities introduced by digitalisation. This bundling of expertise is essential in order to be able to apply impartial knowledge to create an electricity system in which public interests are protected on a long-term basis.
4. The government should seek cooperation with other European and EU member states in addressing the vulnerabilities caused by the digitalisation of the electricity system, not only in terms of research but also with a view to the further development of product safety requirements and pan-European network codes.

1

INTRODUCTION

1.1 Context

The reliability and continuity of electricity provision is a matter of great importance. Any disruption has the potential to cause personal injury, physical damage and/or financial loss. A protracted power outage could lead to considerable public unrest and would therefore create further risks to safety and public order.

To ensure the continued reliability, safety, affordability and sustainability of electricity provision, it is necessary to organise all aspects of production, transport and distribution in an effective manner. Overall responsibility for these processes lies with the government, as established by the Electricity Act (*Elektriciteitswet*) 1998. Practical implementation falls partly to private sector parties and is partly the task of public sector bodies. Under the terms of the Act, private utility companies undertake the generation, trading and supply of electricity, doing so on a commercial basis. The infrastructure is managed by public bodies which oversee the transport and distribution of electricity on the national grid and subsidiary networks. The utility companies and grid managers therefore help the government to fulfil its societal obligation to ensure safe, reliable and affordable electricity provision.[1]

The transition to clean, sustainable energy will result in radical changes to the current electricity system, and these changes will be accompanied by its further digitalisation. To ensure that the transition is managed effectively, the Minister of Economic Affairs and Climate Policy has presented a legislative agenda for the energy transition (House of Representatives 2017a) and proposals for a Climate and Energy Agreement (2017b). In addition, the proposed Cyber Security Act (*Cybersecuritywet*) and the Cyber Security Data Processing and Reporting Requirements Act (*Wet Gegevensverwerking en Meldplicht Cybersecurity, WGMC*) provide enhanced protection for digital systems, including the electricity system, against deliberate disruption, i.e. sabotage.[2] Efforts continue to identify and reduce high-risk mutual dependencies between critical infrastructures, such as electricity provision and telecommunications.

The Council acknowledges the importance of such government action but notes the absence of any wider perspective. A more comprehensive programme is important because the risks raised by the digitalisation of the electricity system are not confined to cyber crime. The Council is not alone in drawing attention to the digitalisation of the electricity system. The Netherlands Environmental Assessment Agency (PBL) has already done so (Hollander *et al.*, 2017), as have the International Energy Agency (IEA, 2017) and the Dutch Cyber Security Council (CSR, 2017).

1.2 Terms of reference

This report focuses on the question of whether the government is able to fulfil its societal obligation to ensure clean, safe, reliable and affordable

1 See Explanatory Memorandum accompanying the Gas and Electricity Act 1998 (Proceedings of the House of Representatives, 25 621, Parliamentary Year 1997-1998).

2 The Cyber Security Act and the Cyber Security Data Processing and Reporting Requirements Act implement 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.

electricity provision, given that the process of digitalisation is about to enter a new phase in the coming years. What risks will the changes bring in terms of reliability and continuity? Are adequate measures in place to manage these risks?[3]

1.3 Structure of the report

Chapter 2 describes the changes that will affect the electricity system within the foreseeable future. Chapter 3 examines the vulnerabilities that such changes can introduce. The final chapter (Chapter 4) presents recommendations which will help the government to identify these vulnerabilities and to mitigate or prevent any adverse effects.

3 Further to this study, the Council interviewed many experts and organisations. They are listed in the Appendix, as are the members of the Council and the advisory committee for this report.

2

FAR-REACHING CHANGES TO THE ELECTRICITY SYSTEM

The coming years will see far-reaching changes to our electricity system as the result of a number of developments. In this section, the Council discusses four of those developments before examining the change which is central to this report: the digitalisation of the electricity system.

2.1 Current developments

Various developments, some already underway, will have a significant effect on the Netherlands' electricity system. Without attempting to be comprehensive, the Council can cite:

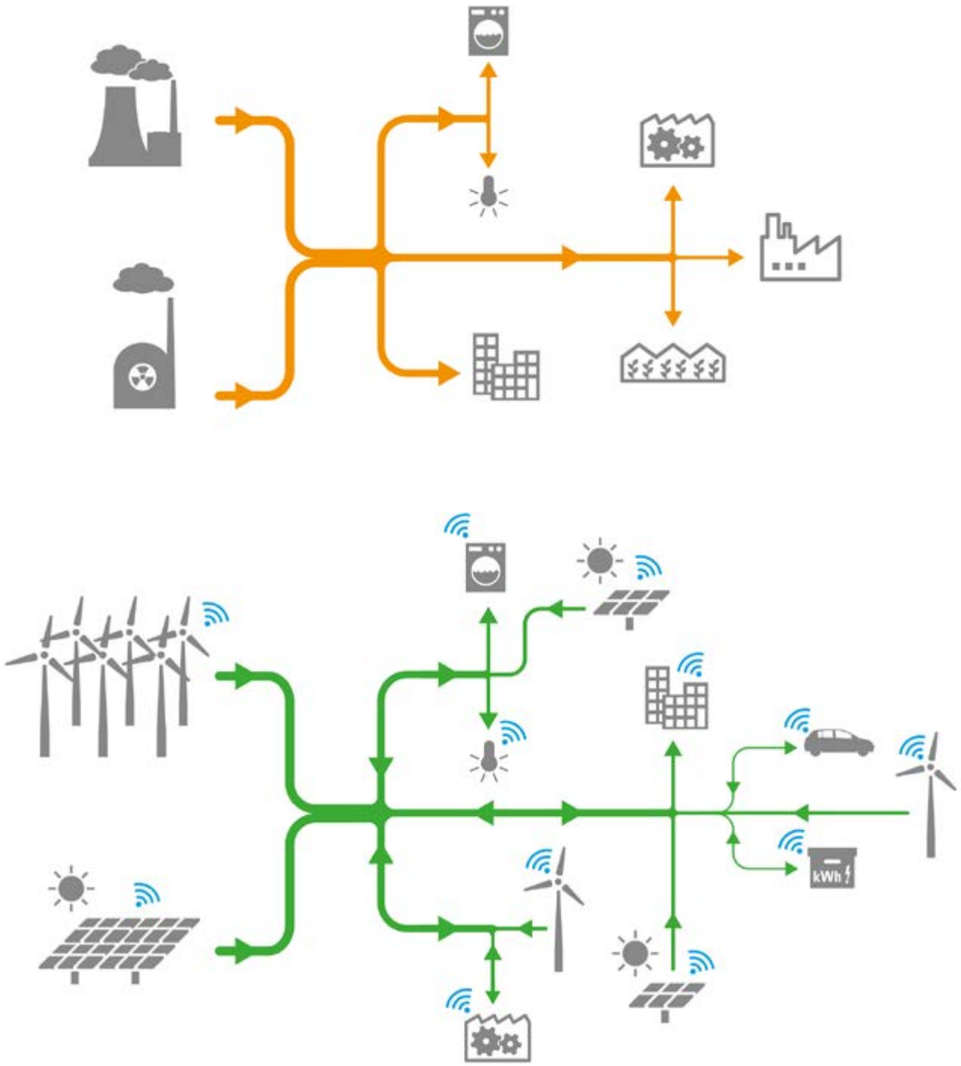
- *Electricity will represent a far greater share of the overall 'energy mix'* as we start to abandon the use of fossil fuels such as oil and gas. A far greater number of functions will then become dependent on electricity (ECN et al., 2017). Eventually, not only private cars will make the transition to alternative (non-fossil fuel) energy sources: so will goods vehicles, the aviation sector and heavy industry. Consequently, there will be a significant increase in demand for electricity. In the Netherlands, consumption is expected to double by the year 2050.
- *More electricity is being generated from renewable sources,* e.g. using solar panels, wind turbines or cogeneration units. Sustainable energy is expected to represent a far greater proportion of overall production: from 8% in 2015 to 44% in 2023 and 80% by 2050 (Sijm et al., 2017). In fact, the government has announced the ambition of achieving 100% sustainable electricity production by 2050. One result of this development is that electricity will be generated at a far greater number of locations than is currently the case. Another is that our reliance on imports of coal, oil and gas will be greatly reduced.
- *The electricity market will become less transparent* due to the inclusion of new market entrants, who will also fill a greater number of roles. Not only the established energy companies are installing solar panels, wind turbines and cogeneration units: so are companies in other sectors and private individuals, who are therefore taking on the dual role of producer and consumer. These parties will adjust electricity supply and demand in line with market price fluctuations, whereupon the role of the 'aggregators' (electricity brokers) will become more important.
- *Balancing supply and demand will become a more complex undertaking* as more electricity is generated from solar and wind energy. Production will then be more dependent on weather conditions (sunny or overcast, windy or calm). Grid stability will also be more difficult to achieve.[4] There are various potential solutions which will allow a quick response to fluctuations in supply and demand, all of which can help to safeguard continuity and affordability. However, it is not yet clear which of these solutions will be most appropriate in the Dutch situation.

2.2 A key role for digital technology

Digital technology will play an even more important role within the electricity system, and will facilitate the developments described above.

4 Grid stability is crucial to the safety and reliability of electricity provision. To ensure stability at all times, supply and demand must be carefully matched on an ongoing basis in a process known as 'grid balancing'. This task falls to the national grid operator, TenneT.

Figure 1: Major changes in electricity generation methods



From centralised generation to digitalised, decentralised, local generation by utility companies, other private sector parties and private individuals; all components of the system must be able to communicate with each other.

For example, digital technology will allow a rapid response to fluctuations in supply and demand. Not only large (utility) companies, but also smaller organisations and private individuals will be involved. There will be digital platforms through which the supply and demand of all producers and consumers can be coordinated and balanced.

Digital technology will also support and encourage the increasing use of generating equipment, monitoring equipment, storage facilities and appliances which consume electricity, all of which can communicate with each other through automated processes.[5] All equipment will be permanently interconnected by advanced software based on pre-programmed rules (algorithms). The supply of electricity and its consumption will then be automatically adjusted in line with fluctuations in price. Surplus electricity will be stored in batteries and accumulators, in electric vehicles, or sold on to neighbours. (Preventive) maintenance work can be optimised by ongoing monitoring, which may eventually rely on self-learning systems.

Within this ‘digitalised’ electricity system, there is a key role for the switching points: hubs at various points of the system at which various data is analysed and correlated, such as information relating to the volume of electricity being generated and consumed, price fluctuations, consumption patterns, and the contracts for the supply and purchase of electricity that are in place. Based on this information, the switching points

5 Also known as the ‘Internet of Things’ (IoT).

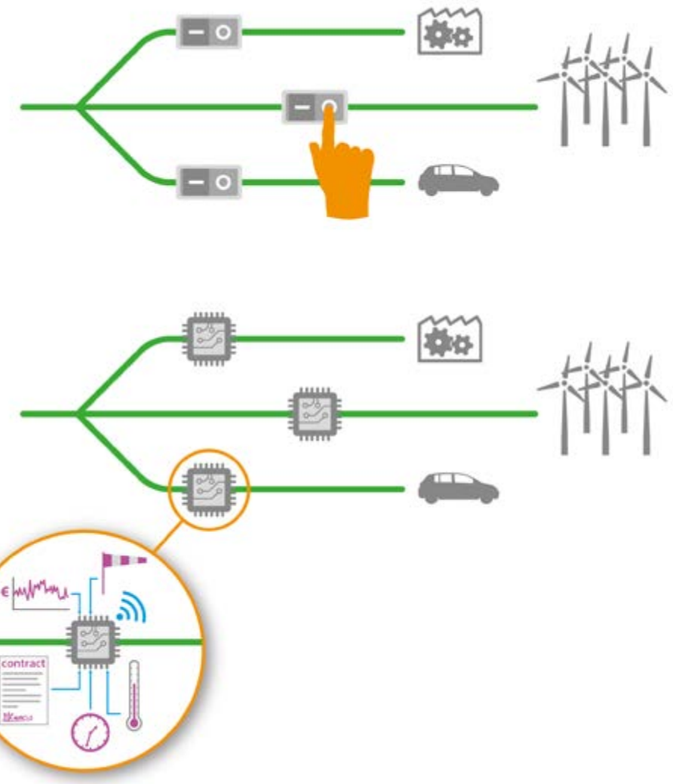
are able to control devices remotely to manage electricity production, distribution and usage.[6]

Digital switching points will come in various shapes and sizes. Some will be built into devices, while others are purely virtual. They can connect the most diverse types of equipment. In the industrial setting, switching points will monitor and manage the process installations' requirement for power and heat. In a private household, they will perform the same function for various domestic appliances such as thermostats, refrigerators, solar panels and heat pumps. Wind turbine and solar energy farms will be controlled via switching points. The charging points for electric (goods) vehicles will be interconnected via switching points in order to optimise loading efficiency. Endless combinations are possible.

In all these applications, the digital technologies on which the switching points rely will enable data to be read remotely and processes to be adjusted in real time and automatically. The underlying software in the switching points can also be updated remotely.

In combination, the developments outlined above will create a fully automated electricity system[7] in which decisions relating to storage, distribution and consumption are taken by pre-programmed or self-learning software, not only in the Netherlands but in neighbouring countries as well. There are clearly many advantages to such a system. However, there is also one significant disadvantage: the entire electricity system will be wholly dependent on vulnerable digital resources. This has implications in terms of reliability and continuity, and those implications transcend national borders.

Figure 2. The difference between analogue and digital switching points



Analogue switches are operated manually. Digital switching points control devices based on data such as the amount of electricity being generated and consumed, prices, consumption patterns and weather conditions.

6 Switching points should not be confused with 'allocation points' ('allocatiepunten'), a Dutch term for virtual hubs at which the transfer of electricity from the grid to an individual electrical connection (e.g. a household) takes place.

7 A fully digitalised electricity network is also known as a 'smart grid'.

3

NEW VULNERABILITIES

The digitalisation of the electricity system creates new vulnerabilities in the electricity supply. There could be problems at various points: the equipment which remotely controls generation and storage requirements, the networks (grids), or the complex digital processes underlying communication between the various system components. Moreover, because those components are increasingly interdependent, any problem or fault can lead to a cascade of 'knock-on' effects which, in combination, may cause the complete failure of the system and widespread power outages.

System failure can have far-reaching societal effects, as past incidents have shown. In January 2017, for example, much of Amsterdam suffered a power cut. The problem on the grid managed by TenneT was resolved within two hours, while power on the subsidiary network managed by Alliander was restored in five hours. However, there were major knock-on effects which continued to be felt for some time (see insert).

Power outage in Amsterdam: hours of chaos

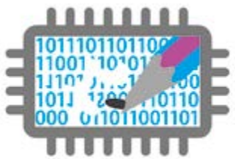
The January 2017 power outage which affected parts of Amsterdam, Zaandam and Landsmeer was, according to the local grid manager, caused by problems at a high-voltage substation. Over 360,000 households were without electricity for several hours. The situation caused major problems, not least in communications. The mobile phone network went down, Wi-Fi did not work, and even the national emergency number (112) was unreachable. Problems continued even after the power supply had been restored. It was a day of chaos on the railways, extending far beyond the area affected by the power outage itself. There were long tailbacks on the roads and the shelves in some supermarkets remained empty as it was impossible to deliver new stock. The Slotervaart Hospital was forced to cancel all operations on the day of the outage (Bouma, 2017; Stokmans and Logtenberg, 2017).

In future, the effects of this type of incident will be even more serious because a greater number of societal functions will rely on electricity. A power failure could lead to serious public unrest and social disruption. Mobile communications and the Internet would be unavailable. The entire transport system and large sections of industry would be brought to a halt, with all the economic losses that entails. People may have to spend hours or days without heating, which in certain high-risk groups could result in deaths. A large-scale power outage would hinder the authorities' ability to maintain public order. It would also undermine people's trust in each other and in the government should there be, say, food shortages or any unfair allocation of resources such as emergency generators.

Several organisations have drawn attention to the vulnerabilities that accompany the digitalisation of the electricity system. Reports have been produced by the Netherlands Environmental Assessment Agency (Hollander et al., 2017), the Cyber Security Council (CSR, 2017) and the International Energy Agency (IEA, 2017). In the Council's opinion, these publications do not adequately distinguish between the various types of vulnerabilities and threats, nor sufficiently consider the interrelationships between them. We therefore discuss the three most important vulnerabilities within a

digitalised system below, together with their implications in terms of the reliability and continuity of the electricity supply and the international context. A number of examples are given as text inserts: all have prompted measures to prevent a recurrence.

3.1 Errors in software design

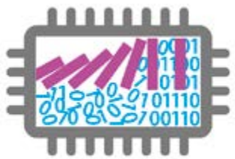


Processes in electricity generating stations and transport grids are managed by software of ever-increasing complexity. The risk of system failure due to programming errors is therefore much greater (Next Generation Infrastructures, 2017). It is, it appears, difficult to predict how the vital components of the electricity system will respond to the introduction of a new software element. It is therefore almost inevitable that design errors can occur. Unfortunately, even minor errors can lead to system failure (see insert). Sometimes, software updates are to blame.

Software error leads to major blackout in USA and Canada

A programming error was responsible for a major blackout affecting parts of the USA and Canada on 14 August 2003. Due to this software error, no warning was given of an impending system overload. A series of connections cut out, whereupon several production resources were automatically disconnected from the grid and shut down. Some 55 million people were without electricity. The equipment involved was old and past its best. The electricity systems of the Netherlands and its neighbouring countries also include some rather antiquated components, some installed in the 1970s and 80s.

3.2 Unexpected behaviour of autonomous digital systems

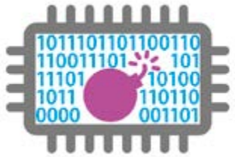


Disruptions to the electricity supply can also result from unintended and unexpected 'behaviour' on the part of autonomous digital systems. Such systems are now built in to an ever larger range of equipment. They automatically monitor and control electricity production (e.g. by solar panels) or storage (e.g. in home batteries) based on current market prices. In a free market, people respond to price incentives in various ways. Human behaviour can be erratic. The autonomous systems may respond in a more uniform manner, and this can lead to unexpected cumulative effects which will disrupt electricity provision.

Germany: pre-programmed generating equipment switches off completely unexpectedly

The transformers of most wind turbines and solar panels sold in Germany have pre-programmed algorithms to prevent network instability. If there is a deviation of more than a few points from the standard network frequency of 50 Hz, the algorithm will automatically shut off the electricity supply to the network, while ensuring that not all generating equipment is disconnected at precisely the same moment.

3.3 Deliberate disruption: sabotage



A failure of the power supply may also result from deliberate action by parties with malicious intent. A fully automated, digitalised electricity system is particularly vulnerable to this type of sabotage because so many of its components are connected to the Internet. The turbines of large wind farms, for example, are controlled remotely via the Internet. Software updates are also installed remotely via the Internet.

There might be various motives for wishing to disrupt the power supply. For individual 'hackers' it is often a question of virtual vandalism, a personal challenge or activism (e.g. to expose weaknesses in large companies' security arrangements). For the organised cyber criminal, sabotage is more likely to be a deliberate attempt to cause social disruption, possibly with some ulterior motive such as personal gain. Where these criminals have the support of foreign government regimes, there are clearly also political and/or strategic motives at play.

Hackers and cyber criminals use various methods. Some might attempt to block communication by means of a 'Distributed Denial of Service' (DDoS) attack, which involves bombarding a website server with so much data that it can no longer cope and shuts down. Another sabotage method is to introduce malware (harmful or malicious code) into the operating system.

The target of sabotage can also vary. Some attacks may focus on the hardware while others target the software. A network can be hacked online, or the criminal might cause physical damage to the equipment itself. All components of the electricity system, including the supply chain, are in principle vulnerable to deliberate disruption (National Coordinator for Security and Counterterrorism 2017; Munnichs et al., 2017; Verhagen, 2016).

Cyber attacks on electricity generating stations in Ukraine

On 23 December 2015, around 700,000 people in Ukraine's Ivano-Frankivsk region were affected by a power outage lasting several hours. One year later, on 17 December 2016, a similar power failure struck parts of the capital Kiev. Both incidents were the result of cyber attacks, i.e. hacking. Investigators concluded that they were related.

In 2015, the hackers managed to penetrate a control centre using a 'Trojan Horse' which installed malware. The 2016 incident is thought to have been planned for some time, the hackers having penetrated the systems some six months earlier. They used the intervening period to explore the infrastructure, gain access to subsystems, and perform a series of tests before launching the attack proper.

International experts regard the Ukraine attacks as the first examples of deliberate criminal action intended to cut off the power supply to a large number of consumers.

3.4 The international dimension

Because the electricity grids of several European countries are now interconnected, vulnerabilities in the system of one country also pose a

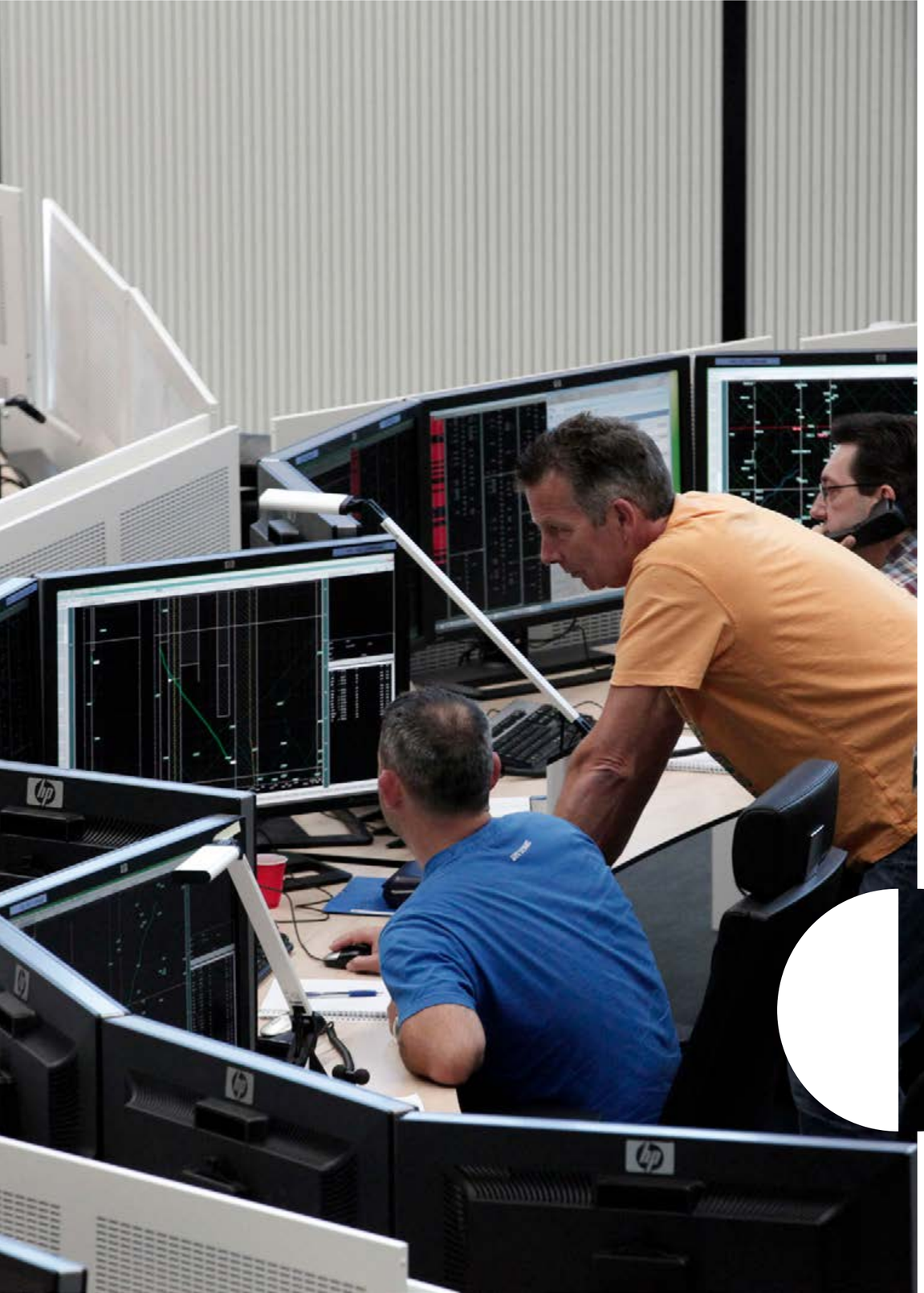
threat to those of other countries. Preventing network overload requires careful international coordination of supply and demand. Should something go amiss, the effects will be immediately apparent far beyond the national borders (see text insert).

Electricity transport coordination error in North-Western Europe

Shortly after 10 pm on Saturday 4 November 2006, a significant part of North-Western Europe was plunged into darkness by a switching error on the German high-voltage grid. Grid manager E.ON.Netz had disconnected a high-voltage line at the request of a harbour authority to allow a cruise liner to pass. This action had been planned well in advance and other national grid managers had been informed accordingly. However, just one day before the planned switch-off, the harbour authority contacted E.ON.Netz to request that it should be brought forward by three hours. E.ON.Netz agreed, since the network load prognoses suggested that this would not cause any problems. Unfortunately, national grid managers TenneT and RWE TSO were not informed of the change of plan and were therefore unprepared.
The result was a chain reaction of overloaded secondary networks in several countries, which were automatically shut down for safety reasons. Over 15 million people were left without power. The main countries affected were France, Italy, Spain and Portugal. In the Netherlands, the effects were relatively minor, restricted to a few areas in the south and east of the country.

The precise effects of the digitalisation of various parts of the European electricity system in terms of continuity of supply are, as yet, unknown. It is however clear that the new vulnerabilities call for a concerted international approach. After all, the physical electricity system within European borders is becoming increasingly interwoven with the worldwide virtual digital network.

There are various international design standards which apply to elements of a reliable electricity production and distribution system. They include the de ISA/IEC series, concerned with industrial automation and control systems, and the international standards covering the design of ICT systems, which comprise three elements: availability, confidentiality and integrity. It is, however, uncertain whether these existing standards address the full breadth of safe and reliable digital systems. Standards governing the design and maintenance of consumer appliances, transport vehicles, and systems for the production, storage and transport of energy do not always take full account of the fact that such equipment may be interconnected with the electricity system, which will have consequences in terms of the reliability of electricity provision. It is also unclear whether the existing standards address vulnerabilities other than those relating to cyber security alone. The Council believes that standards are useful resources, but notes that they are unlikely to be enough to counter any adverse effects of digitalisation. The speed at which standards and procedures can be developed lags behind that of the digital changes.



4

RECOMMENDATIONS

The Netherlands occupies a good starting position with regard to the transformation of its electricity system. Our current electricity provision is marked by a high degree of reliability, and is achieved at relatively low costs (ECN et al., 2016). In short, the government is currently fulfilling its societal obligation to ensure a safe, reliable and affordable electricity supply.

However, the ongoing digitalisation of the electricity system brings new vulnerabilities which go further than the threat of deliberate sabotage by cyber criminals. These vulnerabilities also include the effects of software design errors and the unpredictable behaviour of autonomous systems. Moreover, digitalisation will take place at all parts of the production, transmission, distribution and usage chain, whereupon the stability of the overall system can no longer be guaranteed through efficient grid management alone. Supply, transport and distribution will all be subject to new digital risks.

The Council concludes that an integrated approach to the digital vulnerabilities is required. All components of the electricity system must be subject to careful scrutiny. In other words, the government must not only examine those parts which are in public ownership (such as the grid managers), but those which are in private hands as well. This calls for additional expertise on the part of stakeholders outside the electricity sector itself, as well as knowledge of all potential risks posed by digitalisation, above and beyond the question of cyber security. The Council's main concern is that the parties involved have indicated that they have little understanding of the effects of digitalisation at this time, particularly in terms of the continuity and reliability of electricity provision. As a result, it is not yet possible to carefully assess whether the instruments currently in place to safeguard continuity will be adequate in the future. The Council therefore makes the following four recommendations.

4.1 Research the potential effects of digitalisation in terms of the reliability of electricity provision

The Council advises the central government to instigate a research programme in close cooperation with the parties within the electricity, ICT and telecommunications sectors in order to identify the vulnerabilities that could be introduced by the further digitalisation of the electricity system. This is important given the projected growth in the demand for electricity from all sectors of society. The central question of this research programme should be: What are the possible effects of vulnerabilities introduced by the digitalisation of the electricity system in terms of the reliability and continuity of supply?

The programme must consider all vulnerabilities listed in this advisory report, i.e.

- Errors in software design
- Unforeseen or undesirable behaviour on the part of automated digital systems
- Deliberate disruption (sabotage)

The Council has in mind a joint research programme in which knowledge about both energy systems and digitalisation is represented. We foresee

input from the research field, knowledge institutes, grid managers, large and small electricity producers, telecommunication operators, the providers of digital systems, regulatory authorities and the relevant ministries.

The follow-up question is whether, in the light of the new vulnerabilities, existing legislation and the current division of responsibilities will be adequate. Are all parties adequately equipped to fulfil their allocated tasks? This will entail examining the current legislative instruments governing the role of the grid managers, the regulations which apply to electricity producers, the guidelines and directives for service providers (such as those which supply digital platforms) and the standards governing various types of equipment and devices. Aspects to be examined should include:

- *Crisis management during a power outage:* Do the protocols for situations in which there is a large-scale or protracted power cut take adequate account of the digital character of the electricity system?
- *Requirements for digital switching points:* Should the design of the digital systems incorporate measures which will regulate the production, distribution and consumption of electricity by means of an emergency control system (which diverts all electricity being generated and stored by all parties to support essential public interests)?
- *Division of tasks and responsibilities in the event of disruptions:* Are there provisions which clearly establish who does what if, say, hacked consumer equipment places overall electricity provision at risk

4.2 Implement 'no regret' measures which mitigate or obviate the effects of digital vulnerabilities

The Council advises the government to implement specific 'no regret' measures at the earliest possible opportunity, even before the findings of the research programme are known. They should include:

- Expansion of the current financial and legislative incentives which encourage parties to implement preventive measures to avoid software design errors, unpredictable system behaviour and deliberate disruption. This category of measures includes liability claims, restricting access to the energy market, and financial penalties for proven negligence.
- Ensure that current knowledge regarding the safe design of digital systems which are interconnected with the electricity system is incorporated into general standards such as the network codes. Where equipment or installations are covered by EU product safety regulations, this must be done at the European level. It is also necessary to ascertain whether periodic system tests to detect unpredictable behaviour can help to reduce vulnerability.
- Explore options which would allow software updates to be installed in a more secure manner, either in accordance with or supplementing the international standards already in place.

4.3 Make ongoing investments in an independent knowledge infrastructure

The Council advises the government to join all stakeholders within the electricity sector in setting up a joint infrastructure for the development and

dissemination of knowledge regarding the potential vulnerabilities resulting from the digitalisation of the electricity system. Such an infrastructure, provided it is of high quality and suitably authoritative, will be essential in managing the rapid developments in the electricity system which are to take place. It should facilitate joint fact finding whereby both public sector authorities and market parties within the electricity sector are able to share knowledge. This joint knowledge infrastructure should also have a mandatory reporting requirement for cyber attacks and potential security leaks. It will then be able to reach consensus regarding the measures to be taken to mitigate or obviate the vulnerabilities further to the digitalisation of the electricity system.

In this context, the Council sees an analogy with the International Panel on Climate Change (IPCC), a 'think tank' which operates under the guidance of the United Nations, and the Dutch national knowledge institute for water and water management, Deltares. Both organisations exist to gather and disseminate scientific knowledge, whereby differences of opinion can be broached and resolved.

4.4 Seek cooperation with European partners

The national grids of several European countries are now interconnected, as are the digital systems on which they rely. It is therefore important to establish pan-European cooperation in order to address the vulnerabilities caused by further digitalisation of the electricity supply system. Such cooperation will usefully extend to the research programme outlined above, as well as concrete product guidelines. In this context, the Council offers the following recommendations to the central government:

- Ensure that the national research programme examining digital vulnerabilities affecting the electricity supply system is coordinated with the programmes of European partners, or invites input from those partners.
- Examine whether it is possible to subscribe to the European product safety requirements for digitally controlled equipment which has the potential to affect the proper functioning of the electricity supply system.
- Examine whether it is desirable for new European network codes to establish procedures for safe software updates, whereby such procedures make specific reference to the international safety codes.

REFERENCES

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

Dutch Cyber Security Council (2017). *Naar een veilig verbonden digitale samenleving: advies inzake de cybersecurity van het Internet of Things (IoT).* The Hague.

Dutch House of Representatives (2017a). *Duurzame ontwikkeling en beleid. Brief van de minister van Economische Zaken en Klimaat aan de Tweede Kamer van 11 december 2017*. Parliamentary Year 2016-2017, 30196, no. 566.

Dutch House of Representatives (2017b). *Kabinetsaanpak Klimaatbeleid. Brief van de minister van Economische Zaken en Klimaat aan de Tweede Kamer van 8 december 2017.* Parliamentary Year 2017-2018, 32813, no. 157.

Energy Research Centre of the Netherlands, Netherlands Environmental Assessment Agency, Statistics Netherlands and Netherlands Enterprise Agency (2017). *Nationale energieverkenning 2017*. Amsterdam/Petten: Energy Research Centre of the Netherlands.

Energy Research Centre of the Netherlands, Energie-Nederland and Netherlands Association of Energy Network Operators (2016). *Energietrends 2016*. Petten.

Hollander, G. de; Vonk, M.; Snellen, D.; and Huitzing, H. (2017). *Mobiliteit en elektriciteit in het digitale tijdperk: publieke waarden onder spanning*. The Hague: Netherlands Environmental Assessment Agency.

Munnichs, G.; Kouw, M.; and Kool, L. (2017). *Een nooit gelopen race: over cyberdreigingen en versterking van weerbaarheid.* The Hague: Rathenau Institute.

National Coordinator for Security and Counterterrorism (2017). *Cybersecuritybeeld Nederland*. The Hague.

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

Sijm, J.; Gockel, P.; Hout, M. van; Özdemir, Ö.; Stralen, J. van; Smekens, K.; Welle, A. van der; Joode, J. de; Westering, W. van; and 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 and Energy Research Centre of the Netherlands.

Stokmans, D. and Logtenberg, H. (2017). 'Hoe één verroest draadje de halve Randstad platlegt'. *NRC*, 7 July 2017.

TenneT (2016). *Rapport monitoring leveringszekerheid 2016 (2015-2031): AOC 2016-060*. Arnhem.

Verhagen, H. (2016). *De economische en maatschappelijke noodzaak van meer cybersecurity: Nederland digitaal droge voeten*. The Hague: Cyber Security Council.

APPENDICES

RESPONSIBILITY AND ACKNOWLEDGEMENTS

Advisory committee

Prof. N.S.J. Koeman, member of the Council for the Environment and Infrastructure

M.W.B. Lubben MSc, junior Council member

A.G. Nijhof MBA, Council member and committee chair

Prof. Dr M.R. van Steen, external committee member (Scientific Director of the Centre for Telematics and Information Technology (CTIT) at the University of Twente)

R. Wit, external committee member (Director of Corporate Strategy at Eneco)

Project team

Y.M. Oostendorp, project staff member

C.I.A. de Vries BC, project assistant

B. Waterhout PhD, project staff member

D.K. Wielenga, project leader

Experts and organisations consulted

Participants in experts' meeting on 18 and 19 September 2017

Erwin Bleumink, Managing Director, SURFnet

Pieter Bloemen, Strategy and Knowledge Adviser, Staff of Delta Programme Commissioner

Aad Correljé, Associate Professor of Economics of Infrastructures, Delft University of Technology

Hugo Gastkemper, Director, RIONED

Pieter van Gelder, Professor of Safety Science, Delft University of Technology

Leendert Gooijer, Senior Researcher and National Security Coordinator, Dutch National Institute for Public Health and the Environment (RIVM)

Jaap van den Herik, Professor of Computer Science and Law, Leiden University

Luc Kohsiek, Dike Reeve, Hollands Noorderkwartier Water Authority

Annette Ottolini, Managing Director, Evides Waterbedrijf

Abobakr Rassa, Corporate Strategy, Alliander

Theo van Ruijven, Researcher and Adviser on the Protection of Vital Infrastructure, Netherlands Organisation for Applied Scientific Research (TNO)

Monique Sweep, Director, Deltawind

Participants in meeting on 7 December 2017

Herbert Bos, Professor of Systems and Network Security, VU University Amsterdam

Annelies Huygen, Senior Researcher at the Netherlands Organisation for Applied Scientific Research and Professor of Energy Market Regulation at the University of Amsterdam

Machiel Mulder, Professor of Energy Market Regulation at the University of Groningen

Hans-Peter Oskam, Regulation and Market Facilitation Manager, Netherlands Association of Energy Network Operators

Frans Rooijers, Director, CE Delft

Walter Ruijgrok, Production, Environment & Climate Programme Manager, Energie-Nederland

Jos Sijm, Senior Researcher of International Energy and Climate Issues, Energy Research Centre of the Netherlands (ECN)

Other persons consulted

Maarten Abbenhuis, Senior Manager System Operations, TenneT

Pallas Agterberg, Strategy Director, Alliander

Erwin Bleumink, Director, SURFnet

Frans Brom, Council Secretary and Director of the WRR Office, Scientific Council for Government Policy (WRR)

Alan Croes, Senior Manager Corporate Asset Owner, TenneT

Michel van Eeten, Professor of Cybersecurity Governance, Delft University of Technology

Sabine Gielens, Secretary of Security & Crisis Management Steering Group, Netherlands Association of Drinking Water Companies (VEWIN)

Leendert Gooijer, Senior Researcher and National Security Coordinator, Dutch National Institute for Public Health and the Environment (RIVM)

Hans Grünfeld, Managing Director, Dutch Association for Energy, Environment & Water (VEMW)
Rudi Hakvoort, D-Cision, Zwolle
Sebastiaan Hers, Senior Researcher / Consultant, CE Delft
Anke van Houten, Policy Officer for Delta Programme / Crisis Management, Dutch Water Authorities
Bart Jacobs, Professor of Digital Security, Radboud University Nijmegen
Frank Jansen, Senior Business Continuity Consultant, KPN
Wendy Kloeg, Manager of Customer and Business Support Division, Dunea
Paul Koutstaal, Energy Markets Programme Manager, Energy Research Centre of the Netherlands
Matthijs Kouw, Researcher, Rathenau Institute
Tom van der Lee, Member of Parliament (Dutch House of Representatives)
Eric Luiijf, Adviser, Netherlands Organisation for Applied Scientific Research (TNO)
Nicole Mallens, Secretary, Confederation of Netherlands Industries and Employers (VNO-NCW)
Jos Meeuwsen, D-Cision, Zwolle
Geert Munnichs, Thematic Coordinator, Rathenau Institute
Annette Ottolini, Managing Director, Evides Waterbedrijf
Angela Puts, Asset Manager, Dunea
Johan Rambi, Corporate Privacy & Security Consultant, Alliander N.V.
Nils Rosmuller, Lecturer in Transport Safety, Institute for Safety
Arno Rutte, Member of Parliament (Dutch House of Representatives)
Jos Sijm, Senior Researcher of International Energy and Climate Issues, Energy Research Centre of the Netherlands (ECN)
Ben Voorhorst, Chief Operational Officer (COO), TenneT
Margot Weijnen, Professor of Process and Energy Systems Engineering at Delft University of Technology and member of the Scientific Council for Government Policy (WRR)
Annemarie Zielstra, Director of Cyber Security & Resilience, Netherlands Organisation for Applied Scientific Research (TNO)

Persons consulted at ministries

Nel Aland, Head of Generic Security, National Coordinator for Security and Counterterrorism
Esther van Beurden, Head of Analysis & Strategy Department, National Coordinator for Security and Counterterrorism
Gijsbert Borgman, Senior Policy Adviser, Ministry of Infrastructure and Water Management
Hidde Brugmans, Policy Assistant, Ministry of Economic Affairs
Maaike Daanen, Senior Policy Officer, Ministry of Economic Affairs
Bob Ent, Senior Policy Officer, Ministry of Economic Affairs
Saskia Ferf Jentink, Senior Policy Officer, Ministry of Infrastructure and Water Management
Sandor Gaastra, Director-General of Energy, Telecommunications and Competition, Ministry of Economic Affairs
Paul Gelton, Director of Security Regions & Crisis Management, National Coordinator for Security and Counterterrorism
Annemarieke Grinwis, Senior Policy Officer, Ministry of Infrastructure and Water Management

Daniël de Groot, Senior Policy Officer, Ministry of Infrastructure and Water Management

Peter Heij, Director-General of Spatial Planning & Water Affairs, Ministry of Infrastructure and Water Management

Dick Jung, Manager, Ministry of Infrastructure and Water Management

Maarten van Kesteren, employee, Ministry of Economic Affairs

Ronald van der Luit, employee, Ministry of Economic Affairs

Martin Lok, Coordinating Policy Officer, Ministry of Economic Affairs

Inge Quist, Coordinating Policy Officer, National Coordinator for Security and Counterterrorism

Dick Schoof, Director-General, National Coordinator for Security and Counterterrorism

Hannah van Vorselen, trainee, Ministry of Economic Affairs

Reviewers

Herbert Bos, Professor of Systems and Network Security, VU University Amsterdam

Han Slootweg, part-time Professor of Smart Grids, Department of Electrical Engineering, Eindhoven University of Technology

Paulien Herder, Professor of Engineering Systems Design in Energy, Delft University of Technology

Research

The Council commissioned the consultancy firm D-Cision to analyse the causes and consequences of a number of international power supply incidents.

OVERVIEW OF PUBLICATIONS

2017

A Broad View of Heritage: The Interactions between Heritage and Transitions in the Physical Environment [*'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. [only available in Dutch].

Land for Development: Land Policy Instruments for an Enterprising Society [*'Grond voor Gebiedsontwikkeling. Instrumenten voor grondbeleid in een energieke samenleving'*]. June 2017 (Rli 2017/02).

Assessing the Value of Technology: Guidance Document [*'Technologie op waarde schatten. Een handreiking'*]. January 2017 (Rli 2017/01).

2016

Faster and Closer: Opportunities for Improving Accessibility in Urban Regions [*'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).

The Connecting Landscape [*'Verbindend landschap'*]. November 2016 (Rli 2016/04).

Challenges for Sustainable Development: Main Focus Areas Identified in Advisory Reports Published in the Past Four Years by the Council for the Environment and Infrastructure [*'Opgaven voor duurzame ontwikkeling: hoofdlijnen uit vier jaar advisering door de Raad voor de leefomgeving en infrastructuur'*]. July 2016 (Rli 2016/03).

Beyond Mainports [*'Mainports voorbij'*]. July 2016 (Rli 2016/02).

System Responsibility in the Physical Living Environment. [*'Notitie Systeemverantwoordelijkheid in de fysieke Leefomgeving'* – only available in Dutch]. May 2016 (Rli 2016/01).

2015

Reform of Environmental Law: Realise your Ambitions [*'Vernieuwing omgevingsrecht: maak de ambities waar'*]. December 2015 (Rli 2015/07).

A Prosperous Nation Without CO_2: Towards a Sustainable Energy Supply by 2050 [*'Rijk zonder CO_2: naar een duurzame energievoorziening in 2050'*]. September 2015 (RIi 2015/06).

Room for the Regions in European Policy [*'Ruimte voor de regio in Europees beleid'*]. September 2015 (RIi 2015/05).

Changing Trends in Housing: Flexibility and Regionalisation Within Housing Policy [*'Wonen in verandering, over flexibilisering en regionalisering in het woonbeleid'*]. June 2015 (RIi 2015/04).

Stelselherziening omgevingsrecht. May 2015 (RIi 2015/03).

Circular Economy: From Wish to Practice [*'Circulaire economie: van wens naar uitvoering'*]. June 2015 (RIi 2015/02).

Survey of Technological Innovations in the Living Environment [*'Verkenning technologische innovaties in de leefomgeving'*]. January 2015 (RIi 2015/01).

2014

Managing Surplus Government Real Estate: Balancing Public Interest and Financial Gain [*'Vrijkomend rijksvastgoed, over maatschappelijke doelen en geld'*]. December 2014 (RIi 2014/07).

Risks Assessed: Towards a Transparent and Adaptive Risk Policy [*'Risico's gewaardeerd, naar een transparant en adaptief risicobeleid'*]. June 2014 (RIi 2014/06).

Recovering the Costs of Environmental Damage: Advisory Letter on Financial Indemnity to be Provided by High-Risk Companies [*'Milieuschade verhalen, advies financiële zekerheidstelling milieuschade Brzo- en IPPC4-bedrijven'*]. June 2014 (RIi 2014/05).

International Scan 2014: Signals: Emerging Issues in an International Context [*'Internationale verkenning 2014. Signalen: de opkomende vraagstukken uit het internationale veld'*]. May 2014 (RIi 2014).

The Future of the City: The Power of New Connections [*'De toekomst van de stad, de kracht van nieuwe verbindingen'*]. April 2014 (RIi 2014/04).

Quality Without Growth: On the Future of the Built Environment [*'Kwaliteit zonder groei, over de toekomst van de leefomgeving'*]. April 2014 (RIi 2014/03).

Influencing Behaviour: More Effective Environmental Policy through Insight into Human Behaviour [*'Doen en laten, effectiever milieubeleid door mensenkennis'*]. March 2014 (RIi 2014/02).

Living Independently for Longer: A Shared Responsibility of the Housing, Health and Welfare Policy Domains [*'Langer zelfstandig, een gedeelde opgave van wonen, zorg en welzijn'*]. January 2014 (RIi 2014/01).

2013

Sustainable Choices in the Implementation of the Common Agricultural Policy in the Netherlands [*'Duurzame keuzes bij de toepassing van het Europese landbouwbeleid in Nederland'*]. October 2013 (RIi 2013/06).

Pulling Together: Governance in the Schiphol/Amsterdam Metropolitan Region [*'Sturen op samenhang, governance in de metropolitane regio Schiphol/Amsterdam'*]. September 2013 (RIi 2013/05).

Safety at Companies Subject to the Major Accidents Risks Decree: Responsibility and Effective Action [*'Veiligheid bij Brzo-bedrijven, verantwoordelijkheid en daadkracht'*], June 2013 (RIi 2013/04).

Dutch Logistics 2040: Designed to Last [*'Nederlandse logistiek 2040, designed to last'*]. June 2013 (RIi 2013/03).

Nature's Imperative: Towards a Robust Nature Policy [*'Onbeperkt houdbaar, naar een robuust natuurbeleid'*]. May 2013 (RIi 2013/02).

Room for Sustainable Agriculture [*'Ruimte voor duurzame landbouw'*]. March 2013 (RIi 2013/01).

2012

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

Original title
Stroomvoorziening onder digitale spanning

Text Editing
Saskia van As, Tekstkantoor Van As

Photo Credits
Cover: Jamesteohart / Shutterstock
Page 5: spainter_vfx / Shutterstock
Page 7: Thomas Boelaars Creative
Page 10: Flip Franssen / Hollandse Hoogte
Page 14: Robin Utrecht / Hollandse Hoogte
Page 19: Jan Lankveld / Hollandse Hoogte

Infographics
Slimme Financiering

Graphic Design
Jenneke Drupsteen Grafische vormgeving, The Hague

Publication Rli 2018/01
February 2018

Translation
DBF Communicatie B.V.

ISBN 978-90-77166-66-6
NUR 740