# Themarapportage bedreiging vitale infrastructuur

## Deze themarapportage is onderdeel van de Rijksbrede Risicoanalyse Nationale Veiligheid

**Analistennetwerk Nationale Veiligheid**

# Themarapportage bedreiging vitale infrastructuur

## Deze themarapportage is onderdeel van de Rijksbrede Risicoanalyse Nationale Veiligheid

**Analistennetwerk Nationale Veiligheid**

## Colofon

Deze themarapportage is gemaakt door het Analistennetwerk Nationale Veiligheid in opdracht van de NCTV.

Het Rijksinstituut voor Volksgezondheid en Milieu (RIVM)
Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek (TNO)
Stichting Nederlands Instituut voor Internationale Betrekkingen 'Clingendael' (Clingendael)
SEO Economisch Onderzoek (SEO)
Algemene Inlichtingen- en Veiligheidsdienst (AIVD)
Militaire Inlichtingen- en Veiligheidsdienst (MIVD)
Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC)



Contact: ir. L. Gooijer (*leendert.gooijer@rivm.nl*)

# Inhoudsopgave

# 1. Inleiding

Deze themarapportage is onderdeel van de Rijksbrede Risicoanalyse (RbRa), uitgevoerd door het Analistennetwerk Nationale Veiligheid (ANV). Het doel van de RbRa is het in kaart brengen van verschillende typen dreigingen voor de nationale veiligheid van het Koninkrijk der Nederlanden. Hiertoe worden mogelijke dreigingen niet alleen geïdentificeerd, maar wordt ook een inschatting gemaakt van waarschijnlijkheid van optreden en mogelijke gevolgen (het 'risico'). Deze inschatting vindt plaats aan de hand van door het ANV opgestelde scenario's. De dreigingen in kwestie zijn verdeeld over negen verschillende inhoudelijke dreigingsthema's, elk onderverdeeld in meerdere categorieën met daarin één of meerdere scenario's. Voor elk van de thema's wordt een themarapport opgesteld. De themarapporten dienen als basis voor het hoofdrapport van de RbRa. De verschillende thema's en daaronder vallende categorieën worden in dit eindproduct gezamenlijk beschouwd aan de hand van de zes nationale veiligheidsbelangen. Zodoende wordt een overzicht gegeven van de belangrijkste risico's voor de nationale veiligheid.

Deze rapportage bevat de door het ANV uitgevoerde analyses voor het thema *bedreiging vitale infrastructuur*. Onder dit thema vallen drie dreigingscategorieën, met verschillende scenario's die de dreigingen illustreren. Hoofdstuk twee gaat in op de gehanteerde aanpak. Hoofdstuk drie geeft een algemene introductie tot het thema, de drie in deze rapportage opgenomen dreigingscategorieën en het algemene bouwstenenoverzicht met relevante actoren en factoren. In hoofdstuk vier worden de relevante ontwikkelingen voor dit thema beschreven. In hoofdstuk vijf, zes en zeven worden per dreigingscategorie de ontwikkelingen die relevant zijn voor deze categorie kort toegelicht, de actoren en factoren die van belang zijn worden beschreven en de scenario's worden toegelicht en beoordeeld. Tevens wordt per dreigingscategorie een beschouwing gegeven. In hoofdstuk acht wordt ingegaan op een relevante sluimerende dreiging voor dit thema. Hierin wordt een ontwikkeling besproken die binnen de tijdshorizon van 5 jaar nog geen concrete dreiging voor de nationale veiligheid oplevert, maar op de langere termijn wel een dreiging kan vormen. In hoofdstuk negen vindt u de slotbeschouwing over het thema *bedreiging vitale infrastructuur*.

# 2. Aanpak

Dit themarapport bevat voor elk van de drie dreigingscategorieën een overzicht van relevante ontwikkelingen en een nadere analyse van de dreiging (het fenomeen) binnen de categorie. Deze analyse is vormgegeven aan de hand van scenario's. Voor elke categorie zijn één of meerdere scenario's uitgewerkt ter illustratie van hoe de dreiging zich mogelijk kan manifesteren. In totaal zijn er voor het gehele thema vier scenario's uitgewerkt in de vorm van een verhaallijn. Daarnaast worden twee scenario's uit het thema *klimaat- en natuurrampen* besproken, maar dan vanuit het perspectief van natuurlijke verstoringen van vitale processen. De scenario's zijn tot stand gekomen in samenspraak met deskundigen behorende tot organisaties verbonden aan het ANV. De scenario's zijn nadrukkelijk bedoeld om de verschillende typen verstoringen van vitale processen (moedwillig, technisch/menselijk falen, natuurlijke oorzaak) te illustreren en zijn niet uitputtend. Binnen de RbRA wordt geen volledigheid nagestreefd met betrekking tot de opgenomen scenario's.

Voor elk van de scenario's zijn op basis van *expert judgement* zowel de waarschijnlijkheid van optreden als de mogelijke gevolgen in kaart gebracht aan de hand van de door het ANV ontwikkelde methodiek nationale veiligheid. In Bijlage 1 staat een overzicht van de organisaties die hebben deelgenomen aan de expertsessies voor dit thema.

## 2.1 Methodiek nationale veiligheid

Binnen deze methodiek wordt gekeken of en in welke mate een bepaalde gebeurtenis de zes nationale veiligheidsbelangen raakt. De nationale veiligheid is in het geding als één of meer van de zes nationale veiligheidsbelangen zodanig worden bedreigd dat er sprake is van (potentiële) maatschappelijke ontwrichting.[1] De zes belangen zijn elk opgesplitst in één of meerdere meetbare impactcriteria die helpen bij het in kaart brengen van een mogelijke aantasting. Onderstaande Tabel 1 geeft een kort overzicht van alle belangen en criteria. Een uitgebreide uitleg voor elk van deze onderdelen bevindt zich in de door het ANV opgestelde leidraad risicobeoordeling.[2]

[1] ANV, Leidraad Risicobeoordeling Rijksbrede Risicoanalyse Nationale Veiligheid (Bilthoven: RIVM, 2022), *https://www.rivm.nl/onderwerpen/nationale-veiligheid*.

[2] Idem.

**Tabel 1** Belangen en impactcriteria behorende toe de methodiek nationale veiligheid

| Belang | Impactcriteria |
|---|---|
| 1. Territoriale veiligheid | 1.1 Aantasting van de integriteit van het grondgebied van het Koninkrijk der Nederlanden |
| | 1.2 Aantasting van de integriteit van de internationale positie van het Koninkrijk der Nederlanden |
| | 1.3 Aantasting van de integriteit van de digitale ruimte |
| | 1.4 Aantasting van de integriteit van het bondgenootschappelijk grondgebied |
| 2. Fysieke veiligheid | 2.1 Doden |
| | 2.2 Ernstig gewonden en chronisch zieken |
| | 2.3 Gebrek aan primaire levensbehoeften |
| 3. Economische veiligheid | 3.1 Kosten |
| | 3.2 Aantasting van de vitaliteit van de economie van het Koninkrijk der Nederlanden |
| 4. Ecologische veiligheid | 4.1 Langdurige aantasting van het milieu en de natuur |
| 5. Sociale en politieke stabiliteit | 5.1 Verstoring van het dagelijkse leven |
| | 5.2 Aantasting van de democratische rechtstaat |
| | 5.3 Sociaal-maatschappelijke impact |
| 6. Internationale rechtsorde | 6.1 Aantasting van de normen van staatssoevereiniteit, vreedzame co-existentie en vreedzame geschillenbeslechting |
| | 6.2 Aantasting van de werking, legitimiteit dan wel naleving van de internationale verdragen en normen inzake de rechten van de mens |
| | 6.3 Aantasting van een op regels gebaseerd internationaal financieel-economisch bestel |
| | 6.4 Aantasting van de effectiviteit, legitimiteit van multilaterale instituties |
| | 6.5 Instabiliteit van staten grenzend aan het Koninkrijk der Nederlanden en in de directe omgeving van de Europese Unie |

Voor het geven van een oordeel over de precieze omvang van de gevolgen van een scenario, wordt aan elk van de criteria een impactscore toegekend, namelijk: niet van toepassing, beperkt (A), aanzienlijk (B), ernstig (C), zeer ernstig (D) of catastrofaal (E). Deze classificering is gebaseerd op een logaritmische schaal. Voor criterium 2.1 (aantal doden) betekent dit bijvoorbeeld dat een beperkte score staat voor 0-10 doden, een aanzienlijke score voor 10-100 doden, et cetera. Eenzelfde redenatie wordt gehanteerd voor criterium 3.1 (kosten) (zie Tabel 2). Er is sprake van maatschappelijke ontwrichting als één of meer van de belangen ernstig (klasse C) of hoger wordt aangetast.

**Tabel 2** Voorbeeld van verschillende klassen van gevolg binnen de methodiek nationale veiligheid

| Klasse van gevolgen | Voorbeeld criterium: Aantal doden (2.1) | Voorbeeld criterium: kosten (3.1) |
|---|---|---|
| A. Beperkt | Minder dan 10 | < 50 miljoen euro |
| B. Aanzienlijk | 10 tot 100 | < 500 miljoen euro |
| C. Ernstig | 100 tot 1000 | < 5 miljard euro |
| D. Zeer ernstig | 1000 tot 10.000 | < 50 miljard euro |
| E. Catastrofaal | Meer dan 10.000 | > 50 miljard euro |

In tegenstelling tot de bovenstaande criteria 2.1 en 3.1, zijn sommige criteria niet uit te drukken in een absoluut aantal. Een voorbeeld is criterium 5.2, aantasting van de democratische rechtsstaat. Hier wordt de uiteindelijke score bepaald door te kijken of, in welke mate en voor hoe lang verschillende onderdelen van de democratische rechtsstaat worden aangetast. Deze onderdelen zijn:

- Het functioneren van de politieke vertegenwoordiging;
- Het functioneren van het openbaar bestuur en daaraan verbonden ambtenaren;
- Het functioneren van het openbare orde en veiligheidssysteem;
- Het functioneren van een onafhankelijke rechtspraak;
- Vrijheden en rechten zoals vastgelegd in grondwet en wetgeving (vrijheid van godsdienst, meningsuiting, vereniging, kiesrecht, etc.).

Naarmate de aantasting groter is, voor meerdere onderdelen van toepassing blijkt en langer duurt, neemt de score toe. Voor elk van de in dit rapport beoordeelde scenario's zal aan de hand van een scorekaart per criterium worden weergegeven van welke orde grootte de verwachte gevolgen zijn.

Binnen de methodiek wordt niet alleen gekeken naar de gevolgen van gebeurtenissen, maar ook naar de waarschijnlijkheid van optreden. Voor het bepalen van de waarschijnlijkheid wordt gekeken naar de kans van optreden binnen het moment van analyse (eerste kwartaal 2022) en vijf jaar. Deze kans wordt afhankelijk van het type gebeurtenis kwalitatief of kwantitatief weergegeven op een vijfpuntschaal van zeer onwaarschijnlijk tot zeer waarschijnlijk. Voor moedwillige gebeurtenissen wordt een kwalitatieve schaal gehanteerd (zie Tabel 3).

**Tabel 3** Klassen van waarschijnlijkheid binnen de methodiek nationale veiligheid

| Klasse van waarschijnlijkheid | Kwalitatieve omschrijving van de dreiging |
|---|---|
| A. Zeer onwaarschijnlijk | Geen concrete aanwijzingen en het scenario wordt niet voorstelbaar geacht |
| B. Onwaarschijnlijk | Geen concrete aanwijzingen, maar het scenario wordt enigszins voorstelbaar geacht |
| C. Enigszins waarschijnlijk | Geen concrete aanwijzingen, maar het scenario is voorstelbaar |
| D. Waarschijnlijk | Het scenario wordt zeer voorstelbaar geacht; er zijn enige aanwijzingen dat het scenario zich daadwerkelijk zal voordoen, |
| E. Zeer waarschijnlijk | Concrete aanwijzingen dat het scenario geëffectueerd zou kunnen worden |

Ook de ingeschatte waarschijnlijkheid zal voor elk van de geanalyseerde scenario's worden weergegeven in de eerder genoemde scorekaart. Om te helpen bij de uiteindelijke vergelijking van alle scenario's, bevat hoofdstuk negen een risicodiagram met daarin geplot een overzicht van de scenario's langs de assen waarschijnlijkheid en totale impact.

## 2.2 Bouwstenen, wild card en sluimerende dreiging

Ten behoeve van het identificeren en uitwerken van de scenario's is gebruik gemaakt van 'bouwstenen'. Bouwstenen bieden een overzicht van de voor een dreigingscategorie relevante actoren en factoren. Door actoren en factoren te combineren kunnen meerdere situaties ofwel scenario's worden gecreëerd. Uiteraard zullen verschillende combinaties leiden tot verschillende scenario's met wisselende uitkomsten. De bouwstenen helpen om in één oogopslag duidelijk te maken wat wel en wat niet is meegenomen in het scenario en dienen als referentiekader voor de uiteindelijke verhaallijn. De in deze rapportage opgenomen scenario's betreffen enkele voorbeelden van hoe de dreiging behorende tot één van de drie dreigingscategorieën zich kan manifesteren. Ze zijn nadrukkelijk niet uitputtend, maar streven ernaar een zo goed mogelijke afspiegeling te zijn van relevante actoren en factoren.

Naast de op bouwstenen gebaseerde scenario's, wordt er binnen dit thema ook een 'wild card' scenario beschouwd met betrekking tot ruimteweer fenomenen. Een wild card is een scenario met een relatief lage waarschijnlijkheid en een hoge impact of een grote mate van onzekerheid ten opzichte van de scenario's die op de bouwstenen zijn gebaseerd.

Tot slot wordt er binnen dit thema ook een sluimerende dreiging beschouwd. Deze beschouwing betreft een bepaalde trend of ontwikkeling waarbij er niet alleen een inhoudelijke uiteenzetting plaatsvindt, maar er ook (per belang en op hoofdlijnen) een indicatie wordt gegeven van mogelijke gevolgen voor de nationale veiligheid.

## 2.3 Overzicht van ontwikkelingen

Voor het overzicht van ontwikkelingen is geput uit verschillende openbare rapporten en analyses, aangevuld met de kennis van aan het ANV verbonden organisaties.

# 3. Achtergrond en dreigingscategorieën

In dit hoofdstuk wordt ingegaan op de vitale processen in Nederland [3], worden de dreigingscategorieën toegelicht en wordt besproken welke actoren en factoren van belang zijn voor dit thema.

## 3.1 Vitale processen

Sommige processen zijn zo vitaal voor het functioneren van onze samenleving dat verstoring leidt tot ernstige maatschappelijke ontwrichting. Deze processen samen vormen de Nederlandse vitale infrastructuur. Onder 'bedreiging vitale infrastructuur' verstaan we niet alleen de gedeeltelijke of volledige uitval of verstoring van een vitaal proces (al dan niet moedwillig), maar bijvoorbeeld ook (gedeeltelijk) verlies van zeggenschap over vitale processen door ongewenste buitenlandse overnames of beïnvloeding, waardoor de continuïteit en integriteit van vitale processen niet langer gewaarborgd kan worden. Verstoring van vitale infrastructuur kan op zichzelf een dreiging voor de nationale veiligheid vormen, maar verstoring van vitale infrastructuur kan ook een versterkend effect hebben op de totale impact van een dreiging als een overstroming of een zwaar ongeval. Andersom kan een overstroming, ongeval, of bijvoorbeeld een cyberaanval ook weer een verstoring van vitale infrastructuur teweeg brengen. Er is dan ook een sterke verwevenheid tussen de dreigingen met betrekking tot vitale infrastructuur en andere dreigingen.

De processen in Tabel 4 zijn op dit moment als vitaal geïdentificeerd in Nederland. Categorie A vitale processen hebben grotere gevolgen bij uitval dan categorie B vitale processen [4]. Bij het ontwikkelen en beschouwen van de diverse scenario's is ook gekeken welke vitale processen direct en indirect geraakt worden en waarom.

**Tabel 4** Overzicht vitale processen in Nederland

| Vitale processen | Categorie | Sector | Ministerie |
|---|---|---|---|
| Landelijk transport, distributie en productie elektriciteit | A | Energie | EZK |
| Regionale distributie elektriciteit | B | | |
| Gasproductie, landelijk transport en distributie gas | A | | |
| Regionale distributie gas | B | | |
| Olievoorziening | A | | |
| Internet en datadiensten | B | ICT/Telecom | EZK |
| Internettoegang en dataverkeer | B | | |
| Spraakdienst en SMS | B | | |
| Plaats- en tijdsbepaling middels GNSS | B | | IenW |

[3] Deze themarapportage richt zich op Europees Nederland. In de themarapportage over het Caribisch deel van het Koninkrijk wordt op hoofdlijnen ingegaan op de relevante infrastructuur voor het Caribisch deel. In deze rapportage wordt op enkele plekken naar die themarapportage verwezen.

[4] Overzicht vitale processen, NCTV, bezocht op 2 maart, 2022, *https://www.nctv.nl/onderwerpen/vitale-infrastructuur/overzicht-vitale-processen*.

| Vitale processen | Categorie | Sector | Ministerie |
|---|---|---|---|
| Drinkwatervoorziening | A | Drinkwater | IenW |
| Keren en beheren waterkwantiteit | A | Water | IenW |
| Vlucht- en vliegtuigafhandeling | B | Transport | IenW |
| Scheepvaartafwikkeling | B | | |
| Vervoer van personen en goederen over (hoofd)spoorweginfrastructuur | B | | |
| Vervoer over (hoofd)wegennet | B | | |
| Grootschalige productie/verwerking en/of opslag (petro)chemische stoffen | B | Chemie | IenW |
| Opslag, productie en verwerking nucleair materiaal | A | Nucleair | IenW |
| Toonbankbetalingsverkeer | B | Financieel | FIN |
| Massaal giraal betalingsverkeer | B | | |
| Hoogwaardig betalingsverkeer tussen banken | B | | |
| Effectenverkeer | B | | |
| Communicatie met en tussen hulpdiensten middels 112 en C2000 | B | OOV | JenV |
| Inzet politie | B | | |
| Basisregistraties personen en organisaties | B | Digitale overheids-processen | BZK |
| Interconnectiviteit (transactie-infrastructuur voor informatie uit basisregistraties) | B | | |
| Elektronisch berichtenverkeer en informatieverschaffing aan burgers | B | | |
| Identificatie en authenticatie van burgers en bedrijven | B | | |
| Inzet defensie | B | Defensie | DEF |

## 3.2 Dreigingscategorieën

Binnen het thema bedreiging vitale infrastructuur wordt onderscheid gemaakt tussen drie dreigingscategorieën:
- Moedwillige bedreiging vitale processen;
- Verstoring vitale processen als gevolg van technisch of menselijk falen;
- Natuurlijke verstoring vitale processen.

Dit onderscheid is gemaakt omdat de oorzaak van een verstoring invloed kan hebben op de mogelijke effecten van een verstoring en de maatregelen die getroffen kunnen worden om ze te voorkomen of mitigeren.

Zo speelt het type actor bij moedwillige bedreigingen een grote rol in hoe waarschijnlijk het is dat een verstoring zich voordoet, maar ook hoe groot de mogelijke impact is en wat een organisatie kan doen om het risico te mitigeren. Bij technisch of menselijk falen is er geen sprake van een moedwillige handeling, maar gaat het om uitval van systemen of infrastructuur door een technische of menselijke fout. Tot slot onderscheiden we verstoringen met een natuurlijke oorzaak, bijvoorbeeld extreem weer, waardoor één of meer vitale processen tegelijkertijd verstoring of uitval ondervinden. In Tabel 5 staat een overzicht van de dreigingscategorieën en bijbehorende scenario's.

**Tabel 5** Overzicht dreigingscategorieën en scenario's binnen het thema bedreiging vitale infrastructuur

| Dreigingscategorie | Scenario |
|---|---|
| Moedwillige bedreiging vitale processen | Ransomware aanval telecomprovider |
| | Ketenafhankelijkheden (elektriciteit) |
| Verstoring vitale processen als gevolg van technisch of menselijk falen | Landelijke black-out |
| Natuurlijke verstoring vitale processen | Wild card: ruimteweer |
| | Common cause extreem weer (overstroming) |
| | Common cause extreem weer (natuurbrand) |

## 3.3 Overzicht actoren en factoren

Het overzicht in onderstaande Tabel 6 wordt bij ieder scenario gebruikt om aan te geven welke actoren en factoren relevant zijn voor het scenario dat wordt besproken. Naast het type **oorzaak** en (eventueel) de **actor** die achter een gebeurtenis zit is het bij dit thema belangrijk onderscheid te maken in het **type verstoring** dat wordt geanalyseerd. Zo kan een verstoring *eigenstandig* zijn, waarbij slechts één vitaal proces wordt verstoord, uitvalt of wordt aangetast. Het kan ook zijn dat door een gebeurtenis direct meerdere vitale processen worden geraakt, dan spreekt men van een *common-cause* verstoring (er is sprake van eenzelfde oorzaak voor uitval of verstoring). Tot slot is het kenmerkend voor vitale infrastructuur dat vitale processen ook van elkaar afhankelijk zijn en er dus *keteneffecten* kunnen optreden bij andere processen wanneer één proces uitvalt of gedeeltelijk verstoord raakt. Dit betekent dat na het verstoren of uitvallen van één vitaal proces daarna op den duur ook andere vitale processen uitvallen of verstoord raken.

Vanwege de afhankelijkheden tussen vitale processen, worden in het overzicht van actoren en factoren zowel de **direct** getroffen vitale processen als de getroffen processen door **cascade effecten** (keteneffecten) in een kolom weergegeven. Daarnaast is het relevant om aan te geven wat de **schaal van het brongebied** is en de **schaal van het effectgebied**, dit heeft namelijk invloed op de impact. Tot slot is de **duur** van uitval of verstoring van vitale processen een belangrijke factor. Gezien het belang van vitale infrastructuur zijn er vaak noodmaatregelen getroffen voor eventuele uitval of verstoring van deze processen. Echter, bij een langere duur van uitval of verstoring kunnen deze noodmaatregelen het ook begeven en kunnen de gevolgen een stuk groter zijn.

**Tabel 6** Actoren en factoren relevant voor het thema bedreiging vitale infrastructuur

| Oorzaak | Actor | Type verstoring | Verstoorde vitale processen |
|---|---|---|---|
| Moedwillige bedreiging | Statelijke actor | Eigenstandige verstoring, uitval of aantasting | Landelijk transport, distributie en productie elektriciteit |
| Technisch of menselijk falen | Terroristen | Common-cause | Regionale distributie elektriciteit |
| Natuurlijke verstoring | Criminelen | Keten effecten | Gasproductie, landelijk transport en distributie gas |
| | | | Regionale distributie gas |
| | | | Olievoorziening |
| | | | Internet en datadiensten |
| | | | Internettoegang en dataverkeer |
| | | | Spraakdiensten en SMS (mobiel en vast) |
| | | | Plaats- en tijdsbepaling middels GNSS |
| | | | Drinkwater voorziening |
| | | | Keren en beheren waterkwantiteit |
| | | | Vlucht- en vliegtuig afhandeling |
| | | | Scheepvaart afwikkeling |
| | | | Vervoer van personen en goederen over (hoofd)spoorweg infrastructuur |
| | | | Vervoer over (hoofd)wegennet |
| | | | Grootschalige productie/ verwerking en/of opslag (petro) chemische stoffen |
| | | | Opslag, productie en verwerking nucleair materiaal |
| | | | Toonbankbetalingsverkeer |
| | | | Massaal giraal betalingsverkeer |
| | | | Hoogwaardig betalingsverkeer tussen banken |
| | | | Effectenverkeer |
| | | | C2000 |
| | | | Inzet politie |
| | | | Basisregistratie personen en organisaties |
| | | | Interconnectiviteit (transactie-infrastructuur voor informatie uit basisregistraties) |
| | | | Elektronisch berichtenverkeer en informatie verschaffing aan burgers |
| | | | Identificatie en authenticatie van burgers en bedrijven |
| | | | Inzet defensie |

**Tabel 6** Actoren en factoren relevant voor het thema bedreiging vitale infrastructuur (vervolg)

| Vitale processen verstoord door cascade effecten | Schaal brongebied | Schaal effect gebied | Duur |
|---|---|---|---|
| Landelijk transport, distributie en productie elektriciteit | Internationaal | Internationaal | 1 tot 4 uur |
| Regionale distributie elektriciteit | Nationaal | Nationaal | 4 tot 8 uur |
| Gasproductie, landelijk transport en distributie gas | Regionaal | Regionaal | 8 tot 24 uur |
| Regionale distributie gas | Lokaal | Lokaal | 24 tot 72 uur |
| Olievoorziening | | | 72 uur tot 1 week |
| Internet en datadiensten | | | 1 tot 4 weken |
| Internettoegang en dataverkeer | | | > 1 maand |
| Spraakdiensten en SMS (mobiel en vast) | | | |
| Plaats- en tijdsbepaling middels GNSS | | | |
| Drinkwater voorziening | | | |
| Keren en beheren waterkwantiteit | | | |
| Vlucht- en vliegtuig afhandeling | | | |
| Scheepvaart afwikkeling | | | |
| Vervoer van personen en goederen over (hoofd)spoorweg infrastructuur | | | |
| Vervoer over (hoofd)wegennet | | | |
| Grootschalige productie/ verwerking en/of opslag (petro) chemische stoffen | | | |
| Opslag, productie en verwerking nucleair materiaal | | | |
| Toonbankbetalingsverkeer | | | |
| Massaal giraal betalingsverkeer | | | |
| Hoogwaardig betalingsverkeer tussen banken | | | |
| Effectenverkeer | | | |
| C2000 | | | |
| Inzet politie | | | |
| Basisregistratie personen en organisaties | | | |
| Interconnectiviteit (transactie-infrastructuur voor informatie uit basisregistraties) | | | |
| Elektronisch berichtenverkeer en informatie verschaffing aan burgers | | | |
| Identificatie en authenticatie van burgers en bedrijven | | | |
| Inzet defensie | | | |

# 4. Relevante ontwikkelingen

In dit hoofdstuk wordt een aantal trends en ontwikkelingen binnen het thema *bedreiging vitale infrastructuur* van de afgelopen jaren geschetst. Deze trends kunnen niet geheel los van elkaar worden gezien, zij overlappen gedeeltelijk en grijpen op elkaar in. Hoewel er in sommige gevallen ingegaan wordt op implicaties van ontwikkelingen die betrekking hebben op specifieke vitale processen, zoals de elektriciteitsvoorziening, worden over het algemeen alleen overkoepelende ontwikkelingen besproken die ingrijpen op meerdere vitale processen of het geheel van de vitale infrastructuur van Nederland.

**Toenemende afhankelijkheid van digitale systemen**

Door vergaande digitalisering wordt de Nederlandse maatschappij in toenemende mate afhankelijk van digitale systemen, dit geldt ook voor vitale processen. Zo worden systemen die gebruikt worden voor het aansturen van vitale processen, zoals sluizen of bruggen, steeds vaker automatisch aangestuurd. Dit heeft ertoe geleid dat de Cybersecurity Raad om meer aandacht heeft gevraagd voor specifieke kwetsbaarheden van digitale systemen in vitale infrastructuur, waaronder van *Industrial Automation and Control Systems* (IACS).[5] Door deze digitalisering en automatisering wordt niet alleen de afhankelijkheid van digitale systemen vergroot, maar kan er ook een netwerk aan afhankelijkheden ontstaat tussen verschillende organisaties binnen een vitaal proces, omdat systemen verbonden worden of omdat er gebruik gemaakt wordt van hard- of software van dezelfde leverancier. Hierdoor ontstaan ketenrisico's; een storing bij één organisatie kan dan doorwerken op andere organisaties.[6]

Binnen vitale processen ontstaat een groeiende afhankelijkheid van derde partijen die cruciale IT diensten en producten leveren. Hoewel deze partijen zelf niet vitaal zijn, kan het uitvallen van de systemen en diensten die zij aanbieden wel verstoringen teweeg brengen binnen vitale processen.

Groeiende afhankelijkheid van digitale systemen zorgt ook voor ongewenste afhankelijkheden van buitenlandse marktleiders. Deze afhankelijkheden zijn dusdanig groot geworden dat de Cyber Security Raad heeft geconcludeerd dat de digitale autonomie van Nederland onder druk staat; "Dit kan grote gevolgen hebben voor onze nationale en economische veiligheid en daarmee het verdienvermogen van Nederland".[7] Deze ontwikkelingen worden ook geadresseerd binnen de dreigingsthema's *cyberdreigingen, economische dreigingen en ongewenste inmenging en beïnvloeding democratische rechtsstaat*. Hierbij wordt onder andere ingegaan op de dreiging van spionage of zelfs sabotage door staatsondersteunde leveranciers van soft- en hardware en kwetsbaarheden die ontstaan omdat heel veel organisaties gebruik maken van dezelfde producten, waardoor het benutten van een kwetsbaarheid om bijvoorbeeld malware te verspreiden of de effecten van technische verstoringen direct een zeer grote reikwijdte kennen. Ook onze vitale infrastructuur is in hoge mate afhankelijk van digitale systemen en het verlies van controle over, of verstoring van vitale processen kan potentieel tot ernstige gevolgen leiden.[8]

5 "Cyberweerbaarheid IACS in Nederland onvoldoende op orde", Cyber Security Raad, 29 april 2020. *https://www.cybersecurityraad.nl/actueel/nieuws/2020/04/29/'cyberweerbaarheid-iacs-in-nederland-onvoldoende-op-orde'*.

6 NCTV, Midterm review 2021, Nationale Veiligheid Strategie (Den Haag: NCTV, 2021).

7 "Digitale autonomie Nederland staat onder druk", Cyber Security Raad (14 mei 2021) *https://www.cybersecurityraad.nl/actueel/nieuws/2021/05/14/'digitale-autonomie-nederland-staat-onder-druk'*.

8 "Economische Veiligheid", NCTV, bezocht op 2 maart 2022, *https://www.nctv.nl/onderwerpen/economische-veiligheid*.

### Veranderend dreigingslandschap

Vitale infrastructuur is voor zowel statelijke actoren als cybercriminelen een interessant doelwit.[9] Voor statelijke actoren is vitale infrastructuur interessant als strategisch doelwit, vanwege de potentieel grote impact die verstoring kan hebben op een maatschappij als geheel. Daarnaast is er ook sprake van een professionalisering van de actoren die misbruik kunnen maken van de kwetsbaarheden die ten gevolge van de toegenomen digitalisering zijn ontstaan. In het Dreigingsbeeld Statelijke Actoren[10] wordt aangegeven dat statelijke actoren de afgelopen jaren steeds professioneler worden en meer digitale middelen hebben. Hoewel er in Nederland nog geen voorbeelden zijn van significante verstoringen van vitale infrastructuur door een digitale aanval, is Nederland volgens de AIVD wel doelwit geweest van voorbereidingshandelingen van statelijke actoren op vitale infrastructuur.[11]

In het Cybersecurity Beeld Nederland 2021[12] wordt beschreven dat ook het ecosysteem van cybercriminelen steeds verder professionaliseert en dat criminele groepen ook steeds vaker samenwerken met statelijke actoren (zie ook thema *cyberdreigingen*). Cybercriminelen zijn over het algemeen op zoek naar doelwitten voor financieel gewin en verwachten mogelijk veel geld te kunnen verdienen met het inzetten van bijvoorbeeld ransomware om vitale aanbieders onder druk te zetten. Ransomware aanvallen kunnen de bedrijfsvoering van aanbieders van vitale processen ernstig verstoren en hiermee grote impact genereren. Een recent voorbeeld is de aanval op Colonial Pipepline, beheerder van de grootste oliepijplijn van de Verenigde Staten. Als gevolg van de aanval moest het hele leidingsysteem van Colonial Pipeline worden stilgelegd, wat resulteerde in olietekorten in de hele oostkust van de VS.[13] In Nederland zijn tot op heden nog geen voorbeelden voorgekomen van significante verstoringen van vitale infrastructuur door ransomware.

Wel zijn universiteiten en ziekenhuizen de afgelopen jaren door ransomware aanvallen getroffen.[14] Ook in het Caribisch deel van het Koninkrijk zijn voorbeelden van dergelijke aanvallen, zoals een ransomware aanval op het ziekenhuis van Aruba in 2019.[15] Zie verder de themarapportage Rijksbrede risicoanalyse Caribisch deel van het Koninkrijk der Nederlanden.

### Wetgeving vanuit de Europese Unie over vitale processen

De EU heeft recentelijk de contouren voor nieuwe wetgeving gepubliceerd met betrekking tot vitale infrastructuur.[16] In deze wetgeving worden meer sectoren als vitaal aangewezen (tien sectoren in plaats van twee) en er wordt aandacht besteed aan het versterken van Europese samenwerking om de continuïteit van vitale processen te waarborgen. Daarnaast komt er meer aandacht voor de samenhang tussen vitale processen en cybersecurity: de entiteiten die onder de nieuwe wet over vitale infrastructuur vallen moeten ook voldoen aan de eisen in de nieuwe Europese cybersecurity wet, de *NIS2 Directive*.[17] Uit de twee nieuwe wetten blijkt dat de Europese Commissie naar een integrale aanpak op het gebied van de bescherming van vitale infrastructuur streeft. Hierbij moet rekening worden gehouden met de samenhang tussen verschillende sectoren, afhankelijkheden van de infrastructuur van andere Europese lidstaten en afhankelijkheden op digitaal vlak. De wetgeving beoogt daarmee een antwoord te formuleren op de trend van toenemende complexiteit en verwevenheid binnen en tussen vitale processen en sectoren.

9 AIVD, MIVD, NCTV, Dreigingsbeeld statelijke actoren (Den Haag: AIVD, MIVD, NCTV, 2021), *https://www.rijksoverheid.nl/documenten/rapporten/2021/02/03/dreigingsbeeld-statelijke-actoren*; NCTV, Cybersecuritybeeld Nederland CSBN 2021 (Den Haag: NCTV, 2021), *https://www.nctv.nl/documenten/publicaties/2021/06/28/cybersecuritybeeld-nederland-2021*

10 AIVD, MIVD, NCTV, Dreigingsbeeld statelijke actoren.

11 AIVD, Jaarverslag 2018 (Den Haag: AIVD, 2019), *https://www.aivd.nl/documenten/jaarverslagen/2019/04/02/jaarverslag-aivd-2018*.

12 NCTV, Cybersecuritybeeld Nederland CSBN 2021.

13 W. Turton and K. Mehrotra, "Hackers Breached Colonial Pipeline Using Compromised Password," Bloomberg (4 juni 2021), *https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password*.

15 "Hackers leggen ziekenhuis Aruba plat", Dutch Caribbean Legal Portal (28 november 2019), *http://www.dutchcaribbeanlegalportal.com/news/latest-news/9386-hackers-leggen-ziekenhuis-aruba-plat*

16 European Commission, Proposal for a Directive of the European Parliament and of the Council on the Resilience of Critical Entities (Brussel: Europese Commissie, 16 december 2020), *https://ec.europa.eu/home-affairs/system/files/2020-12/15122020_proposal_directive_resilience_critical_entities_com-2020-829_en.pdf*; European Commission, Proposal for a Directive of the European Parliament and of the Council on Measures for a High Common Level of Cybersecurity across the Union (Brussel: Europese Commissie, 16 december 2020), *https://op.europa.eu/en/publication-detail/-/publication/be0b5038-3fa8-11eb-b27b-01aa75ed71a1*.

17 Mar Negreiro, "The NIS2 Directive. A high common level of cybersecurity in the EU," EU Legislation in Progress Briefing (Brussel: Europees Parlement, 2021), *https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf*

### Klimaatverandering

Recent heeft het IPCC een nieuw rapport gepubliceerd dat nieuwe inzichten verschaft over klimaatverandering. [18] Klimaatonderzoekers en waterexperts geven aan dat de toename in weersextremen grote gevolgen voor Nederland kan hebben. [19] Door de stijging van de zeespiegel kunnen delen van Nederland onder water komen te staan, maar ook extreem regenval kan zorgen voor overstromingen. Verder kunnen zeer droge zomers de kans op bijvoorbeeld natuurbranden vergroten. [20] Een recent voorbeeld van extreem weer zijn de overstromingen in Limburg. [21] Hierbij is echter niet in kaart gebracht of, en in hoeverre, vitale processen geraakt zijn. Het is echter wel denkbaar dat in de toekomst extreem weer in heel Nederland grote gevolgen kan hebben voor de continuïteit van vitale processen als drinkwatervoorziening. In een analyse naar aanleiding van de overstromingen in Limburg geven onderzoekers van Deltares aan dat dergelijke extreme regenval in andere delen van Nederland tot zeer ernstige gevolgen zou kunnen leiden, waaronder lokale verstoring van bijvoorbeeld elektriciteit en transportproblemen. [22]

Hoewel er dus nog geen duidelijkheid bestaat over de precieze impact die dit op vitale processen kan hebben, kan men er vanuit gaan dat de gevolgen van klimaatverandering vitale processen kunnen verstoren en (grote) kosten met zich mee brengen. [23]

### Energietransitie

De overheid zet de komende jaren fors in op het versnellen van de energietransitie, waarbij het doel is om fossiele brandstoffen grotendeels te vervangen door duurzame energiebronnen als wind- en zonne-energie. Deze versnelling is een antwoord op klimaatverandering, maar wordt ook gevoed door de zorg over afhankelijkheid van energiebronnen uit het buitenland. In Nederland speelt ook mee dat de gaswinning in Groningen steeds verder zal worden afgebouwd, waardoor de vraag naar andere energiebronnen zal toenemen.

De inzet op transitie van fossiele brandstoffen naar duurzame energiebronnen zorgt er voor dat steeds meer gebruik wordt gemaakt van elektriciteit in plaats van bijvoorbeeld gas of olie, denk aan de toename van elektrische auto's. Uit de klimaat- en energieverkenning uit 2021 van PBL blijkt dat het elektriciteitsverbruik mogelijk 10 procent toeneemt in 2030 ten opzichte van 2019. [24]
De toegenomen vraag naar elektriciteit zorgt voor een grotere afhankelijkheid van en druk op het elektriciteitsnet. [25] Dit kan op sommige plaatsen tot capaciteitsproblemen leiden, zo heeft netbeheerder Liander al gewaarschuwd dat het stroomnet in delen van Amsterdam tegen zijn grenzen aanloopt. [26] Daarnaast wordt verwacht dat de kans op verstoringen en de omvang daarvan, zowel qua duur als qua geografische schaal, zullen toenemen. [27] Recent is er voor gekozen om de 'vluchtstrook' van het hoogspanningsnet voor het eerst in gebruik te nemen om ervoor te zorgen dat meer duurzame opwekkers van energie kunnen worden aangesloten. Gevolg hiervan is dat er bij gebruik hiervan een stuk reservecapaciteit wegvalt. [28]

---

18 V. Masson-Delmotte, P. Zhai, A. Pirani, S.L. Connors, C. Péan, S. Berger, N. Caud, Y. Chen, L. Goldfarb, M.I. Gomis, M. Huang, K. Leitzell, E. Lonnoy, J.B.R. Matthews, T.K. Maycock, T. Waterfield, O. Yelekçi, R. Yu, and B. Zhou (eds.), Climate Change 2021: The Physical Science Basis. Contribution of Working Group I to the Sixth Assessment Report of the Intergovernmental Panel on Climate Change (Cambridge: Cambridge University Press, 2021), *https://www.ipcc.ch/report/ar6/wg1/downloads*.

19 Heleen Ekker, "Klimaatexperts: IPCC-rapport alarmerend voor Nederland," NOS (9 augustus 2021), *https://nos.nl/artikel/2393306-klimaatexperts-ipcc-rapport-alarmerend-voor-nederland*.

20 "Nieuw IPCC-rapport: temperatuur stijgt sneller dan verwacht," Kennisportaal Klimaatadaptatie (9 augustus 2021), *https://klimaatadaptatienederland.nl/actueel/actueel/nieuws/2021/nieuw-ipcc-rapport/*.

21 "Extreme wateroverlast in Limburg", Rijksoverheid (16 juli 2021), *https://www.rijksoverheid.nl/actueel/nieuws/2021/07/16/extreme-wateroverlast-in-limburg*.

22 Karin De Bruijn en Kymo Slager, Wat als de 'waterbom' elders in Nederland was gevallen? Hackathon Deltares, november 2021 (Deltares, 17 januari 2022), *https://publications.deltares.nl/11206890_010_0006.pdf*.

23 Jonathan Woetzel, Dickon Pinner, Hamid Samandari, Hauke Engel, Mekala Krishnan, Brodie Boland, Peter Cooper and Byron Ruby, "Will infrastructure bend or break under climate stress?," McKinsey Global Institute (19 augustus 2020), *https://www.mckinsey.com/business-functions/sustainability/our-insights/will-infrastructure-bend-or-break-under-climate-stress*.

24 Planbureau voor de Leefomgeving (PBL), Klimaat- en Energieverkenning 2021 (Den Haag: Planbureau voor de Leefomgeving (PBL), 2021), *https://www.pbl.nl/sites/default/files/downloads/pbl-2021-klimaat-en-energieverkenning-2021-4681.pdf*.

25 ANV, Verkenning risico's van de energietransitie voor de nationale veiligheid (Bilthoven: RIVM, 2019), *https://www.rivm.nl/sites/default/files/2019-10/Verkenning%20risicos%20energietransitie%202019.pdf*.

26 "Netbeheerder waarschuwt: stroomnet bereikt maximum in delen Amsterdam," NOS (24 juni 2021), *https://nos.nl/artikel/2386392-netbeheerder-waarschuwt-stroomnet-bereikt-maximum-in-delen-amsterdam*.

27 E.J. Wiggelinkhuizen, B. H. Bulder, A.B. Schwedersky, en M.P.W. van Berlo, Verkenning van toekomstige risico's van het elektriciteitsnet (Den Haag: TNO, 2021), *https://repository.tudelft.nl/islandora/object/uuid%3Ab39a1668-b2c3-445a-9bd1-c9dce0d57fdc*.

28 "'Vluchtstrook' hoogspanningsnet voor het eerst opengesteld," TenneT (11 februari 2022), *https://www.tennet.eu/nl/tinyurl-storage/nieuws/vluchtstrook-hoogspanningsnet-voor-het-eerst-opengesteld/*.

De toenemende vraag naar elektriciteit vergt een versnelde uitbreiding van het elektriciteitsnet, waarbij de infrastructuur ook sterk zal veranderen, bijvoorbeeld door de komst van *smart grids*. Ook zal in de toekomst steeds meer sprake zijn van een bi-directioneel netwerk, waarbij de afnemer ook elektriciteit terug stuurt in het net (vanuit zonnepanelen en elektrische auto's). Dit kan leiden tot sterkere fluctuatie van vraag en aanbod in het netwerk, bijvoorbeeld doordat op piekmomenten heel veel elektriciteit tegelijk het netwerk in komt en overbelasting ontstaat. Om te zorgen dat het netwerk stabiel kan blijven is het nodig dat er mogelijkheden komen waarbij zelf opgewekte energie tijdelijk kan worden opgeslagen in bijvoorbeeld een batterij en pas in het elektriciteitsnetwerk wordt gestuurd wanneer er minder aanbod komt. De uitbreidingen en technologische veranderingen van het elektriciteitsnetwerk zorgen voor een toename van de complexiteit voor bijvoorbeeld beheer op afstand. Zo kan er een gebrek aan overzicht optreden van waar en op welke termijn nieuwe installaties als zonneparken, laadstations en datacenters worden gerealiseerd. Daardoor kan er overbelasting van het net of een tekort aan elektriciteitsaanbod ontstaan, met als gevolg het (gereguleerd) afschakelen van de aangesloten verbruikers of aanbieders, inclusief het tijdelijk stilleggen van (delen van) het net.

Ook kunnen nieuwe elektriciteitsvoorzieningen ervoor zorgen dat andere belangrijke infrastructuur niet meer naar behoren functioneert: zo heeft het Agentschap Telecom gewaarschuwd dat het groeiend aantal zonnepanelen in Nederland een risico vormt voor de communicatiesystemen (C2000) van hulpdiensten, omdat de panelen ruis op en verstoringen van het netwerk kunnen veroorzaken. [29]

Tenslotte kan de energietransitie ervoor zorgen dat infrastructuur op de Noordzee steeds belangrijker wordt voor de elektriciteitsvoorziening (windparken op zee). Recent zijn er zorgen geuit over de beveiliging van deze infrastructuur [30] al is op dit moment nog niet duidelijk hoe belangrijk deze infrastructuur is of zal gaan worden voor de continuïteit van de elektriciteitsvoorziening.

### Toenemende schaarste van grondstoffen en technische expertise

De beschikbaarheid van grondstoffen en van personeel (in het bijzonder technische expertise) staat in toenemende mate onder druk. Dit heeft diverse oorzaken, zoals toenemende complexiteit van systemen, geopolitieke en economische ontwikkelingen, demografische ontwikkelingen en diverse crises, zoals de COVID-19-pandemie.

Vanwege wereldwijde lockdowns ontstonden er vertragingen in veel transportstromen waardoor tijdens de COVID-19-crisis aanvoerproblemen van allerlei grondstoffen en producten optraden. Hierdoor groeide de bewustwording over hoe belangrijk bepaalde technologieën [31] of grondstoffen zijn voor de productie en continuïteit van essentiële producten en diensten en dit bevestigde opnieuw hoe afhankelijk onze samenleving is van internationale leverancierssketens voor de aanvoer van deze grondstoffen of producten. [32] Dit versterkt de zorgen over strategische afhankelijkheden en roept de vraag op of er niet meer aandacht zou moeten worden geschonken aan technologieën of grondstoffen die van groot belang zijn voor onze samenleving, en dus lokaal geproduceerd of beschermd moeten worden (zie hiervoor ook het dreigingsthema *economische dreigingen*).

Anderzijds zien we dat er grote behoefte is aan bepaalde (technische) expertises over het functioneren van infrastructuur. Veel processen binnen vitale infrastructuur worden geautomatiseerd, waardoor kennis over deze processen verloren gaat en er een gebrek ontstaat aan terugvalmogelijkheden via handmatige bediening, mochten deze automatische processen uitvallen of niet meer goed functioneren. Hier speelt ook mee dat op dit moment een tekort is aan arbeidskrachten. Op de lange termijn kan deze groeiende schaarste een dreiging vormen voor de continuïteit van processen, de mate waarin men kan reageren op een (grootschalige) verstoring, of het ontwikkelen van producten die essentieel zijn.

[29] Agentschap Telecom, Verbinding, vertrouwen, voortuitgang. Jaarbericht 2020 (Den Haag: Agentschap Telecom, 2021), *https://www.agentschaptelecom.nl/documenten/jaarverslagen/2021/05/26/jaarbericht-2020*.

[30] Ties Gijzel, "Wie beveiligt de bodem van de Noordzee tegen sabotage?," Follow the Money (4 juni 2022), *https://www.ftm.nl/artikelen/noordzee-kwetsbaar-voor-sabotage?*; Frank Bekkers, Joris Teer, Dorith Kool, Lucia van Geuns, Patrick Bolder, Irina Patrahau en Max Sarel, The High Value of the North Sea (Den Haag: HCSS, 2021), *https://hcss.nl/report/high-value-of-the-north-sea/*.

[31] Kimmy Bettinger, "COVID-19: emerging technologies are now critical infrastructure – what that means for governance," World Economic Forum (10 april 2020), *https://www.weforum.org/agenda/2020/04/covid-19-emerging-technologies-are-now-critical-infrastructure-what-that-means-for-governance/*.

[32] Tim Sweijs, Hugo van Manen, Katarina Kertydova en Frank Bekkers, Flow Security and Dutch Defense and Security Policies (Den Haag: HCSS, 2018), *https://hcss.nl/report/flow-security-and-dutch-defense-and-security-policies/*; Rob de Wijk, Gaat de Coronacrisis de wereld veranderen? (Den Haag: HCSS, 2021), *https://hcss.nl/report/gaat-de-coronacrisis-de-wereld-veranderen/*.

# 5. Dreigingscategorie moedwillige bedreiging vitale processen

De dreigingscategorie moedwillige bedreiging vitale processen gaat in op de moedwillige oorzaken van de uitval of verstoring van vitale infrastructuur. Het gaat hier om actoren als terroristen, statelijke actoren, cybercriminelen of activisten die met een bepaalde motivatie aanvallen uitvoeren op vitale infrastructuur. Daarbij kan het gaan om een fysieke aanval, zoals een aanslag of sabotage op een installatie, of een digitale aanval, waardoor de processen van één of meerdere vitale aanbieders als doelwit worden gekozen of als bijkomende schade van een aanval verstoord raken.

## 5.1 Scenario's

In deze paragraaf worden twee scenario's binnen de dreigingscategorie moedwillige bedreiging vitale processen beschreven. Het gaat om een cyberaanval op een telecomprovider en een terroristische aanslag op de elektriciteitsvoorziening. In beide scenario's wordt ruime aandacht besteed aan de keteneffecten die dergelijke incidenten met zich mee kunnen brengen.

### 5.1.1 Scenario ransomware aanval telecomprovider

Dit scenario beschrijft een moedwillige digitale aanval van een criminele partij op een telecomprovider. Het gaat hierbij om een verstoring van internet en datadiensten, waardoor meerdere cascade effecten optreden bij andere vitale processen. De aanval wordt uitgevoerd door een buitenlandse criminele partij en duurt 8 tot 24 uur binnen Nederland.

*Bouwstenen*
In Tabel 7 staan de relevante bouwblokken voor dit scenario weergegeven.

**Tabel 7** Bouwstenen voor het scenario ransomware aanval telecomprovider

| Oorzaak | Actor | Type verstoring | Verstoorde vitale processen | Vitale processen verstoord door cascade effecten | Schaal brongebied | Schaal effect gebied | Duur |
|---|---|---|---|---|---|---|---|
| Moedwillige bedreiging | Criminelen | Eigenstandige verstoring, uitval of aantasting | Internet en datadiensten | Internet en datadiensten | Internationaal | Nationaal | 8 tot 24 uur |
| | | | | Spraakdiensten en SMS (mobiel en vast) | | | |
| | | | | Drinkwater voorziening | | | |
| | | | | Keren en beheren waterkwantiteit | | | |
| | | | | Vlucht- en vliegtuig afhandeling | | | |
| | | | | Scheepvaart afwikkeling | | | |
| | | | | Vervoer over (hoofd)wegennet | | | |
| | | | | Toonbank-betalingsverkeer | | | |
| | | | | Massaal giraal betalingsverkeer | | | |

*Verhaallijn*

Een criminele partij wil geld verdienen en gebruikt daarbij ransomware. [33] De netwerk management systemen van een Nederlandse telecomprovider worden door deze ransomware geïnfecteerd en versleuteld. Het gaat hier om de control plane van de telecomprovider, oftewel de routering- en signaleringfuncties die bepalen hoe dataverkeer binnen de telecomnetwerken (c.q. de *data plane*) verloopt. [34] Omdat de control plane systemen ontoegankelijk zijn geworden kan het dataverkeer nauwelijks meer worden gemonitord en de configuratie van de data plane systemen niet meer worden aangepast. Hoewel dit niet direct tot problemen leidt, wordt al wel snel duidelijk dat de geplande (de-)activatie van netwerkdiensten voor individuele klanten niet worden uitgevoerd. Ook storingsmeldingen via het customer callcenter kunnen niet meer worden afgehandeld.
Dus hoewel de aanval slecht zeer beperkt opgemerkt wordt door haar klanten, slaat de paniek in het netwerk operations center toe en wordt het management van de telecomprovider gealarmeerd.

Om meer druk op de telecomprovider uit te oefenen om het losgeld te betalen, passen de aanvallers lukraak een aantal configuratie instellingen aan. Onwetend over de precieze impact die de wijzigingen zullen hebben, leiden de eerste pogingen niet tot grote problemen in het netwerk. Totdat ze (bij toeval) een fout in de configuratie van het interne Border Gateway Protocol teweeg brengen.
Het gevolg is dat sommige Internet- en datadiensten verstoord raken voor een deel van de klanten van de provider. Het aantal klachtmeldingen in het callcenter neemt nu snel toe en de telecomprovider gaat onmiddellijk aan de slag met het zoeken van een oplossing en het afwegen van de verschillende opties.

Ongeveer een uur na de verstoring beginnen steeds meer consumenten en bedrijven uitval van het netwerk te ondervinden. Bij sommigen is het dataverkeer in hoge mate vertraagd, anderen kunnen helemaal geen toegang meer krijgen tot het netwerk. Ook spraakdiensten en SMS werken niet geheel naar behoren. Omdat de monitoring- en controlesystemen van de provider zijn versleuteld, is het onduidelijk hoeveel en welke afnemers precies last hebben van de verstoring.

Langzaam wordt echter wel duidelijk dat verschillende vitale aanbieders problemen ondervinden door de verstoring. Binnen de watersector functioneren de automatische meetsystemen van meerdere organisaties die waterkwaliteit- en kwantiteit meten niet meer goed. Ook de havendienst in Rotterdam en de luchtverkeersleiding-centra in Amsterdam en Maastricht ondervinden problemen. Doordat hun netwerkverbindingen naar hun business partners af en toe wegvallen worden de regie-voerende en controlerende taken van de havenbeambten ernstig belemmerd.

De luchtverkeersleidingcentra constateren dat hun verbindingen naar naburige centra onbetrouwbaar zijn geworden; hun veiligheidsprotocol schrijft daarom voor om het vliegverkeer stil te leggen. Dit verstoort ook de doorstroom op de luchthavens. Daar komt nog bij dat verkeer op de snelweg enige problemen ondervindt door de uitval van matrixborden. Dit zorgt landelijk voor grote drukte op de stations en files in delen van het land.
Het treinverkeer kan wel doorgang vinden, aangezien ProRail gebruik maakt van een communicatienetwerk dat zij zelf in beheer hebben.

De verstoring heeft ook invloed op een deel van het betalingsverkeer; [35] men kan niet meer betalen bij een deel van de supermarkten, bedrijven kunnen tijdelijk geen facturen meer betalen. Dit zorgt voor onrust onder burgers.

De telecomprovider slaagt er na 10 uur in om weer toegang te krijgen tot de monitoring en controlesystemen, die inzicht kunnen verschaffen in welke eindgebruikers precies last hebben van de storing. Hierdoor kan na 12 uur vanaf het begin van de verstoring een deel van het netwerk-verkeer worden overgenomen door andere telecom-operators, wat ervoor zorgt dat de dienstverlening langzaam wordt hersteld. Hoewel het voor de provider nog weken duurt om alle schade aan de netwerken helemaal te herstellen, is de verstoring voor de eindgebruikers na zo'n 16 uur opgelost.

33 Beveiliging Nieuws, "Ransomwarebende opgerold na aanvallen op vitale infrastructuur," Beveiliging Nieuws (29 oktober 2021), *https://beveiligingnieuws.nl/ransomwarebende-opgerold-na-aanvallen-op-vitale-infrastructuur/*

34 De control plane is het deel van het netwerk dat bepaalt waar dataverkeer heen wordt gestuurd. Als deze ontoegankelijk is loopt het dataverkeer wel door, maar kunnen er geen wijzigingen worden gedaan in de route die het verkeer aflegt.

35 Het betreft geen volledige verstoring van betaalverkeer (SWIFT).

*Beoordeling van de impact en waarschijnlijkheid*

De aanval heeft een direct effect op Internet- en datadiensten van deze leverancier. Ook is het denkbaar dat diverse andere vitale processen geraakt worden omdat zij afhankelijk zijn van deze diensten. Het is niet vanzelfsprekend dat die vitale processen ook per definitie verstoord raken, maar organisaties die bij die processen betrokken zijn krijgen wel te maken met effecten. Verder is ook niet ondenkbaar dat er in andere vitale processen effecten kunnen optreden vanuit deze gebeurtenissen, maar welke en op welke manier, dat is moeilijk in te schatten. In Tabel 8 staat een overzicht van de vitale processen waarvan experts verwachten dat deze (potentieel) geraakt zullen worden als gevolg van de beschreven gebeurtenissen en wat hierbij de redenering is. Door de complexiteit van het technische landschap is het moeilijk te voorspellen wat er precies gaat gebeuren als er een dergelijke storing optreedt. Omdat het hier een van de grote Nederlandse telecomproviders betreft zullen er veel effecten merkbaar zijn op veel plekken in de samenleving. Hoewel de precieze effecten onzeker zijn geven experts aan dat de gebeurtenissen in het ergste geval kunnen leiden tot zeer ernstige situaties waarbij bijvoorbeeld ook gewonden of doden vallen.

**Tabel 8** Geraakte vitale processen bij het scenario ransomware aanval telecomprovider

| Vitale processen | Categorie | Sector | Geraakt? |
|---|---|---|---|
| Landelijk transport en distributie elektriciteit | A | Energie | |
| Regionale distributie elektriciteit | B | | |
| Gasproductie, landelijk transport en distributie gas | A | | |
| Regionale distributie gas | B | | |
| Olievoorziening | A | | |
| Internet en datadiensten | B | ICT/Telecom | Direct geraakt door verstoring van het interne BGP en de control plane |
| Internettoegang en dataverkeer | B | | |
| Spraakdienst en SMS* | B | | Gedeeltelijk) verstoord door verstoring van het interne BGP en de control plane |
| Plaats- en tijdsbepaling middels GNSS | B | | |
| Drinkwatervoorziening | A | Drinkwater | Verwachting is dat de meetsystemen niet meer naar behoren werken |
| Keren en beheren waterkwantiteit | A | Water | Verwachting is dat de meetsystemen niet meer naar behoren werken |
| Vlucht- en vliegtuigafhandeling | B | Transport | Vliegverkeer wordt stilgelegd omdat verbindingen onbetrouwbaar zijn geworden |
| Scheepvaartafwikkeling | B | | Regievoerende en controle-rende taken van de havenbe-ambten worden belemmerd |
| Vervoer van personen en goederen over (hoofd) spoorweginfrastructuur | B | Transport | |
| Vervoer over (hoofd)wegennet | B | Transport | Matrixborden werken niet meer |
| Grootschalige productie/verwerking en/of opslag (petro) chemische stoffen | B | Chemie | |

**Tabel 8** Geraakte vitale processen bij het scenario ransomware aanval telecomprovider (vervolg)

| Vitale processen | Categorie | Sector | Geraakt? |
|---|---|---|---|
| Opslag, productie en verwerking nucleair materiaal | A | Nucleair | |
| Toonbankbetalingsverkeer | B | Financieel | Men kan naar verwachting niet meer betalen bij een deel van de winkels, bedrijven kunnen geen facturen meer betalen. |
| Massaal giraal betalingsverkeer | B | | |
| Hoogwaardig betalingsverkeer tussen banken | B | | |
| Effectenverkeer | B | | |
| Communicatie met en tussen hulpdiensten middels 112 en C2000 | B | OOV | |
| Inzet politie | B | | |
| Basisregistraties personen en organisaties | B | Digitale overheids-processen | |
| Interconnectiviteit (transactie-infrastructuur voor informatie uit basisregistraties) | B | | |
| Elektronisch berichtenverkeer en informatieverschaffing aan burgers | B | | |
| Identificatie en authenticatie van burgers en bedrijven | B | | |
| Inzet defensie | B | Defensie | |

**Tabel 9** Scorekaart scenario ransomware Telecomsector

| Thema | Bedreiging vitale infrastructuur | |
|---|---|---|
| **Dreigingscategorie** | Moedwillige bedreiging vitale processen | |
| **Scenario** | Ransomware Telecomsector | |
| **Scenariotoelichting** | Een criminele partij infecteert en versleutelt het netwerk management systeem van een Nederlandse telecomprovider. Bij activiteiten in het systeem om druk op de telecomprovider uit te oefenen om losgeld te betalen, ontstaat een fout in het BGP waardoor sommige Internet- en datadiensten verstoord raken voor een deel van de klanten. Na ongeveer 12-16 uur wordt de dienstverlening aan klanten hersteld. | |
| **Waarschijnlijkheidsbeoordeling (binnen 5 jaar)** | | **Toelichting** |
| **Waarschijnlijkheid:** | A | Ransomware is een voorstelbaar fenomeen, maar het wordt minder waarschijnlijk geacht dat een criminele groepering met financieel motief dit bij een telecomprovider zou doen. Een statelijke actor is mogelijk waarschijnlijker, maar ook dan geldt dat de telecomprovider als doelwit niet het meest waarschijnlijk is omdat daarmee ook de infrastructuur waar de kwaadwillenden gebruik van maken kan worden verstoord. Andere vitale processen zijn dan wellicht eerder doelwit. Telecomproviders doen er bovendien alles aan te voorkomen dat kwaadwillenden kunnen doordringen tot de kern van het netwerk (wat in het scenario gebeurt), al kan dat nooit helemaal voorkomen worden. |

| Beoordeling gevolgen (impact) | | | |
|---|---|---|---|
| **Veiligheidsbelang** | **Criterium** | **Score** | **Toelichting** |
| **Territoriaal** | 1.1 Grondgebied | 0 | Niet van toepassing |
| | 1.2 Internationale positie | 0 | Niet van toepassing. Alleen wanneer het ook invloed heeft op internationaal dataverkeer en de situatie langer duurt, dan zou de Nederlandse telecomprovider hier op aangekeken worden maar dan nog is het onzeker of dit tot acties tegen Nederland zal leiden. Bedrijf kan er wel op aangekeken worden, en wellicht heeft dat effect op commerciële overeenkomsten. |
| | 1.3 Digitale ruimte | C | Schending van één vitale aanbieder, geen politiek of ideologisch motief. Keteneffecten bij andere vitale aanbieders tellen niet mee omdat er geen sprake is van ongewenste toegang tot hun systemen. |
| | 1.4 Bondgenootschappelijk grondgebied | 0 | Niet van toepassing |
| **Fysiek** | 2.1 Doden | C | Er kan door deze verstoring veel misgaan omdat heel veel organisaties geraakt worden. Doordat ook spraakdiensten en SMS geraakt worden kan ook de bereikbaarheid van 112 verstoord raken. Er zijn bij veel organisaties mitigerende maatregelen, maar de impact kan groot worden, afhankelijk van hoe de effecten precies vorm krijgen. Het gaat om een telecom verstoring met heel veel afhankelijkheden. Dat levert flink wat potentiële rampsituaties op, het is dus denkbaar dat er meer dan 100 doden kunnen vallen. |
| | 2.2 Ernstig gewonden en chronisch zieken | C | Er kan door deze verstoring veel misgaan omdat heel veel organisaties geraakt worden. Doordat ook spraakdiensten en SMS geraakt worden kan ook de bereikbaarheid van 112 verstoord worden. Er zijn bij veel organisaties wel mitigerende maatregelen, maar de impact kan groot worden, afhankelijk van hoe de effecten precies vorm krijgen. Het gaat om een telecom verstoring met heel veel afhankelijkheden. Dat levert flink wat potentiële rampsituaties op, het is dus denkbaar dat er veel gewonden vallen. |
| | 2.3 Gebrek primaire levensbehoeften | 0 | Niet van toepassing. De duur is korter dan een dag. |
| **Economisch** | 3.1 Kosten | B | De kosten betreffen met name materiële (gevolg) schade, bestrijdingskosten van gevolgincidenten en gezondheidsschade. Veel bedrijven hebben er last van (veel keteneffecten). Het gaat met name om gevolgschade (claims luchtsector, koelingen die uitvallen, zaken die bederven, logistiek). Financiële schade zal beperkter zijn omdat omzetverlies veelal nog wordt ingehaald de dagen erna. Herstelkosten voor de getroffen provider. Vanwege de relatief korte duur zal het niet snel boven 500 miljoen uitkomen. |
| | 3.2 Aantasting vitaliteit | 0 | Niet van toepassing |

| Veiligheidsbelang | Criterium | Score | Toelichting |
|---|---|---|---|
| **Ecologisch** | 4.1 Aantasting natuur en milieu | 0 | Niet van toepassing. Bedrijven die onder het Besluit risico's zware ongevallen (BRZO) vallen, hebben fail safe systemen om lekkages bij storing van besturingssystemen te voorkomen. |
| **Sociaal-politiek** | 5.1 Verstoring dagelijks leven | C | Vier indicatoren, gemiddeld.<br>**Onderwijs:** beperkt, 1 dag, < 1 miljoen<br>Werk: beperkt, 1 tot enkele dagen, < 1 miljoen<br>**Maatschappelijke voorzieningen:** beperkt, 1 dag, < 1 miljoen.<br>**Virtuele bereikbaarheid:** 1 dag, kan > 1 miljoen treffen, want voor klanten die van deze provider gebruik maken is Internet verstoord. |
| | 5.2 Aantasting democratische rechtsstaat | 0 | Niet van toepassing. Enige impact in functioneren van openbaar bestuur, veiligheidssysteem is denkbaar; maar het betreft niet gerichte (fysieke) belemmering, heeft geen structureel karakter en ook niet voor lange duur. |
| | 5.3 Sociaal-maatschappelijke impact | B | Door de brede effecten zal er veel negatieve berichtgeving zijn en ook angst en onrust. Mogelijk gaan mensen hamsteren omdat ze niet weten hoe snel e.e.a. weer hersteld wordt en omdat bepaalde diensten beperkt leverbaar lijken te zijn. De gebeurtenissen kunnen ook leiden tot verlies van vertrouwen in systemen en olie op het vuur zijn voor complotten etc. waardoor spanningen ontstaan. |
| **Internationale rechtsorde en stabiliteit** | 6.1 Staatssoevereiniteit, vreedzame co-existentie en vreedzame geschillenbeslechting | 0 | Niet van toepassing |
| | 6.2 Mensenrechten | 0 | Niet van toepassing |
| | 6.3 Internationaal financieel-economisch bestel | 0 | Niet van toepassing |
| | 6.4 Multilaterale instituties | 0 | Niet van toepassing |
| | 6.5 Instabiliteit rondom Koninkrijk/EU | 0 | Niet van toepassing |

### 5.1.2 Scenario keteneffecten elektriciteitsuitval

Dit scenario beschrijft een terroristische aanval op de elektriciteitsvoorziening van Nederland. Dit zorgt voor een grootschalige regionale uitval van elektriciteit, met als gevolg dat diverse keteneffecten op andere vitale processen ontstaan. De verstoring heeft een duur van 1 tot 4 weken.

Het gaat bij dit scenario niet zozeer om het fenomeen terrorisme (dat wordt binnen het dreigingsthema polarisatie, extremisme en terrorisme uitgewerkt), maar om inzicht te geven in de keteneffecten die te verwachten zijn bij een dergelijke regionale elektriciteitsuitval en wat daar de impact van kan zijn op de nationale veiligheid.

*Bouwstenen*

In Tabel 10 staan de relevante bouwblokken voor dit scenario weergegeven.

**Tabel 10** Bouwstenen voor het scenario keteneffecten elektriciteit

| Oorzaak | Actor | Type verstoring | Verstoorde vitale processen | Vitale processen verstoord door cascade effecten | Schaal brongebied | Schaal effect gebied | Duur |
|---|---|---|---|---|---|---|---|
| Moedwillige bedreiging | Terrorist(en) | Keten effecten | Landelijk transport, distributie en productie elektriciteit | Internet en datadiensten | Regionaal | Regionaal | 1 tot 4 weken |
| | | | Regionale distributie elektriciteit | Internettoegang en dataverkeer | | | |
| | | | | Spraakdiensten en SMS (mobiel en vast) | | | |
| | | | | Drinkwater voorziening | | | |
| | | | | Vlucht- en vliegtuig afhandeling | | | |
| | | | | Scheepvaart afwikkeling | | | |
| | | | | Vervoer van personen en goederen over (hoofd)spoorweg infrastructuur | | | |
| | | | | Vervoer over (hoofd) wegennet | | | |
| | | | | Toonbankbetalingsverkeer | | | |
| | | | | C2000 | | | |
| | | | | Basisregistratie personen en organisaties | | | |
| | | | | Interconnectiviteit (transactie-infrastructuur voor informatie uit basisregistraties) | | | |
| | | | | Elektronisch berichtenverkeer en informatie verschaffing aan burgers | | | |

*Verhaallijn*

In een regio van Nederland valt de stroom uit, waardoor de 2 miljoen klanten van een netbeheerder zonder stroom komen te zitten. Aanvankelijk gaat men ervan uit dat de stroom na enkele uren weer zou zijn hersteld. Een uur na de uitval wordt echter duidelijk dat het om een terroristische aanslag gaat als reactie op de aanwezigheid van Nederland en andere Westerse landen in een conflictgebied. Deze aanslag komt op een moment dat er al veel spanningen in de samenleving heersen. Bij de aanslag zijn op meerdere plekken verdeelstations kapot gemaakt. De energiesector geeft aan dat het onduidelijk is hoe lang het zal duren voor de elektriciteitsvoorziening weer is hersteld.

De uitval heeft onmiddellijk grote gevolgen op het dagelijks leven. Mobiele netwerken en internetvoorzieningen vallen na enkele uren uit. Elektrische apparaten met een accu, zoals mobiele telefoons en laptops, maar ook medische thuisapparatuur en elektrische auto's kunnen enkele uren functioneren, maar vallen vervolgens ook uit.
Het toonbankbetalingsverkeer raakt verstoord, waardoor men niet meer kan afrekenen in onder andere supermarkten en apotheken. Ook contant geld opnemen is niet meer mogelijk door de uitval van pinautomaten.
Het treinverkeer valt uit, wat voor grote drukte op de stations zorgt. Het verkeer op de wegen loopt vast vanwege het uitvallen van matrixborden, verkeerslichten en op afstand bestuurbare infrastructuur als bruggen. Schiphol ligt buiten het gebied waar de stroom is uitgevallen, maar raakt wel ontregeld door het vastlopen van de snelwegen en de treinen.

Na de aanslag schaalt de overheid onmiddellijk op naar het hoogste dreigingsniveau. Er worden extra veiligheidsmaatregelen genomen voor de energiesector, maar ook voor andere vitale sectoren. De politie gaat de straat op om extra te surveilleren en ongeregeldheden te voorkomen. Ondanks oproepen van de overheid om af te wachten tot er meer duidelijkheid is over de duur van de uitval ontstaat er grote onrust in het getroffen gebied. In heel Nederland vreest men voor meer aanslagen. Specifiek in het getroffen gebied wordt de onrust gevoed door het feit dat men 112 niet kan bereiken door de uitval van mobiele netwerken. De extra inzet van de politie kan niet voorkomen dat in een aantal steden supermarkten worden geplunderd om voedsel veilig te stellen. Anderen proberen het getroffen gebied te verlaten, wat voor nog meer drukte op de wegen zorgt.

Ongeveer een dag na de uitval vallen meer nutsvoorzieningen uit; de verwarming doet het niet meer en bij woningen boven de tweede verdieping komt er geen water meer uit de kraan. Er ontstaan ook problemen met de noodstroomvoorzieningen bij vitale objecten, omdat de aanvoer van diesel ontregeld is geraakt. Zo zijn in de meeste ziekenhuizen in het getroffen gebied de noodaggregaten aangeslagen na de uitval. Deze kunnen ongeveer 24 uur stroom verzorgen voordat ze moeten worden aangevuld. De ziekenhuizen anticiperen op de mogelijkheid dat de verstoring enkele dagen kan duren door spoedtransporten te organiseren om hun patiënten naar andere ziekenhuizen over te brengen naar niet-getroffen gebieden. Ook neemt de druk op de ziekenhuizen toe door het falen van medische thuisapparatuur; hierdoor moeten verschillende mensen worden opgenomen. In één ziekenhuis is de noodstroomvoorziening niet aangeslagen. De patiënten in dit ziekenhuis moeten onmiddellijk worden overgebracht naar de dichtstbijzijnde ziekenhuizen waar wel stroom is. Deze evacuaties worden bemoeilijkt door de aanhoudende drukte op de wegen.

Ook overheidssystemen worden geraakt door de verstoring. Zo is de Basisregistratie Personen niet meer beschikbaar, net als DigiD. Hierdoor komt de dienstverlening van een aantal gemeenten stil te liggen, waardoor er bijvoorbeeld geen paspoorten meer kunnen worden uitgegeven.

Het duurt een aantal dagen om een deel van de stroomvoorziening in het getroffen gebied weer op gang te brengen met behulp van noodoplossingen, hulp uit het buitenland en provisorische oplossingen. Er moet echter nog wel geprioriteerd worden voor de verdeling van elektriciteit. Het duurt vervolgens een week tot het stroomnetwerk weer volledig functioneert; eerst moeten reparatie- en opbouwwerkzaamheden worden uitgevoerd en moet het netwerk gefaseerd worden opgestart.

*Beoordeling van de impact en waarschijnlijkheid*

De transport, distributie en productie van elektriciteit wordt direct geraakt voor meerdere weken. Dit heeft enorme keteneffecten en veel andere vitale processen worden door ofwel de uitval van elektriciteit zelf, of door de gevolgen ervan geraakt. Op basis van de gebeurtenissen beschreven in het scenario schatten expert in dat er effecten ontstaan in de onderstaande sectoren (zie Tabel 11). Het is niet vanzelfsprekend dat die vitale processen ook per definitie verstoord raken, maar organisaties die bij die processen betrokken zijn krijgen wel te maken met effecten.
Verder is ook niet ondenkbaar dat er in andere vitale processen effecten kunnen optreden vanuit deze gebeurtenissen, maar welke en op welke manier, dat is moeilijk in te schatten.

**Tabel 11** Geraakte vitale processen bij het scenario keteneffecten elektriciteit

| Vitale processen | Categorie | Sector | Geraakt? |
|---|---|---|---|
| Landelijk transport, distributie en productie elektriciteit | A | Energie | Geraakt door de aanval op verdeelstations. |
| Regionale distributie elektriciteit | B | | Geraakt door de aanval op verdeelstations, voor een bepaalde regio is er uitval gedurende +/- 2 weken. |
| Gasproductie, landelijk transport en distributie gas | A | | |
| Regionale distributie gas | B | | Als er gasproductie zit in het gebied waar de elektriciteit uitvalt, dan valt ook de gasproductie stil in dat gebied. Daarnaast is er een daling in de vraag, doordat heel veel warmtebronnen die op gas werken het niet meer doen. |
| Olievoorziening | A | | Benzinestations in de getroffen regio vallen waarschijnlijk uit door elektriciteitsuitval. Als de wegen volstromen (alleen de eerste uren zal er opstopping zijn) zal aanvoer van benzine wellicht ook stokken. |
| Internet en datadiensten | B | ICT/ Telecom | Lokale uitval daar waar stroom uitvalt. |
| Internettoegang en dataverkeer | B | | Lokale uitval daar waar stroom uitvalt. |
| Spraakdienst en SMS* | B | | Lokale uitval daar waar stroom uitvalt. |
| Plaats- en tijdsbepaling middels GNSS | B | | De satellieten zullen blijven werken, maar eindgebruikers zijn wel afhankelijk van elektriciteit voor het ontvangen van signalen. |
| Drinkwatervoorziening | A | Drinkwater | Drinkwatervoorziening als proces zal doorgaan (eigen energievoorziening). In hoge gebouwen in het getroffen gebied zullen de hogere verdiepingen geen drinkwater meer hebben door uitval elektrische pomp. |
| Keren en beheren waterkwantiteit | A | Water | Grotendeels noodstroomvoorziening bij grote sluizen en keringen. Bij langere duur zullen waterschappen in het getroffen gebied minder goed in staat zijn om het waterpeil laag te houden. Waterkwaliteit gaat achteruit, evt. verziltingseffecten. |
| Vlucht- en vliegtuigafhandeling | B | Transport | Effecten zijn afhankelijk van locatie. Vanuit keteneffecten is het niet ondenkbaar dat er verstoring optreedt. Waarschijnlijk initiële stillegging (1-1.5 uur). |
| Scheepvaartafwikkeling | B | | Bruggen functioneren niet. Logistieke processen in havens in het getroffen gebied gehinderd. |
| Vervoer van personen en goederen over (hoofd) spoorweginfrastructuur | B | Transport | Door elektriciteitsverstoring zal (een deel van) het treinverkeer ontregeld raken |
| Vervoer over (hoofd)wegennet | B | Transport | Wegen kunnen dichtslibben op de korte termijn, maar lost zich op een gegeven moment vanzelf op. |

**Tabel 11** Geraakte vitale processen bij het scenario keteneffecten elektriciteit (vervolg)

| Vitale processen | Categorie | Sector | Geraakt? |
|---|---|---|---|
| Grootschalige productie/ verwerking en/of opslag (petro) chemische stoffen | B | Chemie | Bij langdurige uitval wel effecten. Veel bedrijven hebben noodstroom voorzieningen, maar houden dat niet lang vol. Afhankelijk van aanvoer van diesel voor aggregaten. Ligt ook aan de locatie. |
| Opslag, productie en verwerking nucleair materiaal | A | Nucleair | Bij langdurige uitval wel effecten. Meeste bedrijven hebben noodstroom voorzieningen, maar houden dat niet lang vol. Afhankelijk van aanvoer van diesel voor aggregaten. Ligt ook aan de locatie. Weinig alternatieven voor medicijnproductie. |
| Toonbankbetalingsverkeer | B | Financieel | Door uitval elektriciteit kunnen er verstoringen zijn in pinbetalingen. |
| Massaal giraal betalingsverkeer | B | | |
| Hoogwaardig betalingsverkeer tussen banken | B | | |
| Effectenverkeer | B | | |
| Communicatie met en tussen hulpdiensten middels 112 en C2000 | B | OOV | Door de problemen met het mobiele netwerk in het gebied kan communicatie met en tussen hulpdiensten bemoeilijkt worden (bereikbaarheid 112 en mogelijk verstoringen in C2000 netwerk) |
| Inzet politie | B | | Bemoeilijkt door o.a. communicatieproblemen |
| Basisregistraties personen en organisaties | B | Digitale overheids-processen | Beperkte verstoringen |
| Interconnectiviteit (transactie-infrastructuur voor informatie uit basisregistraties) | B | | Beperkte verstoringen |
| Elektronisch berichtenverkeer en informatieverschaffing aan burgers | B | | NL-ALERT zal ook niet werken voor de inwoners van het getroffen gebied, gaat gelijk met de uitval van mobiele netwerk |
| Identificatie en authenticatie van burgers en bedrijven | B | | Beperkte verstoringen |
| Inzet defensie | B | Defensie | |

In onderstaand overzicht wordt de beoordeling van de waarschijnlijkheid en impact op de nationale veiligheidsbelangen voor dit scenario weergegeven.

**Tabel 12** Scorekaart scenario keteneffecten elektriciteitsuitval

| **Thema** | **Bedreiging vitale infrastructuur** | | |
|---|---|---|---|
| **Dreigingscategorie** | Moedwillige bedreiging vitale processen | | |
| **Scenario** | Keteneffecten elektriciteitsuitval | | |
| **Scenariotoelichting** | Terroristische aanslag op het elektriciteitsnetwerk met als gevolg stroomuitval in een deel van Nederland. Het dagelijks leven komt abrupt tot stilstand. Herstel duurt enkele dagen tot enkele weken. | | |
| **Waarschijnlijkheidsbeoordeling (binnen 5 jaar)** | | | **Toelichting** |
| **Waarschijnlijkheid:** | | B--mid-den | De kans dat een terrorist of terroristische organisatie een dergelijke aanval kan plegen is klein, maar niet afwezig. We zijn als Nederland bovendien afhankelijker geworden van elektriciteit. |
| **Beoordeling gevolgen (impact)** | | | |
| **Veiligheidsbelang** | **Criterium** | **Score** | **Toelichting** |
| **Territoriaal** | 1.1 Grondgebied | 0 | Niet van toepassing. Er is wel fysieke sabotage door de terroristen op Nederlands grondgebied, maar deze effecten scoren elders. |
| | 1.2 Internationale positie | B | Er zijn twee indicatorcategorieën van toepassing, door mogelijke acties tegen Nederland in het buitenland en mogelijk teruglopend toerisme; de aanslag is een gevolg van Nederlands militair optreden, dit kan demonstraties opleveren. Het toerisme kan tijdelijk teruglopen als gevolg van een terroristische aanslag. |
| | 1.3 Digitale ruimte | 0 | Niet van toepassing |
| | 1.4 Bondgenootschappelijk grondgebied | 0 | Niet van toepassing |
| **Fysiek** | 2.1 Doden | A | Mogelijk vallen enkele doden door de stroomuitval, door uitval van medische apparatuur thuis en gebrek aan warmte. Ook is het mogelijk dat hulpdiensten niet op tijd ter plaatse kunnen komen. |
| | 2.2 Ernstig gewonden en chronisch zieken | A | Mogelijk vallen enkele gewonden door de stroomuitval, bijvoorbeeld ook omdat mensen zelf gaan proberen verwarming te regelen waardoor ongelukken kunnen gebeuren. |
| | 2.3 Gebrek primaire levensbehoeften | D | Voor de mensen in het getroffen gebied (ca. 2 miljoen huishoudens) betekent elektriciteitsuitval ook geen warm water en verwarming. Bovendien kunnen supermarkten niet meer draaien, waarbij uiteindelijk overgeschakeld zal worden naar centrale voedseldistributiestations, maar die zullen niet meteen operationeel kunnen zijn. Mensen zullen naar plekken gaan (familie, vrienden) die niet getroffen zijn door de storing, maar kwetsbare groepen hebben die mogelijkheid niet. Uiteindelijk is de verwachting dat minder dan 1 miljoen mensen een gebrek aan primaire levensbehoeften zullen ervaren omdat er snel redelijke oplossingen gevonden kunnen worden. |

**Tabel 12** Scorekaart scenario keteneffecten elektriciteitsuitval (vervolg)

| Veiligheidsbelang | Criterium | Score | Toelichting |
|---|---|---|---|
| **Economisch** | 3.1 Kosten | D | Door de stroomstoring ontstaan grote economische kosten (meer dan 5 miljard), onder meer door onze afhankelijkheid van elektriciteit en ICT, die als gevolg van de stroomstoring uitvalt. Bovendien zal in de nasleep van de stroomstoring ook economische schade zijn. |
| | 3.2 Aantasting vitaliteit | A | Nauwelijks effect op de staatsschuld en/of werkloosheid. Hoewel het aandeel van de bruto toegevoegde waarde van de getroffen sectoren meer dan 10% is van het BNP, is de tijdsduur van invloed minder dan een maand (dus geen correctiefactor). |
| **Ecologisch** | 4.1 Aantasting natuur en milieu | 0 | Niet van toepassing. Kritieke systemen hebben een fail-safe modus waar ze op terug kunnen vallen, onder andere zodat er geen gevaarlijke stoffen worden geloosd. |
| **Sociaal-politiek** | 5.1 Verstoring dagelijks leven | E | 2 miljoen huishoudens worden gedurende een week aanzienlijk aangetast in de zin dat er in het getroffen gebied geen onderwijs zal zijn, mensen zullen niet naar hun werk kunnen, maatschappelijke voorzieningen kunnen niet meer worden gebruikt, er zullen winkelsluitingen zijn en mensen zullen bovendien een verminderde virtuele/sociale bereikbaarheid hebben. |
| | 5.2 Aantasting democratische rechtsstaat | A | Er is een beperkte verstoring van het functioneren van de politieke vertegenwoordiging (lokaal), openbaar bestuur, rechtspraak en openbare orde en veiligheid. Dit gaat om een fysieke belemmering, het gaat niet om een structurele ondermijning van de rechtsstaat. Hoewel het wellicht de bedoeling van de terroristen zou zijn geweest om de democratische rechtsstaat aan te tasten door het vertrouwen in de overheid te proberen te ondermijnen, zal er geen sprake zijn van structurele aantasting. |
| | 5.3 Sociaal-maatschappelijke impact | C | Omdat er al onrust heerst in de samenleving, zullen we gedragingen van woede en angst zien (zoals hamsteren), zeker omdat elektriciteitsuitval mensen heel direct raakt en dit de spreekwoordelijke druppel zou kunnen zijn. De maatschappelijke reactie op een dergelijke terroristische aanslag kan vaak ook een collectief gevoel van saamhorigheid teweegbrengen, vandaar dat gewelddadige incidenten n.a.v. van deze aanslag naar verwachting niet zullen voorkomen. Gezien het feit dat er sprake is van een terroristische aanslag, kan er wel maatschappelijk wantrouwen ontstaan jegens de etnische of culturele groep waartoe de dader(s) behoren. De aanslag kan dus een polariserende werking hebben. |

| Veiligheidsbelang | Criterium | Score | Toelichting |
|---|---|---|---|
| **Internationale rechtsorde en stabiliteit** | 6.1 Staatssoevereiniteit, vreedzame co-existentie en vreedzame geschillenbeslechting | 0 | Niet van toepassing |
| | 6.2 Mensenrechten | 0 | Niet van toepassing |
| | 6.3 Internationaal financieel-economisch bestel | 0 | Niet van toepassing |
| | 6.4 Multilaterale instituties | 0 | Niet van toepassing |
| | 6.5 Instabiliteit rondom Koninkrijk/EU | 0 | Niet van toepassing |

## 5.2 Beschouwing

De ontwikkelingen binnen deze dreigingscategorie en de uitkomst van de analyse laten zien dat (moedwillige) verstoring van vitale processen tot serieuze impact kan leiden op de nationale veiligheid. Ook komt – net als bij eerdere analyses – duidelijk naar voren dat er veel keteneffecten te verwachten zijn bij de uitval van onder meer de elektriciteitsvoorziening en telecommunicatiediensten. De toenemende complexiteit van systemen en netwerken maakt dat de het lastig is om exacte keteneffecten in te schatten, met name bij verstoring van digitale processen. Ook zijn de effecten van dit type gebeurtenissen sterk afhankelijk van de locatie en de specifieke configuratie van systemen en netwerken bij gebruikers.

De waarschijnlijkheid van dergelijke moedwillige aanvallen zoals beschreven in beide scenario's wordt op dit moment relatief laag ingeschat. Dit heeft deels te maken met de keuze voor actoren, hoewel ook een dergelijke aanval van een statelijke actor op Nederlandse vitale infrastructuur op dit moment een lage waarschijnlijkheid kent. Desalniettemin zijn vitale processen een interessant doelwit voor kwaadwillenden (zie ook het dreigingsthema *ongewenste inmenging en beïnvloeding democratische rechtsstaat* en het thema *cyberdreigingen*). De waarschijnlijkheid van dit type dreiging neemt wel toe wanneer het gebeurtenissen met minder ernstige gevolgen betreft. Dit heeft deels te maken met de preventieve en mitigerende maatregelen van de vitale aanbieders en deels met de capaciteit en motivatie van actoren die nodig is om doelbewust en doelgericht een dergelijke aanval uit te voeren.

# 6. Dreigingscategorie verstoring vitale processen als gevolg van technisch of menselijk falen

De dreigingscategorie verstoring vitale processen als gevolg van technisch of menselijk falen gaat in op incidenten waarbij de uitval van vitale infrastructuur wordt veroorzaakt door technisch of menselijk falen. Het gaat binnen deze dreigingscategorie vaak om een eigenstandige verstoring, waar in de categorie natuurlijke verstoring vaker sprake is van een common-cause. Binnen deze categorie is geen sprake van een moedwillige actor (denk aan een crimineel of statelijke actor met voldoende middelen) of andere externe factoren. Factoren zoals het weer kunnen wel bijdragen aan de impact op het moment van het technisch falen van een vitaal systeem, hier is dan ook rekening mee gehouden bij het opstellen van de scenario's.

## 6.1 Scenario's

In deze paragraaf wordt de dreiging die relevant is binnen de categorie Verstoring vitale processen als gevolg van technisch of menselijk falen beschreven aan de hand van een scenario dat gaat over een landelijke elektriciteitsuitval door een niet moedwillige oorzaak.

### 6.1.1 Scenario landelijke black-out

In de ontwikkelingen is reeds de toenemende elektrificatie van de samenleving beschreven, mede ten gevolge van de energietransitie. Dit zorgt ervoor dat de maatschappij in toenemende mate afhankelijk is van elektriciteit, maar ook dat de druk op het elektriciteitsnetwerk toeneemt.
In het scenario wordt beschreven hoe een technische of menselijke fout tot een totale black-out in grote delen van Europa leidt. Ook in heel Nederland valt de stroom gedurende 24 uur uit.

*Bouwstenen*
In Tabel 13 staan de relevante bouwstenen voor dit scenario weergegeven.

**Tabel 13** Bouwstenen scenario landelijke black-out

| Oorzaak | Type verstoring | Verstoorde vitale processen | Vitale processen verstoord door cascade effecten | Schaal brongebied | Schaal effect gebied | Duur |
|---|---|---|---|---|---|---|
| Technisch of menselijk falen | Eigenstandige verstoring, uitval of aantasting | Landelijk transport, distributie en productie elektriciteit | Olievoorziening | Internationaal | Internationaal | 8 tot 24 uur |
| | | Regionale distributie elektriciteit | Vervoer van personen en goederen over (hoofd)spoorweg infrastructuur | | Nationaal | |
| | | | Vervoer over (hoofd)wegennet | | | |
| | | | Toonbank-betalingsverkeer | | | |
| | | | Massaal giraal betalingsverkeer | | | |

*Verhaallijn*
Het is een maandag, 8 uur 's ochtends. De weersverwachting is 17°C; af en toe een bui; weinig wind. De vraag naar elektriciteit is erg groot: kantoren en fabrieken starten weer op na het weekend. De beschikbare hoeveelheid reservecapaciteit is minimaal. Door een willekeurige oorzaak [36] treedt een grote frequentiedaling op in het Europese net (*voltage collapse*).

De frequentiedaling zorgt er onmiddellijk voor dat energienetten uitvallen. Vanwege de grote verbondenheid van het Europese net vallen in grote delen van Europa (waaronder heel Nederland) de stroom uit.

Direct hierna werken TenneT en de Europese TSO's (*Transmitting System Operators*; netbeheerders) met man en macht om de levering van elektriciteit in Nederland en Europa weer aan de praat te krijgen. Doordat in heel Nederland de stroom is uitgevallen en het netwerk 'plat is gegaan', moet hiervoor gebruik gemaakt worden van *black start*-voorzieningen. [37] Hiermee wordt het net lokaal weer onder spanning gebracht. Geleidelijk aan wordt belasting bijgeschakeld om een stabiele situatie te realiseren. Na wat complicaties bij het opbouwen van het net, is het 24 uur na het uitvallen van de elektriciteit afgerond. [38]

[36] Een grote frequentiedaling kan door velerlei oorzaken optreden. Een plotseling, onvoorzien groot aanbod van windenergie, terwijl het systeem al maximaal belast is; een fout bij het afschakelen van een hoogspanningsleiding; etc. De exacte oorzaak is niet van invloed op het scenario; reden waarom de oorzaak niet specifiek benoemd is.

[37] Nederland zal zich in dit geval los gaan koppelen van het Europese net. Vervolgens worden vanaf 3 blackstart locaties gefaseerd de schakelaars omgezet (het vermogen wordt regionaal verdeeld). Als die 3 eilanden afzonderlijk draaien, wordt landelijk gesynchroniseerd, en tot slot Europees.

[38] Er zijn geen ervaringscijfers met een zo grootschalige storing als in dit scenario beschreven. Op basis van de ervaringen bij kleinschaliger uitval is de volgende berekening van de hersteltijd in dit scenario gemaakt. Bij een kleinschalige black-out is de hersteltermijn 4 tot 8 uur. Deze hersteltijd is verdubbeld (16 uur). Daar is (als marge) nog een keer hetzelfde aantal uren aan toegevoegd om mogelijk optredende complicaties (bijvoorbeeld het mislukken van de black-start) te ondervangen. De in het scenario gehanteerde 24 uur wordt door TenneT gezien als de maximale duur voor het herstel van een storing van deze orde.

De gevolgen voor bedrijven, instellingen en burgers zijn groot aangezien allerlei processen geheel of gedeeltelijk uitvallen (zoals openbaar vervoer, medische thuisapparatuur, betalingsverkeer, tankstations, winkels blijven dicht, e.d.). Aanname is dat de meeste onderdelen van de vitale infrastructuur (op noodstroom) blijven functioneren totdat de elektriciteitsvoorziening is hersteld.

*Beoordeling van de impact en waarschijnlijkheid*

De landelijke black-out in het scenario zal ook vitale processen raken. Bij de beoordeling van de impact van het scenario is er van uit gegaan dat een groot deel van de vitale processen enige tijd kan blijven functioneren via een noodstroomvoorziening, maar of dat in de praktijk ook echt zo werkt, is onzeker (vaak zitten de aggregaten niet vol met diesel en wordt de aanvoer van diesel na verloop van tijd lastig. Veelal betekent dit dat na 12u op veel plekken ook de noodstroom niet meer functioneert). Het is dus niet vanzelfsprekend dat de getroffen vitale processen ook per definitie verstoord raken, maar organisaties die bij die processen betrokken zijn krijgen wel te maken met effecten. Verder is ook niet ondenkbaar dat er in andere vitale processen effecten kunnen optreden vanuit deze gebeurtenissen, maar welke en op welke manier, dat is moeilijk in te schatten. Zie Tabel 14 voor een overzicht de vitale processen waarvan door experts verwacht wordt dat deze (potentieel) geraakt zullen worden als gevolg van de beschreven gebeurtenissen en wat hierbij de redenering is.

**Tabel 14** Geraakte vitale processen bij scenario landelijke black-out

| Vitale processen | Categorie | Sector | Geraakt? |
|---|---|---|---|
| Landelijk transport, distributie en productie elektriciteit | A | Energie | De stroomvoorziening in heel Nederland valt uit. |
| Regionale distributie elektriciteit | B | | De stroomvoorziening in heel Nederland valt uit. |
| Gasproductie, landelijk transport en distributie gas | A | | Afhankelijk van de noodstroomvoorzieningen zou de grote voeding van aardgasinstallaties kunnen wegvallen, waardoor de kwetsbaarheid ten aanzien van de totale leveringsverplichtingen aan binnen- en buitenland toenemen. |
| Regionale distributie gas | B | | Het aardgasgebruik door bedrijven en particulieren kan verstoord raken doordat elektrische componenten (bijv. (veiligheids)kleppen) in hun installaties niet functioneren. |
| Olievoorziening | A | | Tankstations hebben geen noodvoorziening en kunnen dus geen brandstof leveren. De (logistieke) organisatie van de dieselvoorziening t.b.v. noodaggregaten wordt gecompliceerd door de problemen die het wegverkeer ondervindt. |
| Internet en datadiensten | B | ICT/ Telecom | Het proces zelf zal blijven functioneren maar eindgebruikers hebben alleen beschikking over deze diensten als zij noodstroom hebben, of totdat accu's van apparaten leeg zijn. |
| Internettoegang en dataverkeer | B | | Internettoegang voor eindgebruikers hebben alleen beschikking over deze diensten als zij noodstroom hebben, of totdat accu's van apparaten leeg zijn. |
| Spraakdienst en SMS* | B | | Mobiele netwerken vallen na enkele uren uit, tenzij zij zijn voorzien van noodstroom. Eindgebruikers hebben alleen beschikking over deze diensten als zij noodstroom hebben, of totdat accu's van apparaten leeg zijn. |

**Tabel 14** Geraakte vitale processen bij scenario landelijke black-out (vervolg)

| Vitale processen | Categorie | Sector | Geraakt? |
|---|---|---|---|
| Plaats- en tijdsbepaling middels GNSS | B | | De satellieten zullen blijven werken, maar eindgebruikers zijn wel afhankelijk van elektriciteit voor het ontvangen van signalen. |
| Drinkwatervoorziening | A | Drinkwater | Drinkwatervoorziening als proces zal doorgaan (eigen energievoorziening). In hoge gebouwen zullen de hogere verdiepingen geen drinkwater meer hebben door uitval van elektrische pompinstallaties. |
| Keren en beheren waterkwantiteit | A | Water | Objecten zoals gemalen zullen niet lang blijven functioneren. |
| Vlucht- en vliegtuigafhandeling | B | Transport | LVNL kan besluiten tot sluiting van het vliegverkeer van en naar Schiphol. |
| Scheepvaartafwikkeling | B | | |
| Vervoer van personen en goederen over (hoofd) spoorweginfrastructuur | B | Transport | Eventuele noodstroomvoorziening zal niet voldoende zijn om al het treinverkeer doorgang te laten vinden. |
| Vervoer over (hoofd)wegennet | B | Transport | Matrixborden en verkeerslichten kunnen uit vallen (tenzij er noodstroomvoorzieningen zijn, bijvoorbeeld via zonnecellen). Automobilisten kunnen stranden door een gebrek aan brandstof. |
| Grootschalige productie/ verwerking en/of opslag (petro) chemische stoffen | B | Chemie | |
| Opslag, productie en verwerking nucleair materiaal | A | Nucleair | |
| Toonbankbetalingsverkeer | B | Financieel | Bij winkels zonder noodstroomvoorziening kunnen geen pinbetalingen meer worden uitgevoerd. |
| Massaal giraal betalingsverkeer | B | | Er kunnen geen overschrijvingen worden gerealiseerd. |
| Hoogwaardig betalingsverkeer tussen banken | B | | |
| Effectenverkeer | B | | |
| Communicatie met en tussen hulpdiensten middels 112 en C2000 | B | OOV | Het alarmnummer kan overbelast raken door groot aantal meldingen, hoewel het ook de vraag is in hoeverre mensen nog kunnen bellen naar het alarmnummer omdat er ook problemen zijn met telecommunicatie. C2000 zal na ong. 8 uur uitvallen en het mobiele verkeer tussen hulpdiensten na 2-3 uur. Communicatie zal beperkt zijn. |
| Inzet politie | B | | Er kunnen problemen ontstaan met betrekking tot o.a. de communicatie. De politie heeft, net als veel andere hulpdiensten een speciale brandstofvoorziening ingeregeld |
| Basisregistraties personen en organisaties | B | Digitale overheids-processen | |

**Tabel 14:** Geraakte vitale processen bij scenario landelijke black-out (vervolg)

| Vitale processen | Categorie | Sector | Geraakt? |
|---|---|---|---|
| Interconnectiviteit (transactie-infrastructuur voor informatie uit basisregistraties) | B | | |
| Elektronisch berichtenverkeer en informatieverschaffing aan burgers | B | | Wordt verstoord door uitval ICT en Telecom. |
| Identificatie en authenticatie van burgers en bedrijven | B | | |
| Inzet defensie | B | Defensie | |
| | | | |

In onderstaand overzicht wordt de beoordeling van de waarschijnlijkheid en impact op de nationale veiligheidsbelangen voor dit scenario weergegeven.

**Tabel 15** Scorekaart scenario landelijke black-out

| Thema | Bedreiging vitale infrastructuur | |
|---|---|---|
| **Dreigingscategorie** | Verstoring vitale infrastructuur als gevolg van technisch/menselijk falen | |
| **Scenario** | Landelijke black-out | |
| **Scenariotoelichting** | Door een willekeurige oorzaak treedt een grote frequentiedaling op in het Europese net (voltage collapse). De frequentiedaling zorgt er onmiddellijk voor dat energienetten uitvallen. Vanwege de grote verbondenheid van het Europese net vallen in grote delen van Europa (waaronder heel Nederland) de stroom uit. Geleidelijk aan wordt belasting bijgeschakeld om een stabiele situatie te realiseren. Na wat complicaties bij het opbouwen van het net, is het 24 uur na het uitvallen van de elektriciteit afgerond. Aanname is dat veel onderdelen van de vitale infrastructuur (op noodstroom) blijven functioneren totdat de elektriciteitsvoorziening is hersteld. | |
| **Waarschijnlijkheidsbeoordeling (binnen 5 jaar)** | | **Toelichting** |
| **Waarschijnlijkheid:** | D | Nederland is nog nooit getroffen door een algehele black-out. Wel zijn we enkele keren door het oog van de naald gekropen bij grootschalige stroomuitval in Europa (bijvoorbeeld in november 2006). Hoewel de kans op een Europese black-out waarin Nederland wordt meegetrokken (aanzienlijk) kleiner is dan de kans op een grote storing of een partiële black-out, is het mogelijk dat dit gebeurt. Experts schatten in dat de waarschijnlijkheid van dergelijke stroomuitval een keer in de 50 jaar is. |
| **Beoordeling gevolgen (impact)** | | |

**Tabel 15** Scorekaart scenario landelijke black-out (vervolg)

| Veiligheidsbelang | Criterium | Score | Toelichting |
|---|---|---|---|
| **Territoriaal** | 1.1 Grondgebied | 0 | Niet van toepassing |
| | 1.2 Internationale positie | 0 | Niet van toepassing. Oorzaak ligt niet in Nederland, dus Nederland zal er niet op aangekeken worden. |
| | 1.3 Digitale ruimte | 0 | Niet van toepassing. Er vallen wel systemen uit, maar dat betekent ook dat kwaadwillenden geen toegang hebben. |
| | 1.4 Bondgenootschappelijk grondgebied | 0 | Niet van toepassing |
| **Fysiek** | 2.1 Doden | B | Mogelijk vallen enkele tientallen doden door de landelijke stroomuitval, bijvoorbeeld door uitval van medische apparatuur en gebrek aan warmte. Ook is het mogelijk dat hulpdiensten niet op tijd ter plaatse kunnen komen. Kwetsbaren kunnen niet verplaatst worden en kunnen niet terecht in de ziekenhuizen. Ook vallen er mogelijk enkele verkeersslachtoffers door uitval van verkeersleidingsystemen. |
| | 2.2 Ernstig gewonden en chronisch zieken | B | Omdat er overal in Nederland geen stroom is (alhoewel dit voor een korte periode het geval is), is het mogelijk dat er tientallen gewonden vallen door verkeers-, bedrijfs- of ongevallen in huis. |
| | 2.3 Gebrek primaire levensbehoeften | A | Alle inwoners van Nederland hebben gedurende 24 uur geen elektriciteit. Huishoudens hoger dan twee verdiepingen hebben veelal ook geen drinkwater (niet alle pompen hebben noodstroom). Het is niet uit te sluiten dat op de tweede dag nog steeds niet alles werkend is. |
| **Economisch** | 3.1 Kosten | D | Door de stroomstoring ontstaan grote economische kosten (meer dan 5 miljard en meer dan de regionale uitval bij het scenario keteneffecten elektriciteit), onder meer door onze afhankelijkheid van elektriciteit en ICT, die als gevolg van de stroomstoring uitvalt. Hoewel de uitval geen weken duurt, is er wel sprake van uitval in heel Nederland, waardoor de kosten zeer snel zullen oplopen. Bovendien zal in de nasleep van de stroomstoring ook economische schade zijn. |
| | 3.2 Aantasting vitaliteit | 0 | Niet van toepassing |
| **Ecologisch** | 4.1 Aantasting natuur en milieu | 0 | Niet van toepassing. Kritieke systemen hebben een fail-safe modus waar ze op terug kunnen vallen, onder andere zodat er geen gevaarlijke stoffen worden geloosd. |

**Tabel 15** Scorekaart scenario landelijke black-out (vervolg)

| Veiligheidsbelang | Criterium | Score | Toelichting |
|---|---|---|---|
| **Sociaal-politiek** | 5.1 Verstoring dagelijks leven | D | Gedurende 24 uur hebben alle inwoners van Nederland geen stroom. 5 indicatoren: werk, onderwijs, maatschappelijke voorzieningen, winkels, virtuele netwerken. |
| | 5.2 Aantasting democratische rechtsstaat | 0 | Niet van toepassing. Wel fysieke belemmering van betreffende vertegenwoordigers (politieke vertegenwoordiging, openbaar bestuur, rechtspraak en openbare orde en veiligheid) bij het uitoefenen van hun functie, maar geen structurele aantasting van de democratische rechtsstaat. |
| | 5.3 Sociaal-maatschappelijke impact | A | Beperkte impact (ondanks de landelijke black-out), maar er zal wel wat onrust ontstaan en een beperkte groep mensen zal (tijdelijk) vertrouwen in overheid (en de energiesector) verliezen. Bevolking wordt mogelijk ongerust over de (toegenomen) afhankelijkheid van elektriciteit en dat fluctuaties in het Europese net een dermate grote impact hebben op Nederland. |
| **Internationale rechtsorde en stabiliteit** | 6.1 Staatssoevereiniteit, vreedzame co-existentie en vreedzame geschillenbeslechting | 0 | Niet van toepassing |
| | 6.2 Mensenrechten | 0 | Niet van toepassing |
| | 6.3 Internationaal financieel-economisch bestel | 0 | Niet van toepassing |
| | 6.4 Multilaterale instituties | 0 | Niet van toepassing |
| | 6.5 Instabiliteit rondom Koninkrijk/EU | 0 | Niet van toepassing |

## 6.2 Beschouwing

De afgelopen jaren hebben getoond dat incidenten als gevolg van technisch of menselijk falen grote impact kunnen hebben op de maatschappij. Zo ontstond er in 2019 een storing in de systemen van KPN door het niet goed functioneren van een digitale teller in het telefoonsysteem.[39] De storing zorgde ervoor dat het 4G netwerk uitviel en dat men niet meer kon bellen. Ook het alarmnummer 112 was enige tijd niet meer bereikbaar.

Ook de in het scenario beschreven uitval van de elektriciteitsvoorziening in Europa en dus ook Nederland heeft grote impact op de samenleving. Hoewel een dergelijke landelijke black-out nog niet is voorgekomen, schatten experts in dat het wel degelijk een hoge waarschijnlijkheid kent. De afhankelijkheid van elektriciteit in onze samenleving zal naar verwachting alleen maar toenemen door de energietransitie en dat kan ervoor zorgen dat ook de impact van uitval in de komende jaren toeneemt. Tegelijkertijd zal de energietransitie ook voor veel verandering van de infrastructuur zorgen, waardoor er ook enige mate van onzekerheid is met betrekking tot de toekomstige aard en impact van elektriciteitsuitval.

In algemene zin zorgen de toegenomen (technische) complexiteit en verwevenheid van systemen en infrastructuur ervoor dat de mogelijke impact van verstoringen kan toenemen door toenemende afhankelijkheden en potentiële keteneffecten. Ook zorgt de toegenomen complexiteit ervoor dat het lastiger is om overzicht en grip te houden op het netwerk van systemen.

[39] Hans Nauta, "De boosdoener van de 112-storing: een KPN-teller die doortelde totdat het niet meer ging," Trouw (26 juni 2020), *https://www.trouw.nl/economie/de-boosdoener-van-de-112-storing-een-kpn-teller-die-doortelde-totdat-het-niet-meer-ging~bbbab906/*.

# 7. Dreigingscategorie natuurlijke verstoring vitale processen

De dreigingscategorie natuurlijke verstoring van vitale infrastructuur gaat in op de natuurlijke oorzaken van de verstoring of uitval van vitale infrastructuur. Hier kan gedacht worden aan extreem weer, bijvoorbeeld een overstroming of grote brand, waarbij één of meerdere vitale processen verstoord raken. Bij dit soort natuurlijke verstoringen is het vaak zo dat meerdere vitale processen tegelijkertijd verstoord raken, wat betekent dat er sprake is van een zogenaamde common-cause verstoring.
Een ander kenmerk van deze dreigingscategorie is de duur van het incident, vaak is hier sprake van een langere periode, met name ook de nasleep. Denk bijvoorbeeld aan een overstroming waar het repareren en weer opbouwen maanden kan kosten. Bij deze natuurlijke verstoringen ligt de oorzaak buiten de controle van organisaties van de vitale infrastructuur. Organisaties kunnen voorzorgsmaatregelen treffen door bepaalde systemen uit te zetten of te beschermen, of juist een terugvaloptie in te bouwen waardoor een proces doorgang kan vinden bij een verstoring.

## 7.1 Scenario's

Binnen de dreigingscategorie natuurlijke verstoring van vitale infrastructuur is een wild card scenario opgesteld over ruimteweer. Daarnaast worden twee scenario's uit het thema *klimaat- en natuurrampen* in deze dreigingscategorie opnieuw behandeld, vanuit het perspectief van de vitale processen: overstroming [40] en natuurbrand. In deze paragraaf laten we zien welke vitale processen worden getroffen; voor de beoordeling van het gehele scenario wordt verwezen naar het themarapport *klimaat- en natuurrampen*.

### 7.1.1 Scenario overstroming vanuit een rivier

Het overstromingsscenario vanuit een rivier beschrijft een situatie met extreme neerslag in het stroomgebied van de Rijn en Maas, waardoor extreem hoge waterstanden ontstaan. Uiteindelijk breekt op één locatie langs de Boven-Merwede de dijk door. De vitale processen die direct door de overstroming verstoord raken of volledig uitvallen (dus als gevolg van het onderwater komen te staan van de infrastructuur) zijn: elektriciteitsvoorziening, telecommunicatie, transport (snelwegen, treinverkeer), drinkwatervoorziening, afvalwaterzuivering en gasvoorziening. Naast vitale infrastructuur zullen er ook objecten zoals ziekenhuizen worden geraakt. Met name de verstoring van elektriciteit en telecommunicatie veroorzaken ook keteneffecten.
De verstoring van elektriciteit zorgt er daarbij voor dat primaire levensbehoeften zoals warmte en drinkwater niet beschikbaar zijn. Dit is één van de redenen dat dit scenario hoog scoort.

In Tabel 16 is het scenario aan de hand van de bouwblokken van het thema bedreiging vitale infrastructuur weergegeven.

[40] In de themarapportage van klimaat- en natuurrampen is nog een tweede overstromingsscenario meegenomen. De effecten op vitale infrastructuur zijn vergelijkbaar en zijn daarom niet apart in deze rapportage behandeld.

**Tabel 16** Bouwstenen scenario overstroming vanuit een rivier

| Oorzaak | Type verstoring | Direct getroffen vitale processen | Getroffen vitale processen door cascade effecten | Schaal brongebied | Schaal effect gebied | Duur |
|---|---|---|---|---|---|---|
| Natuurlijke verstoring | Common cause | Landelijk transport, distributie en productie elektriciteit | Internettoegang en dataverkeer | Regionaal | Nationaal | 1 tot 4 weken |
| | | Regionale distributie elektriciteit | Toonbankbetalings-verkeer | | Regionaal | |
| | | Gasproductie, landelijk transport en distributie gas | Massaal giraal betalingsverkeer | | | |
| | | Regionale distributie gas | Hoogwaardig betalingsverkeer tussen banken | | | |
| | | Olievoorziening | Effectenverkeer | | | |
| | | Internet en datadiensten | | | | |
| | | Spraakdiensten en SMS (mobiel en vast) | | | | |
| | | Drinkwater voorziening | | | | |
| | | Keren en beheren waterkwantiteit | | | | |
| | | Vlucht- en vliegtuig afhandeling | | | | |
| | | Scheepvaart afwikkeling | | | | |
| | | Vervoer van personen en goederen over (hoofd)spoorweg infrastructuur | | | | |
| | | Vervoer over (hoofd)wegennet | | | | |
| | | C2000 | | | | |
| | | Inzet politie | | | | |

### 7.1.2 Scenario onbeheersbare natuurbranden met grootschalige evacuatie

Het scenario onbeheersbare natuurbranden met grootschalige evacuatie beschrijft een natuurbrand in Nederlandse natuurgebieden, waar meerdere brandhaarden zich verspreiden.

Vitale processen worden in geval van een natuurbrand met name verstoord als er infrastructuur of objecten in het getroffen gebied aanwezig zijn, hoewel er ook keteneffecten kunnen optreden. In dit specifieke scenario worden de volgende vitale processen verstoord: elektriciteitsvoorziening, telecommunicatie, oppervlaktewater (drinkwater), transport (snelwegen), drinkwatervoorziening en als keteneffect OOV. Naast vitale infrastructuur zullen er ook objecten zoals ziekenhuizen worden geraakt. In het verloop van het scenario vormt met name de keteneffecten van verstoring van vitale processen op het gebied van telecommunicatie een probleem tijdens de crisisbestrijding omdat dit de communicatie van hulpdiensten bemoeilijkt. Indien dit scenario zich in een ander gebied afspeelt, waar bijvoorbeeld meer elektriciteitsvoorzieningen aanwezig zijn, dan kan er zelfs een black-out ontstaan, ook omdat brandschade veel tijd in beslag kan nemen om te herstellen.

In Tabel 17 is het scenario aan de hand van de bouwstenen van het thema bedreiging vitale infrastructuur weergegeven.

**Tabel 17** Bouwstenen scenario onbeheersbare natuurbranden

| Oorzaak | Type verstoring | Direct getroffen vitale processen | Getroffen vitale processen door cascade effecten | Schaal brongebied | Schaal effect gebied | Duur |
|---|---|---|---|---|---|---|
| Natuurlijke verstoring | Common-cause | Landelijk transport, distributie en productie elektriciteit | Internettoegang en dataverkeer | Regionaal | Nationaal | 72 uur tot 1 week |
| | | Regionale distributie elektriciteit | C2000 | | Regionaal | |
| | | Internet en datadiensten | Inzet politie | | | |
| | | Spraakdiensten en SMS (mobiel en vast) | | | | |
| | | Drinkwater voorziening | | | | |
| | | Vlucht- en vliegtuig afhandeling | | | | |
| | | Scheepvaart afwikkeling | | | | |
| | | Vervoer van personen en goederen over (hoofd)spoorweg infrastructuur | | | | |
| | | Vervoer over (hoofd)wegennet | | | | |

### 7.1.3 Wild card scenario ruimteweer [41]

Dit wild card scenario gaat in op diverse ruimteweerfenomenen en benoemt een aantal mogelijke effecten. Dit scenario wordt meegenomen als wild card, met name omdat er veel onzekerheid bestaat over de effecten van dit soort fenomenen. Experts verwachten wel dat we in de toekomst te maken gaan hebben met diverse ruimteweerfenomenen, maar de schaal en met name de impact op de maatschappij en in specifieke zin op vitale processen is onzeker.

*Achtergrond ruimteweer*

Ruimteweer is de fysische en fenomenologische toestand van de natuurlijke omgevingen in de ruimte. De hiermee verbonden discipline heeft als doel om – door middel van observaties, analyse en modellering – de toestand van de zon, de interplanetaire en planetaire omgeving, en de verstoringen die hierop invloed hebben, beter te begrijpen en te voorspellen. Daarnaast is het doel ook om de mogelijke impact op biologische en technologische systemen te onderzoeken en te voorspellen. [42]

Ruimteweer wordt voornamelijk veroorzaakt door de variabiliteit van het magneetveld van de zon. De buitenste lagen van de zon worden gedomineerd door dit dynamische magneetveld, dat veranderingen in de elektromagnetische straling (met name röntgen-, extreem ultraviolet-, en radiostraling) en de stroom geladen deeltjes in het zonnestelsel (de zonnewind) veroorzaakt. Soms zijn dat explosieve veranderingen, tijdens zogenaamde zonnevlammen, waarbij altijd een intensivering van röntgenstraling optreedt. Soms gaat een zonnevlam ook gepaard met intense radiostraling (solar radio burst) of een stroom van elektronen en protonen met zeer hoge snelheid (deeltjesstorm/solar energetic particle event).

De energie die vrijkomt bij een zonnevlam is typisch $10^{22-26}$Joule (een miljoen keer meer dan de jaarlijkse energieconsumptie in Nederland van $10^{18-19}$Joule). Gedurende zonnevlammen kan ook een deel van het materiaal in de zonneatmosfeer wegschieten van de zon: een zogenaamde coronal mass ejection (CME). Hierbij gaat het om een veel lagere snelheid dan bij een deeltjesstorm, maar een CME heeft nog altijd een snelheid van honderden tot enkele duizenden km/s, en een massa van $10^{12}$ tot $10^{14}$ kg. Dat is ongeveer de massa van een berg op aarde, maar zich verspreidend over een groot deel van het zonnestelsel. Dit zijn grootschalige verstoringen in de ruimte en als die de aarde raken, kan dit een grote impact hebben.
De magnetosfeer, de ionosfeer en het bovenste deel van de atmosfeer zijn binnen het ruimteweer de belangrijkste lagen rond de aarde, die enerzijds het leven beschermen tegen effecten uit de ruimte, maar die tevens sterk beïnvloed worden door het ruimteweer, en een steeds belangrijke rol spelen voor het functioneren van technische systemen. [43]

*Mogelijke effecten van ruimteweer*

Effecten van ruimteweer fenomenen manifesteren zich op verschillende manieren: [44]

1. Satellieten bewegen zich buiten de bescherming van de atmosfeer van de aarde en kunnen door snelle deeltjes (tijdelijk) uitvallen. Dit heeft een directe impact op een vitaal proces (Plaats- en tijdsbepaling middels GNSS).
2 De ionosfeer van de aarde wordt gevormd door extreem ultraviolet en röntgenlicht van de zon, en door snelle deeltjes vanuit de magnetosfeer. Hierdoor kan de ionosfeer ernstig worden verstoord als gevolg van ruimteweer. Bij verstoringen in de ionosfeer kunnen satellietservices zoals GPS en Galileo onnauwkeuriger worden of wegvallen. Deze effecten betreffen niet alleen navigatiediensten (plaats en tijd), maar ook verschillende vormen van telecommunicatie. Vergelijkbare effecten kunnen optreden door variaties in de zonnewind, maar ook weersinvloeden van lager in de atmosfeer hebben hun invloed in de ionosfeer. Ionosfeerverstoringen zullen mogelijk leiden tot verstoringen in vitale processen.

41 Het wild card scenario ruimteweer is tot stand gekomen in zeer nauwe samenwerking met het KNMI.

42 Jean Lilensten, Anna Belehaki, Mauro Messerotti, Rami Vainio, Jurgen Watermann, Stefaan Poedts (eds), COST 724 final report. Developing the scientific basis for monitoring, modeling and predicting Space Weather (Brussels: COST, 2008), *https://www.researchgate.net/publication/278777800_COST_724_final_report_Developing_the_scientific_basis_for_monitoring_modelling_and_predicting_Space_Weather*.

43 Voorbeelden die zijn gebruikt ter inspiratie: 1) Carrington event (1859): heftigste geomagnetische storm ooit waargenomen, ongecontroleerde stromen door telegraafnetwerken; 2) New York Railroad Storm (1921): ongecontroleerde stromen door telegraafnetwerken, meerdere branden ontstaan; 3) Radio- en radarverstoringen tijdens de Koude Oorlog (mei 1967): radio uitval en geomagnetische stormen zorgen voor grote problemen in defensiesystemen; 4) Quebec (1989): zes miljoen mensen negen uur lang zonder stroom; 5) Halloween zonnestorm (2003): elektriciteitsstoring in Zweden, geen communicatie boven polen, satellieten aangetast; 6) 2012: protonenstorm zorgt voor communicatieverlies en verhoogde stralingsdoses voor vluchten boven de polen; 7) 2015: een solar radio burst legt vliegvelden in Europa plat; en 8) 2017: het Europees EGNOS systeem (belangrijk voor vliegtuignavigatie) is tijdelijk onbruikbaar.

44 Ruimteweer effecten zullen nooit (slechts) nationaal zijn en er zijn mogelijk ketenafhankelijkheden met effecten in omringende landen.

3. Tenslotte is er de impact van een CME. Deze verstoort het magneetveld van de aarde zodanig dat er sterke stromen en elektrische spanningen worden opgewekt in de ionosfeer en in het aardoppervlak. Indien daar elektrisch geleidende infrastructuur aanwezig is, zoals elektriciteitsnetwerken of een spoorwegnetwerk, dan kan daar verstoring of schade ontstaan, met in uitzonderlijke gevallen bijvoorbeeld de uitval van transformatoren als gevolg.

Daarnaast zijn er kleinere en/of kortdurende effecten. Intense radiostraling (solar radio bursts) verblinden radar- en antennesystemen zodat telecommunicatie verstoord wordt en objecten niet meer zichtbaar zijn op radarsystemen. Dit is vooral een risico voor Air Traffic Managementsystemen van de luchtvaart en voor militaire toepassingen.

**Figuur 1** Oorzaken en effecten ruimteweer

| Oorzaak op de Zon | | | | | Beïnvloedt | Veroorzaakt uitval Verstoring van | Optreden keten effecten |
|---|---|---|---|---|---|---|---|
| *Zonnevlam röntgen* | *Zonnevlam radio* | *Deeltjesstorm* | *CME* | *Zonnewind coronal hole* | | | |
| | | ++ | + | + | Satelliet direct<br>Vliegtuig direct | Satellietiensten<br>Risico pasagiers | + |
| +++ | | + | +++ | ++ | Magnetosfeer/ ionosfeer | Satelietdiensten:<br>- navigatie<br>- satcom<br>Telecommuni-catie algemeen | +++ |
| | | | ++++ | | Elektrische spanningen in aardkorst | Netwerken:<br>- elekctriciteit<br>- spoorweg | +++ |
| | +++ | | | | Antenne/radar system direct. | Navigatie-diensten<br>Air traffic<br>Telecom-municate | + |
| Direct | Direct | Direct | 20-72 uur | 2-4 dagen | **Reactietijd** | | |
| Minuten-uren | Tiental minuten | Uren-dagen | Dagen | Dagen | **Tijdspan oorzaak** | | |

Vanuit satellieten kan direct worden gesignaleerd dat een zonnevlam of deeltjesstorm optreedt. Voor variaties in de zonnewind en bij het optreden van een CME is er voldoende tijd (uren tot dagen) om maatregelen te nemen, al bestaan er bij het maken van verwachtingen nog erg grote onzekerheden wat betreft de timing en sterkte van de impact.

Ruimteweer leidt als natuurlijke oorzaak tot meerdere vormen van verstoring en uitval van verschillende systemen op aarde, waaronder systemen die onderdeel zijn van vitale processen. In bovenstaande Figuur 1 wordt per oorzaak op de zon in de kolom met het kopje “Beïnvloedt” aangegeven hoe sterk die aangrijpt op een systeem (satelliet, vliegtuig, antenne of radar) of deel van de aarde (magnetosfeer, ionosfeer, aardkorst). In de kolom “Veroorzaakt uitval/ verstoring van” wordt de (vitale) sector of het systeem vermeld die (vaak) door meerdere vitale processen wordt gebruikt. De rechterkolom geeft de waarschijnlijkheid van optreden van keteneffecten aan. Onderaan wordt de beschikbare reactietijd aangegeven per oorzaak en de typische duur van het verschijnsel (niet de duur van de impact). De tabel geeft aan dat verstoringen in de magnetosfeer of ionosfeer verschillende oorzaken kunnen hebben, maar wel leiden tot hetzelfde type uitval of verstoring. Belangrijkste gevolgen zijn uitval van

satellietdiensten en het elektriciteitsnetwetwerk, verlies van tijdcode uit het navigatiesignaal [45] en het wegvallen van telecommunicatie. Alle andere effecten zijn eerder lokaal (een verstoord radarsysteem, spoorweg vertragingen, e.d.). Rode plusjes benadrukken dat het om mondiale verschijnselen gaat met corresponderende mondiale consequenties.

Het KNMI is verantwoordelijk voor het uitgeven van waarschuwingen voor gevaarlijk ruimteweer. Het KNMI werkt samen met internationale partners, zoals Met Office (VK), en staat ook in nauw contact met deze organisaties in geval van dreigend ruimteweer. De ruimteweer berichten (notificaties) worden afgenomen door het Departementaal Coördinatiecentrum Crisisbeheersing (DCC) van het Ministerie van I&W. Het DCC is verantwoordelijk voor de verdere verspreiding van de waarschuwingen binnen hun netwerk (vitale sectoren en andere departementen). De vitale sectoren zijn zelf verantwoordelijk voor het mitigeren van de mogelijke impact.

Voor de effecten gebruikt het KNMI in haar berichten aanduidingen op internationaal gebruikte ruimteweerschalen van 1-5:

- Zonnevlammen (Röntgen) R1 t/m R5
- Deeltjesstormen S1 t/m S5
- Geomagnetische stormen G1 t/m G5 (verstoringen door zonnewind en CME)

*Bouwstenen*

In onderstaande Tabel 18 staan de bouwblokken voor het ruimteweer wild card scenario.

**Tabel 18** Bouwstenen wild card scenario ruimteweer

| Oorzaak | Type verstoring | Verstoorde vitale processen | Vitale processen verstoord door cascade effecten | Schaal brongebied | Schaal effect gebied | Duur |
|---|---|---|---|---|---|---|
| Natuurlijke verstoring | Common-cause | Landelijk transport, distributie en productie elektriciteit | Landelijk transport, distributie en productie elektriciteit | Internationaal | Internationaal | 1 tot 4 weken |
| | | Plaats- en tijdsbepaling middels GNSS | Regionale distributie elektriciteit | | | |
| | | Vlucht- en vliegtuig afhandeling | Gasproductie, landelijk transport en distributie gas | | | |
| | | | Regionale distributie gas | | | |
| | | | Internettoegang en dataverkeer | | | |
| | | | Spraakdiensten en SMS (mobiel en vast) | | | |
| | | | Toonbankbetalingsverkeer | | | |
| | | | Massaal giraal betalingsverkeer | | | |
| | | | Hoogwaardig betalingsverkeer tussen banken | | | |
| | | | Effectenverkeer | | | |
| | | | C2000 | | | |
| | | | Inzet politie | | | |

45 Cap Gemini Consulting, Inventarisatie Kwetsbaarheden Uitval Satellieten. Synthese Rapport (Den Haag: Ministerie van Infrastructuur en Milieu, 2016), *https://www.eerstekamer.nl/overig/20121113/bijlage_9_synthese_rapport/document3/f=/vkh7ivszouz2.pdf*.

*Verhaallijn* [46]

### Eerste activiteiten rondom de zon

Op een dag begint een groot actief gebied met zonnevlekken zichtbaar te worden rondom de zon die de komende dagen in toenemende mate in ons gezichtsveld komen te liggen. Enkele gemiddelde (C-klasse, onder R1 niveau) zonnevlammen en een CME worden geobserveerd. Het actieve gebied blijft groeien en krijgt na twee dagen de bèta-gamma-delta classificatie. In 24 uur zijn er vier M-klasse (R1 of R2) zonnevlammen geweest. Op een gegeven moment wordt er een X1.1 (R3) zonnevlam gedetecteerd. Direct is er aan de zonzijde van de aarde een tijdelijke (ongeveer 30 minuten) black-out van HF radiocommunicatie. Ook satellietcommunicatie is soms enigszins verhinderd. Het KNMI volgt de procedures en geeft nog geen waarschuwing af naar DCC.

### De eerste effecten

In de derde tot vijfde dagen blijft het actieve gebied groeien en zijn er meerdere zonnevlammen. Door een solar radio burst (radiostraling) in het frequentiegebied worden radars op vliegvelden verstoord. Hierdoor kan de luchtverkeersleiding gedurende tientallen minuten echte vliegtuigen niet meer onderscheiden van 'valse echo's' en is op een groot aantal vliegvelden in West-Europa het vliegverkeer volledig ontregeld. Vluchten moeten uitwijken en er ontstaan grote vertragingen die pas in de nacht worden opgelost.

### Een sterke zonnevlam en radio burst

Op dag zes worden om 11:00 uur een zeer sterke X20 (R5) zonnevlam en sterke *radio burst* gedetecteerd. Om 11:13 uur meten meerdere neutronenmonitor grondstations een *ground level enhancement* en om 11:15 uur wordt er door satellieten nabij de aarde een grote hoeveelheid protonen gemeten: er is sprake van een S4 protonenstorm. Het KNMI geeft waarschuwingen af voor de zonnevlam en de protonenstorm aan het DCC van Ministerie I&W.

Beide fenomenen hebben direct hun weerslag. Voor een periode van enkele uren ligt alle HF communicatie stil aan de zonzijde van de aarde. Afgelegen (marine)schepen en vliegtuigen hebben geen contact met de buitenwereld. Ook is satellietcommunicatie niet mogelijk door de ionosferische verstoringen. GNSS kan enkele uren niet worden gebruikt. De protonenstorm zorgt voor een verhoogde stralingsdosis van passagiers en bemanning in vliegtuigen, vooral rond de polen en bij grote hoogte. De protonenstorm zorgt voor onverwachte/incorrecte computerresultaten (single events) in satellieten en vliegtuigen. Diverse (internationale) media berichten over de verschillende effecten en onzekerheden en er heerst paniek onder de bevolking, wat gaat er komen?

### Voorspelling van aankomende CME

Om 16:00 uur wordt er via coronograafbeelden van satellieten duidelijk dat er ook een CME ontstaat en ruimteweersvoorspellers simuleren de CME. Het KNMI houdt simulaties van internationale collega's over deze CME in de gaten. Op Twitter wordt gesproken over een *electronic armageddon*. Dit leidt tot nog grotere onrust en onzekerheid over wat er nog meer gaat komen.
Om 19:00 uur zijn de simulatieresultaten van het Britse Met Office binnen. Het gaat om een zeer snelle CME gericht op de aarde. Een extreme geomagnetische storm wordt verwacht, al is er nog veel onzekerheid over de precieze karakteristieken van de CME. Het KNMI geeft een waarschuwing uit naar DCC. Op dag zeven om 03:50 uur wordt er een schok gemeten door een satelliet. Omdat de CME zo snel is, komt hij 15 minuten later om 04:05 uur aan op aarde. Om 06:00 uur wordt er een G5 (hoogste categorie) alarm afgegeven door het KNMI.

### De CME impact

*Geomagnetically induced currents* zorgen voor problemen in transformatoren in het elektriciteitsnetwerk.
De netbeheerder was gelukkig op tijd gewaarschuwd en slaagt erin de situatie onder controle te houden. Door de slechtere geleidbaarheid van de bodem, een andere topologie van het elektriciteitsnetwerk en door de ligging van Nederland (effect sterker op hogere breedtegraden) is de impact groter in andere Europese landen. Omdat Nederland is aangesloten op het Europese net, moet er actief gecorrigeerd worden om schommelingen in de netspanning tegen te gaan. De verbinding met een groot noordelijk gelegen windmolenpark gaat stuk, Duitse gascentrales schalen op om het tekort op te vangen. Ook een gastransportbedrijf meet elektrische stromen die door hun pijpleidingen lopen, dit levert vooralsnog geen problemen op. Een aantal zendmasten valt tijdelijk uit, maar Internet en telefoonverkeer kan worden omgeleid. Whatsapp en Facebook zijn onbereikbaar vanwege een storing bij een belangrijk Europees datacentrum. Het is onduidelijk of dit te maken heeft met de geomagnetische storm, een overbelasting door het berichtenverkeer of iets anders.

HF radiocommunicatie en satellietnavigatie zijn niet of zeer beperkt mogelijk gedurende meerdere dagen.
De Nederlandse luchtverkeersleiding is onlangs (zomer 2021) overgestapt op satellietnavigatie. De voorheen gebruikte fysieke grondbakens worden gereviseerd en zijn niet bruikbaar. Gedurende enkele uren is landen op Schiphol niet mogelijk omdat satellietnavigatie niet beschikbaar is, vluchten moeten uitwijken of aan de grond blijven. Alle poolvluchten worden geannuleerd omdat geen HF communicatie mogelijk is.

[46] Gebaseerd op ESA technical note SSA-SWE-NCPA-I, aangepast voor de Nederlandse situatie.

Nederlandse militaire operaties hebben moeite om orders uit Nederland te ontvangen. Omdat veel financiële transacties afhankelijk zijn van de precieze tijdstempels uitgegeven door GNSS-systemen, besluit een aantal internationaal opererende banken en instituten alle handel stil te leggen totdat de storm voorbij is. Er heerst paniek en er komt een run op de supermarkten en benzinestations, pinbetalingen zijn niet mogelijk. Bij de poging om nog een laatste fles water of liter brandstof te bemachtigen ontstaan enkele schermutselingen.

Een groot aantal satellieten raakt beschadigd of functioneert tijdelijk niet naar behoren. Een aantal hiervan is permanent beschadigd. Sommige tv-kanalen kunnen alleen nog via internet worden bekeken vanuit Nederland. Vanwege de grote vraag raken sommige van deze websites overbelast.

**Het einde is in zicht**

Op dag acht begint het actieve gebied op de zon te krimpen, maar behoudt dezelfde classificatie. Meerdere C-klasse zonnevlammen blijven ontstaan, maar er worden geen nieuwe CMEs waargenomen. Ook de protonenstorm lijkt af te nemen, al blijven de niveaus boven de drempelwaarden, en de geomagnetische storm neemt af. Ruimteweersvoorspellers waarschuwen voor aanhoudende geomagnetische instabiliteit, maar geven aan dat de situatie verbetert.

Operatoren van satellieten slagen er in veel gevallen in om met correctieve acties hun systemen weer werkend te krijgen. Op hogere breedtegraden blijft HF communicatie moeilijk. Op dag 9 daalt de flux van protonen weer onder de drempelwaarde en de protonenstorm is voorbij. Ook de geomagnetische storm is over nu de magnetometer grondstations weer rustige condities meten. In de dagen hierna draait het actieve gebied op de zon verder ten opzichte van de centrale meridiaan. Het gebied blijft magnetisch verbonden met de aarde en eventuele *solar energetic particles* kunnen nog steeds op aarde aankomen. De kans op een tweede CME die op de aarde is gericht is vrijwel verdwenen. Op de rand van de zon doemen nieuwe actieve gebieden op, maar die zijn dit keer gelukkig minder groot. De impact van uitval zal in veel gevallen nog wat langer aanhouden nu het ruimteweer voorbij is, maar langzaam zal het leven weer verder gaan.

*Inschatting van de impact en waarschijnlijkheid*

Een dergelijk ruimteweerfenomeen komt eens in de 150 jaar voor. Er is echter grote onzekerheid over hoe vaak een heftige gebeurtenis (à la het Carrington event) voorkomt. Het kan zijn dat een gebeurtenis met lichtere vormen van de ruimteweerfenomenen dan die in de wild card zijn toegelicht wat vaker kan voorkomen. In de komende 5 jaar zitten we in een zonnemaximum, dus de kans is wellicht wat hoger (hoewel het de laatste 20 jaar wel een stuk rustiger is).

Er is een potentieel direct effect op enkele vitale processen, zoals elektriciteit en plaats- en tijdsbepaling. Afhankelijk van de mate en de duur van verstoringen in de elektriciteitsvoorziening, kunnen diverse keteneffecten optreden (zie ook paragraaf 5.1.2). Ook de verstoringen in plaats- en tijdsbepaling middels GNSS zorgen voor keteneffecten op andere vitale processen (zoals in de financiële sector, de vlucht- en vliegtuigafhandeling en de openbare orde en veiligheid (onder meer C2000 zal hinder ondervinden)).

De ruimteweer fenomenen kunnen er ook voor zorgen dat het radiospectrum tijdelijk verstoord raakt. Hierdoor kunnen zendmasten en radarsystemen uitvallen en kan het ruisniveau in specifieke frequentiebanden omhoog gaan. Deze effecten kunnen leiden tot verstoring van Internettoegang en datadiensten, spraakdienst en SMS. De verwachting is dat niet alle zendmasten in één keer uitvallen, waardoor dataverkeer kan worden omgeleid. Internettoegang en dataverkeer zullen dus gedeeltelijk worden verstoord, maar niet geheel uitvallen. Hetzelfde geldt voor de scheepvaartafwikkeling, dat beperkte hinder zal ondervinden door het uitvallen van radarsystemen. Het ruimteweer en de uitval of verstoring van vitale processen zal ook andere impact op de nationale veiligheid teweeg brengen. Dit is deels wederom afhankelijk van de mate waarin voorzieningen als elektriciteit en betalingsverkeer uitvallen.

De fysieke veiligheid kan zeer beperkt worden aangetast, omdat er een hele kleine kans is dat mensen kanker krijgen door de protonenstorm waar mensen in vliegtuigen aan worden blootgesteld (de protonen dringen niet door tot het aardoppervlak). In een dergelijke situatie wordt het waarschuwingssysteem voor de civiele luchtvaart geactiveerd, met de boodschap om lager of via een andere route te vliegen. Door de uitval van satellietnavigatie is de luchtverkeersleiding ontregeld, waardoor ongelukken op vliegvelden plausibel kunnen zijn.

Het is te verwachten dat er maatschappelijke angst en onrust zal ontstaan. Mensen gaan mogelijk hamsteren in supermarkten of zelfs plunderen, aangezien men geen boodschappen kan doen als het betalingsverkeer verstoord is. De politie is bovendien mogelijk minder snel ter plaatse bij plunderingen door verstoringen van C2000. Er is echter een waarschuwingssysteem, dus mensen weten wat er gaat komen en kunnen zich enigszins voorbereiden. Door de onbekendheid met het fenomeen ruimteweer zal anderzijds des- en misinformatie kunnen toenemen wat kan leiden tot polarisatie.

Afhankelijk van de duur en mate van verstoring van vitale processen (zoals elektriciteit), zullen er waarschijnlijk voornamelijk herstelkosten zijn vanwege schade aan infrastructuur en het stil komen te liggen van processen. Het zou kunnen dat transformatorstations doorbranden, die beperkt voorradig zijn en dus voor langere tijd uitvallen (met mogelijk keteneffecten), maar dit is zeer onzeker.

Tot slot, ruimteweer kent een mondiale impact, bij reeds instabiele landen in de ring van Europa is er de mogelijkheid dat herstel van uitval of schade zeer traag verloopt.

*Relevante ontwikkelingen*

Bewustzijn en kennis van kwetsbaarheden als gevolg van ruimteweer zijn van belang op de korte en lange termijn. We begeven ons de komende jaren in een actieve zonnecyclus waarbij gevolgen die hierboven beschreven zijn realistisch zijn. Zeker gezien onder meer de komst van intelligent transport systems (zelfrijdende auto's, schepen met minimale bezetting, etc.), het toenemende belang van de ruimte (zowel civiel als militair), de ontwikkelingen in de telecommunicatie (5G, 6G op termijn, *virtual reality, videoconferencing*) en grootschalige aanpassingen van elektriciteitsnetwerken vanwege de klimaatdoelstellingen, is het cruciaal om dergelijke kwetsbaarheden in act te nemen. Ook voor thema's als *space traffic management* van lage satellieten en *space debris* speelt ruimteweer een belangrijke rol.

## 7.2 Beschouwing

Deze dreigingscategorie gaat in op het fenomeen dat er vanuit een natuurlijke oorzaak, zoals een overstroming, natuurbrand of extreem weer, verstoring van één of meerdere vitale processen ontstaat (common cause). Als gevolg hiervan kunnen ook andere vitale processen verstoord raken (keteneffecten). Het overstromingsscenario en natuurbrandscenario laten zien dat veel verschillende vitale processen direct verstoord kunnen raken, al zal de daadwerkelijke impact altijd afhankelijk zijn van de locatie van vitale objecten (al dan niet aanwezig binnen het effectgebied van het incident). Met name de verstoring van elektriciteit en telecommunicatie veroorzaken ook keteneffecten, zo kunnen bijvoorbeeld door verstoring van de elektriciteitsvoorziening ook problemen optreden met de drinkwatervoorziening. Verstoringen in de telecommunicatie kunnen de werkzaamheden van hulpdiensten bij dit type rampen bemoeilijken. De verstoring van dit type vitale infrastructuur leidt tot ernstige impact omdat er vaak een gebrek ontstaat aan primaire levensbehoeften en een ernstige verstoring van het dagelijks leven.

Ook het fenomeen ruimteweer kan een natuurlijke verstoring van vitale processen teweeg brengen, al is de impact lastig in te schatten. Deels is de impact afhankelijk van de mate waarin een vitaal proces als elektriciteit verstoord raakt, maar deels is de impact lastig in te schatten doordat een dergelijk grootschalig fenomeen zoals in de wild card is beschreven, in de moderne tijd nog niet is voorgekomen. Er zijn meerdere studies gedaan naar de mogelijke gevolgen van satellietuitval, maar de daadwerkelijke impact op het functioneren van vitale processen (en de Nederlandse maatschappij in het algemeen), blijft veelal onzeker.

Voor alle scenario's geldt dat met name ernst en duur van de verstoring van de elektriciteitsvoorziening bepalend zijn voor de impact, waarbij ook de specifieke locatie een belangrijke rol speelt. Afhankelijk van de plek en welke vitale objecten geraakt worden (bijvoorbeeld hoogspanning of niet), kan sprake zijn van een relatief kleine verstoring of juist van grootschalige uitval.

# 8. Sluimerende dreiging

Er is in toenemende mate schaarste op de arbeidsmarkt en in het bijzonder is er een tekort aan personeel in specifieke beroepsgroepen, waaronder personeel met technische expertise. Op de langere termijn kan dit voor problemen zorgen, waaronder voor de continuïteit van vitale processen.

In de cybersecurity gemeenschap wordt al langere tijd de zorg geuit dat het gebrek aan personeel toeneemt, zowel op het gebied van technische als niet-technisch gerelateerde banen. [47] Dit zorgt ervoor dat organisaties zich niet goed kunnen voorbereiden op cyberaanvallen, wat het risico op een impactvolle verstoring vergroot. Concurrentie onder werkgevers kan ertoe leiden dat arbeidskrachten voor bepaalde organisaties moeilijker aan te trekken zijn, bijvoorbeeld omdat zij gebonden zijn aan vaste salarisschalen.

Deze ontwikkelingen kunnen er toe leiden dat aanbieders van vitale infrastructuur onvoldoende gekwalificeerd personeel kunnen aantrekken. Dit kan ervoor zorgen dat vitale aanbieders kwetsbaar worden omdat ze geen capaciteit hebben om *state-of-the-art* systemen te installeren en good practices rondom digitale veiligheid binnen de organisatie in te voeren en te behouden.

Ook kan het gebrek aan technische kennis over het aansturen en onderhouden van systemen op de lange termijn problemen opleveren. Processen binnen vitale infrastructuur worden steeds vaker automatisch aangestuurd en deze automatisering heeft een transformerend effect op de arbeidsmarkt, wat ertoe kan leiden dat bedrijven te weinig arbeidskrachten met de juiste vaardigheden kunnen aantrekken. [48]

Het automatiseren van processen zorgt voor efficiëntie, maar ook voor een gebrek aan flexibiliteit en aanpassend vermogen. [49] In het geval van een incident is juist menselijk ingrijpen nodig om de verstoring op te vangen. Het is dus van cruciaal belang dat er genoeg gekwalificeerd personeel is om in te grijpen wanneer dat nodig is. Het gebrek aan de juiste expertise kan er toe leiden dat de terugvalmogelijkheden in het geval van een incident of crisis beperkt zijn. Wanneer bijvoorbeeld de geautomatiseerde bediening van bruggen/sluizen uitvalt, moet men op handmatige aansturing van objecten kunnen overgaan. De mogelijkheid bestaat dat er niet genoeg personeel is om de objecten handmatig aan te sturen, of dat niet de juiste kennis voor handen is om de bron van de verstoring op te lossen. Dit zou tot gevolg hebben dat een incident niet adequaat of tijdig opgelost kan worden, of dat er een grotere impact is dan wanneer er voldoende personeel met de benodigde expertise beschikbaar zou zijn.

Daarnaast kan de combinatie van enerzijds toenemende complexiteit en afhankelijkheden binnen systemen er voor zorgen dat er bij het merendeel van het personeel onvoldoende inzicht meer is in de precieze werking van systemen. Dat kan als resultaat hebben dat men geen zicht meer heeft op de gevolgen die aanpassingen aan de infrastructuur kunnen hebben op het functioneren van een systeem (of systemen die er van afhankelijk zijn). Er is zeer specifieke kennis en expertise vereist is om systemen aan te sturen, te onderhouden of te reageren op incidenten en als die kennis en expertise niet voldoende beschikbaar is kan dit leiden tot ernstige problemen.

47 Borka Jerman Blažič, "The cybersecurity labour shortage in Europe: Moving to a new concept for education and training," Technology in Society 67 (2021), *https://doi.org/10.1016/j.techsoc.2021.101769*; Jan Piet Barthel en Floor Frederiks, Cybersecurity-onderzoek aan universiteiten, wetenschappelijke kennisinstituten en hogescholen. Een kwalitatieve en kwantitatieve sterkte-zwakte analyse, (Den Haag: NWO, 2020), *https://www.rijksoverheid.nl/documenten/rapporten/2020/04/09/cybersecurity-onderzoek-aan-universiteiten-wetenschappelijke-kennisinstituten-en-hogescholen*.

48 ANV, Horizonscan Nationale Veiligheid 2020, (Bilthoven: RIVM, 2020), *https://www.rivm.nl/sites/default/files/2020-11/Horizonscan%20Nationale%20Veiligheid%202020.pdf*.

49 Curtis J. Marshall, Blake Roberts, Michael W. Grenn, Thomas H. Holzer, "Context-based automation of critical infrastructure systems for efficiency, stakeholder equity, and resilience," Systems Engineering 23, no. 5 (september 2020): 617-632, *https://doi.org/10.1002/sys.21552*.

# 9. Slotbeschouwing

Vitale infrastructuur is nauw verbonden met veel verschillende dreigingen voor de nationale veiligheid. De vitale processen die gezamenlijk de Nederlandse vitale infrastructuur vormen zijn vitaal omdat uitval of verstoring ervan al gauw leidt tot maatschappelijke ontwrichting. Het is dan ook logisch dat de impact van veel verschillende dreigingstypen voor een deel ontstaat door verstoringen van vitale infrastructuur. De scenario's die binnen dit thema worden behandeld laten zien dat hier een grote verscheidenheid van dreigingen is. Zo wordt ingegaan op en terroristische- en cyberaanvallen, maar ook op natuurlijke verstoringen als overstromingen en natuurbranden, technisch of menselijk falen en een fenomeen als ruimteweer. Ook in veel andere dreigingsthema's wordt impact op vitale infrastructuur geadresseerd (bijvoorbeeld in de thema's klimaat- en natuurrampen, cyberdreigingen, ongewenste inmenging en ondermijning democratische rechtsstaat, en economische bedreigingen). In Figuur 2 staat het risicodiagram voor het thema b*edreiging vitale infrastructuur*.

**Figuur 2:** Risicodiagram thema bedreiging vitale infrastructuur

| | | | | | |
|---|---|---|---|---|---|
| **Catastrofaal** | | | | | |
| **Zeer ernstig** | | • Keteneffecten elektriciteitsuitval | • Overstroming rivier (uit thema klimaat- en natuurrampen) | | |
| **Ernstig** | • Ransomeware telecom | | | • Landelijke black-out | • Natuurbranden (uit thema klimaat- en natuurrampen) |
| **Aanzienlijk** | | | | | |
| **Beperkt** | | | | | |
| | **Zeer onwaarschijnlijk** | **Onwaarschijnlijk** | **Enigzins waarschijnlijk** | **Waarschijnlijk** | **Zeer waarschijnlijk** |

De analyse bevestigt opnieuw het beeld dat we als samenleving sterk afhankelijk zijn van vitale processen, waarbij vitale processen in de energiesector en telecomsector eruit springen vanwege de vele afhankelijkheden hiervan in de samenleving. Net als vrijwel alle delen van de samenleving wordt ook de vitale infrastructuur steeds afhankelijker van digitale systemen. Tegelijkertijd is het belangrijk om te realiseren dat deze afhankelijkheden niet statisch zijn, maar kunnen veranderen. De complexiteit van systemen en afhankelijkheden tussen systemen en processen nemen steeds verder toe waardoor het moeilijk is om een goede inschatting te maken van de gevolgen van gebeurtenissen zoals beschreven in de scenario's, aangezien er veel onderlinge, verborgen afhankelijkheden binnen en tussen processen bestaan. Bovendien zorgen de veranderlijkheid in het gebruik en de constante technologische ontwikkeling en vernieuwing van systemen en infrastructuur ervoor dat het een uitdaging is om constant zicht te blijven houden op deze afhankelijkheden.

Op de langere termijn kunnen schaarste op de arbeidsmarkt en in het bijzonder gebrek aan technisch geschoold personeel, bijvoorbeeld op het gebied van cybersecurity of benodigde kennis en expertise om de energietransitie vorm te geven, ervoor zorgen dat er onvoldoende capaciteit is om de weerbaarheid van vitale infrastructuur op peil te houden. Dit wordt dan ook gezien als een sluimerende dreiging.

Kijkend naar de dreigingen met betrekking tot de vitale infrastructuur voor de komende vijf jaar komt naar voren komt dat zowel statelijke actoren als cybercriminelen een steeds grotere bedreiging vormen voor de continuïteit van vitale processen. Vanwege de belangrijke maatschappelijke rol van vitale processen zijn ze een aantrekkelijk doelwit van kwaadwillende actoren. Om die reden wordt de bescherming van de continuïteit van de vitale infrastructuur ook steeds meer onderdeel van discussies over strategische autonomie en economische veiligheid.

De waarschijnlijkheid van moedwillige aanvallen op de Nederlandse vitale infrastructuur, zoals uitgewerkt in deze analyse, wordt op dit moment relatief laag ingeschat. Dit heeft deels te maken met de preventieve en mitigerende maatregelen van de vitale aanbieders en deels met de capaciteit en motivatie van actoren die nodig is om doelbewust en doelgericht een dergelijke aanval uit te voeren.

Als het gaat om niet-moedwillige bedreigingen vormen vooral de effecten van klimaatverandering en de energietransitie een bedreiging voor vitale infrastructuur, wat in de komende jaren steeds reëler zal worden en meer impact zal hebben. Door klimaatverandering zullen steeds vaker extreme weersomstandigheden ontstaan, zoals extreme regenval, overstromingen en droogte. De waarschijnlijkheid van verstoring van vitale infrastructuur door een natuurlijke oorzaak zal dan ook steeds verder toenemen.

De energietransitie, in combinatie met geopolitieke ontwikkelingen, zorgt er voor dat er meer en meer ingezet wordt op elektrificatie, maar ook dat er veranderingen plaatsvinden in de manier waarop elektriciteit wordt geproduceerd en gedistribueerd. Met name in de transitiefase kan dit ervoor zorgen dat er onverwachte effecten optreden omdat de ontwikkeling van de infrastructuur continu in beweging is. In onderstaand tekstkader is de energietransitie nader beschreven als overkoepelend onderwerp waarbij meerdere facetten van de nationale veiligheid spelen.

Tenslotte is digitalisering een belangrijke ontwikkeling die ervoor zorgt dat de digitale infrastructuur ook continu aan verandering onderhevig is en dat verbindingen en afhankelijkheden tussen systemen ook dynamisch zijn. Niet alleen de infrastructuur zelf verandert, maar ook het gebruik (en dus de maatschappelijke afhankelijkheid). De COVID-19 pandemie heeft er bijvoorbeeld voor gezorgd dat we massaal zijn gaan thuiswerken, waardoor de Internettoegang voor huishoudens een veel belangrijkere rol kreeg en de datastromen veranderden. Deze dynamieken zorgen ervoor dat de directe impact en keteneffecten van uitval of verstoring van een vitaal proces lastig in te schatten is. Bij de voorbereiding op dit type gebeurtenissen is het dan ook van belang om ook altijd rekening te houden met onverwachte effecten.

## Energietransitie

De energietransitie is een ingrijpende verandering waar veel facetten aan zitten die relevant zijn voor de nationale veiligheid. Zo zal het gebruik van bepaalde technieken en stoffen risico's met zich meebrengen, zoals het gebruik van waterstof. Deze risico's heeft het ANV eerder in een studie in kaart gebracht. [50] Daaruit volgde onder andere dat de risico's gekoppeld aan het gebruik van gevaarlijke stoffen voor de nationale veiligheid door de energietransitie niet wezenlijk anders zullen zijn dan in de huidige situatie, alhoewel er op onderdelen zoals het gebruik van waterstof in de woonomgeving expliciet aandacht nodig is. Ook komt naar voren dat met name de transitiefase waarin oude en nieuwe technieken naast elkaar bestaan en steeds meer met elkaar geïntegreerd gaan worden tot (onverwachte) knelpunten kan leiden. [51]

Qua technieken zijn onder meer windenergie en kernenergie relevant, met als optie de ontwikkeling van nieuwe kerncentrales. De risico's hiervan zijn in het thema *zware ongevallen* in kaart gebracht, waaruit volgt dat de waarschijnlijkheid van ongevallen extreem klein is. Los van de vraag naar de risico's van een centrale an sich, zal een besluit om een nieuwe centrale tot maatschappelijke ophef kunnen leiden. Voor windenergie geldt dat er ingezet wordt op windparken in de Noordzee. Het aantal windparken op zee zal toenemen, waardoor ook de kans op ongevallen van scheepvaart op de windparken toeneemt, zodat er nagedacht wordt over de beveiliging van deze parken. [52] Naast ongevallen op de Noordzee die via de windparken de energievoorziening kunnen raken, kan er sprake zijn van moedwillige dreigingen. HCSS wijst in hun rapport op de dreiging dat componenten van de vitale infrastructuur, waaronder windparken op zee, doelwit kunnen zijn van o.a. cyberaanvallen en sabotage. [53]

Elektrificatie is één van de pijlers van de energietransitie. Er zal steeds meer gebruik worden gemaakt van elektriciteit in plaats van bijvoorbeeld gas of olie, denk bijvoorbeeld elektrisch vervoer. Dit leidt tot een grotere afhankelijkheid van en druk op het elektriciteitsnet. Dit kan op sommige plaatsen tot capaciteitsproblemen leiden en kan de kans op verstoringen vergroten.

Omdat onze maatschappij sterk afhankelijk is van de elektriciteitsvoorziening zijn vragen rondom betrouwbaarheid en leveringszekerheid relevant. Een verstoring kan grote impact hebben op de nationale veiligheid (zoals ook blijkt uit de twee scenario's die binnen het thema bedreiging vitale infrastructuur zijn uitgewerkt met betrekking tot de elektriciteitsvoorziening). Met het oog op de energietransitie zijn technische aspecten van belang zoals het omgaan met verschillen tussen vraag en aanbod (van verschillende bronnen op verschillende momenten) en de beschikbare netwerkcapaciteit, zeker gezien de genoemde elektrificatie. Voor de aansturing en optimalisatie zal technologie als smart grids en AI een belangrijke rol kunnen vervullen, waardoor aandacht moet zijn voor potentiële kwetsbaarheden gerelateerd aan cyberaanvallen.

Tenslotte zijn vraagstukken rondom afhankelijkheid, kosten en draagvlak van belang. Dit raakt onder andere de economische veiligheid. Zo is het verstandig om in een vroeg stadium stil te staan bij de vraag over de afhankelijkheid van bronnen, materialen, technologie en (buitenlandse) actoren, waarvan de afhankelijkheid van Russisch gas een actueel voorbeeld is. De betaalbaarheid en de kosten van de energietransitie met daaraan gerelateerd vragen over de verdeling hiervan zijn onderwerpen die raken aan de haalbaarheid van en het draagvlak voor de energietransitie in de maatschappij. Discussies rondom de plaatsing van windturbines laten zien dat draagvlak een belangrijk issue is en dat de energietransitie ook voeding kunnen zijn voor spanningen in de samenleving, wat vervolgens kan leiden tot polarisatie en extremisme. Ook de haalbaarheid van de transitie zelf, met de beschikbaarheid van voldoende materialen en technisch personeel is een aandachtspunt.

Samenvattend betekent bovenstaande dat bij de energietransitie veel vraagstukken naar voren komen die vanuit het perspectief van de nationale veiligheid relevant zijn en integraal aandacht behoeven. Juist in de fase waarin keuzen worden gemaakt over de energietransitie kan invulling worden gegeven aan '*safe and secure by design*'.

50 ANV, Verkenning risico's van de energietransitie voor de nationale veiligheid (Bilthoven: RIVM, 2019), *https://www.rivm.nl/sites/default/files/2019-10/Verkenning%20risicos%20energietransitie%202019.pdf*.

51 Idem.

52 Heleen Ekker, "'Vangrails' op zee kunnen botsing met windmolens voorkomen," NOS (18 maart 2022), *https://nos.nl/artikel/2421741-vangrails-op-zee-kunnen-botsing-met-windmolens-voorkomen*.

53 Frank Bekkers, Joris Teer, Dorith Kool, Lucia van Geuns, Patrick Bolder, Irina Patrahau, en Max Sarel, The High Value of the North Sea (Den Haag: HCSS, 2021), *https://hcss.nl/report/high-value-of-the-north-sea/*.

# Bronnenlijst


Agentschap Telecom. *Verbinding, vertrouwen, vooruitgang. Jaarbericht 2020*. Den Haag: Agentschap Telecom, 2021. *https://www.agentschaptelecom.nl/documenten/jaarverslagen/2021/05/26/jaarbericht-2020*.

AIVD. *Jaarverslag 2018*. Den Haag: AIVD, 2019. *https://www.aivd.nl/documenten/jaarverslagen/2019/04/02/jaarverslag-aivd-2018*.

AIVD, MIVD, NCTV. *Dreigingsbeeld statelijke actoren*. Den Haag: AIVD, MIVD, NCTV, 2021. *https://www.rijksoverheid.nl/documenten/rapporten/2021/02/03/dreigingsbeeld-statelijke-actoren*.

ANV. *Horizonscan Nationale Veiligheid 2020*. Bilthoven: RIVM, 2020. *https://www.rivm.nl/sites/default/files/2020-11/Horizonscan%20Nationale%20Veiligheid%202020.pdf*.

ANV. *Leidraad Risicobeoordeling Rijksbrede Risicoanalyse Nationale Veiligheid*. Bilthoven: RIVM, 2022. https://www.rivm.nl/onderwerpen/nationale-veiligheid.

ANV. *Verkenning risico's van de energietransitie voor de nationale veiligheid*. Bilthoven: RIVM, 2019. *https://www.rivm.nl/sites/default/files/2019-10/Verkenning%20risicos%20energietransitie%202019.pdf*.

Barthel, Piet en Frederiks, Floor. *Cybersecurity-onderzoek aan universiteiten, wetenschappelijke kennisinstituten en hogescholen. Een kwalitatieve en kwantitatieve sterkte-zwakte analyse*. Den Haag: NWO, 2020. *https://www.rijksoverheid.nl/documenten/rapporten/2020/04/09/cybersecurity-onderzoek-aan-universiteiten-wetenschappelijke-kennisinstituten-en-hogescholen*.

Bekkers, Frank, Joris Teer, Dorith Kool, Lucia van Geuns, Patrick Bolder, Irina Patrahau, en Max Sarel. *The High Value of the North Sea*. Den Haag: HCSS, 2021. *https://hcss.nl/report/high-value-of-the-north-sea/*.

Bettinger, Kimmy. "COVID-19: emerging technologies are now critical infrastructure – what that means for governance". World Economic Forum, 10 april, 2020. *https://www.weforum.org/agenda/2020/04/covid-19-emerging-technologies-are-now-critical-infrastructure-what-that-means-for-governance/*.

Beveiliging Nieuws. "Ransomwarebende opgerold na aanvallen op vitale infrastructuur." *Beveiliging Nieuws*, 29 oktober 2021. *https://beveiligingnieuws.nl/ransomwarebende-opgerold-na-aanvallen-op-vitale-infrastructuur/*.

Blažič, Borka Jerman. "The cybersecurity labour shortage in Europe: Moving to a new concept for education and training." *Technology in Society*, 67 (2021): 101769. *https://doi.org/10.1016/j.techsoc.2021.101769*.

Cap Gemini Consulting. *Inventarisatie Kwetsbaarheden Uitval Satellieten. Synthese Rapport*. Den Haag: Ministerie van Infrastructuur en Milieu, 2016. *https://www.eerstekamer.nl/overig/20121113/bijlage_9_synthese_rapport/document3/f=/vkh7ivszouz2.pdf*.

Cyber Security Raad. "Cyberweerbaarheid IACS in Nederland onvoldoende op orde". 29 april 2020. *https://www.cybersecurityraad.nl/actueel/nieuws/2020/04/29/'cyberweerbaarheid-iacs-in-nederland-onvoldoende-op-orde'*.

Cyber Security Raad. "Digitale autonomie Nederland staat onder druk". 14 mei 2021. *https://www.cybersecurityraad.nl/actueel/nieuws/2021/05/14/'digitale-autonomie-nederland-staat-onder-druk'*.

De Bruijn, Karin en Kymo Slager. *Wat als de 'waterbom' elders in Nederland was gevallen? Hackathon Deltares, november 2021*. Deltares, 17 januari 2022. *https://publications.deltares.nl/11206890_010_0006.pdf*.

De Wijk, Rob. *Gaat de Coronacrisis de wereld veranderen?* Den Haag: HCSS, 2021. *https://hcss.nl/report/gaat-de-coronacrisis-de-wereld-veranderen/*.

Dutch Caribbean Legal Portal. "Hackers leggen ziekenhuis Aruba plat". *Dutch Caribbean Legal Portal*, 28 november 2019. *http://www.dutchcaribbeanlegalportal.com/news/latest-news/9386-hackers-leggen-ziekenhuis-aruba-plat*.

Ekker, Heleen. "Klimaatexperts: IPCC-rapport alarmerend voor Nederland." *NOS*, 9 augustus 2021. *https://nos.nl/artikel/2393306-klimaatexperts-ipcc-rapport-alarmerend-voor-nederland*.

Ekker, Heleen. "'Vangrails' op zee kunnen botsing met windmolens voorkomen." *NOS*, 18 maart, 2022. *https://nos.nl/artikel/2421741-vangrails-op-zee-kunnen-botsing-met-windmolens-voorkomen*.

European Commission. *Proposal for a Directive of the European Parliament and of the Council on Measures for a High Common Level of Cybersecurity across the Union*. Brussels: European Commission, December 16, 2020. *https://op.europa.eu/en/publication-detail/-/publication/be0b5038-3fa8-11eb-b27b-01aa75ed71a1*.

European Commission. *Proposal for a Directive of the European Parliament and of the Council on the Resilience of Critical Entities*. Brussels: European Commission, December 16, 2020. *https://ec.europa.eu/home-affairs/system/files/2020-*.

Gijzel, Ties. "Wie beveiligt de bodem van de Noordzee tegen sabotage?." Follow the Money, 4 juni, 2022. *https://www.ftm.nl/artikelen/noordzee-kwetsbaar-voor-sabotage?*.

Kennisportaal Klimaatadaptatie. "Nieuw IPCC-rapport: temperatuur stijgt sneller dan verwacht." 9 augustus 2021,*https://klimaatadaptatienederland.nl/actueel/actueel/nieuws/2021/nieuw-ipcc-rapport/*.

Lilensten, Jean, Belehakim, Anna, Messerotti, Mauro, Vainio, Rami, Watermann, Jurgen and Poedts, Stefaan (eds). COST 724 final report. *Developing the scientific basis for monitoring, modeling and predicting Space Weather*. Brussels: COST, 2008. *https://www.researchgate.net/publication/278777800_COST_724_final_report_Developing_the_scientific_basis_for_monitoring_modelling_and_predicting_Space_Weather*.

Marshall, Curtis, J., Roberts, Blake, Grenn, Michael, W., Holzer, Thomas, H. "Context-based automation of critical infrastructure systems for efficiency, stakeholder equity, and resilience." *Systems Engineering*, 23, 5 (September 2020): 617-632. *https://doi.org/10.1002/sys.21552*.

Masson-Delmotte, V., P. Zhai, A. Pirani, S.L. Connors, C. Péan, S. Berger, N. Caud, Y. Chen, L. Goldfarb, M.I. Gomis, M. Huang, K. Leitzell, E. Lonnoy, J.B.R. Matthews, T.K. Maycock, T. Waterfield, O. Yelekçi, R. Yu, and B. Zhou (eds.), *Climate Change 2021: The Physical Science Basis. Contribution of Working Group I to the Sixth Assessment Report of the Intergovernmental Panel on Climate Change*. Cambridge: Cambridge University Press, 2021. *https://www.ipcc.ch/report/ar6/wg1/downloads*.

Nauta, Hans. "De boosdoener van de 112-storing: een KPN-teller die doortelde totdat het niet meer ging". *Trouw*, 26 juni, 2020. *https://www.trouw.nl/economie/de-boosdoener-van-de-112-storing-een-kpn-teller-die-doortelde-totdat-het-niet-meer-ging~bbbab906/*.

NCTV. *Cybersecuritybeeld Nederland. CSBN 2021. Den Haag: NCTV,* 2021. *https://www.nctv.nl/documenten/publicaties/2021/06/28/cybersecuritybeeld-nederland-2021*.

NCTV. "Economische Veiligheid". Bezocht op 2 maart 2022. *https://www.nctv.nl/onderwerpen/economische-veiligheid*.

NCTV. Midterm review 2021, *Nationale Veiligheid Strategie*. Den Haag: NCTV, 2021. *https://www.rijksoverheid.nl/documenten/rapporten/2021/03/08/tk-bijlage-nvs19-midterm-review-2021*.

NCTV. "Overzicht vitale processen". Bezocht op 2 maart 2022. *https://www.nctv.nl/onderwerpen/vitale-infrastructuur/overzicht-vitale-processen*.

Negreiro, Mar. "The NIS2 Directive. A high common level of cybersecurity in the EU", *EU Legislation in Progress Briefing*. Brussels: European Parliament, 2021. *https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf*.

NOS. "Hackers Universiteit Maastricht zaten maanden in het netwerk, 200.000 euro betaald," *NOS*, 5 februari, 2020. *https://nos.nl/artikel/2321732-hackers-universiteit-maastricht-zaten-maanden-in-netwerk-200-000-euro-betaald*.

NOS. "Netbeheerder waarschuwt: stroomnet bereikt maximum in delen Amsterdam," *NOS*, 24 juni 2021. *https://nos.nl/artikel/2386392-netbeheerder-waarschuwt-stroomnet-bereikt-maximum-in-delen-amsterdam*.

Planbureau voor de Leefomgeving (PBL). *Klimaat- en Energieverkenning 2021*. Den Haag: Planbureau voor de Leefomgeving (PBL), 2021. *https://www.pbl.nl/sites/default/files/downloads/pbl-2021-klimaat-en-energieverkenning-2021-4681.pdf*.

Rijksoverheid. "Extreme wateroverlast in Limburg", 16 juli 2021, *https://www.rijksoverheid.nl/actueel/nieuws/2021/07/16/extreme-wateroverlast-in-limburg*.

Schellevis, Joost en Meindertsma, Ben. "Zeker vijftien ziekenhuizen geïnfecteerd met ransomware," *NOS*, 25 juni, 2021. *https://nos.nl/artikel/2179941-zeker-vijftien-ziekenhuizen-geinfecteerd-met-ransomware*.

Sweijs, Tim, van Manen, Hugo, Kertydova, Katarina, en Bekkers, Frank. *Flow Security and Dutch Defense and Security Policies*. Den Haag: HCSS, 2018. *https://hcss.nl/report/flow-security-and-dutch-defense-and-security-policies/*.

TenneT. "'Vluchtstrook' hoogspanningsnet voor het eerst opengesteld". 11 februari, 2022. *https://www.tennet.eu/nl/tinyurl-storage/nieuws/vluchtstrook-hoogspanningsnet-voor-het-eerst-opengesteld/*.

Turton, W. and Mehrotra, K. "Hackers Breached Colonial Pipeline Using Compromised Password." *Bloomberg*, June 4, 2021. https://*www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password*.

Wiggelinkhuizen, E.J., B. H. Bulder, A.B. Schwedersky, en M.P.W. van Berlo, *Verkenning van toekomstige risico's van het elektriciteitsnet*. Den Haag: TNO, 2021. *https://repository.tudelft.nl/islandora/object/uuid%3Ab39a1668-b2c3-445a-9bd1-c9dce0d57fdc*.

Woetzel, Jonathan, Dickon Pinner, Hamid Samandari, Hauke Engel, Mekala Krishnan, Brodie Boland, Peter Cooper and Byron Ruby. "Will infrastructure bend or break under climate stress?", *McKinsey Global Institute,* 19 augustus, 2020. *https://www.mckinsey.com/business-functions/sustainability/our-insights/will-infrastructure-bend-or-break-under-climate-stress*

# Bijlage 1 Deelnemende organisaties expertsessies

Voor deze analyse zijn expertsessies gehouden waar deelnemers van de volgende organisaties bij betrokken waren.

**Deelnemende organisaties**

- FOX-IT
- KNMI
- KPN
- Ministerie van EZK
- Ministerie van IenW
- Stedin
- TenneT
- TNO

Rijksoverheid

**Analistennetwerk Nationale Veiligheid**
**redactie: TNO**

Dit is een uitgave van:

Het Rijksinstituut voor Volksgezondheid en Milieu (RIVM)
Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek (TNO)
Stichting Nederlands Instituut voor Internationale Betrekkingen 'Clingendael' (Clingendael)
SEO Economisch Onderzoek (SEO)
Algemene Inlichtingen- en Veiligheidsdienst (AIVD)
Militaire Inlichtingen- en Veiligheidsdienst (MIVD)
Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC)

juli 2022

012454