VOORBEREIDEN OP DIGITALE ONTWRICHTING

WRR

Voorbereiden op digitale ontwrichting

Voorbereiden op digitale ontwrichting is een advies aan de regering uit naam van de voltallige Wetenschappelijke Raad voor het Regeringsbeleid. WRR-Rapport 101 is voorbereid en geschreven door:

Prof. mr. J.E.J. Prins (eerstverantwoordelijk raadslid),
Dr. E.K. Schrijvers (projectcoördinator),
Mr. dr. R. Passchier (staflid),
Prof. dr. M. de Visser (raadslid).

De Wetenschappelijke Raad voor het Regeringsbeleid werd in voorlopige vorm ingesteld in 1972. Zijn positie is definitief vastgelegd bij wet van 30 juni 1976 (Stb. 413). De Wetenschappelijke Raad voor het Regeringsbeleid (WRR) is een onafhankelijk adviesorgaan. De WRR informeert en adviseert de regering en het parlement over sectoroverstijgende vraagstukken die grote impact hebben op de samenleving. De adviezen zijn gebaseerd op wetenschappelijke onderzoek en gericht op een lange termijn perspectief.

De huidige zittingsperiode loopt tot 31 december 2022. De samenstelling van de raad is:

Prof. dr. mr. C.C.J.H. Bijleveld (per 1-12-2019)
Prof. dr. A.W.A. Boot,
Prof. dr. mr. M.A.P. Bovens,
Prof. dr. G.B.M. Engbersen,
Prof. dr. S.J.M.H. Hulscher,
Prof. mr. J.E.J. Prins (voorzitter),
Prof. dr. M. de Visser,
Prof. dr. C.G. de Vries,

Secretaris: Prof. dr. F.W.A. Brom.

WRR

WETENSCHAPPELIJKE RAAD VOOR HET REGERINGSBELEID

Voorbereiden op digitale ontwrichting

Wetenschappelijke Raad voor het Regeringsbeleid, Den Haag 2019

Redactie: Hans Hogenkamp, Amsterdam
Uitgever: WRR

Vormgeving binnenwerk: Xerox OBT, Den Haag
Omslagafbeelding: Idee aan Zee, Den Haag
Figuren en tabellen: Idee aan Zee, Den Haag

ISBN 978-94-90186-77-7
e-ISBN 978-94-90186-78-4
NUR 740

Wetenschappelijke Raad voor het Regeringsbeleid
Buitenhof 34
Postbus 20004
2500 EA Den Haag
wrr.nl

WRR

WETENSCHAPPELIJKE RAAD VOOR HET REGERINGSBELEID

Aan de Minister-President
Voorzitter van de Ministerraad
De heer drs. M. Rutte
Postbus 20001
2500 EA Den Haag

ons kenmerk
2019101

telefoonnummer
070 356 4600

onderwerp
WRR-rapport nr. 101
Voorbereiden op digitale ontwrichting

e-mail
secretariaat@wrr.nl

datum
21 augustus 2019

Het doet ons genoegen u hierbij het rapport *Voorbereiden op digitale ontwrichting* aan te bieden. In dit rapport pleit de WRR voor een betere voorbereiding op digitale ontwrichting.

Met 'digitale ontwrichting' doelt de WRR op ernstige verstoringen van het maatschappelijke leven met zowel digitale als fysieke dimensies. Met de voortschrijdende digitalisering van de maatschappij zullen zulke verstoringen zich vaker voordoen. Voor maatschappelijke ontwrichting in het fysieke domein zijn er goed uitgeruste en geoefende hulpdiensten. Maar wie te bellen als er een 'digitale brand' uitbreekt? Welke instrumenten heeft een 'digitale brandweer' nodig om effectief op te treden en schade te beperken?

Dit rapport start vanuit de constatering dat verstoring en uitval van digitale infrastructuur grote gevolgen kunnen hebben voor economie en samenleving, alsmede voor het vertrouwen in de democratische rechtstaat. Opeenvolgende kabinetten hebben veel werk gemaakt van het voorkomen van digitale ontwrichting. Maar er is meer nodig dan preventieve maatregelen. Evenals in het fysieke domein is ook in de digitale wereld 100% veiligheid geen garantie. Een betere voorbereiding op digitale ontwrichting is urgent vanwege de snelle digitalisering van de samenleving, de stijgende kosten van verstoringen en het gebruik van cyberwapens in geopolitieke conflicten.

De WRR adviseert dat de nationale overheid zich inspant voor een goede voorbereiding op digitale ontwrichting. Vanwege het grensoverschrijdende karakter zullen deze inspanningen tevens een internationale component moeten hebben. De raad besteedt in zijn aanbevelingen bijzondere aandacht aan de wijze waarop in Nederland valt te sturen op afhankelijkheden tussen de digitale en fysieke wereld en tussen talloze partijen die in netwerken zijn verbonden. Met een adequaat zicht op deze afhankelijkheden staat of valt immers het handelingsrepertoire van de overheid bij een digitale ontwrichting. In het verlengde hiervan komt tevens de bevoegdheid bij incidentbestrijding aan de orde. Ook gaat de raad in op de manier waarop partijen schade kunnen herstellen en lessen kunnen trekken uit incidenten.

Overeenkomstig de Instellingswet ziet de raad graag de bevindingen van de ministerraad tegemoet.

De voorzitter,

Prof. mr. J.E.J. Prins

De secretaris,

Prof. dr. F.W.A. Brom

Buitenhof 34, Postbus 20004, 2500 EA Den Haag
telefoon (070) 356 46 00, website: www.wrr.nl, e-mail: info@wrr.nl

INHOUD

SAMENVATTING

Voor de omgang met incidenten in de fysieke wereld bestaan een uitgebreide crisisorganisatie en allerlei voorzieningen en wettelijke regels. Deze ontbreken grotendeels voor incidenten in de digitale wereld. Dat is een probleem nu digitale verstoringen steeds vaker gevolgen hebben voor het maatschappelijke leven. Een betere voorbereiding op digitale ontwrichting stelt Nederland in staat om bij verstoringen effectiever op te treden en sneller de draad op te pakken na een ernstig incident.

INCIDENTEN RAKEN HET HART VAN ONZE SAMENLEVING

De afgelopen jaren hebben zich in Nederland en daarbuiten allerhande digitale verstoringen voorgedaan. Sommige daarvan zijn snel verholpen en veroorzaakten vooral ongemak. Er waren echter ook incidenten met aanzienlijk grotere consequenties. Als gevolg van de besmetting van computers van de Britse National Health Service door de vermeende gijzelsoftware *WannaCry* (2016) moesten 19.000 patiëntafspraken worden geannuleerd. De *NotPetya*-aanval (2016) trof in Nederland de Rotterdamse Haven, waardoor het containertransport via haven, snelweg en spoor deels stil kwam te liggen. In Oss werd bij deze aanval de vestiging van farmaceutisch bedrijf MSD getroffen, met als gevolg dat de medicijnproductie tot stilstand kwam en veel documentatie verloren ging. In 2018 waren door de hack van de stad Atlanta talloze gemeentelijke basisvoorzieningen maandenlang niet beschikbaar. En in de vroege zomer van 2019 trof een urenlange storing zowel het noodnummer 112 als 0900-8844, het landelijke servicenummer van de politie. Bovendien waren ook ziekenhuizen, gemeenten en bedrijven lange tijd onbereikbaar.

Hoewel cyberaanvallen een belangrijke oorzaak zijn van incidenten, kunnen ook menselijke fouten, kapotte servers, softwareproblemen of externe factoren als kabelbreuken of elektriciteitsstoringen een groot effect hebben op het functioneren van digitale infrastructuur. De genoemde storing van het noodnummer 112, maar ook de uitval van Google Cloud, eveneens in juni 2019, vormen treffende illustraties.

Het zorgwekkende van deze incidenten is dat zij ook vitale processen in de samenleving aantasten. Zij brengen daarmee essentiële voorzieningen in gevaar zoals de zorg, het betalingsverkeer, overheidsdiensten en de elektriciteitsvoorziening. Vanzelfsprekend stijgen ook de economische en maatschappelijke kosten van dergelijke incidenten. Alhoewel er nog te weinig voorvallen zijn geweest om deze kosten goed te kunnen voorspellen, blijkt uit de praktijk dat deze kosten voor individuele organisaties en bedrijven kunnen oplopen tot honderden miljoenen

Euro's. Bovendien is duidelijk dat het potentieel voor schade en slachtoffers groeit naarmate de samenleving verder digitaliseert.

Tot slot dienen we ons te realiseren dat aanvallen op en langs digitale infrastructuren inmiddels een gangbaar instrument zijn in geopolitieke conflicten. De klassieke strijd om de beheersing van land, zee en luchtruim is uitgebreid naar de digitale wereld. Die strijd gaat ditmaal niet om een afbakening van grenzen, maar om beïnvloeding van processen en strategische posities in andere landen. De vraag is al lang niet meer of dergelijke aanvallen zijn te voorkomen. De kwestie is vooral wat ertegen te doen valt, of en onder welke omstandigheden ze om vergelding vragen en wat dan een passende reactie is.

WE ZIJN ONVOLDOENDE VOORBEREID

De afgelopen jaren is het besef gegroeid dat er met het toenemende gebruik van digitale technologie ook nieuwe, grote kwetsbaarheden ontstaan voor de samenleving. Opvallend is echter dat vrijwel alle cybersecurity-maatregelen en ambities van de overheid en andere belangrijke partijen zijn gericht op preventie: op het *voorkomen* van incidenten dus. De ongemakkelijke waarheid dat volledige digitale veiligheid niet bestaat, is een boodschap die stelselmatig naar de achtergrond verdwijnt. Maar of het nu binnen of buiten het digitale domein is, incidenten zijn van alle tijden en kunnen ontwrichtende consequenties hebben. Voor de omgang met incidenten in de fysieke wereld bestaan inmiddels een uitgebreide crisisorganisatie, talloze voorzieningen en allerlei wettelijke regels. Op het terrein van cybersecurity krijgt de *voorbereiding* op ontwrichting echter weinig aandacht. De analyse in dit rapport toont dat de overheid onvoldoende middelen heeft om adequaat te handelen, zeker wanneer deze verstoringen ontwrichtende consequenties hebben voor de fysieke wereld en het vertrouwen in de rechtstaat.

DIGITALE ONTWRICHTING

Zoals gezegd, door de groeiende verwevenheid van de digitale wereld met de fysieke en de sociale wereld hangen verstoringen van het maatschappelijke leven steeds vaker samen met een ernstige verstoring of uitval van digitale processen. De WRR noemt dit type ontwrichting 'digitale maatschappelijke ontwrichting', of kortweg 'digitale ontwrichting'.

Van digitale ontwrichting is sprake wanneer het normale leven ernstig is verstoord. Met de groeiende verwevenheid van de digitale en fysieke wereld kunnen digitale incidenten resulteren in maatschappelijke ontwrichting met de zichtbare aantasting van belangrijke processen. Het openbaar vervoer, internet, het betalingsverkeer of de elektriciteitsvoorziening functioneren dan niet meer of schakelen over op een minder efficiënte modus. Dergelijke verstoringen leiden vaak tot grote economische schade.

Behalve deze schade speelt ook het vertrouwen dat mensen hebben in de instituties van overheid, markt en samenleving. Hoe mensen een verstoring ervaren is afhankelijk van de waardesystemen die zij hanteren. Een grote rol spelen ook hun zelfredzaamheid bij een ontwrichting en hun verwachtingen ten aanzien van organisaties, bedrijven en in het bijzonder de overheid. Hebben deze partijen voldoende maatregelen getroffen om ontwrichting te voorkomen en zijn zij in staat om de maatschappelijke orde tijdig te herstellen?

Bij digitale ontwrichting verdienen twee aspecten in het bijzonder aandacht. Om te beginnen zijn digitale processen grotendeels onzichtbaar, wat het vertrouwen daarin wankel maakt. Het vermoeden van een verstoring is soms al voldoende om dat vertrouwen te ondermijnen. Bovendien overstijgt digitalisering geografische grenzen. De bevoegdheden van nationale overheden om het normale maatschappelijke leven in hun land snel te kunnen herstellen zijn daardoor mogelijk ontoereikend.

NIEUWE UITDAGINGEN

Bij de omgang met digitale ontwrichting spelen voor beleidsmakers verschillende uitdagingen:

- Het fysieke en digitale domein zijn inmiddels zeer sterk met elkaar verweven. Door ontwikkelingen als dataficatie, het gebruik van algoritmen om beslissingen te nemen en de complexe verbindingen tussen systemen wereldwijd, vloeien het digitale domein en het fysieke domein inmiddels naadloos in elkaar over. Dit vergt van de overheid een doordacht beleid ten aanzien van maatschappelijke ontwrichting, dat zich nu nog voornamelijk richt op gebeurtenissen in de fysieke wereld. Bijzondere aandacht verdient daarbij de lijst met vitale processen, waarvan de uitval als maatschappelijk ontwrichtend wordt aangemerkt.
- Digitalisering maakt de samenleving op nieuwe manieren kwetsbaar voor verstoringen, vanwege instabiele en vaak slecht beveiligde software en hardware, en de complexe en grensoverschrijdende toeleverings- en productieketens, die kwaadwillenden veel mogelijkheden bieden om maatschappelijke processen te verstoren of zelfs geheel stil te leggen. Door het gebruik van generieke hard- en software kunnen deze verstoringen potentieel een enorme schaal en bereik hebben.
- Veel publieke voorzieningen zijn als gevolg van het beleid van de afgelopen decennia in private handen. Digitalisering heeft deze tendens verder versterkt, doordat bedrijven, organisaties en ook de overheid zelf de digitale ondersteuning van hun activiteiten hebben uitbesteed aan softwareleveranciers en digitale dienstverleners. De continuïteit van de samenleving is hierdoor sterk afhankelijk geworden van het doen en laten van private partijen, die in veel gevallen vanuit het buitenland opereren. De medewerking van deze partijen is nodig als het misgaat en voor maatregelen om verstoringen beheersbaar te houden.

– Met digitalisering worden geografische grenzen minder relevant. Talloze incidenten tonen dat verstoringen vrijwel tegelijkertijd in meerdere landen tot ontwrichtende situaties kunnen leiden. Digitale ontwrichting is daarmee een dossier dat agendering binnen internationale gremia vereist, waaronder de Europese Unie.

INVESTEREN IN DE VOORBEREIDING OP DIGITALE ONTWRICHTING

Digitale ontwrichting valt nooit geheel uit te sluiten. Het is daarom belangrijk om op een ontwrichting voorbereid te zijn, te beginnen met paraatheid en mechanismen om vroegtijdig te signaleren dat er iets misloopt. Wanneer een gebeurtenis ontwrichtend blijkt, is adequate gevolgbestrijding noodzakelijk. Herstel en wederopbouw zijn ten slotte belangrijk om het normale maatschappelijke leven zo snel mogelijk weer doorgang te laten vinden.

Paraatheid

Momenteel ontbreekt voor de vitale infrastructuur een coherent beleid aangaande terugvalopties, het isoleren van ketens en netwerken, het doen van oefeningen en informatie over hoe te handelen tijdens calamiteiten. Niet alleen is dit per sector en per organisatie anders geregeld, er zijn ook ontwikkelingen waarneembaar die de paraatheid juist verzwakken. Zo vermindert het aantal terugvalopties doordat analoge alternatieven verdwijnen en besteden organisaties belangrijke voorzieningen uit aan derde partijen. De onderlinge verwevenheid van processen en sectoren neemt hierdoor toe.

Signalering

De organisatie van de informatie-uitwisseling wordt bemoeilijkt door een te sterke nadruk op individuele organisaties in plaats van ketens en netwerken, sectorale scheidslijnen en een deels achterhaald onderscheid tussen vitale aanbieders en niet-vitale aanbieders, waardoor signalen niet of te laat bij de juiste partijen terechtkomen. Mede hierdoor is het perspectief wat betreft te verzamelen en te delen kennis te beperkt. De focus ligt momenteel op het delen van kennis en informatie over beveiligingsmaatregelen, kwetsbaarheden en incidenten. Er is minder inzicht in ketens en netwerken, de afhankelijkheden daarbinnen en het effect van overnames en investeringen. Dergelijke kennis is van groot belang om de ernst van incidenten te kunnen vaststellen en invloed uit te kunnen oefenen op de wijze waarop een digitale ontwrichting zich voltrekt.

Bestrijding

De overheid is bij de bestrijding van digitale ontwrichting in hoge mate afhankelijk van de informatie en medewerking van (buitenlandse) private partijen, maar ontbeert een duidelijk omschreven bevoegdheid om in te grijpen. Ook zijn er vragen over wie daarbij het voortouw moet nemen, omdat vaak niet onmiddellijk duidelijk is welke oorzaak aan een incident ten grondslag ligt. Meer bevoegdheid voor de overheid dient

gepaard te gaan met een voldoende beschermingsniveau voor private partijen, omdat ingrijpen met dwang gepaard gaat en financiële consequenties kan hebben. Bovendien zal duidelijk moeten worden hoe opschaling plaatsvindt, wanneer de ernst van incidenten daartoe aanleiding geeft. Dit veronderstelt een categorisering van digitale incidenten, die in Nederland vooralsnog ontbreekt.

Herstel en wederopbouw

Na ontwrichtende gebeurtenissen breekt er doorgaans ook weer een periode van herstel en wederopbouw aan. Om uit de gebeurtenissen lessen te kunnen trekken, is een breed georganiseerde reflectie op incidenten nodig. Mede vanwege nieuwe wetgeving is er meer aandacht voor de melding van deze incidenten. Maar de data afkomstig uit deze meldingen worden niet ten volle benut, mede door een geïsoleerde verwerking door verschillende toezichthoudende instanties. Ook schadevergoeding is belangrijk, maar deze verloopt moeizaam, onder meer vanwege de grote onbekendheid met zowel de risico's als het type kosten dat daaraan is verbonden. Bovendien weigeren grote verzekeraars momenteel de compensatie van schade als gevolg van wereldwijde cyberaanvallen, die ze kwalificeren als gewapend conflict.

Verantwoordelijkheden

De voorbereiding op digitale ontwrichting zal een combinatie moeten zijn van nationale maatregelen en internationale samenwerking en sturing. De huidige aanpak leunt op – deels ontoereikende – nationale mechanismen, wat vooral risicovol is bij spillovereffecten naar kritieke infrastructuur elders in Europa en aanvallen op Europese instituties. Europese en internationale samenwerking is buitengewoon urgent vanwege de geopolitieke dynamiek rondom digitale ontwrichting.

Op nationaal vlak is grotere betrokkenheid van de overheid vereist. Sommige verstoringen blijven beperkt tot Nederland. Maar ook een wereldomspannende digitale ontwrichting zal uiteindelijk vitale processen op Nederlandse bodem treffen. Nederland kan bij een groot aantal maatregelen, zoals het realiseren van terugvalopties, scenario's voor het afschakelen van digitale voorzieningen maar ook compensatie van schade en verzekeren, grotendeels zelfstandig opereren. Van groot belang is ten slotte dat een betere voorbereiding op digitale ontwrichting door de overheid geen vrijbrief is voor andere partijen om onverantwoorde risico's te nemen. Wanneer een van hen achteroverleunt en nalaat om voorbereidende maatregelen te treffen, heeft iedereen daar last van op het moment dat het misgaat.

AANBEVELINGEN

De belangrijkste aanbeveling van dit rapport is dat de voorbereiding op digitale ontwrichting nadrukkelijk onderdeel dient te zijn van het veiligheidsbeleid en het

beleid gericht op de continuïteit van de samenleving. Deze centrale aanbeveling wordt in dit rapport verder uitgewerkt met de volgende aanbevelingen:

– Voer een publiek debat over de toerusting van de Nederlandse samenleving met het oog op de mogelijkheid van een digitale ontwrichting.

– Stel in aanvulling op het huidige Cybersecuritybeeld een Cyberafhankelijkheidsbeeld op, dat inzichtelijk maakt van welke partijen, digitale processen en diensten het functioneren van vitale processen in de Nederlandse samenleving afhankelijk is.

– Besteed bij het beleid voor vitale infrastructuur meer aandacht aan de ketens en netwerken die vitale processen ondersteunen. Onderzoek bovendien of digitalisering het nodig maakt de prioritering van vitale processen aan te passen.

– Creëer een helder afgebakende wettelijke bevoegdheid voor digitale hulptroepen ten dienste van de bestrijding van digitale verstoringen die een maatschappelijk ontwrichtend effect kunnen hebben. Onderzoek in dat kader de noodzaak van een aparte regeling voor overheidshandelen gericht op het tegengaan van verdere escalatie. Een categorisering van incidenten kan hierbij behulpzaam zijn.

– Stimuleer onderzoek naar de haalbaarheid van een Nederlandse of Europese cyberpool om financiële dekking mogelijk te maken voor schade als gevolg van digitale ontwrichting.

– Zorg op nationaal en op Europees niveau voor een meer systematische ontsluiting van incidentdata, benut deze data beter en realiseer een effectieve terugkoppeling naar de betrokken partijen om het collectieve leervermogen te versterken.

TEN GELEIDE

Dit rapport is opgesteld door een projectgroep bestaande uit prof. mr. Corien Prins (eerstverantwoordelijk raadslid), dr. Erik Schrijvers (projectcoördinator), mr. dr. Reijer Passchier (staflid) en prof. dr. Marianne de Visser (raadslid). Tim Puts (stagiair) en Bas Roos (junior medewerker) waren tijdelijk verbonden aan de projectgroep.

Voorbereiden op digitale ontwrichting kwam tot stand op basis van een uitvoerige studie van de wetenschappelijke literatuur en beleidsstukken, gesprekken en discussiebijeenkomsten alsmede eigen analyse.

Door dr. Véronique Bruggeman en prof. dr. Michael Faure is ter voorbereiding van dit rapport een vergelijkend onderzoek gedaan naar de compensatie van slachtoffers van rampen. Dit onderzoek is onder de titel *Compensation for Victims of Disasters in Belgium, France, Germany and The Netherlands* gepubliceerd als WRR-working paper en beschikbaar op de WRR-website.

De gesprekken werden gevoerd met ruim honderd externe deskundigen in de publieke en private sector: politici, beleidsmakers, toezichthouders, bestuurders van bedrijven, burgemeesters, beveiligingsdeskundigen, academici en vertegenwoordigers van het bedrijfsleven. Er zijn diverse werkbezoeken afgelegd, onder andere aan de Gemeente Rotterdam en de Nationaal Coördinator Terrorismebestrijding. Ook hebben we specifieke bijeenkomsten georganiseerd over rampenbestrijding, scenario's voor digitale ontwrichting, en de compensatie van slachtoffers. Onze gesprekspartners zijn we zeer erkentelijk voor hun bijdrage aan dit rapport. Hun namen staan achterin vermeld.

In de laatste fase van het project hebben we teksten voorgelegd aan drs. Erik Akerboom (Korpschef Nederlandse politie), prof. dr. Arjen Boin (Hoogleraar Publieke Instituties en Governance, Universiteit Leiden; wetenschappelijk adviseur en partner bij Crisisplan BV), Freddy Dezeure (onafhankelijk adviseur in cyberveiligheid), prof. dr. Bart Jacobs (Hoogleraar Computerbeveiliging, Radboud Universiteit). We danken hen voor de waardevolle suggesties en hun commentaar.

1 BRAND IN EEN DIGITALISERENDE WERELD

Stel dat er in de digitale wereld een 'brand' uitbreekt waardoor maatschappelijke ontwrichting dreigt te ontstaan: welke 'brandweer' kunnen we dan bellen? Hebben we voldoende zicht op wat kwetsbare voorzieningen zijn en weten we welke prioriteiten we bij het bluswerk moeten stellen? Welke bevoegdheden hebben de betrokken instanties momenteel om slachtoffers te voorkomen en schade te beperken en zijn ze nog adequaat? Deze vragen zijn in het bijzonder relevant als de 'brand' niet beperkt blijft tot het digitale domein, maar ook potentieel ontwrichtende consequenties heeft voor de fysieke wereld en het basisvertrouwen in de samenleving. Wie deze vragen wil beantwoorden stuit onherroepelijk op de rol van de overheid, en ook op die van burgers en bedrijven. Om deze thematiek draait dit rapport.

1.1 KLEINE EN GROTE INCIDENTEN ZIJN EEN REALITEIT

Het staat buiten kijf dat we in het sterk digitaliserende Nederland incidenten met digitale infrastructuur kunnen verwachten.[1] Het Cybersecuritybeeld 2019 waarschuwde hier onlangs nog voor.[2] Bovendien hebben zich inmiddels allerhande verstoringen voorgedaan.[3] Vaak betreft het problemen die snel zijn verholpen en vooral ongemak veroorzaken. Dat zijn 'kleine uitslaande brandjes' die al snel weer zijn geblust. Maar de afgelopen jaren hebben zich wereldwijd ook incidenten voorgedaan met zeer grote consequenties. Hieronder volgen enkele voorbeelden.

– In ons land was de Diginotar-kwestie in 2011 het eerste echte incident dat onze afhankelijkheid toonde van digitale technologie.[4] Hackers waren erin geslaagd om vervalste certificaten van certificaatautoriteit Diginotar vrij te geven. De certificaten van Diginotar werden onbetrouwbaar en browserleveranciers als Microsoft dreigden ze ongeldig te verklaren. Belangrijke overheidsfuncties, zoals de inklaring van goederen of de uitkering van toeslagen, zouden hierdoor niet langer uitgevoerd kunnen worden. Het incident liep met een sisser af maar werd wereldnieuws, omdat bleek hoe kwetsbaar en belangrijk private certificaatautoriteiten waren voor veilige communicatie op het internet.[5]

---

1 In hoofdstuk 2 gaan we nader in op termen als incident, verstoring, ramp en ontwrichting.
2 NCTV 2019.
3 Schneier 2018; Sanger 2018; NCTV 2019; ENISA 2019.
4 Prins 2011. Zie p. 62 van dit rapport voor een uitgebreidere behandeling van Diginotar.
5 Van der Meulen 2013.

– In 2016 vond een omvangrijke DDoS-aanval plaats op het Amerikaanse bedrijf Dyn, een zgn. Domain Name System (DNS)-provider.[6] Het gevolg was dat grote internetplatforms als Twitter, Netflix en Reddit voor het grootste deel van de dag onbereikbaar waren voor gebruikers in de VS en Europa. De aanval op Dyn werd uitgevoerd met het botnet Mirai, dat bestond uit grote aantallen gecompromitteerde consumentenapparaten, zoals webcams en digitale videorecorders. DNS-providers vertalen webadressen in IP-nummers, waardoor computers de locaties van websites kunnen vinden. De aanval op Dyn werd daarom door sommigen getypeerd als een aanval op het internet zelf.[7]

– In 2017 besmette de vermeende ransomware *WannaCry* de computers van onder meer Chinese universiteiten, Spaanse elektriciteits- en gasbedrijven, het Franse autobedrijf Renault en spoorwegvervoerder Deutsche Bahn. Het bekendste slachtoffer was de Britse National Health Service (NHS).[8] WannaCry – inmiddels toegeschreven aan Noord-Korea – ontwrichtte in het Verenigd Koninkrijk de dienstverlening van zo'n 600 zorginstellingen. Dit leidde onder meer tot het annuleren van zo'n 19.000 afspraken van patiënten. Een deel van de spoedeisende hulplocaties was niet in staat om aan alle patiënten zorg te verlenen en moest worden verplaatst. Na een week functioneerde de NHS weer normaal. Geschatte kosten: £ 92 miljoen.

– In hetzelfde jaar verspreidden Russische militaire hackers de ransomware *NotPetya*. Zij deden dat via kwetsbaarheden in Oekraïense boekhoudsoftware, die door hen al eerder was gehackt. De besmetting beperkte zich niet tot Oekraïne en trof wereldwijd verschillende bedrijven en organisaties, met naar verluid vele miljarden euro's schade. In de grensoverschrijdende keten van besmetting werd ook de Rotterdamse vestiging van het containerbedrijf Maersk slachtoffer. Het containertransport via haven, snelweg en spoor kwam deels stil te liggen waardoor opstoppingen ontstonden, met lange files tot gevolg. Ook werd in Oss de vestiging van farmaceutisch bedrijf MSD getroffen, waardoor de medicijnproductie tot stilstand kwam en veel documentatie verloren ging.

– En in maart 2018 werd de Amerikaanse stad Atlanta slachtoffer van een digitale aanval. Maanden later waren veel gemeentelijke basisvoorzieningen nog steeds niet beschikbaar, zat de stad met een schadepost van tientallen miljoenen dollars en waren talloze databestanden, onder andere van de politie, voorgoed verloren.[9]

---

6 Voor meer uitleg zie https://en.wikipedia.org/wiki/2016_Dyn_cyberattack.

7 Over het cruciale belang van basisprotocollen als het DNS voor het functioneren van het internet zie WRR 2015. Zie p. 47 van dit rapport voor een uitgebreidere toelichting op Dyn en aanvallen op het internet.

8 Zie ook box 3.1 op p. 42 van dit rapport.

9 http://nakedsecurity.sophos.com/2018/06/08/atlanta-ransomware-attack-destroyed-years-of-police-dashcam-video/

– Hoewel cyberaanvallen een belangrijke oorzaak zijn van incidenten, kunnen ook menselijke fouten, kapotte servers, softwareproblemen of externe factoren als kabelbreuken of elektriciteitsstoringen een groot effect hebben op het functioneren van digitale infrastructuur. Zo had Google Cloud in juni 2019 met uitval te maken als gevolg van reguliere onderhoudswerkzaamheden.[10] Google Cloud kon een derde van het eigen verkeer niet langer ondersteunen, waardoor het internet plaatselijk vertraagde. Standaardbeleid van Google is dat het bij storingen prioriteiten stelt wat betreft welk dataverkeer beschikbaar blijft. Saillant detail was dat de vertraging van het internetverkeer ook de eigen herstelcapaciteit van Google raakte, wat leidde tot een langere uitval dan nodig was. Google Cloud viel ook in 2018 al eens uit, net als de clouddienst van Amazon Web Services in 2017. Ditmaal was een typefout de oorzaak.[11] In al deze gevallen duurde de uitval hooguit enkele uren. Onduidelijk is of deze grote cloudaanbieders ook een langdurige storing kunnen opvangen. Hoe dan ook zal het effect van dergelijke storingen toenemen naarmate meer bedrijven van de cloud gebruikmaken en meer maatschappelijke processen afhankelijk zijn van deze aanbieders. Behalve het incident met Google Cloud, is ook de urenlange storing (evneneens in juni 2019) van zowel het noodnummer 112 als 0900-8844, het landelijke servicenummer van de politie, een illustratief voorbeeld. In dit geval werd het voorval vermoedelijk veroorzaakt door een softwarefout.[12]

Over de ernst van dergelijke voorvallen valt te discussiëren. Op mondiaal niveau was de financiële schade als gevolg van WannaCry enorm. Ook kwamen levens van mensen op het spel te staan door de uitval van medische voorzieningen. Maar ontwrichtte deze aanval daadwerkelijk de samenleving? De effecten van WannaCry bleven voor ons land beperkt. Dat gold ook voor de besmetting door NotPetya, die eenzelfde grensoverschrijdend patroon liet zien. Diginotar ligt alweer enige tijd achter ons, en bleek ondanks de onvoorziene problemen uiteindelijk oplosbaar. Dergelijke kanttekeningen maken het lastig om het thema van 'brand' in een digitaliserende wereld te agenderen, laat staan de urgentie daarvan te onderstrepen en breed geaccepteerd te krijgen. Op kleine schaal zien we de

---

10 Zie: www.wired.com/story/google-cloud-outage-catch-22/?cndid=53898727&cndid=53898727&bxid=Mjc0Mzg0ODIwMDk5S0&hasha=100c13df07dc1abb3dd77f24de416e4d&hashb=c00c411b0670ffa64b106b13483864092cbfb5d4&mbid=nl_060819_daily_list1_p4&source=daily_newsletter&utm_brand=wired&utm_mailing=wired%20NL%20060819%20(1)&utm_medium=email&utm_source=nl. Het rapport van Google zelf over de storing is te vinden op: https://status.cloud.google.com/incident/cloud-networking/19009

11 Zie: www.geekwire.com/2017/amazon-explains-massive-aws-outage-says-employee-error-took-servers-offline-promises-changes/

12 www.rijksoverheid.nl/actueel/nieuws/2019/06/26/gezamenlijk-onderzoek-naar-storing-112

effecten die bijvoorbeeld optraden bij de verstoringen waarmee het vliegverkeer, de bagageafhandeling maar ook het treinverkeer rond Schiphol in 2018 te maken kregen.[13] De storing met het noodnummer 112 was van een serieuzer omvang en raakte onze samenleving in bredere zin. Voor een beeld van echt ontwrichtende gebeurtenissen moeten we het echter doen met animaties[14], een spaarzaam artikel in een landelijk dagblad[15] of de literaire verbeelding van een auteur als Marc Elsberg, die een roman schreef over een hack van de Europese elektriciteitsvoorziening.[16] Toch zou het onterecht zijn om de incidenten te bagatelliseren en ontwrichtende scenario's af te doen als onrealistisch.

1.2 CYBERVERSTORINGEN RAKEN HET HART VAN DE SAMENLEVING

De eerste reden daarvoor is dat de schaal waarop verstoringen zich voordoen, de afgelopen jaren flink is toegenomen. Volgens het OECD-project 'Future Global Shocks' uit 2011 konden destijds weinig cybergerelateerde gebeurtenissen een wereldwijde schok veroorzaken.[17] Maar de auteurs signaleerden toen al wel een groeiende kans op financiële schade als gevolg van gecompromitteerde computers en telecommunicatiediensten. Ook voegden ze hieraan toe dat digitale voorzieningen essentieel zijn voor herstel na andersoortige grootschalige rampen.[18]

Bijna tien jaar later blijken beide observaties juist te zijn. De huidige crisisbeheersing en rampenbestrijding zijn ondenkbaar zonder de inzet van digitale hulpmiddelen. Ook is de impact van incidenten met digitale infrastructuur omvangrijker: de geografische reikwijdte is groter en steeds vaker raken ze direct of indirect aan fysieke infrastructuren en het dagelijks leven van burgers.

Dit laatste is zorgwekkend omdat kernprocessen van de samenleving worden aangetast. Incidenten brengen voorzieningen in gevaar die het maatschappelijk leven ondersteunen. De hierboven genoemde voorbeelden laten dat duidelijk zien. De 112-storing bracht mensenlevens in gevaar, door WannaCry viel een deel van de Britse gezondheidszorg uit, Diginotar dreigde het functioneren van de digitale overheid en delen van het betalingsverkeer te verstoren en de hack in Atlanta vernietigde belangrijke publieke databestanden. Inmiddels lijkt een volgende fase te zijn

13 https://nos.nl/l/2247770
14 Voor een dergelijke animatie zie bijvoorbeeld: www.nctv.nl/organisatie/nationale_veiligheid/vitale_infrastructuur/index.aspx
15 NRC 4 oktober 2018, "Wat als het internet uitvalt?" www.nrc.nl/nieuws/2018/10/04/wat-als-het-internet-uitvalt-a2180425; in buitenlandse media: www.ft.com/content/109350ea-c6f2-11e8-ba8f-ee390057b8c9
16 Elsberg 2012.
17 Sommer en Brown 2011.
18 Vergelijk Prins 2010.

aangebroken, waarbij de bediening van voorzieningen wordt overgenomen. In 2016 besmetten hackers een elektriciteitscentrale in Kiev met malware, als gevolg waarvan een vijfde van de totale stroomproductiecapaciteit van de hoofdstad uitviel.[19] Het voorval gaat de geschiedenis in als de eerste keer dat kwaadwillende buitenstaanders erin slaagden om op afstand nutsvoorzieningen uit te zetten. Sindsdien gaat het snel. In 2017 slaagden hackers erin controle te krijgen over de software van energiecentrales in de Verenigde Staten[20] en in juni 2019 berichtten media over ontwrichtende malware die door de VS in het Russische elektriciteitsnet zou zijn geplaatst.[21]

Logischerwijs stijgen ook de kosten voor de samenleving. Het CPB staat in de Risicorapportage Cyberveiligheid Economie 2018 expliciet stil bij enkele internationale schattingen van de potentiële economische en maatschappelijke kosten van cybercriminaliteit bij belangrijke processen in de samenleving.[22] Zo schat Lloyd's volgens het CPB de schade van een uitval van clouddiensten in de Verenigde Staten op 5 tot 53 miljard dollar; het IMF laat zien dat de mogelijke schade voor financiële instellingen door cyberaanvallen kan oplopen tot honderden miljarden dollars. Het betreft hier schattingen. Er zijn nog te weinig voorvallen geweest om mogelijke schade goed te kunnen berekenen. Bovendien ontbreekt overeenstemming over wat voor verliezen verschillende typen incidenten kunnen veroorzaken.[23] Desalniettemin is duidelijk dat met de voortschrijdende digitalisering het potentieel voor schade en slachtoffers groeit. De Amerikaanse cyberexpert Bruce Schneier legt dat glashelder uit:

'with smart homes, attacks can mean property damage. With banks, they can mean economic chaos. With power plants they can mean blackouts. With waste treatment plants they can mean toxic spills. With cars, planes and medical devices, they can mean death. With terrorists and nation-states, the security of entire economies and nations could be at stake.'[24]

Tot slot dienen we ons ervan bewust te zijn dat digitale aanvallen een instrument in geopolitieke conflicten zijn geworden. De afgelopen jaren heeft de klassieke strijd om de beheersing van land, zee en luchtruim zich uitgebreid naar de digitale wereld.[25]

19 Voor een gedetailleerde beschrijving zie Sanger 2018, hoofdstuk 7.
20 www.wired.com/story/hackers-gain-switch-flipping-access-to-us-power-systems/
21 https://nos.nl/2289245
22 CPB 2018: 2-3.
23 OECD 2017.
24 Schneier 2018: 16.
25 WRR 2017a.

De strijd gaat ditmaal niet om een afbakening van grenzen, maar om sabotage van maatschappelijke en economische processen en strategische posities van andere landen. Al met al is de vraag niet meer *of* maar *wanneer* we te maken krijgen met de gevolgen van een grootschalige cyberaanval.

1.3 100% SUCCESVOLLE PREVENTIE BESTAAT NIET – MAAR ZIJN WE WEL VOLDOENDE VOORBEREID OP ONTWRICHTING?

De groeiende schaal, verspreiding en impact van incidenten heeft onder andere te maken met het hoge tempo waarin de wereld digitaliseert. Digitale technologie wordt bovendien alsmaar complexer, door de groei van de hoeveelheid data, de exponentiële toename van rekenkracht, en steeds meer uitwisseling van informatie tussen apparaten onderling, tussen mens en machine of fysieke leefomgeving en technologie. We stoppen overal chips en sensoren in. We sluiten alles aan op het internet. De volgende fase in deze ontwikkeling dient zich reeds aan in de vorm van het 'Internet of Things' en artificiële intelligentie om allerhande processen in de samenleving nog sneller en slimmer te kunnen inrichten. Het resultaat is dat de interactie tussen de digitale wereld en de fysieke wereld intenser wordt. In veel sectoren zijn digitale componenten en fysieke componenten nauwelijks meer van elkaar te scheiden.

Nederland loopt bij deze ontwikkelingen voorop. We hebben een hoogwaardige digitale infrastructuur en snelle verbindingen – consumenten en bedrijven doen enthousiast mee aan de digitale revolutie.[26] Daarbij doet de overheid erg haar best om zoveel mogelijk ruimte te bieden aan innovatie. 'Hier kan het. Hier gebeurt het' luidt de veelzeggende ondertitel van de in 2018 door het kabinet gepresenteerde Nederlandse Digitaliseringsstrategie.[27]

Maar elke technologische ontwikkeling heeft twee kanten. Behalve voordelen (de zogenaamde 'highways of efficiency') heeft ze ook nadelen (de 'highways of failure').[28] Digitalisering vormt hierop geen uitzondering.[29] Enerzijds biedt digitalisering welvaart, individuele vrijheid en gemak. Daar zet de Nederlandse overheid terecht vol op in. Anderzijds brengt digitalisering ook nieuwe kwetsbaarheden en afhankelijkheden met zich mee.[30] Met het toenemend gebruik van digitale technologie kunnen zo uiteindelijk de economie en maatschappelijke processen, maar ook de veiligheid van mensen en hun eigendommen op het spel komen te staan.[31]

---

26 CBS 2018a.
27 Te vinden op: www.rijksoverheid.nl/documenten/rapporten/2018/06/01/nederlandse-digitaliseringsstrategie
28 Perrow 1983, Boin 2017.
29 Pupillo 2018: 1.
30 Schneier 2018; World Economic Forum 2017: 6; NCTV 2018a: 5.
31 Internet Society 2017: 10.

Het goede nieuws is dat bij veel partijen dat besef is toegenomen. Onder regie van de Cyber Security Raad zijn de afgelopen jaren vele initiatieven ontplooid. Het kabinet Rutte III zet nadrukkelijk in op informatieveiligheid en talloze andere (internationale) gremia hebben stappen ondernomen om de cyberveiligheid te vergroten. Opvallend is echter dat vrijwel alle maatregelen en ambities gericht zijn op preventie, op het voorkomen van incidenten dus. De ongemakkelijke waarheid dat 100% informatieveiligheid niet bestaat, is een boodschap die stelselmatig naar de achtergrond verdwijnt. Maar of het nu binnen of buiten het digitale domein is: incidenten zijn van alle tijden en kunnen tot daadwerkelijke ontwrichting leiden. De geschiedenis leert dat ons land met een zekere regelmaat wordt geconfronteerd met ingrijpende verstoringen van het maatschappelijke leven.[32] Voor de omgang met deze crises en rampen bestaan inmiddels een uitgebreide crisisorganisatie en een complex stelsel van wet- en regelgeving. Op het terrein van cybersecurity krijgt de voorbereiding op ontwrichting echter weinig tot geen aandacht.

De meeste beleidsdocumenten bevatten weliswaar passages over de mogelijkheid van ernstige verstoringen, maar richten zich vervolgens op het realiseren van een hoger beschermingsniveau of maatregelen om risico's te verminderen.[33] Het scenario van een ernstige ontwrichting lijkt dus vooral als doel te hebben partijen aan te zetten om preventie nog serieuzer te nemen. Zelden zijn daar concrete maatregelen aan gekoppeld voor de omgang met daadwerkelijke incidenten.[34]

Ook in andere landen is er aandacht voor de groeiende kwetsbaarheid van de samenleving voor digitale verstoringen.[35] Enkele van die landen erkennen inmiddels dat zij te maken kunnen krijgen met een scenario waarin de maatschappij

---

32 Voor een overzicht zie bv. Muller (red.) 2011 en Muller 2014: 9-10. Van Duin, Wijkhuis en Jong (red.) (2017) bespreken jaarlijks crises en mini-crises.

33 Cybersecurity wordt in beleidsstukken gedefinieerd als 'het geheel aan meetregelen om schade door verstoring, uitval of misbruik van ICT te voorkomen en, indien er toch schade is ontstaan, het herstellen hiervan'.

34 Een voorbeeld is de brief van de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties inzake informatieveiligheid bij de overheid. Hierin staat dat 'Burgers, ondernemers en andere organisaties moeten kunnen blijven vertrouwen op de overheid, ook in het digitale tijdperk' (Ministerie van BZK 2018: 6). Hiertoe dienen onder meer maatregelen 'die ervoor zorgen dat belangrijke voorzieningen van de digitale overheid in voldoende mate zijn opgewassen tegen uitval/stilstand'. Toch gaan deze maatregelen - met uitzondering van een algemene mededeling over incidentresponscapaciteit - niet over het reageren op daadwerkelijke incidenten.

35 Er bestaat geen systematische internationale vergelijking van cybersecuritybeleid en de bijbehorende institutionele voorzieningen. Van der Zwan en Spit (2015) bieden een korte vergelijking van de internationale stand van zaken in de bescherming van vitale infrastructuur. Janczewski en Caelli (2016) bespreken de positie van een aantal kleinere landen, waaronder Nederland, bij cyberaanvallen. Boeke (2016) gaat specifiek in op de rol van defensie bij cyberaanvallen in een aantal landen.

ernstig ontwricht raakt. Volgens de Britten zal hun land, alle genomen maatregelen ten spijt, hoe dan ook een keer door een grote cyberaanval worden getroffen.[36] In Oostenrijk bespreekt men het scenario van 'Digitalen Stillstand' als gevolg van cascade-effecten.[37] Frankrijk heeft – evenals de Verenigde Staten – een categorisering van cyberincidenten ontwikkeld, om te kunnen bepalen wanneer welk middel gepast is om ze te bestrijden.[38] Ook binnen de EU worden diverse initiatieven ontplooid om digitale verstoringen adequaat te kunnen aanpakken.[39] Deze en andere ontwikkelingen en initiatieven komen in de navolgende hoofdstukken nader aan de orde.

1.4 OPZET RAPPORT

In tegenstelling tot veel analyses en documenten, vormen preventie, cybersecurity en dus het voorkomen van een digitale verstoring niet de centrale thematiek van dit rapport. De navolgende hoofdstukken vertrekken daarentegen vanuit de vaststelling dat we het scenario van een digitale verstoring met maatschappelijk ontwrichtende gevolgen onder ogen moeten zien. Kortom, we hebben de concrete aanpak te doordenken.[40] De centrale vraag die we in dit rapport aan de orde stellen is: *hoe kan de overheid zich beter voorbereiden op maatschappelijke ontwrichting in een digitaliserende samenleving?*

De opbouw van het rapport is als volgt. In hoofdstuk 2 definiëren we maatschappelijke ontwrichting om zo af te bakenen over welk type gebeurtenissen we het hebben. In hoofdstuk 3 analyseren we vervolgens hoe digitalisering de context verandert waarin deze gebeurtenissen optreden. In hoofdstuk 4 bespreken we de uitdagingen waarvoor de overheid zich gesteld ziet in termen van paraatheid, signalering, bestrijding, en herstel en wederopbouw. In hoofdstuk 5 trekken we conclusies en formuleren we aanbevelingen. Onze voornaamste conclusie zal zijn dat digitalisering resulteert in een nieuw type maatschappelijke ontwrichting en daarmee in nieuwe opgaven voor de overheid. De aanbevelingen die we formuleren als nadere uitwerking van deze centrale conclusie hebben onder meer betrekking op het beleid ten aanzien van afhankelijkheden, vitale infrastructuur, bevoegdheid en prioriteitstelling bij de bestrijding van incidenten, en de compensatie van slachtoffers, waaronder verzekerbaarheid van schade.

---

36 Voor de Britse cyberstrategie zie https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf en voor de parlementaire beraadslagingen en rapportages daarover https://publications.parliament.uk/pa/jt201719/jtselect/jtnatsec /1708/1708.pdf

37 Zie www.darc-c12.de/system/files/Projektbericht-Digitaler-Stillstand-final.pdf

38 Zie p. 68 van dit rapport voor een uitgebreidere bespreking.

39 Bijvoorbeeld http://ec.europa.eu/transparency/regdoc/rep/3/2017/NL/C-2017-6100-F1-NL-MAIN-PART-1.PDF en http://ec.europa.eu/transparency/regdoc/rep/3/2017/NL/C-2017-6100-F1-NL-ANNEX-1-PART-1.PDF

40 Vgl. Prins 2017.

2 MAATSCHAPPELIJK ONTWRICHTING

2.1 INLEIDING

In het voorgaande hoofdstuk hanteerden we termen als 'incident', 'verstoring', 'crisis', 'ramp' en 'ontwrichting'. In het vervolg spreken we over 'maatschappelijke ontwrichting', een begrip dat we hieronder toelichten. We doen dat om duidelijk te maken op welk type gebeurtenissen we ons in dit rapport richten. Wanneer die gebeurtenissen een grote digitale component bezitten, spreken we van 'digitale ontwrichting'. Omdat maatschappelijke ontwrichting in de beleidspraktijk veelal wordt gekoppeld aan de nationale veiligheid en 'vitale' belangen, staan we in dit hoofdstuk ook stil bij de classificatie van vitale processen en infrastructuur.

2.2 MAATSCHAPPELIJKE ONTWRICHTING

Maatschappelijke ontwrichting treedt op als gevolg van een catastrofale gebeurtenis, bijvoorbeeld een grote overstroming of pandemie. Maatschappelijke ontwrichting is zodoende nauw verbonden met het risicobegrip. Risico wordt in de literatuur vaak gedefinieerd als 'kans x gevolg'.[41] Bij maatschappelijke ontwrichting draait het enkel om het gevolg: het risico heeft daadwerkelijk schade veroorzaakt. Maatschappelijke ontwrichting is een begrip dat regelmatig in beleidsteksten wordt genoemd, vooral als het de nationale veiligheid betreft. Desalniettemin ontbreekt een heldere afbakening. Het is duidelijk dat er van ontwrichting van de samenleving kan worden gesproken bij grote rampen. Een ondergrens blijkt echter lastig te definiëren: verschillende typen gebeurtenissen kunnen in verschillende mate tot ontwrichting van samenleving, economie en overheid leiden. Bovendien hoeft een ontwrichting geen duidelijk aanwijsbaar aanvangsmoment te kennen. Een ontwrichting kan als een veenbrand eerst een sluimerend bestaan leiden en pas later in volle omvang aan de oppervlakte komen. De betekenis en reikwijdte van het begrip maatschappelijke ontwrichting lichten we hieronder toe door in te gaan op 1) het normale maatschappelijk leven; 2) de ernst van de verstoring en 3) de rol van het tijdsverloop bij verstoringen.

EEN VERSTORING VAN HET 'NORMALE' MAATSCHAPPELIJKE LEVEN

Bij maatschappelijke ontwrichting is sprake van een verstoring van het normale maatschappelijke leven. Met het 'normale' maatschappelijke leven bedoelen wij het reguliere functioneren van de instituties van overheid, samenleving en economie. Wanneer maatschappelijke processen geen doorgang meer kunnen vinden en instituties niet meer adequaat, zonder extra kosten of gebaseerd op voldoende

41 Zie WRR 2008: 53-86 voor een uiteenzetting over de 'klassieke' risicobenadering.

maatschappelijk vertrouwen kunnen functioneren, dan geldt dit als een ernstige verstoring. Bij deze verstoring gaat het om effecten op de samenleving, de economie en de overheid, inclusief processen als rechtspraak, verkiezingen en het wetgevingsproces. Over wat geldt als het reguliere functioneren van deze instituties is discussie mogelijk. Er zijn dan ook verschillende manieren om te bepalen wanneer een verstoring ernstig genoeg is om van ontwrichting te kunnen spreken. Hierbij gaat het zowel om de zichtbare aantasting van de continuïteit van de samenleving als om de perceptie van verstoringen.[42]

EEN 'ERNSTIGE' VERSTORING: UITVAL VAN KERNPROCESSEN

Bij een ernstige verstoring houden voorzieningen als het betalingsverkeer, internet, openbaar vervoer, zorg, drinkwater of elektriciteit daadwerkelijk op te functioneren of zij schakelen over op een minder efficiënte modus. Kortom, kernprocessen van de samenleving worden geraakt. Als gevolg daarvan is de continuïteit van de samenleving niet langer gegarandeerd. Lange files en wachtrijen ontstaan, grote hoeveelheden goederen stapelen zich op of informatie en diensten zijn ontoegankelijk of onbetrouwbaar geworden, waardoor veel handelingen niet langer te verrichten zijn. Dergelijke verstoringen leiden bovendien vaak tot grote economische schade. Dit kan materiële schade zijn, zoals schade aan dijken, woningen, computers of bedrijfsinstallaties, maar ook immateriële schade, doordat bedrijfsuitval plaatsvindt of de activiteiten van derde partijen hinder ondervinden. Tot slot kunnen er ook slachtoffers vallen, in termen van doden en gewonden.

PERCEPTIE VAN VERSTORINGEN

De bovenstaande zaken zijn in principe redelijk in kaart te brengen en in geld uit te drukken, bijvoorbeeld om schade te compenseren. Bij de perceptie van verstoringen draait het om andere zaken. Relevant is hier allereerst of mensen een verstoring als ongemak of juist als een ernstige inbreuk op het dagelijks leven beschouwen. De perceptie van verstoringen is verder afhankelijk van de waardesystemen die mensen hanteren.[43] Ook hun mate van zelfredzaamheid[44] tijdens en na een ontwrichting is hierop van grote invloed. Met andere woorden, met de voorbereiding van de samenleving op een ontwrichtende situatie, bijvoorbeeld via voorlichting aan burgers en bedrijven, valt de perceptie van een verstoring te beïnvloeden.

Hiernaast spelen verwachtingen een rol, ten aanzien van organisaties en bedrijven, en in het bijzonder de overheid. Relevant is daarbij ook het vertrouwen dat mensen hebben in de instituties van overheid, samenleving en markt. Heeft de overheid voldoende maatregelen getroffen om ontwrichting te voorkomen en is zij in staat om

42 Vgl. PBL 2014: 7-11.
43 Douglas en Wildavsky 1982; Hood 1998.
44 Vgl. WRR 2017b.

de orde tijdig te herstellen? Wanneer burgers, bedrijven of organisaties voor hun gevoel niet meer kunnen rekenen op de doorgang van het normale maatschappelijke leven, dan kunnen ook de fundamenten van de democratische rechtstaat worden aangetast. Wat digitalisering in dit verband problematisch maakt, is het ontbreken van geografische grenzen. De bevoegdheden van nationale overheden om het normale maatschappelijk leven in hun land snel te kunnen herstellen zijn daardoor mogelijk niet toereikend.[45]

De rechtstaat – en daarmee een fundamentele zekerheid in onze samenleving – is gebouwd op het uitgangspunt dat er een nationale staat is die binnen een duidelijk begrensd grondgebied legitiem het geweldsmonopolie kan uitoefenen. Wanneer dit uitgangspunt onder druk komt te staan, bijvoorbeeld omdat de staat vanwege het ontbreken van duidelijke territoriale grenzen niet langer met succes aanspraak op dit monopolie kan maken, kunnen mensen hun vertrouwen in de samenleving en de rechtstaat verliezen. Er is dan geen instantie meer om legitiem een maatschappelijke orde te waarborgen en te herstellen. Een extra complicatie voor het digitale domein is dat onduidelijk is welke middelen de staat daar kan inzetten.[46] Dergelijke overwegingen beïnvloeden onherroepelijk de perceptie van een verstoring.

Maar of het nu gaat om de uitval van maatschappelijke voorzieningen, de economische schade, het aantal slachtoffers of het verlies van vertrouwen in samenleving en overheid, deze elementen moeten een zekere omvang krijgen alvorens van maatschappelijke ontwrichting kan worden gesproken.

DE ROL VAN TIJDSVERLOOP

Belangrijk bij verstoringen is daarom ook het tijdsverloop. Een trage, vaak onopgemerkte reeks van kleine verstoringen kan op termijn hetzelfde effect hebben als een gebeurtenis die razendsnel escaleert. In het eerste geval wordt pas gaandeweg duidelijk wat de gevolgen van bepaalde gebeurtenissen zijn, omdat zij lang onder de radar blijven. De gestage verspreiding van desinformatie ondermijnt bijvoorbeeld het vertrouwen in instituties, wat op de lange termijn schadelijk kan zijn voor het maatschappelijke functioneren. In het tweede geval vallen oorzaak en gevolg min of meer samen, zodat de ernst van de situatie onmiddellijk zichtbaar wordt.

---

45 Bovens 1998 en WRR 1998.

46 Met de komst van digitalisering is ook de vraag aan de orde op welke specifieke vormen van geweld het geweldsmonopolie van de overheid ziet. In een digitale samenleving gaat het immers niet langer alleen om fysiek geweld, maar ook om nieuwe vormen van 'digitaal geweld'. Maar welke digitale middelen en maatregelen zijn geoorloofd?

Het tijdsverloop is eveneens belangrijk voor de kosten van verstoringen. Naarmate een verstoring langer aanhoudt, stijgen vaak ook de kosten.[47] Immers, de nadelige gevolgen van een gebeurtenis ontvouwen zich met het verstrijken van de tijd, waardoor het feitelijke schadebeeld kan veranderen. Schade is kortom een veranderlijk verschijnsel.[48] Dit geldt in bredere zin ook voor de reputatie van bedrijven, organisaties en overheden die bij ontwrichting een rol spelen. Een gebrekkige signalering en onvoldoende tijdige bestrijding van ontwrichtende situaties kan daarom ook gevolgen hebben voor het vertrouwen in de overheid, die immers geldt als instantie bij uitstek om dergelijke situaties snel en adequaat aan te pakken.

2.3 VITALE INFRASTRUCTUUR EN VITALE PROCESSEN

In de beleidspraktijk wordt maatschappelijke ontwrichting gekoppeld aan de nationale veiligheid, een begrip dat is uitgewerkt in verschillende 'vitale' belangen. Deze belangen zijn territoriale veiligheid, economische veiligheid, ecologische veiligheid, fysieke veiligheid en sociale en politieke stabiliteit. Bij de recente aanpassing van het Nationaal Handboek Crisisbesluitvorming is deze afbakening verruimd naar 'andere situaties die een grote uitwerking op de maatschappij (kunnen) hebben'.[49] Een verdere inkleuring vindt plaats door de identificatie van zogenaamde 'vitale' processen die dermate cruciaal zijn dat verstoring of uitval daarvan tot maatschappelijke ontwrichting leidt of een bedreiging vormt voor de nationale veiligheid. Deze processen tezamen vormen de Nederlandse 'vitale infrastructuur'.[50]

De bescherming van de vitale infrastructuur is niet alleen verbonden met de invloed van de natuur (overstromingen) en technologische rampen (kernongeval); zij vormt van oudsher ook een belangrijk onderdeel van de landsverdediging. Het huidige concept van vitale infrastructuur ontstijgt echter de traditionele blik op nationale defensie en militaire overwegingen. De focus van het veiligheidsbeleid is verbreed van dreigingsactoren, hun capaciteit en motivaties naar de algemene kwetsbaarheden van de gehele samenleving. Het diffusere dreigingsspectrum van na de Koude Oorlog en de nieuwe kwetsbaarheid van de samenleving als gevolg van de afhankelijkheid van informatiesystemen liggen ten grondslag aan deze verbreding.[51]

---

47 Jocqué 2016. Voor de kosten van 'cyber breaches' afgezet tegen het moment van detectie, zie bv. EPSC 2017: 4.

48 Hebly en Lindenbergh 2016.

49 NCTV (2016), p. 8. Genoemd worden 'een lokaal of regionaal incident of ongeval met veel slachtoffers, een incident of ongeval in het buitenland met een groot aantal Nederlandse slachtoffers, of evenementen met een (inter)nationale gebeurtenissen uitstraling in Nederland.'

50 Zie Kamerstukken II 2014/15, 30 821, nr. 23 en Kamerstukken II 2015/16, 30 821, nr. 32.

51 Dunn Cavalty 2007: 16; WRR 2017a; Ministerie van Justitie en Veiligheid 2019.

VITALE PROCESSEN

Met deze verbreding is ook een andere omgang met risico's tot stand gekomen. Bij gebrek aan betrouwbare data over de waarschijnlijkheid en impact van de risico's die de samenleving bedreigen, werd al snel de blik verlegd van de mogelijke oorzaken naar de potentiële gevolgen van uitval van vitale voorzieningen. In 2014 stelde het Ministerie van Justitie en Veiligheid één integrale lijst van vitale processen vast, die sindsdien enkele keren is geactualiseerd.[52] Tabel 2.1 bevat de meest recente versie.[53]

Tabel 2.1 Vitale processen

Vitale processen	Categorie
Landelijk transport en distributie elektriciteit	A
Regionale distributie elektriciteit	B
Gasproductie, landelijk transport en distributie gas	A
Regionale distributie gas	B
Olievoorziening	A
Internet en datadiensten	B
Internettoegang en dataverkeer	B
Spraakdienst en SMS	B
Plaats- en tijdsbepaling middels GPS	B
Drinkwatervoorziening	A
Keren en beheren waterkwantiteit	A
Vlucht- en vliegtuigafhandeling	B
Scheepvaartafwikkeling	B
Grootschalige productie/verwerking en/of opslag (petro)chemische stoffen	B
Opslag, productie en verwerking nucleair materiaal	A
Toonbankbetalingsverkeer	B
Massaal giraal betalingsverkeer	B
Hoogwaardig betalingsverkeer tussen banken	B
Effectenverkeer	B
Communicatie met en tussen hulpdiensten middels 112 en C2000	B
Inzet politie	B
Basisregistraties personen en organisaties	B
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

52 Zie Kamerstukken II 2014/15, 30 821, nr. 23.
53 www.nctv.nl/organisatie/nationale_veiligheid/vitale_infrastructuur/index.aspx

Een classificatie van vitale processen biedt politici, beleidsmakers en andere betrokkenen houvast bij het bepalen of een bepaalde situatie als ernstig moet worden aangemerkt – en dus of de overheid haar verantwoordelijkheid dient te nemen en zo ja, op wat voor manier. Het is namelijk onmogelijk om alle processen van een samenleving voortdurend tegen alle dreigingen te beschermen. In de praktijk is daarom een onderscheid nodig tussen vitale en niet-vitale processen. Het ministerie heeft hiertoe een beoordeling uitgevoerd van de mate van vitaliteit van maatschappelijke processen, waarbij de gevolgen van uitval van deze processen een score is toegekend op potentiële economische, fysieke en sociaal-maatschappelijke impact. Daarnaast is ook gekeken naar cascadegevolgen.

Op basis hiervan zijn twee categorieën vitale processen onderscheiden:

Box 2.1 Categorieën vitale processen

Categorie A
In deze categorie staat de infrastructuur die bij verstoring, aantasting of uitval de ondergrenzen van minstens één van de drie impactcriteria (economisch, fysiek of sociaal-maatschappelijk) voor categorie A raakt en daarnaast ook voldoet aan het criterium van cascadegevolgen:
- Economische gevolgen: > ca. 50 miljard euro schade of ca. 5,0 % daling reëel inkomen
- Fysieke gevolgen: meer dan 10.000 personen dood, ernstig gewond of chronisch ziek
- Sociaal-maatschappelijke gevolgen: meer dan 1 miljoen personen ondervinden emotionele problemen of ernstige maatschappelijke overlevingsproblemen
- Cascadegevolgen: Uitval heeft als gevolg dat minimaal twee andere sectoren uitvallen.

Categorie B
In deze categorie staat de infrastructuur die bij verstoring, aantasting of uitval de ondergrenzen van minstens één van de drie impactcriteria voor categorie B raakt:
- Economische gevolgen: > ca. 5 miljard euro schade of ca. 1,0 % daling reëel inkomen
- Fysieke gevolgen: meer dan 1.000 personen dood, ernstig gewond of chronisch ziek
- Sociaal-maatschappelijke gevolgen: meer dan 100.000 personen ondervinden emotionele problemen of ernstige maatschappelijke overlevingsproblemen.

Bron: www.nctv.nl/organisatie/nationale_veiligheid/vitale_infrastructuur/index.aspx

Het 'vitale' karakter van maatschappelijke processen is echter ook sterk afhankelijk van hoe deze processen in de praktijk zijn georganiseerd en van het risico op verstoringen.[54] Dergelijke aspecten, inclusief de aanwezigheid van bijvoorbeeld terugvalopties en hersteltijden, zijn cruciaal voor de omvang van de schade of het aantal slachtoffers op het moment dat het misgaat. Impact is met andere woorden geen

54 Sharma 2017: 33-36.

onveranderlijke grootheid, maar mede afhankelijk van de veerkracht van de partijen die verantwoordelijk zijn voor de vitale processen.

Lijstjes met vitale processen kunnen dus van elkaar verschillen, van moment tot moment en ook per land. Zo leggen landen in de praktijk verschillende lijsten aan, of ze voegen daar onder invloed van recente ontwikkelingen nieuwe processen aan toe. De Verenigde Staten hebben in 2017 de infrastructuur voor verkiezingen ondergebracht in de vitale infrastructuur.[55] Duitsland rekent ook de media en sommige cultuurgoederen hiertoe.[56] De zorg figureert regelmatig in internationale overzichten van vitale infrastructuur, maar in Nederland zijn ziekenhuizen en andere zorginstellingen daar onlangs nog van uitgesloten.[57] Regelmatig wordt het vitale belang van bepaalde processen bovendien pas na een verstoring duidelijk – denk aan de in het voorgaande hoofdstuk genoemde Diginotar-kwestie. Op de implicaties van dergelijke leemtes en verschillen komen we in hoofdstuk 4 terug.

2.4 DIGITALE ONTWRICHTING

In dit rapport richten we ons op een specifieke verschijningsvorm van maatschappelijke ontwrichting, namelijk een ontwrichting die verband houdt met een ernstige verstoring of uitval van digitale infrastructuur. Digitalisering maakt processen in de samenleving op nieuwe en onverwachte manieren kwetsbaar. Die kwetsbaarheid geldt zowel voor reguliere processen als voor de door de overheid als vitaal aangemerkte processen. Op de lijst van vitale processen genoemd in de voorgaande paragraaf prijken diverse processen die verknoopt zijn met digitale infrastructuur. Onder digitale infrastructuur verstaan we daarbij het geheel van voorzieningen voor de opslag, uitwisseling en verwerking van digitale gegevens. Tot een jaar of tien geleden ontbrak het risico op verstoring of uitval van deze voorzieningen in vrijwel alle nationale en internationale risicoanalyses. Dat is intussen veranderd. Het risico op verstoringen en uitval van digitale infrastructuur is een belangrijke stijger op ranglijstjes van risico's met ontwrichtende gevolgen voor de samenleving.[58]

Verstoring of uitval van digitale infrastructuur kan velerlei oorzaken hebben, variërend van onbewust (fouten) of bewust menselijk handelen (dit handelen heeft dan vaak een crimineel of in elk geval onrechtmatig karakter), het spontaan falen

55 Zie https://fas.org/sgp/crs/misc/if10677.pdf
56 www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/kritis.pdf?__blob=publicationFile&v=3
57 https://zoek.officielebekendmakingen.nl/kst-27529-158.html
58 Het World Economic Forum scoort jaarlijks dezelfde risico's en biedt inzicht in de relatieve positie van het risico op digitale verstoringen ten opzichte van andere risico's. Vgl. Analistennetwerk 2018: 29.

van systemen tot het semi-autonome gedrag van machines dat informatieprocessen verstoort en indirectere oorzaken als een brand, stroomuitval of overstromingen die bijvoorbeeld servers beschadigen. Deze oorzaken kunnen afzonderlijk of in samenspel optreden en zowel een acute als een geleidelijke ontwrichting tot gevolg hebben. Wanneer maatschappelijke ontwrichting een belangrijke digitale component heeft, spreken we in dit rapport van 'digitale ontwrichting'.

De vraag hoe groot precies de kans op en gevolgen van digitale ontwrichting zijn, laten we in dit rapport buiten beschouwing. Hiernaar zijn de afgelopen jaren reeds verschillende onderzoeken verricht. Ter voorbereiding van de Strategie Nationale Veiligheid vindt bijvoorbeeld regelmatig een beoordeling plaats van het risico op maatschappelijke ontwrichting.[59] In deze beoordelingen komt ook het risico van digitale verstoringen aan de orde. In 2010 werd bijvoorbeeld het scenario onderzocht van een mogelijk conflict in cyberspace met gerichte aanvallen op Nederland en van uitval van de Amsterdam Internet Exchange (AMS-IX), de grootste Nederlandse Internet Exchange.[60] In de risicobeoordeling 2011 kreeg cyberspionage aandacht en in 2012 cyberhacktivisme.[61] Elk van deze scenario's is gescoord op impact en waarschijnlijkheid.

De meest recente risicobeoordeling dateert van 2016 en bespreekt twee scenario's voor een digitale ontwrichting.[62] In het eerste scenario nemen activisten het controlesysteem voor netbeheerders over en schakelen dit uit, waardoor de stroomvoorziening stokt. Het tweede scenario betreft de aantasting van IP-netwerken en het Border Gate Way Protocol (BGP), dat regelt langs welke weg pakketjes informatie over het internet reizen. Voor beide scenario's geldt dat ze 'enigszins waarschijnlijk' worden geacht en gevolgen kunnen hebben die variëren van 'beperkt' tot 'zeer ernstig'.[63] De kans op fysieke schade wordt beperkt geacht, maar de maatschappelijke onrust en economische schade kunnen volgens het onderzoek desalniettemin groot zijn (zie figuur 2.1).[64] De Horizonscan Nationale Veiligheid 2018 constateert dat er op het terrein van de informatietechnologie meerdere ontwikkelingen plaatsvinden,

---

59 Deze beoordeling vindt plaats in opdracht van de Nationaal Coördinator Terrorisme en Veiligheid en is het werk van het Analistennetwerk Nationale Veiligheid, waarvan RIVM, WODC, AIVD, TNO, Clingendael en het Institute of Social Studies van de Erasmus Universiteit Rotterdam de kern vormen.

60 Analistennetwerk Nationale Veiligheid 2010: 7-22.

61 Analistennetwerk Nationale Veiligheid 2011: 28-38 en 2012: 22-39.

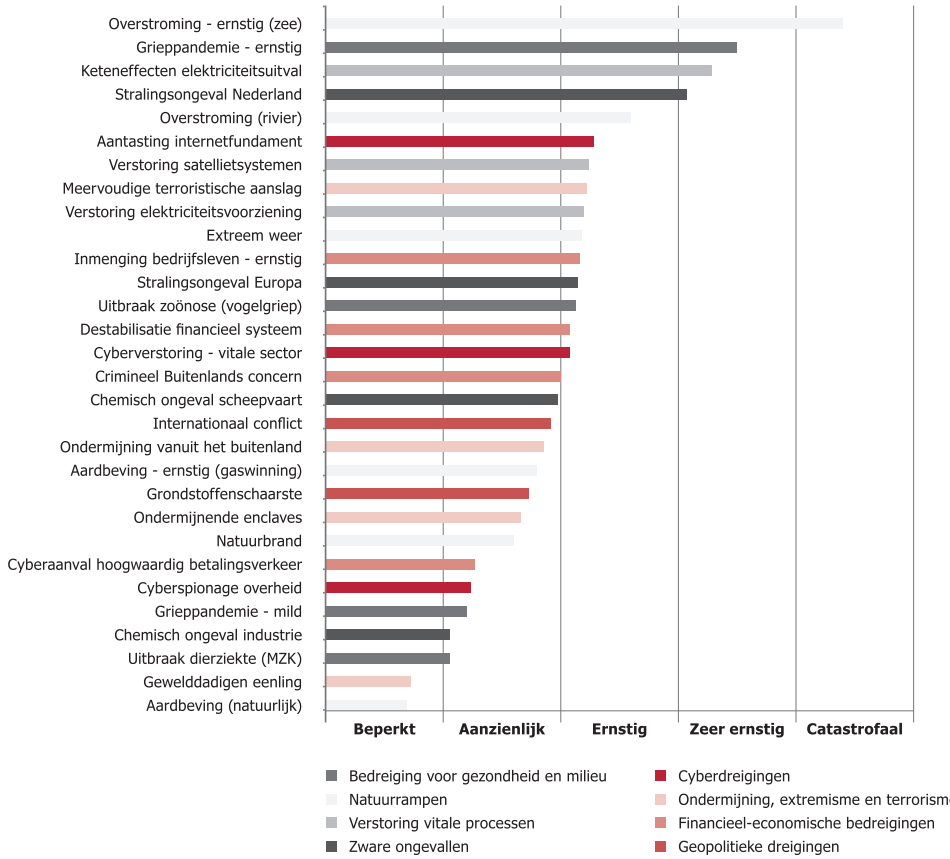
62 Analistennetwerk Nationale Veiligheid 2016: 117-133. De geïntegreerde risicoanalyse nationale veiligheid 2019 is in de bovenstaande analyse is vanwege de recente verschijningsdatum niet meegenomen.

63 Voor de bijbehorende criteria zie p. 31 van Analistennetwerk Nationale Veiligheid 2016.

64 Voor een kritische bespreking van de beoordelingssystematiek van het Analistennetwerk zie WRR 2017a: 92-101. Een van de problemen is dat het verband tussen verschillende risico's uit zicht verdwijnt. Zo kan 'destabilisatie financieel systeem' een 'cyberverstoring' als oorzaak hebben, maar beide risico's worden apart geanalyseerd.

die 'potentieel maatschappijontwrichtend zijn en grote gevolgen kunnen hebben voor de Nederlandse veiligheidsbelangen', zeker op de wat langere termijn.[65]

Figuur 2.1 Impact van diverse typen risico's



Bron: Analistennetwerk 2016: 11.

Een digitale ontwrichting met mogelijk veel economische schade en maatschappelijke onrust is dus een reëel scenario. Deze vaststelling is het vertrekpunt voor de analyse in de volgende hoofdstukken. Met die analyse beogen we een agenda te formuleren voor maatregelen waarmee de samenleving zich op een dergelijke ontwrichting kan voorbereiden. We richten ons daarbij specifiek op de bijdrage van de overheid.

65 Analistennetwerk Nationale Veiligheid 2018: 22. Vgl. DeNardis 2014: 86, 104-106 over het verband tussen cybersecurity governance en nationale veiligheid.

2.5 CONCLUSIE

In dit rapport hanteren we de term 'maatschappelijke ontwrichting' voor ernstige verstoringen van het normale maatschappelijke leven. Wat doorgaat voor het 'normale' maatschappelijke leven en een 'ernstige' verstoring daarvan, hangt behalve met onderbrekingen van kernprocessen in de samenleving ook samen met het vertrouwen dat burgers, bedrijven en private en publieke organisaties in deze kernprocessen hebben. Deze aspecten beïnvloeden elkaar: een grote ontwrichtende gebeurtenis zal onvermijdelijk ook het vertrouwen in de samenleving schaden. Omgekeerd kan een reeks kleinere gebeurtenissen het gevoel van dreiging vergroten en het vertrouwen in de overheid verminderen, zelfs wanneer er feitelijk nog niets aan de hand is.

Door vitale processen aan te wijzen, probeert de overheid prioriteiten te stellen en ervoor te zorgen dat niet alle verstoringen als ontwrichtend worden gezien. Schaarse middelen zijn aldus effectief en legitiem in te zetten. De lijst met vitale processen is daarbij het product van een beoordeling van het vitale belang van bepaalde processen en de mate waarin deze processen kwetsbaar zijn voor verstoring en uitval. Dat ook de verstoring en uitval van digitale infrastructuur maatschappelijk ontwrichtende effecten kunnen hebben, wordt intussen steeds vaker onderkend. In de volgende hoofdstukken hanteren we voor deze effecten het begrip digitale ontwrichting.

3 DIGITALISERING EN MAATSCHAPPELIJKE ONTWRICHTING

3.1 INLEIDING

Digitalisering stelt nieuwe eisen aan de omgang met incidenten die kernprocessen in de samenleving onder druk zetten. In dit hoofdstuk betogen we allereerst dat maatschappelijke ontwrichting onlosmakelijk is verbonden met verstoring of uitval van digitale infrastructuur. Een belangrijke verklaring hiervoor is de sterke verwevenheid van de fysieke en de digitale wereld. Hierdoor hebben incidenten in de digitale wereld steeds vaker een effect in de fysieke wereld en omgekeerd zullen incidenten in de fysieke wereld ook steeds vaker implicaties hebben voor digitale voorzieningen. Ten tweede maken we duidelijk dat digitalisering beleidsmakers voor een aantal nieuwe uitdagingen plaatst. De reden hiervoor is dat het gebruik van digitale technologie leidt tot complexe netwerken. Bovendien heeft digitalisering een sterk grensoverschrijdend karakter, met steeds vaker ook geopolitieke aspecten.

3.2 GROEIENDE AFHANKELIJKHEID VAN DIGITALE TECHNOLOGIE

Digitale technologie is de afgelopen decennia een steeds grotere rol in onze samenleving gaan spelen. Deze ontwikkeling verloopt via de assen van dataficatie, sterk toegenomen rekenkracht en groeiende connectiviteit. Elk van deze drie elementen biedt talloze nieuwe kansen, maar verandert tegelijkertijd ook het risicolandschap voor burgers, bedrijven, organisaties en staten.

DATAFICATIE

Steeds meer maatschappelijke processen zijn gebaseerd op informatiestromen.[66] Deze 'dataficatie' heeft betrekking op drie aspecten.[67] Om te beginnen worden heel veel gegevens opgeslagen en uitgewisseld. De exponentiële groei van data wordt niet alleen veroorzaakt door gerichte verzameling of vrijwillige verstrekking maar in toenemende mate ook door data die het product zijn van geautomatiseerde processen.[68] Ook verandert dataficatie de aard van dataverzamelingen en de analyse daarvan door algoritmen. Data krijgen een autonomere en bepalende positie in het functioneren van de samenleving. Ze worden ingezet voor tal van belangrijke en ingewikkelde processen die de mens niet of nauwelijks meer zelf kan uitvoeren,

66 WRR 2011a.
67 WRR 2015: 27-28.
68 Kitchin 2014: 87-98.

laat staan doorgronden. Tot slot groeit het toepassingsbereik van data: in steeds meer sectoren en voor steeds meer individuen zijn data de grondstof waarop de processen draaien en handelingen vorm en inhoud krijgen. Het is voor talloze bedrijven inmiddels een cruciale zo niet de wezenlijke productiefactor. Ook publieke voorzieningen kunnen niet meer zonder: illustratief is het fijnmazige systeem van zorg- en huurtoeslagen.[69] En voor burgers, ten slotte, zijn data welhaast een dagelijks 'levensmiddel' om ten volle in de samenleving te kunnen functioneren.

Dataficatie kan bijdragen aan maatschappelijke ontwrichting. Door de schaalvergroting neemt de kwetsbaarheid van gegevensprocessen en -bestanden toe. De afgelopen jaren heeft een groot aantal incidenten plaatsgevonden waarbij de gegevens van gebruikers onveilig bleken te zijn opgeslagen, werden ontvreemd door criminelen dan wel 'gegijzeld' in het kader van geopolitieke conflicten. Bovendien neemt door de schaalvergroting niet alleen de kwetsbaarheid als zodanig toe, maar worden steeds meer actoren door een kwetsbaarheid geraakt. In sommige gevallen betrof een incident de gegevens van vele miljoenen gebruikers. Kwaadwillende partijen gaan daarbij steeds gerichter te werk, en proberen in te breken bij organisaties met waardevolle gegevens, zoals banken en ziekenhuizen. Met zowel het groeiende toepassingsbereik als afhankelijkheid van data hebben problemen met de betrouwbaarheid, beschikbaarheid of integriteit van gegevens bovendien steeds grotere gevolgen, ook omdat ze gekoppeld zijn aan alledaagse processen in de samenleving. Uitval of verstoring van een digitaal systeem betekent dat een belangrijke productiefactor niet langer betrouwbaar of beschikbaar is. We hebben dan te maken met een fabriek of overheidsdienst 'zonder personeel', of op z'n minst met flink wat zieke werknemers.

REKENKRACHT

Door de sterk toegenomen rekenkracht van computers is het mogelijk om steeds meer processen, en vooral ook complexe processen, te automatiseren. De meest recente stap in deze ontwikkeling is dat we met behulp van algoritmen niet alleen grotere hoeveelheden data dan voorheen kunnen verwerken, maar ook sneller beslissingen kunnen nemen en dat deels in handen van systemen kunnen leggen. Als ze goed zijn geprogrammeerd en getraind zijn slimme digitale systemen zelfs betrouwbaarder dan mensen bij het maken van snelle en ingewikkelde keuzes. De snelheid waarmee gedigitaliseerde systemen complexe beslissingen nemen, en de schaal waarop dat gebeurt, heeft echter als keerzijde dat processen snel uit de hand kunnen lopen wanneer het misgaat. Vanwege de complexiteit is de oorzaak daarvan voor mensen niet langer snel inzichtelijk, zeker wanneer zulke systemen automatisch op elkaar reageren. Illustratief is het incident waarbij in 2017 de Dow Jones Newswire per ongeluk een bericht publiceerde over de aankoop van Apple door Google, dat louter voor een technische test bedoeld was. De geautomatiseerde handelsrobots reageerden

69 WRR 2011a.

binnen milliseconden, met grote gevolgen voor de aandelenkoersen.[70] Een ander voorbeeld is de zogenaamde 'flitscrisis' die zich voordeed in 2010. Binnen enkele minuten verdampte duizend miljard dollar aan aandelenwaarde door onbedoelde interacties tussen machines.[71] Een recente kwestie betreft de Russische inmenging in de Amerikaanse verkiezingen, waarvan pas na grootschalig onderzoek bleek hoe omvangrijk deze was geweest, mede vanwege het gebruik van automatische nieuwssystemen.[72]

Als de automatische systemen ons in de steek laten, kan dat bovendien tot gevolg hebben dat maatschappelijke processen minder efficiënt gaan draaien, onveilig worden of zelfs helemaal uitvallen.[73] Een voorbeeld is de treinstoring van 21 augustus 2018 op Schiphol, die werd veroorzaakt door een fout in de software van het Dynamisch Verkeersmanagement-systeem (DVM).[74] Het DVM bedient de railinfrastructuur rond Schiphol en zorgt er normaal gesproken voor dat de doorstroom in de Schipholtunnel optimaal is. Toen het DVM uitviel moest de ingewikkelde treindienst tussen Amsterdam en Schiphol met de hand worden geregeld. In plaats van het normale gemiddelde van 20 treinen per uur konden langere tijd slechts 4 treinen per uur op dit traject rijden. Zo'n 50.000 reizigers werden door de verstoring getroffen. Het voorval toont hoe belangrijk een goed werkende terugvaloptie is en de beschikbaarheid van mensen die zonder de hulp van systemen de regie weer in handen kunnen nemen.

CONNECTIVITEIT

Een derde aspect van digitalisering is de groeiende connectiviteit. Het aantal internetgebruikers groeit nog altijd snel, evenals het aantal aan het internet verbonden apparaten, de hoeveelheid data die we uitwisselen en het aantal applicaties en diensten dat loopt via het internet. Het gebruik van cloudcomputing en de opkomst van het Internet of Things (IoT) en artificiële intelligentie zullen de connectiviteit naar verwachting verder versterken en consequenties hebben wanneer maatschappelijke ontwrichting zich voordoet. Goed functionerende netwerken zijn immers cruciaal voor de continuïteit van kernprocessen in de samenleving en kunnen dienstbaar zijn aan een goede en snelle omgang met maatschappelijke ontwrichting, mocht het onverhoopt ergens misgaan.

---

70 www.nytimes.com/2017/10/10/business/media/dow-jones-google-apple.html

71 Schneier 2018: 85.

72 David A. Sanger 2018: 185, 255 noemt 80,000 posts op Facebook, mogelijk gezien door 126 miljoen mensen; en 288 miljoen mensen die Twitterberichten lazen. Het totale aantal geregistreerde Amerikaanse kiezers betrof 200 miljoen, waarvan er 139 miljoen stemden in 2016. De impact van de beïnvloeding is onbekend.

73 Zie bijvoorbeeld Stratix 2017: 4 voor uitval van telecom.

74 Van Gompel 2018.

Bij de meeste digitale diensten en toepassingen kunnen organisaties in principe uit verschillende aanbieders kiezen. Voor enkele onderdelen van het internet ontbreekt echter een alternatief, omdat ze het fundament vormen waarop het internet is gebouwd.[75] Over de kwetsbaarheid van dit fundament verschillen de meningen.[76] Het internet blijkt verrassend betrouwbaar en veerkrachtig te zijn, het vindt – vanwege de decentrale opzet altijd een weg rond problemen. Een grote crisis heeft zich waarschijnlijk mede daarom nog niet voorgedaan. Bovendien zal het effect van een eventuele crisis daarvan sterk samenhangen met de mate van connectiviteit. Tegelijkertijd is het denkbaar dat de bestaande aanvalsmiddelen worden opgeschaald – denk aan een DDoS-aanval met IoT-aparaten.[77] Ook het simpele feit dat onze afhankelijkheid van het internet groeit, maakt dat eenzelfde oorzaak toch een groter gevolg kan hebben.

Bovendien is het lastig te bepalen welke onderdelen van het internet nu werkelijk onmisbaar zijn.[78] Technisch valt dat onderscheid nog wel te maken, maar in de praktijk is dat niet altijd zinvol. Als grote datacenters, grote internet exchanges of authenticatiediensten uitvallen, dan heeft een groot deel van de bevolking daar last van. Hetzelfde geldt voor grote cloud-providers, zoals recente storingen bij Google en Amazon hebben laten zien. In strikte zin betreft het hier geen kernfuncties van het internet, maar de beschikbaarheid van veel internetdiensten komt door dergelijke verstoringen wel degelijk in de gevarenzone terecht. Dit geldt ook voor de lokale fysieke infrastructuur om organisaties aan het internet te koppelen of anderszins aan elkaar te verbinden, bijvoorbeeld via mobiele voorzieningen.[79] Voorbeelden zijn grote netwerkbeheerders. Van uitval bij een van deze beheerders, bijvoorbeeld door een elektriciteitsstoring, heeft het internet als zodanig geen last, maar plaatselijk beperkt dit de connectiviteit en kan dit tot grote problemen leiden.[80] Dergelijke organisaties zijn dermate verbonden met de wereld, dat zij eigenlijk niet mogen uitvallen.[81]

3.3 KETENS, NETWERKEN, GRENZELOOSHEID EN COMPLEXITEIT

De drie hierboven beschreven ontwikkelingen hebben voor grote veranderingen gezorgd in de organisatie van het maatschappelijke leven. Organisatieprocessen en informatiesystemen zijn vervlochten geraakt, de ketens en netwerken die hieruit resulteren overschrijden landsgrenzen en groeien in complexiteit. Hierdoor wordt het steeds lastiger om te anticiperen en te reageren op maatschappelijke ontwrichting.

---

75 Vlg. WRR 2015: 66.
76 Bijvoorbeeld Van Eeten en Bauer 2012 en Van Ruijven en Duijnhoven 2018.
77 Voor dit argument zie bv. Pras 2014.
78 Broeders 2017. Zie Mueller 2017 voor een uiteenzetting over fragmentatie en het internet.
79 Van Ruijven en Duijnhoven 2018.
80 Een voorbeeld is de brand in een gebouw van Vodafone in Rotterdam in 2012, waar de provider netwerkapparatuur had staan. Hierop volgde een grote netwerkstoring, die dagenlang aanhield.
81 Snyder 2017 noemt ze om die reden 'too connected to fail'.

KETENS & NETWERKEN[82]

De overvloedige beschikbaarheid van snelle en goedkope hardware en software heeft organisaties ertoe aangezet om hun productie en dienstverlening zoveel mogelijk *real time* te organiseren. Dit reduceert opslagkosten, zorgt voor efficiënt gebruik van bedrijfskapitaal en maakt het mogelijk zich aan te passen aan veranderende omstandigheden. Wanneer computers of netwerkverbindingen uitvallen, droogt bijvoorbeeld de aanvoer van goederen snel op. Aan het andere einde van de keten dan wel elders in een netwerk gebeurt precies het tegenovergestelde. Zo leidde NotPetya wereldwijd tot grote opstoppingen bij de terminals van Maersk, omdat het internationale registratiesysteem voor containers platlag. Met de onderbreking van dergelijke stromen en productieketens komt ook de economische veiligheid van Nederland in de gevarenzone terecht.[83]

Door de opkomst van het internet en andere grootschalige netwerken is het bovendien mogelijk om processen op afstand aan te sturen. Organisaties maken daarbij steeds vaker gebruik van open netwerkmodellen, waarbij apparaten communiceren via protocollen. Regelmatig vindt deze communicatie plaats over het publieke internet, om te besparen op de kosten van een eigen communicatienetwerk. Een probleem bij de koppeling van beheerssystemen aan grotere netwerken of het internet is echter dat deze systemen soms sterk zijn verouderd en geen ondersteuning meer krijgen van externe leveranciers of de eigen organisatie. Op zichzelf staand kunnen deze systemen in principe veilig functioneren, maar gekoppeld aan grotere netwerken is hun kwetsbaarheid een groot risico omdat buitenstaanders er nu veel gemakkelijker toegang tot kunnen krijgen. Dit geldt onder meer voor systemen waarvan gebruik wordt gemaakt voor de drinkwatervoorziening, het betalingsverkeer en de bediening van sluizen.[84]

Van ketens en netwerken is bekend dat ze kwetsbaar zijn: ze raken verstoord wanneer een afzonderlijke schakel uitvalt. Informatie is verspreid aanwezig over de partijen en het handelen van deze partijen beïnvloedt elkaar onbedoeld. Digitalisering voegt hier een aantal nieuwe kwetsbaarheden aan toe, die gerelateerd zijn aan interfaces met de buitenwereld; keteninformatiesystemen zoals Portbase in de Rotterdamse haven of elektronische patiëntendossiers in zieken-

---

82 Zie voor het onderscheid tussen ketens en netwerken: WRR 2011a, p. 72. De keten is een lineair proces waarin verschillende organisaties buiten hun eigen organisatiegrenzen met behulp van digitale systemen werken aan een gemeenschappelijk resultaat. De term 'netwerk' verwijst naar een relatief open verband waarbij verschillende onderdelen (knooppunten) in relatie staan tot andere onderdelen via veelvoudige, doorkruisende en vaak redundante verbindingen.

83 Zie WRR 2017a voor een analyse van flow security en de aandacht daarvoor in het beleid.

84 NCSC 2015; CPB 2018: 14; Algemene Rekenkamer 2019.

huizen, en gezamenlijke ICT-diensten zoals dataopslag en clouddiensten.[85] Dergelijke toepassingen brengen nieuwe partijen in het spel en daarmee ook nieuwe afhankelijkheden. Ze vergroten vaak ook het aantal interacties, met alle bijbehorende risico's op verstoringen.

Uitval binnen ketens en netwerken kan cascade-effecten tot gevolg hebben, zeker wanneer de verschillende onderdelen daarvan nauw op elkaar aansluiten. Van cascade-effecten is sprake wanneer een afzonderlijk probleem doorwerkt in de rest van de keten, het netwerk of daarbuiten.[86] De gevolgen zijn vooral groot wanneer veel partijen afhankelijk zijn van dezelfde dienst of toeleverancier. Traditioneel geldt dit voor de elektriciteitsvoorziening, waardoor stroomuitval bovenaan de lijstjes prijkt met grote ontwrichtende gevolgen. De vraag is echter of bepaalde delen van de digitale infrastructuur inmiddels niet een soortgelijke positie hebben verworven. Hoewel hard bewijs ontbreekt, blijkt uit een grootschalige analyse van Europese incidenten dat de telecom (37%) en het internet (7%) een goede tweede en derde zijn achter de energiesector (47%) als het gaat om het veroorzaken van cascade-effecten.[87] Voorbeelden van grote afhankelijkheden zijn er in ieder geval te over, variërend van het gebruik van de besturingssystemen van Microsoft, Intelchips die in vrijwel elke computer zitten, de diensten van grote internationale beveiligingsbedrijven voor het mitigeren van cyberaanvallen van banken, bedrijven die draadloze communicatie verzorgen, en het overgrote deel van de software voor elektronische patiëntendossiers, dat in Nederland wordt geleverd door twee aanbieders.[88] Ook is er een uiterst beperkt aantal bedrijven dat – ook in Nederland – dominant is op de markt van clouddiensten voor omvangrijke dataverwerking en -opslag (Amazon, Google, Microsoft en Salesforce).

GRENZELOOSHEID

Digitalisering maakt vrijwel elke organisatie kwetsbaar voor verstoringen in een netwerk of toeleveringsketen, omdat zij voor hun voorzieningen intensief gebruikmaken van de producten en diensten van derde partijen. Tegelijkertijd overschrijden deze netwerken en ketens vaak landsgrenzen. De mondiale connectiviteit en groei van het aantal mondiale productieketens en bijbehorende informatietechnologische voorzieningen maken dat de oorzaak van een maatschappelijke ontwrichting ver over de eigen grenzen gelegen kan zijn. Bovendien: het internet zelf is vrijwel grenzeloos, waardoor elke aan het internet verbonden organisatie in principe overal vandaan

85 Van Ruijven en Keijser 2017. Vergelijk Luiijf en Klaver 2015 en ENISA 2018b.
86 Klaver et al. 2013.
87 Van Eeten et al. 2011.
88 Het bedrijf ChipSoft is inmiddels de grootste leverancier van nieuwe ziekenhuis-epd's in Nederland gevolgd door het bedrijf Epic. Negen van de laatste tien implementaties waren afkomstig van één van deze twee bedrijven. Zie: www.zorgvisie.nl/hoe-konden-chipsoft-en-epic-zo-dominant-worden/

onder vuur kan worden genomen.[89] Maatschappelijke ontwrichting heeft door dergelijke factoren al snel een grenzeloos karakter.[90]

Grenzeloosheid toont zich ook in de mondiale verknoping van voorzieningen en diensten. Voor talloze digitale voorzieningen zijn Nederlandse bedrijven, overheidsinstellingen en burgers afhankelijk van een beperkt aantal grote – vooral Amerikaanse – softwareaanbieders, ICT-dienstverleners en beveiligingsbedrijven. Voor vele clouddiensten geldt dat ze *ergens* op het internet draaien. Dat hoeft bovendien niet eenzelfde locatie te zijn. Het gebruik van clouddiensten kan overigens een goede waarborg zijn voor de continuïteit van die processen, juist omdat data op meerdere plekken zijn opgeslagen. Cloudproviders zijn vanwege hun elastische capaciteit bovendien beter in staat om DDoS-aanvallen te mitigeren en kunnen software direct updaten als patches beschikbaar komen. Door hun verdienmodel hebben cloudproviders bovendien een sterke motivatie om de veiligheid van hun voorzieningen te waarborgen, die hierdoor vaak beter is dan die van hun klanten.[91]

Tegelijkertijd roept het gebruik van clouddiensten nieuwe kwetsbaarheden in het leven. Zo vergroot het gebruik van clouddiensten het aantal betrokken partijen, apparaten en toepassingen, wat aanvallers meer ingangen biedt tot de systemen van hun doelwit. Ook stromen er meer data heen en weer, met een grotere kans op verstoringen. Hiernaast zijn er zorgen over het delegeren van controle over data en toepassingen aan de cloudprovider. Veel clouddiensten bestaan uit een gelaagd en complex samenstelsel van platforms en diensten en van aannemers en onderaannemers, waardoor onduidelijk is wie waarvoor verantwoordelijk is – zeker als het een keer misgaat.[92] Juist hun omvang en het zeer grote aantal andere bedrijven en organisaties dat deze cloudproviders bedienen, maakt ze 'too big to fail' en daarmee vormen ze tegelijkertijd een aantrekkelijk doelwit in geopolitieke kwesties.

COMPLEXITEIT

Tot slot brengt het grote aantal verbindingen, producten, diensten en partijen met zich mee dat systemen steeds complexer worden en moeilijker snel te doorgronden en te beheersen zijn. Fysieke en digitale systemen zijn onlosmakelijk met elkaar verbonden. Digitale technologie en operationele technologie vloeien in elkaar over, met als gevolg dat cybersecurity (het beveiligen van systemen) en safety (de veiligheid en betrouwbaarheid van systemen) met elkaar verweven raken. Deze combinatie is niet zonder problemen. Updates in besturingssystemen en gebruikerssoftware kunnen bijvoorbeeld onbedoeld grote gevolgen hebben voor het

89 Dunn Cavalty 2007: 14.
90 Boin 2017.
91 Hon en Millard 2018: 350.
92 Michels en Walden 2018: 32-37.

functioneren van systemen in ziekenhuizen. De constatering dat de schade als gevolg van WannaCry mede het gevolg was van ontbrekende updates, zoals bij de Britse NHS, is daarom maar de helft van het verhaal (zie box 3.1). De andere helft is dat updates veel tijd kosten vanwege de complexe digitale omgevingen van organisaties, en risico's met zich meebrengen die eerst verkend moeten worden alvorens de updates veilig doorgevoerd kunnen worden.

Box 3.1 WannaCry en de National Health Service (NHS)[93]

De wereldwijde ransomware-aanval WannaCry begon op vrijdag 12 mei 2017 en trof binnen een dag meer dan 230.000 computers in minstens 150 landen. De Britse NHS was een van de bekendste slachtoffers. WannaCry maakte gebruik van een bekend beveiligingslek in Windows, waarvoor Microsoft al twee maanden eerder een patch had uitgebracht. NHS had deze patch niet uitgevoerd. De malware verspreidde zich voornamelijk via het interne netwerk van de ziekenhuizen.

WannaCry ontwrichtte de dienstverlening van een derde (ongeveer 80) van de Britse ziekenhuistrusts en acht procent van de huisartsenpraktijken en NHS-organisaties (totaal zo'n 600 instellingen). Dit leidde tot het annuleren van zo'n 19.000 afspraken van patiënten. Vijf van de 27 geïnfecteerde spoedeisendehulplocaties waren niet in staat om aan alle patiënten zorg te verlenen en moesten worden verplaatst. De communicatie tijdens de crisis verliep moeizaam, doordat het gebruik van e-mail vaak niet mogelijk was als gevolg van de besmetting. Na een week functioneerde de NHS weer normaal.

Schattingen over de totale kosten die WannaCry wereldwijd veroorzaakte, lopen uiteen van enkele honderden miljoenen tot een astronomische vier miljard dollar. Het Britse ministerie voor Volksgezondheid en Sociale Zaken berekende na afloop de kosten, uitgesplitst naar kosten tijdens de crisis en kosten de week erna, en naar directe kosten (verloren productie van patiëntenzorg) en de extra benodigde IT-ondersteuning om getroffen data en systemen te herstellen.

	Tijdens	Nasleep	Totaal
Directe kosten	£ 19 miljoen	0	£ 19 miljoen
IT-kosten	£ 0.5 miljoen	£ 72 miljoen	£ 73 miljoen
Totaal	£ 20 miljoen	£ 72 miljoen	£ 92 miljoen

93 Gebaseerd op: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747464/securing-cyber-resilience-in-health-and-care-september-2018-update.pdf
www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/#

'Complex' is ook meer dan alleen 'ingewikkeld'. Een ingewikkeld systeem bestaat uit veel onderdelen en verbindingen, maar is uiteindelijk geordend. Een complex systeem bestaat ook uit veel onderdelen en verbindingen, maar is deels ongeordend. Een complex systeem wordt gekenmerkt door veelsoortige interacties die eigen, lokale regels volgen. Kortom, er zijn geen 'hogere' regels of beginselen die de verschillende potentiële interacties kenschetsen.[94] Wanneer die interacties nauw op elkaar aansluiten en strak zijn georganiseerd, kunnen verstoringen bovendien omvangrijke externe effecten hebben en op systeemniveau tot problemen leiden.[95]

Vooral dit laatste gegeven roept veel vragen op over de tendens om ogenschijnlijk zorgeloos allerhande apparaten en systemen aan het internet te koppelen, inclusief bedrijfs- en overheidssystemen, apparaten in ziekenhuizen en infrastructurele werken zoals sluizen. Wanneer dergelijke systemen met het internet zijn verbonden, zijn ze potentieel ook kwetsbaar voor fouten en verstoringen in andere delen van wereldomspannende infrastructuur. Het maakt de samenleving op veel grotere schaal dan voorheen kwetsbaar voor onverwacht systeemfalen.[96] De OECD constateert dat vooral de 'indirecte effecten' van dergelijke fouten of verstoringen hierbij tot zeer grote schade kunnen leiden.[97]

Complexiteit is vooral ook een probleem als er iets misgaat. Een explosie vindt plaats op de locatie waar chemische stoffen abusievelijk vermengd raken of vuurwerk tot ontploffing komt, zoals in Enschede. Bij een terroristische aanslag zijn de daders meestal ter plekke actief, of hebben zij op een eerder moment explosieven achtergelaten. Bij verstoring of uitval van digitale voorzieningen liggen oorzaak en gevolg daarentegen regelmatig ver uiteen. Causaliteit is dientengevolge lastig vast te stellen, zeker wanneer kwade opzet in het spel is. Dit betekent dat onduidelijk is hoe en waar crisisinstanties ontwrichting moeten aanpakken. Bij welke organisatie en waar ter wereld moeten ze daarvoor aankloppen, om welke systemen gaat het precies en wie hebben deze in gebruik? Bovendien kan lang onduidelijk blijven of en wanneer een bepaalde handeling, bijvoorbeeld het binnendringen in een systeem, tot ontwrichting zal leiden. Wat het juiste moment van ingrijpen is, valt daardoor heel lastig te bepalen.

94 West 2017.
95 Perrow 1983.
96 Clearfield en Tilcsik 2018: 242.
97 OECD 2003: 45. Klaver et al. 2013 betogen dat de tweede en derde orde effecten van verstoringen vooral groot zijn als ze processen betreffen die vitaal zijn voor andere sectoren/diensten.

3.4 GEOPOLITIEKE ASPECTEN

Digitalisering heeft tot slot ook de positie van Nederland in de wereld veranderd. Digitalisering heeft het 'aanvalsvlak' voor kwaadwillende partijen sterk verbreed en hen de middelen in handen gegeven om ernstige schade aan te richten, middelen die extra aantrekkelijk zijn door de hoge mate van anonimiteit die het internet biedt. De grote afhankelijkheid van buitenlandse aanbieders roept bovendien vragen op over de technologische voorzieningen die Nederland zelf nodig heeft om de continuïteit van haar kernprocessen adequaat te kunnen waarborgen.

AFHANKELIJKHEID VAN GROTE BUITENLANDSE AANBIEDERS

Een groot deel van de organisaties die deze kernprocessen verzorgen is in private handen. Dit geldt bij uitstek voor de organisaties die zich bezighouden met digitale technologie. Voor de integriteit en vertrouwelijkheid van overheidsinformatie is de Nederlandse overheid bijvoorbeeld in belangrijke mate afhankelijk van Fox-IT. Voor telecommunicatiediensten rekent de overheid op bedrijven als KPN. Door dergelijke vormen van afhankelijkheid is de overname van dergelijke organisaties een gevoelige kwestie. Het alarmnummer 112, het landelijke communicatienetwerk voor hulpdiensten (C2000), de Noodcommunicatievoorziening, het glasvezelnetwerk voor Defensie en de telecomdiensten voor Schiphol zijn bijvoorbeeld mogelijk kwetsbaar voor discontinuïteit bij een buitenlandse overname van een aanbieder.[98] Voor veel diensten van bijvoorbeeld Fox-IT ontbreekt een alternatief, waardoor de recente overname van Fox-IT door een Britse partij te denken geeft.[99]

Behalve bij overnames speelt deze kwestie ook bij aanbestedingen en investeringen in nieuwe technologie. C2000 wordt momenteel onderhouden door een van oorsprong Duits bedrijf (Hytera), dat nu in Chinese handen is. Het Chinese bedrijf Huawei werkt samen met alle grote telecombedrijven in Nederland en heeft in Europa een groot aantal contracten lopen om 5G-netwerken te bouwen. Regelmatig is het vermoeden dat dergelijke bedrijven – met of zonder hun medeweten – bijdragen aan de ondermijning van de Nederlandse samenleving, doordat ze spionage, verstoring en sabotage door staten mogelijk maken. Een belangrijk argument hiervoor is dat de landen waarin ze zijn gevestigd wetgeving kennen die ze op dat vlak tot medewerking kan dwingen. Mede om deze reden besloot het kabinet in 2018 het gebruik van antivirussoftware van Kaspersky voor de Rijksoverheid uit te faseren.[100]

---

98 Bulten et al. 2017: VIII.

99 Bulten et al. 2017; Van den Hoven van Genderen 2017.

100 www.rijksoverheid.nl/documenten/kamerstukken/2018/05/14/voorzorgsmaatregel-ten-aanzien-van-gebruik-kaspersky-antivirussoftware. Intussen is beleid in ontwikkeling voor veilige soft- en hardware, zie Ministerie van Economische Zaken en Klimaat en Ministerie van Justitie en Veiligheid 2018.

De groeiende aanwezigheid van met name Chinese bedrijven in de Europese lidstaten geldt hierbij steeds vaker als een risico voor de nationale veiligheid, met name de economische veiligheid.[101] Een groot onderliggend probleem is het onveilige karakter van het internet. Bedrijven hebben belang bij een open en onafgeschermd internet, omdat dat hen in staat stelt om veel gebruikersdata te verzamelen.[102] Een open internet werkt ook in het voordeel van surveillance- en controleactiviteiten van overheden. Bij die activiteiten maken zij deels gebruik van de bestaande onveilige systemen van bedrijven, met telecombedrijven in de hoofdrol, omdat ze toegang bieden tot een groot deel van het digitale gegevensverkeer. China is dan ook zeker niet het enige land dat inbreekt op digitale systemen teneinde informatie te verzamelen en de capaciteit heeft om volwaardige cyberoperaties uit te voeren. Bijvoorbeeld ook de Verenigde Staten, Frankrijk, Rusland, het Verenigd Koninkrijk, Israël en Duitsland hebben professionele militaire cybereenheden en inlichtingendiensten die eigen aanvalsmiddelen ontwikkelen. De opbouw van offensieve cybercapaciteit is vele malen goedkoper en gemakkelijker te realiseren dan een veilig internet, bijvoorbeeld door investeringen in 'public interest technology' of de regulering van vitale infrastructuur.[103] Door voorrang te geven aan de opbouw van offensieve cybercapaciteit, is het netto-effect dat de digitale wereld steeds onveiliger wordt.

KWAADWILLENDE STATEN

Verschillende actoren hebben de capaciteit en het motief om kernprocessen van de samenleving ook daadwerkelijk te kunnen verstoren. Criminele actoren en staten vormen de grootste bedreiging voor de nationale veiligheid.[104] Criminelen richten zich op plekken waar het meeste gewin of effect valt te behalen. Dat zijn steeds vaker publieke voorzieningen, waardoor hun aanvallen ook het dagelijkse leven van burgers verstoren. Behalve grote financiële instellingen liggen ook ziekenhuizen steeds vaker onder vuur, vanwege de vele gevoelige persoonsgegevens die ze beheren en de maatschappelijke afhankelijkheid van zorgvoorzieningen. Staten richten zich op spionage – wereldwijd hebben meer dan honderd landen hiertoe de middelen – alsmede ondermijning van kernprocessen van de samenleving. Van alle dreigingsactoren hebben staten de meeste middelen tot hun beschikking; zij

101 AIVD 2018.

102 Schneier 2018: 56-59. Vgl. Zuboff 2019.

103 Voor enkele voorbeelden zie www.schneier.com/essays/archives/2019/02/public-interest_tech.html

104 Er is geen algemeen aanvaarde typologie van dreigingsactoren. Ook is onduidelijk wat exact als een dreiging geldt. Het Cybersecuritybeeld Nederland 2018 maakt onderscheid tussen staten, criminelen, terroristen, hacktivisten, cybervandalen en scriptkiddies, en insiders. De indeling is – ietwat gewijzigd – gebaseerd op een uitgebreide studie naar typologieën van dreigingsactoren door De Bruijne et al. 2017. De grens tussen deze actoren is in de praktijk tamelijk fluïde, omdat groepen samenwerken en aanvalsmiddelen na gebruik snel 'ingeburgerd' raken.

kunnen specifieke doelen kiezen, daar langdurig op inzetten en daarom de grootste schade veroorzaken.

Was aanvankelijk de angst dat cyberwapens de nationale elektriciteitsvoorziening of militaire commandostructuren zouden platleggen, inmiddels blijken ze voornamelijk gericht op meer alledaagse voorzieningen, vaak om een bepaald doel te bereiken. Voorbeelden zijn het stilleggen van een oliebedrijf (Saudi Aramco) in Saoedi-Arabië, het vernietigen van een hoogoven in Duitsland[105], de in de inleiding al genoemde verlamming van de gemeentelijke computersystemen in Atlanta of manipulatie van verkiezingen. Dergelijke acties vinden vrijwel dagelijks plaats, niet om andere landen te vernietigen, maar om hun functioneren te ontregelen en het vertrouwen van burgers te ondermijnen. Internationale regels over wat is toegestaan en wat een proportionele respons is ontbreken.[106] Omdat staten zeer terughoudend zijn in de bijdrage aan de ontwikkeling van cyberspecifieke internationale gedragsregels en de eigen activiteiten in cyberspace vaak geheimhouden, blijven deze acties in de praktijk meestal onbeantwoord en kunnen ze ook onbelemmerd voortduren.

HET PERFECTE WAPEN

Digitalisering biedt de mogelijkheid om met relatief eenvoudige middelen grote effecten te sorteren, zoals aanvallen op kernfuncties van het internet laten zien (zie box 3.2).[107] Dergelijke aanvallen kunnen namelijk verschillende sectoren treffen, waardoor ze een aantrekkelijke eerste stap kunnen vormen in een escalerend conflict. Ze zijn bovendien een stuk goedkoper en makkelijker uit te voeren dan aanvallen op specifieke organisaties of netwerken, omdat ze niet eerst toegang tot het systeem van het doelwit vereisen, wat maanden of zelfs jaren van voorbereiding kan vergen. Ook kunnen ze met een druk op de knop aan- of uitgezet worden, wat ze geschikt maakt als drukmiddel. Zorgelijk is dat aanvallen op kernfuncties van het internet nog maar beperkt op het netvlies staan in discussies over de nationale veiligheid en cyberconflicten.[108]

105 Zie www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile, p. 31.

106 Mačák 2017.

107 Zie hiervoor WRR 2015, hoofdstuk 2.

108 Snyder 2017 biedt een uitgebreid overzicht van mogelijke verstoringen van kernfuncties van het internet, vergezeld van veel voorbeelden. Zie ook Van Ruijven en Duijnhoven 2018.

Box 3.2 Aanvallen op kernfuncties van het internet: Dyn, Mirai en het IoT

Het Domain Name System (DNS) werd in 2016 gecorrumpeerd door een DDoS-aanval met het botnet Mirai.[109] Door uitval van de relatief onbekende DNS-provider Dyn werden grote internetplatforms als Twitter, Netflix, Reddit en vele andere populaire websites en diensten voor het grootste deel van de dag ontoegankelijk voor gebruikers in de VS en Europa. Opmerkelijk aan de aanval was dat hiervoor duizenden gecompromitteerde consumentenapparaten werden gebruikt, zoals webcams en digitale videorecorders. Later volgde eenzelfde aanval op grote mediawebsites in Frankrijk.[110] Sommige onderzoekers beschouwen de botnetaanvallen met Mirai als een vingeroefening voor het serieuzere werk.[111]

Aanvallen op het DNS komen vaker voor. China voerde in 2015 een vijfdaagse DDoS-aanval uit op Github, die gastheer was voor websites die de Chinese censuur omzeilden. Het was de eerste keer dat een staat de eigen digitale infrastructuur voor offensieve doeleinden gebruikte. In 2015 vielen hackers het top-level DNS van Turkije (.tr) aan, waardoor alle websites die deze domeinnamen gebruikten, zoals banken, mediabedrijven, alle overheidsorganisaties en militaire netwerken minimaal een dag onbereikbaar waren. De aanval duurde ruim twee weken. In 2002 werden alle 13 DNS-rootservers aangevallen.[112] Aanvallen op het DNS zijn lastig te mitigeren, omdat ze normaal gebruikersgedrag imiteren en daardoor niet of nauwelijks zijn te scheiden van normaal internetverkeer.

Cyberwapens zijn zo bezien het 'perfecte wapen'.[113] Ze zijn voor weinig geld te krijgen en ze zijn inzetbaar voor zeer uiteenlopende doeleinden, van het verstoren van organisaties die kernfuncties in de samenleving vervullen tot het zaaien van onrust en twijfel. Bovendien is het gebruik ervan gemakkelijk te ontkennen.[114] Deze eigenschappen hebben gezorgd voor een grote verschuiving in de machtsbalans, omdat nu ook kleinere landen in het digitale domein een relatief grote slagkracht hebben ontwikkeld. Zij kunnen zich op het mondiale strijdtoneel begeven, zonder een grootschalige militaire confrontatie te hoeven aangaan. Cyberaanvallen als NotPetya en WannaCry hebben bovendien laten zien dat de vermeende daders (resp. Rusland en Noord-Korea) bereid zijn om grote nevenschade voor lief te nemen.[115]

---

109 Zie https://en.wikipedia.org/wiki/2016_Dyn_cyberattack
110 ENISA 2018a: 50.
111 Scott en Spaniel 2016.
112 DeNardis 2014: 98.
113 Sanger 2018.
114 ENISA 2017.
115 Ook de aan Israël en de Verenigde Staten toegeschreven Stuxnet-aanval op de kerncentrales in Iran leidde tot grote nevenschade. Zo'n 50.000 computers raakten besmet in onder India, Indonesië, Pakistan en Duitsland. Zie hiervoor Schneier 2015: 150.

3.5 CONCLUSIE

We trekken een aantal conclusies:

- Er is sprake van een zeer sterke verwevenheid van het digitale domein met het fysieke domein. Door ontwikkelingen als dataficatie, het gebruik van algoritmen om beslissingen te nemen en de complexe verbindingen tussen systemen wereldwijd vloeien het digitale domein en het fysieke domein naadloos in elkaar over. Maatschappelijke ontwrichting zal daarom steeds vaker digitale én fysieke dimensies hebben.
- De continuïteit van het normale functioneren van het maatschappelijke leven vertegenwoordigt van oudsher een groot publiek belang. Dat belang is onverminderd groot in een gedigitaliseerde samenleving.
- Digitalisering heeft de samenleving echter op nieuwe manieren kwetsbaar gemaakt voor verstoringen, vanwege onveilige, instabiele en vaak ook slecht beveiligde software en hardware, en de complexe en grensoverschrijdende toeleverings- en productieketens, die kwaadwillende partijen veel mogelijkheden bieden om maatschappelijke processen te verstoren of zelfs geheel stil te leggen.
- De besproken kenmerkende elementen van digitalisering hebben er mede toe geleid dat de continuïteit van maatschappelijke kernprocessen op nationaal niveau sterk afhankelijk is geworden van het doen en laten van buitenlandse partijen, te weten grote aanbieders van digitale voorzieningen en kwaadwillende staten die het op deze voorzieningen hebben gemunt.

4 VOORBEREIDEN OP DIGITALE ONTWRICHTING

4.1 INLEIDING

Voorkomen is beter dan genezen, luidt een bekend adagium. Daar is veel voor te zeggen, zeker als de gevolgen van ontwrichtende gebeurtenissen te vermijden zijn. Ondanks preventieve maatregelen valt echter nooit geheel uit te sluiten dat het normale maatschappelijke leven ernstig verstoord raakt. Het is daarom belangrijk op een ontwrichting voorbereid te zijn, te beginnen met 'paraat staan' en mechanismen voor het vroegtijdig onderkennen van signalen als er iets misloopt. Wanneer een gebeurtenis potentieel ontwrichtend blijkt, is vervolgens een adequate gevolgbestrijding noodzakelijk. Herstel en wederopbouw zijn ten slotte belangrijk om het normale maatschappelijke leven zo snel mogelijk weer doorgang te laten vinden.

Voor risico's zoals een grote overstroming of ernstige griepepidemie hebben overheid en andere partijen in het verleden maatregelen getroffen om de paraatheid te verhogen, signalen voor een maatschappelijke ontwrichting vroegtijdig op te kunnen merken, de gevolgen daarvan te kunnen bestrijden en de wederopbouw te vergemakkelijken. Het risico op maatschappelijke ontwrichting als gevolg van de uitval of verstoring van digitale infrastructuur en processen wordt daarentegen nog maar recentelijk door de overheid onderkend. Mede daarom ontbreekt het aan maatregelen om de samenleving op deze nieuwe vorm van ontwrichting voor te bereiden. Standaard wordt in beleidsprogramma's bovendien de nadruk gelegd op cyberveiligheid en preventie in plaats van op manieren om ontwrichtende gebeurtenissen op te vangen. In dit hoofdstuk bespreken we op welke wijze de voorbereiding op digitale ontwrichting vorm en inhoud kan krijgen. Daarbij onderscheiden we vier stadia: paraatheid, signalering, bestrijding en ten slotte herstel en wederopbouw.

4.2 PARAATHEID

Signalering, bestrijding en vooral herstel en wederopbouw worden in belangrijke mate beïnvloed door de mate waarin een samenleving is voorbereid op de omgang met maatschappelijke ontwrichting. Anders dan bij preventie gaat het hierbij om maatregelen die de effecten van ontwrichting proberen te beperken en bijdragen aan het herstel. Zo voorkomt een terp geen overstroming maar vormt hij een toevluchtsoord bij wassend water en beperkt daarmee het aantal slachtoffers. Een brandgang in een bos gaat een verdere verspreiding van het vuur tegen en een defibrillator reduceert het aantal slachtoffers, maar helpt hartaanvallen niet de wereld uit. Ook in een digitaliserende wereld zijn er voorbereidende maatregelen die de

effecten van maatschappelijke ontwrichting kunnen beperken. Het eerste stadium in het nemen van deze maatregelen betreft paraatheid. We onderscheiden hier de volgende vier onderdelen: terugvalopties, isoleren, oefenen en informatievoorziening.

TERUGVALOPTIES

Opties om op een andere voorziening terug te vallen zijn er in allerlei soorten en maten. Welbekend is de back-upvoorziening, bijvoorbeeld noodstroom door middel van een dieselgenerator. Belangrijk bij dit soort voorzieningen is de vraag hoe lang ze het vol moeten kunnen houden. Bij back-upvoorzieningen van digitale systemen speelt onder meer hoe ver in de tijd de back-up terug moet kunnen gaan en dus hoelang gegevens bewaard moeten blijven. Duidelijk is dat dit sterk verschilt per gegevenstype. Maersk kon na de NotPertya-aanval veel gegevens redden door wereldwijd datacentra te bellen. Wat echter ontbrak was een back-up van de wijze waarop het eigen ICT-systeem was ingeregeld – de digitale kern van het bedrijf dus.[116] Dit voorbeeld toont hoe belangrijk het is voor bedrijven om opnieuw te doordenken voor welke processen een back-upvoorziening belangrijk is. Sommige processen zijn echter zo omvangrijk en complex geworden dat een dergelijke voorziening praktisch onuitvoerbaar is, onder meer gezien de hoge kosten. Kortom, een back-upvoorziening blijft belangrijk maar is voor bepaalde processen geen vanzelfsprekendheid meer.

Een andere voor de hand liggende mogelijkheid bij het nadenken over terugvalopties is variëteit in aanbieders, toepassingen of infrastructuren, zodat er uitwijkmogelijkheden voorhanden zijn. Zo kondigde de minister van Justitie en Veiligheid na de grootschalige storing van 112 in juni 2019 aan een tweede provider te overwegen. Ook de optie van een tweede faciliteit is echter lang niet altijd haalbaar. Zo is er voor het mondiale internet bijvoorbeeld geen reëel alternatief. De enige realistische aanpak is hier een langdurige gezamenlijke inspanning van nationale overheden, bedrijven, non-gouvernementele organisaties en experts om het internet veiliger te maken.[117] Een ander probleem bij variëteit ten behoeve van terugvalopties is de gebrekkig werkende markt voor digitale diensten en producten, in het bijzonder waar het gaat om cyberveiligheid.[118] Het gevolg is dat overheden, bedrijven en organisaties wereldwijd uit slechts een handvol grote aanbieders kunnen kiezen.[119] Juist vanwege hun omvang en belang, vormen deze aanbieders een aantrekkelijk doelwit voor geopolitiek

116 Door stom toeval was Maersk in staat dit systeem te herstellen. Door een lokale stroomstoring was in Ghana een terminal uitgevallen. Deze terminal ontsnapte daardoor aan NotPetya. Zodoende kon Maersk alsnog een kopie van het systeem laten vervaardigen. Zie hiervoor Greenberg 2018.

117 WRR 2015; Mueller 2017.

118 Overvest et al. 2018.

119 Een voorbeeld is het feit dat de drie grootste Nederlandse banken afhankelijk zijn van de diensten van het beveiligingsbedrijf Akamai, zie Overvest et al. 2018.

gemotiveerde aanvallen. Tegelijkertijd zijn ze voor belangrijke delen van de mondiale economie en de Westerse samenleving in feite 'too big to fail'.

Concentratie heeft overigens ook voordelen als het aankomt op het beperken van een ontwrichting. Juist door hun omvang, zijn de grote cloudproviders bijvoorbeeld vaak beter beschermd tegen cyberaanvallen dan de organisaties die er hun data onderbrengen. Vanwege schaalvoordelen zijn de diensten van deze aanbieders bovendien veelal goedkoper dan die van kleinere partijen. Tegelijkertijd moeten afnemers erop vertrouwen dat de organisaties in wiens handen ze de veiligheid van hun data leggen zelf voldoende maatregelen treffen om verstoringen op te vangen. Wanneer een groot aantal afnemers kampt met hetzelfde probleem, rijst bovendien de vraag wie voorrang krijgt. Bij de uitval van Google Cloud (zie hoofdstuk 1) bleek dat Google daar zelf allerlei plannen voor had klaarliggen. De vraag is in hoeverre dergelijke plannen in lijn zijn met de publieke belangen die de overheid behartigt.

Een terugvaloptie kan ook de 'ouderwetse' manier van werken zijn. Bij verstoring of uitval van digitale voorzieningen kunnen organisaties meestal nog terugvallen op een minder efficiënte modus. Zaken worden dan weer tijdelijk op de klassieke wijze afgehandeld, bijvoorbeeld op papier of via het overschakelen op de handmatige bediening van mechanische installaties. Dit veronderstelt echter dat werknemers nog in staat zijn om deze alternatieve systemen te gebruiken. Ook moeten die systemen nog beschikbaar zijn. Met de digitalisering en robotisering verdwijnen in rap tempo handmatige vaardigheden en 'ouderwetse' voorzieningen, zoals lokale faciliteiten (bankkantoren) en contant geld. Paraat zijn betekent dus ook dat een alternatief handelingsrepertoire beschikbaar blijft en voor cruciale voorzieningen wellicht opnieuw wordt aangeleerd. Een illustratief voorbeeld is de Amerikaanse marine die besloot om rekruten weer te leren navigeren op de sterren, zodat ze bij uitval van het navigatiesysteem alsnog hun koers kunnen bepalen.[120]

ISOLEREN

In een bos beogen brandgangen grote bosbranden in te dammen. En bij een kernramp wordt de reactor met beton ingekapseld om de straling te minimaliseren. Elke vorm van ontwrichting kent strategieën om het incident te isoleren en erger te voorkomen. Bij digitale ontwrichting is netwerkscheiding zo'n strategie. Netwerkscheiding valt te zien als het plaatsen van schotten tussen verschillende systemen en de digitale processen die deze systemen afhandelen. De meest radicale vorm van netwerkscheiding is dat een organisatie of bedrijf een algehele ontkoppeling van het mondiale internet bewerkstelligt. Dit wordt ook wel 'verschansing' of (onder ICT-experts) 'islanding' genoemd. In een sterk vernetwerkte wereld is deze strategie echter niet altijd rea-

120 Genoemd in Snyder 2017.

listisch.[121] Digitale schotten sluiten behalve gevaren immers ook de met digitalisering verbonden voordelen buiten.[122] Het gedeeltelijk scheiden of tijdelijk afschakelen van netwerken zijn daarom aantrekkelijker opties (zie box 4.1).

Een goed uitgevoerde netwerkscheiding kan verstoringen een halt toeroepen of verdere verspreiding van de besmetting voorkomen. Zeker voor kernprocessen in de samenleving is netwerkscheiding wenselijk, ook omdat het de afhankelijkheid van derde partijen verkleint. Toch ontbreekt het momenteel bij de meerderheid van de overheidsorganisaties aan een duidelijke strategie en afstemming wat betreft netwerkscheiding. Organisaties beslissen veelal eigenstandig over de vorm en mate van netwerkscheiding en departementen zijn vaak huiverig om op dit vlak eisen te stellen, vanwege de extra kosten die daaraan zijn verbonden.[123]

Box 4.1 Netwerkscheiding[124]

"Diginetwerk is een voorbeeld van gedeeltelijke netwerkscheiding. Via dit netwerk kunnen overheden op een veilige manier gegevens uitwisselen met andere overheden. Diginetwerk verbindt bestaande netwerken van overheidsorganisaties met elkaar, waaronder de Haagse Ring, die op zijn beurt weer als een virtueel gescheiden netwerk draait op het glasvezelnetwerk van het Netherlands Armed Forces Integrated Network (NAFIN)."

"Het bedrijf Tennet (…) heeft een vergaande vorm van netwerkscheiding doorgevoerd. Tennet maakt voor zijn primaire proces – levering van betrouwbare en ononderbroken elektriciteitsvoorziening aan circa 41 miljoen eindgebruikers – gebruik van een eigen ICT-netwerk dat is losgekoppeld van het internet. (…) Voor optimalisering van het primaire proces, waarvoor continu contact nodig is met de elektriciteitsproducenten, maak Tennet wel gebruik van het internet."

De kernenergiewet (art. 40) stelt: "In de kerncentrale is geen enkel vitaal bedieningssysteem aangesloten op het internet".

OEFENEN

In Nederland, de Europese Unie en in NAVO-verband vinden verschillende oefeningen plaats op het terrein van cybersecurity, vaak met een focus op vitale infrastructuur. Daarnaast zijn er sectorale initiatieven, bijvoorbeeld in de telecom, de watervoorziening en de financiële sector. Door te oefenen ontstaat een realistischer beeld van het verloop en de gevolgen van ontwrichting.[125] Oefenen stelt de betrokken partijen bovendien in staat om eerder gevaar te herkennen, noodprocedures nauwkeuriger te

121 WRR 2017a: 21.
122 Boin 2017: 9-10.
123 Geer et al. 2003.
124 Op basis van Munnichs et al. 2017: 29.
125 Lawson 2013; Bergström et al. 2016.

volgen en beslissingen te nemen onder stressvolle omstandigheden. Een belangrijk doel is de versterking van het onderlinge vertrouwen, dat onmisbaar is om in een kritieke situatie snel te kunnen schakelen.[126]

Het aantal cyberoefeningen is wereldwijd tussen 2002 en 2015 sterk gestegen.[127] Steeds vaker is daarbij sprake van een gemengd gezelschap van private en publieke organisaties (zie box 4.2). Europa neemt het grootste deel van de oefeningen voor zijn rekening. Tegelijkertijd moet worden geconstateerd dat in lang niet alle als vitaal aangemerkte sectoren oefeningen plaatsvinden. Bij sommige oefeningen ontbreekt zelfs elke aandacht voor digitale infrastructuur.[128] Ook wordt spaarzaam geoefend over de grenzen van organisaties heen, bijvoorbeeld met oog voor de complexe ketens en netwerken waarbinnen zij functioneren. Dit type oefeningen is niet alleen belangrijk om afhankelijkheden op het spoor te komen, maar ook om meer zicht te krijgen op de verschillende standaarden en protocollen die de betrokken organisaties hanteren. Oefenen helpt om te leren hoe anderen reageren en wie men in voorkomende situaties moet benaderen.[129]

Box 4.2 Cyberoefeningen voor financiële instellingen[130]

Het Threat Intelligence-Based Ethical Red teaming (TIBER) initiatief van De Nederlandsche Bank (DNB) is een publiek-privaat partnerschap, bestaande uit onder andere de politie, het NCSC en banken, verzekeringsmaatschappijen, pensioenfondsen en de aandelenbeurs en heeft derhalve oog voor connectiviteit binnen de financiële sector .

TIBER richt zich op het nabootsen van cyberaanvallen op financiële instellingen. Ethische hackers simuleren de werkwijze van echte hackers en testen op die manier de staat van de cybersecurity van bijvoorbeeld een bank. Wanneer een bank het doelwit is van een ethische hack, is bijna niemand van die bank daarvan op de hoogte. Zowel de aanvaller als de bank zelf leveren na de test cruciale informatie over de digitale beveiliging, waar vervolgens de gehele financiële sector van kan profiteren.

Volgens DNB is het TIBER-testprogramma een goed voorbeeld van een succesvolle samenwerking op het gebied van cybersecurity en kan het tevens toegepast worden in andere vitale sectoren. Op dit moment vindt in samenwerking met de Cybersecurity Alliantie een pilot plaats in de energiesector.

126 Boeke 2016.
127 ENISA 2015: 22-23.
128 Zie bijvoorbeeld Algemene Rekenkamer 2019: 9.
129 EPSC 2017.
130 www.dnb.nl/en/news/news-and-archive/dnbulletin2018/dnb379565.jsp

INFORMATIEVOORZIENING

De gevolgen van digitale ontwrichting kunnen ook op doeltreffende wijze worden beperkt door informatie te verstrekken over wat er aan de hand is en hoe te handelen. Het verschilt per partij welke informatie beschikbaar moet zijn. Voor de organisaties die door de ontwrichting worden geraakt, is het belangrijk te weten hoe zij zelf de gevolgen zoveel mogelijk kunnen beperken. Voor de uitval van het elektronische betalingsverkeer bestaan gedetailleerde communicatievoorschriften, onder meer gericht op vertrouwensherstel.[131] Hulpdiensten zijn daarentegen gebaat bij inzicht in de situatie ter plekke, terwijl direct getroffenen behoefte hebben aan kennis van vluchtroutes, een noodnummer om bevoegde instanties te kunnen inseinen en EHBO. Het digitale equivalent van het laatstgenoemde is bijvoorbeeld informatie over het installeren van een patch of aanvullende maatregelen om de dreiging af te wenden.

Bijzondere aandacht verdient de informatievoorziening aan burgers. Tijdens en direct na maatschappelijk ontwrichtende gebeurtenissen blijken burgers vaak goed in staat om zichzelf en anderen te redden.[132] Maar hun redzaamheid neemt af naarmate een ontwrichtende situatie langer duurt. Hier valt echter weinig aan te doen. Uit onderzoek blijkt dat burgers zich niet of nauwelijks op ontwrichting voorbereiden. Ze schatten de kans op ontwrichting overwegend laag in of denken dat de gevolgen daarvan te overzien zijn. Wel hechten ze aan een adequate reactie van de overheid op crisissituaties.[133] De Nederlandse overheid spreekt burgers echter vooral aan op het nemen van preventieve maatregelen; informatie over digitale ontwrichting en de omgang daarmee blijft goeddeels achterwege.[134]

Overheden onderkennen de potentie van digitale communicatie en sociale media tijdens een ontwrichting.[135] Juist omdat vrijwel iedereen met iedereen in verbinding staat, zijn mensen snel en zelfs *real time* te informeren over zowel ontwrichtende gebeurtenissen als manieren om het normale leven te herstellen. NL-Alert is hiervan een goed voorbeeld. Maar het is niet alleen de overheid die sociale media benut: burgers delen ook onderling berichten en beelden over incidenten. Illustratief zijn de berichten die op sociale media werden gedeeld over de aanslag tijdens de marathon van Boston in 2013.[136] Sociale media kunnen een doeltreffende crisiscommunicatie

131 Zie: www.dnb.nl/binaries/Joint%20Forum%20High%20Level%20Principles%20for%20Businss%20Continuity_tcm46-145518.pdf?2019070914

132 Helsloot en Ruitenberg 2004.

133 Donahue et al. 2014.

134 Frerks 2018. Op https://crisis.nl/wees-voorbereid/cyberaanval/ biedt de overheid tips aan burgers over wat te doen voor, tijdens en na cyberaanvallen. De tips voor tijdens en na een aanval hebben vooral betrekking op digitale maatregelen, zoals het gebruik van een antivirusprogramma en vervanging van wachtwoorden.

135 Simon, Goldberg en Adini 2015.

136 Cassa, Chunara, Mandl en Brownstein 2013.

echter ook grondig verstoren. Burgers zitten bij een incident via de smartphonecamera van medeburgers 'op de eerste rang'. Via talloze sociale media doen ze live verslag, wordt het handelen van hulpverleners beoordeeld en duidt een ieder op zijn of haar hoogstpersoonlijke wijze de impact van de gebeurtenissen en de bijbehorende emoties. En mocht het incident de digitale communicatiemiddelen zelf verstoren of platleggen, dan zal dit – zeker in een samenleving die aan snelle communicatie gewend is geraakt – de onrust alleen maar enorm in de hand werken. Het is in de huidige tijd voor de overheid daarom razend ingewikkeld om aan de voorkant van de berichtgeving te blijven. Bij een grensoverschrijdende ontwrichting komt hier het probleem bij dat de Europese lidstaten de publieke communicatie rondom de negatieve gevolgen van cyberincidenten en -crises maar beperkt op elkaar afstemmen.

4.3 SIGNALERING

Een tweede stadium in de voorbereiding op een mogelijke ontwrichting is signalering. Een vroegtijdige signalering van ontwrichtende gebeurtenissen is belangrijk, want hoe langer zij onopgemerkt blijven, des te groter zijn vaak de verliezen.[137] Bezien vanuit de context van digitalisering heeft signalering vele kanten, waaronder de monitoring van netwerken en informatiestromen. Deze laatste benadering is vooral technisch en laten we hier buiten beschouwing, ten gunste van informatie-uitwisseling. Informatie-uitwisseling geldt als een zeer effectieve manier om de prestaties en continuïteit van belangrijke sectoren te waarborgen.[138] Zowel de organisatie van de informatie-uitwisseling als een strategisch georiënteerde informatiepositie zijn hierbij belangrijke variabelen.

ORGANISATIE VAN DE INFORMATIE-UITWISSELING

In Nederland is de informatie-uitwisseling georganiseerd in verschillende publiek-private samenwerkingsverbanden, met als spil het Nationaal Cyber Security Centrum (NCSC).

137 EPSC 2017: 4.
138 Settanni 2017; Luiijf en Kernkamp 2015; Choo 2011.

Box 4.3 NCSC en aanpalende organisaties

Het NCSC vormt het centrale informatieknooppunt en expertisecentrum op het gebied van cybersecurity en vertegenwoordigt de overheid in tal van nationale en internationale overlegfora. Het NCSC fungeert als Computer Security Incident Response Team (CSIRT) voor de Rijksoverheid en vitale aanbieders.

Het NCSC ondersteunt zowel het Nationaal Detectie Netwerk (NDN) als de zogenoemde Information Sharing Analysis Centers (ISAC's). Binnen het NDN deelt het NCSC informatie over actuele cyberdreigingen met rijksoverheidsorganisaties en vitale private organisaties. De ISAC's dienen als centrale informatieknooppunten van de vitale sectoren op het terrein van cybersecurity. Het ministerie van Economische Zaken en Klimaat faciliteert hiernaast het Digital Trust Center (DTC) dat dient als evenknie van de ISAC's voor niet-vitale partijen. Het DTC bedient 1,6 miljoen bedrijven, van zzp'ers tot en met het grootbedrijf.[139] AIVD en MIVD zijn naast het NCSC de belangrijkste toeleveranciers van informatie over cyberdreigingen.

Het Europees Agentschap voor Netwerk- en Informatiebeveiliging (ENISA) en het Europese Computer Response Team (Cert-EU) vervullen eenzelfde functie als het NCSC maar dan voor de instellingen van de Europese Unie.

De afgelopen jaren is de informatie-uitwisseling tussen overheidspartijen onderling en publieke en private partijen sterk verbeterd en meer dekkend geworden. Verschillende digitale processen, zoals het elektronische berichtenverkeer van de overheid en de identificatie en authenticatie van burgers en bedrijven t.b.v. overheidsdiensten zijn inmiddels als vitaal aangemerkt. Met de implementatie van de Netwerk- en informatiebeveiliging richtlijn (NIB-richtlijn) vallen ook internetknooppunten, beheerders van een register van topleveldomeinnamen en DNS-diensten onder dit regime.[140] De NIB-richtlijn verplicht bovendien grote digitale dienstverleners om incidenten te melden en maatregelen te nemen om risico's te beheersen en de gevolgen van incidenten te verkleinen.[141] Deze uitbreiding is een belangrijke stap vooruit. Toch is het de vraag of het huidige stelsel nog wel langs de juiste lijnen is ingericht.[142] Om te beginnen is de informatie-uitwisseling overwegend sectoraal georganiseerd. Veel op digitalisering gebaseerde processen in de samenleving zijn echter onderling verbonden, wat impliceert dat ontwrichting gepaard kan gaan met sectoroverstijgende

139 www.digitaltrustcenter.nl/over-het-digital-trust-center

140 Voor de organisaties die vallen onder deze drie categorieën geldt dat ze een dienst verlenen die van essentieel belang is voor de instandhouding van kritieke en/of economische activiteiten; dat de verlening van die dienst afhankelijk is van netwerk- en informatiesystemen en dat een incident aanzienlijke verstorende effecten heeft voor de verlening van die dienst. De NIB-richtlijn spreekt van essentiële diensten in plaats van vitale processen.

141 Hiertoe worden gerekend online marktplaatsen, zoekmachines en clouddienstverleners.

142 Voor verwijzingen naar een aantal kritische rapporten, zie CSR 2017: 3.

cascade-effecten. Een snelle en effectieve aanpak van een ontwrichting impliceert dat de informatie-uitwisseling niet alleen plaatsvindt binnen sectoren maar ook tussen sectoren.[143]

De informatie-uitwisseling wordt bovendien belemmerd door het onderscheid tussen 'vitale aanbieders' en 'niet-vitale aanbieders'. Vitale aanbieders zijn betrokken bij de weerbaarheid van de vitale infrastructuur en wisselen via de ISAC's informatie uit met elkaar en met de overheid. Veel vitale organisaties maken echter gebruik van partijen waarvan diensten en producten niet als vitale processen zijn aangemerkt. Dat betekent dat deze partijen niet zijn gebonden aan dezelfde meldplichten als vitale aanbieders, terwijl hun functioneren van grote invloed kan zijn op de continuïteit van vitale processen (zie box 4.4).

Box 4.4 Stroomvoorziening onder digitale spanning[144]

Het Nederlandse elektriciteitssysteem behoort tot de vitale infrastructuur. Doordat dit systeem steeds meer verweven raakt met digitale technologie kunnen problemen met die technologie een groot effect hebben op stroomvoorziening. De leveranciers van deze technologie hoeven veelal niet te voldoen aan dezelfde veiligheids- en beveiligingseisen als vitale aanbieders.

Levering, transport en distributie van elektriciteit worden steeds meer bepaald door geavanceerde software en algoritmes. Deze ontwikkeling brengt nieuwe kwetsbaarheden met zich mee. De kans op uitval door programmeerfouten neemt toe doordat de processen in de energiecentrales en elektriciteitsnetten worden aangestuurd door steeds complexere softwareprogramma's. Verstoringen kunnen zich ook voordoen doordat autonome digitale systemen zich op onvoorziene wijze gedragen en/of op elkaar reageren. Dit risico bestaat bijvoorbeeld bij voorgeprogrammeerde systemen voor de energieproductie en -levering van zonnepanelen en omvormers van windmolens. Tot slot is het gedigitaliseerde elektriciteitssysteem kwetsbaar voor moedwillige verstoring, vooral nu tal van onderdelen van dat systeem in verbinding staan met het internet.

Doordat er steeds meer maatschappelijke functies afhankelijk zijn van elektriciteit kunnen de gevolgen van dergelijke incidenten toenemen en een maatschappelijk ontwrichtende omvang krijgen. Omdat de stroomvoorziening van veel Europese landen verknoopt is geraakt, vormen kwetsbaarheden in het elektriciteitssysteem van het ene land bovendien ook een risico voor het elektriciteitssysteem in andere landen.

143 Zie ook CSR 2017: 6.
144 Gebaseerd op RLI 2018: 14-19.

De vraag is dan ook in hoeverre het huidige onderscheid tussen vitale en niet-vitale aanbieders gehandhaafd moet blijven. Eenzelfde vraag speelt voor de vitale en niet-vitale onderdelen van de overheid, omdat informatiestromen departementale grenzen en bestuurslagen overschrijden.[145]

Het onderscheid tussen vitaal en niet-vitaal heeft tot slot ook gevolgen voor de informatiepositie van het bedrijfsleven en talloze maatschappelijke organisaties. Deze is minder goed dan die van de vitale aanbieders, omdat niet-vitale bedrijven en organisaties minder informatie over kwetsbaarheden ontvangen. Tegelijkertijd vervullen ook deze niet-vitale partijen vaak een cruciale maatschappelijke functie, bijvoorbeeld door medicijnleverantie (PostNL) of het controleren van de kwaliteit van drink- en zwemwater.[146] Om in deze leemte te voorzien is inmiddels het Digital Trust Center (DTC) in het leven geroepen. Het DTC is kortom voor niet-vitale partijen in de private sector de evenknie van de ISAC's. Maar de bedrijven die het DTC moet bedienen verschillen enorm in hun informatiebehoefte, hun vermogen om beschermende maatregelen te treffen, en de maatschappelijke impact van de verstoring van hun functioneren. Dit probleem speelt ook elders: de Britse Cyber security Strategie onderscheidt daarom naast 13 vitale sectoren enkele 'voorkeurssectoren', met als argument dat ook 'andere bedrijven en organisaties' meer ondersteuning behoeven.[147]

Hoewel de informatie-uitwisseling de afgelopen jaren flink is verbeterd, moet de afbakening van kernprocessen van de samenleving worden aangepast. Deze processen zijn in toenemende mate gedigitaliseerd en ingebed in complexe netwerken, waarmee een helder onderscheid tussen vitale en niet-vitale processen niet langer te maken valt en specifieke maatregelen voor vitale processen dus niet per definitie meer veiligheid impliceren. Bovendien zijn er zoveel 'unknown unknowns' dat het onmogelijk is om vooraf precies te weten welke processen en verstoringen daadwerkelijk tot ontwrichting leiden.[148] Ook zijn de ketens en netwerken waarbinnen vitale aanbieders opereren vrijwel allemaal onafhankelijk van landsgrenzen, wat de informatie-uitwisseling een internationaal karakter geeft. Om beter zicht te krijgen op dergelijke afhankelijkheden is een meer strategisch georiënteerde informatiepositie noodzakelijk.

STRATEGISCHE INFORMATIE

Cyberrisico's zijn relatief nieuw en daardoor nog steeds lastig in kaart te brengen en te wegen. Maar de afgelopen jaren zijn belangrijke stappen gezet bij het uitwisselen van

145 WRR 2011a.
146 Voor dit laatste voorbeeld zie www.volkskrant.nl/nieuws-achtergrond/had-de-storing-van-112-voorkomen-kunnen-worden~b235b093/
147 HM Government 2016. Kritiek hierop is dat een langere lijst met vitale processen het ingewikkeld maakt om prioriteiten te stellen, zie hiervoor House of Lords 2018.
148 Boin 2017; Carr 2015.

informatie over digitale veiligheidsmaatregelen, kwetsbaarheden en incidenten.[149] Zo weten we dat elk stukje commerciële software vele kwetsbaarheden kent, waarvan het merendeel nog niet is ontdekt.[150] Ook hardware (bv. chips) blijkt inmiddels te kraken, waardoor het mogelijk is om ongeautoriseerd het geheugen van computers uit te lezen.[151] Uit verscheidene rapporten en literatuur blijkt bovendien dat het landschap van dreigingsactoren voortdurend verandert. Dit alles betekent dat er constant werk aan de winkel is, zowel bij het identificeren van problemen als bij het onder de aandacht brengen van beschikbare oplossingen. Gezien het wereldwijde en soms ook geopolitieke karakter van de dreigingen is een goede internationale positie en inbedding van de inlichtingendiensten daarbij van groot belang.

Toch is een uitwisseling van veiligheidsmaatregelen, kwetsbaarheden en incidenten onvoldoende voor een adequate signalering. Het beeld van de ketens en netwerken waarlangs digitale ontwrichting potentieel kan optreden is namelijk nog slecht ontwikkeld. Daarbinnen zijn het vooral de wederzijdse afhankelijkheden van bedrijven en organisaties die om aandacht vragen. In het bijzonder is veel meer inzicht nodig in de afhankelijkheden van organisaties die een rol spelen bij kernprocessen van de samenleving. Afhankelijkheden zijn momenteel nog te weinig bekend en het belang ervan wordt vaak onderschat.[152] Daardoor zijn verstoringen verderop in de keten slecht bekend en niet of nauwelijks verwerkt in risicoanalyses en crisisplannen.

Voor een goed begrip van afhankelijkheden is het eveneens nodig om deze te analyseren en bediscussiëren vanuit een internationaal perspectief.[153] Incidenten kunnen op verschillende manieren de Europese lidstaten treffen. Dat kan allereerst doordat bij aanvallen gebruik wordt gemaakt van generieke kwetsbaarheden. Hiernaast kunnen de diensten van de verschillende lidstaten van elkaar afhankelijk zijn, waardoor incidenten in het ene land gevolgen kunnen hebben voor het andere. Internationaal betalingsverkeer is een goed voorbeeld. Tot slot kunnen aanvallers gebruikmaken van netwerken om hun doelen te bereiken, wat verstoringen als vanzelf een groot bereik geeft. Nederland bevindt zich daarbij in een bijzonder verantwoordelijke positie, gezien het hoogwaardige karakter van de digitale infra-

149 Hausken 2007.
150 Volgens Schneier 2015: 145-146 gaat het om honderden of zelfs duizenden kwetsbaarheden. Pupillo et al. 2018 komen tot een veel lager aantal. Zij spreken van tenminste 14 kwetsbaarheden in een gemiddeld softwareprogramma.
151 Zie bijvoorbeeld: https://techcrunch.com/2018/05/01/what-do-meltdown-spectre-and-ryzenfall-mean-for-the-future-of-cybersecurity/?guccounter=1
152 NCTV 2018a; Klaver et al. 2013: 56; CSR 2017.
153 ENISA 2018b: 21.

structuur. Nederland is bijvoorbeeld een belangrijke internationale doorvoerhaven van malware.[154]

Ook is meer kennis over de strategische positie van de overheid gewenst. Wat zijn haar sturingsmogelijkheden tijdens een digitale ontwrichting? Met welke context en afhankelijkheden krijgt zij in een dergelijke situatie te maken? Illustratief is hier dat het merendeel van de vitale aanbieders een privaat karakter heeft en daarmee niet valt onder directe overheidscontrole. Bovendien bevindt een deel van deze aanbieders zich buiten onze landsgrenzen. Welke zeggenschap heeft de overheid over dergelijke partijen in het geval van een ontwrichting? De context waarbinnen de overheid in geval van een digitale ontwrichting moet opereren, kan ook worden beïnvloed door marktconcentratie of buitenlands aandeelhouderschap. Het risico van (buitenlands) aandeelhouderschap is in veel sectoren adequaat ingeperkt, maar bij vitale infrastructuur is deze vraag onverminderd aan de orde, zoals opgemerkt in het voorgaande hoofdstuk.[155] Hiernaast zijn ook de verdere keuzes belangrijk nu vitale processen steeds verder digitaliseren. Hier moet in ieder geval de relatie met en afhankelijkheid van (buitenlandse) private digitale dienstverleners genoemd worden, zoals cloudproviders. Vooruitkijkend spelen beslissingen over investeringen in nieuwe digitale technologie. Wanneer de overheid dergelijke ontwikkelingen niet vroegtijdig in het vizier heeft en daarop probeert te sturen, kan het moeilijker zijn om invloed uit te oefenen op de wijze waarop een digitale ontwrichting zich voltrekt.

VERANTWOORDELIJKHEDEN

Het verleden leert dat in geen enkele sector de veiligheid is verbeterd zonder nadrukkelijk sturen door de overheid. In een complexe en vernetwerkte samenleving en economie zal veiligheid echter ook de collectieve inzet van andere partijen vereisen.[156] De verantwoordelijkheid van de overheid richt zich hier op het scheppen van voorwaarden om informatiedeling goed te laten verlopen. Tegelijkertijd moet zij bevorderen, en soms ook afdwingen, dat marktpartijen hun verantwoordelijkheden nemen en de daartoe benodigde competenties ontwikkelen. Deze rol speelt de overheid van oudsher omwille van de veiligheid van tal van maatschappelijke processen. Door de digitalisering van deze processen zal de overheid deze rol ook in het digitale domein moeten vervullen.

Het delen en analyseren van informatie is nodig om de cybersecurity van organisaties te verhogen, ze weerbaarder te maken tegen incidenten en de schade van die incidenten te beperken. De huidige informatie-uitwisseling wordt echter gekenmerkt door een zekere mate van vrijblijvendheid, omdat niet elke partij deelneemt aan de

154 NCTV 2018a. Volgens een rapport van McAfee host Nederland 24% van de servers wereldwijd waarmee botnets worden aangestuurd. Zie McAfee 2017: 81.

155 Zie ook Bulten et al. 2017: viii.

156 WRR 2012.

ISAC's of de relevante informatie verstrekt. Partijen zijn sowieso vaak huiverig om informatie te delen. Het uitwisselen daarvan is een gevoelige zaak, uit oogpunt van concurrentie, wettelijke beperkingen, nationale veiligheid en de dubbelrol van de overheid, die verkregen informatie ook kan gebruiken voor controles.[157] En tijdens een crisis is dat een nog grotere uitdaging dan ervoor, in de zogenaamde 'koude fase'. Reputatieschade kan dan immers ook een rol gaan spelen.[158] Tegelijkertijd zou op veiligheid niet geconcurreerd mogen worden.[159] De uitdaging is er daarom in gelegen dat de overheid de eigen positie weet te versterken, zonder de veilige, vertrouwelijke en gecontroleerde informatiedeling op het spel te zetten. De recent in Nederland geïmplementeerde NIB-richtlijn biedt hiertoe de handvatten, door aan vitale aanbieders strengere eisen op te leggen over het melden van incidenten.[160] Tegelijkertijd is nog onvoldoende duidelijk hoe het toezicht hierop is geregeld en welke consequenties er zijn verbonden aan het schenden van de vertrouwensbasis die ten grondslag ligt aan het delen van informatie.[161]

4.4 BESTRIJDING

De afgelopen jaren hebben zich met digitale processen verschillende kleine en grotere incidenten voorgedaan. We kunnen stellen dat deze in ieder geval in ons land succesvol zijn bestreden, nu een maatschappelijke ontwrichting is uitgebleven. Ook zou daarmee de conclusie kunnen worden getrokken dat de huidige instrumenten en regelingen afdoende zijn. Toch vraagt digitalisering, en met name de vervlechting van de digitale en fysieke wereld, wat ons betreft om het opnieuw doordenken van bestaande kaders en procedures. We bespreken hieronder een drietal kwesties die tonen dat ook wat betreft bestrijding het bestaande instrumentarium aanpassing behoeft: bevoegdheden, grensoverschrijdende bestrijding en prioriteiten stellen.

BEVOEGDHEDEN

In de fysieke wereld heeft de overheid verschillende middelen om crises te bestrijden en de gevolgen daarvan in te perken. Te denken valt aan de inzet van hulpdiensten als politie, brandweer, ambulancediensten en reddingsbrigades. Deze en andere diensten hebben bovendien bevoegdheden om hun taak uit te oefenen, zoals het afzetten van locaties, het binnentreden van bedrijven of het in gang

157 Koepke 2017.
158 Bharosa et al. 2010.
159 Van Vollenhoven 2019: 80.
160 Er zijn meerdere meldplichten. Zie hiervoor paragraaf 5.
161 Luiijf en Kernkamp 2015: 18 betogen dat vertrouwensrelaties behalve door beloning (informatie van anderen) ook door sanctie van uitsluiting (geen informatie) gereguleerd moeten worden.

zetten van evacuaties.[162] Op welke middelen kan de overheid terugvallen bij een crisis met een sterke digitale component? De hack bij Diginotar in 2011 maakte op pijnlijke wijze duidelijk hoe afhankelijk de overheid was van private partijen om een probleem in de digitale wereld op te lossen.

Box 4.5 De overname van DigiNotar[163]

Op 29 augustus 2011 kreeg de overheid een melding van problemen bij certificaatautoriteit DigiNotar, die mede zorgde voor de beveiliging van de elektronische communicatie door en tussen overheden (de zgn. Public Key Infrastructure of PKI). Hackers waren erin geslaagd om vervalste certificaten van DigiNotar vrij te geven. Hierdoor konden ook de overheidscertificaten niet meer worden vertrouwd en werden ze mogelijk onbruikbaar, met aanzienlijke gevolgen voor de digitale dienstverlening van de overheid. Goederen in de Rotterdamse haven zouden bijvoorbeeld niet meer geaccepteerd kunnen worden, de uitkering van toeslagen zou geblokkeerd raken en ook het betalingsverkeer zou grote hinder kunnen ondervinden.

De directe aanleiding voor deze situatie lag bij de grote browserleveranciers, waaronder Microsoft, die dreigden het vertrouwen op te zeggen in álle DigiNotar-certificaten, inclusief de PKI-overheidscertificaten. Dit was een reëel scenario, aangezien Microsoft bij de maandelijkse beveiligingsupdate ook het gebruik van alle DigiNotar-certificaten kon blokkeren om de vertrouwenspositie veilig te stellen. Microsoft wilde geen potentieel onveilige communicatie blijven ondersteunen, ongeacht de partijen die daarbij waren betrokken.

De Nederlandse overheid had dus alle belang bij helderheid over de mate waarin de certificaten gemanipuleerd of gecompromitteerd waren. Maar onderzoek gaf hierover onvoldoende uitsluitsel. Op 3 september besloot de overheid daarom het bewind van DigiNotar over te nemen. Voor deze handeling bestond geen specifieke rechtsgrond, maar de overheid kon na aandringen rekenen op de 'vrijwillige' medewerking van het Amerikaanse moederbedrijf Vasco. Microsoft stelde daarop de update voor Nederland een week uit, waardoor er voldoende tijd was de certificaten te vervangen.

Kijken we naar de besluitvormingsstructuur bij de inzet van bevoegdheden, dan lijken op het eerste gezicht de zaken goed geregeld, zeker waar het de crisisbesluitvorming betreft. Bij maatschappelijke ontwrichting loopt de besluitvorming via de structuur die is vastgelegd in het Nationaal Handboek Crisisbesluitvorming (NHC).

---

162 Zie o.m. de Wet op de veiligheidsregio's, die stelt dat partijen het bestuur van de veiligheidsregio de informatie moeten verschaffen die nodig is voor een adequate voorbereiding van de rampenbestrijding en crisisbeheersing (artikel 48 lid 1), de burgemeester op de hoogte moeten stellen van een ramp en de veiligheidstechnische gegevens moeten verstrekken die nodig zijn voor de bestrijding daarvan (artikel 50 lid 1-2). De Wet op de veiligheidsregio's bepaalt tevens dat de hulpdiensten bevoegd zijn om elke plaats te betreden, die redelijkerwijs nodig is voor de vervulling van hun taak (artikel 62).

163 Gebaseerd op rapporten van de Onderzoeksraad voor Veiligheid 2012 en Inspectie Veiligheid en Justitie 2012.

Voor digitale ontwrichting bestaat in aanvulling hierop het Nationaal Crisisplan ICT, dat momenteel wordt herzien. De overheid heeft volgens het NHC drie rollen: faciliteren, richting geven en sturen. Voor dat laatste – bijvoorbeeld bijstand door politie of brandweer of het vorderen van schaarse goederen – is bevoegdheid nodig. Het NHC noemt ook 'maatregelen in geval van een groot ICT-incident', maar welke dit zijn wordt niet uitgewerkt.[164]

Box 4.6 Besluitvorming tijdens een ICT-crisis

Het nationaal Crisisplan ICT omschrijft een ICT-crisis als 'een dreiging of crisis waarbij de bron ligt in het ICT-domein, waarbij één of meerdere vitale belangen in het geding zijn waarvoor de reguliere structuren niet toereikend zijn'.

Bij een (dreigende) ICT-crisis wordt de ICT Response Board geactiveerd (IRB), een flexibel samengesteld publiek-privaat samenwerkingsverband. De IRB analyseert de crisis en adviseert als nodig de Interdepartementale Commissie Crisisbeheersing, het ambtelijke voorportaal van de Ministeriële Commissie Crisisbeheersing, voorgezeten door de minister van Justitie en Veiligheid of de minister-president.

Van private partijen mag verlangd worden dat zij hun medewerking verlenen op het moment dat (dreigende) verstoring of uitval van hun systemen publieke belangen in gevaar brengen. Zij dienen inzicht te geven in de situatie en mee te werken aan het bestrijden van de oorzaken en gevolgen van digitale ontwrichting.[165] Maar de belangen van private organisaties vallen zeker niet altijd samen met de publieke belangen die de overheid behartigt, en de overheid heeft weinig middelen om de medewerking van private organisaties af te dwingen. Haar rol op het terrein van cyber beperkt zich tot advies en bijstand aan de private organisaties die deel uitmaken van de vitale infrastructuur. Mede hierdoor kreeg de gemeentelijke crisisorganisatie van Rotterdam geen toegang tot de terminals en systemen van de Rotterdamse vestiging van het containerbedrijf Maersk, toen deze getroffen was door NotPetya (zie box 4.7).

164 Ook het Nationaal Crisisplan ICT, Ministerie van Veiligheid en Justitie 2012 gaat hier niet op in.
165 Luiijf en Klaver 2015: 266 bepleiten in dit kader directe toegang tot relevante ICT-systemen van producenten.

Box 4.7 NotPetya en de gemeente Rotterdam

In juni 2017 verspreidden Russische militaire hackers de ransomware NotPetya. Een van de grote slachtoffers was Maersk, dat wereldwijd containerterminals beheert. Gates konden niet worden gebruikt, kranen werkten niet, vrachtwagens konden hun vracht niet kwijt en er konden geen nieuwe boekingen worden verricht. Het hypermoderne Maersk was gedwongen op papier over te schakelen.[166]

Ook de terminals in de Rotterdamse haven werden getroffen. Containertransport via haven, snelweg en spoor kwam deels stil te liggen waardoor opstoppingen ontstonden, met lange files tot gevolg. De gemeente Rotterdam bleek niet voorbereid op een dergelijke situatie. De juiste partijen waren moeilijk bijeen te brengen en bovendien kreeg de gemeentelijke crisisorganisatie – verantwoordelijk in het geval van problemen met de openbare orde – aanvankelijk geen toegang tot de terminals en systemen van Maersk. Daardoor kon de gemeente zich geen goed beeld vormen van de ernst van de situatie, bijvoorbeeld over de vraag of er problemen voor de openbare orde zouden ontstaan.

Bovendien was formeel geen beroep mogelijk op bijstand van het NCSC omdat de APM-terminals van Maersk in tegenstelling tot het Rotterdamse Havenbedrijf geen onderdeel uitmaakten van de vitale infrastructuur.

Toch staat de overheid niet geheel met lege handen. Om te beginnen omschrijft veel sectorwetgeving de bevoegdheid van de overheid in geval van buitengewone omstandigheden. Deze bevoegdheid komt erop neer dat organisaties tijdens crises verplicht zijn om mee te werken en opvolging te geven aan opdrachten van de overheid. Deze sectorwetgeving is echter zeer complex en uitgebreid.[167] In de praktijk zijn uitgebreide schema's en handboeken nodig om de betrokken partijen wegwijs te maken. Hoewel sectorwetgeving waarschijnlijk bruikbare aanknopingspunten biedt voor overheidsingrijpen bij digitale ontwrichting, is het de vraag of deze bevoegdheid voldoende dekkend is en toegesneden op de problemen van een digitaliserende wereld.

De overheid kan ook optreden zonder van sectorspecifieke bepalingen gebruik te maken. Als het misgaat, dan geldt letterlijk 'nood breekt wet'. Dit is in algemene zin echter geen wenselijke situatie.[168] Allereerst is dan improvisatie geboden. Hoewel de bestrijding van maatschappelijke ontwrichting een zekere mate van improvisatie veronderstelt, heeft het vanuit het oogpunt van rechtsstatelijkheid de voorkeur de

166 Greenberg 2018.
167 Muller 2014: 45.
168 Opmerkelijk is dat ook in het kader van de modernisering van het staatsnoodrecht momenteel wordt nagedacht over het aanvullen van de bestaande noodbevoegdheden met bevoegdheden om bepaalde ICT-diensten te vorderen, juist om niet te hoeven terugvallen op een nietgeregelde inzet van bevoegdheden. Zie hiervoor: www.rijksoverheid.nl/documenten/kamerstukken/2018/07/03/tk-modernisering-staatsnoodrecht

marges voor improvisatie niet te groot te maken.[169] Bovendien is het wenselijk om het handelen van de overheid voorspelbaar te maken en daarmee beter controleerbaar. Dit argument geldt bij uitstek als opsporingsinstanties als de politie en de Officier van Justitie interveniëren.[170] Een cruciale vraag is of een dergelijke interventie gerechtvaardigd is als deze niet ook een opsporings- of vervolgingsdoel dient. De Commissie Koops suggereerde in dit verband een aparte regeling voor overheidshandelen gericht op het verstoren van strafbare activiteiten.[171] Een dergelijke regeling is wellicht ook denkbaar voor handelen gericht op de aanpak van incidenten met als doel escalatie tegen te gaan.

Overigens blijft het niet bij de vraag *of* er een bevoegdheid is. Belangrijk is ook *wie* feitelijk besluiten nemen en noodzakelijke acties in gang zetten. Net als in de fysieke wereld zullen bedrijven in de digitale wereld in eerste instantie voor hun eigen veiligheid moeten zorgen en in een eigen bedrijfshulpverlening moeten voorzien. Grote bedrijven zullen een eigen digitale brandweer moeten hebben, bijvoorbeeld in de vorm van cybersecurityafdelingen, sectoraal opererende CERT's of particuliere cybersecuritybedrijven.[172] Pas bij (potentieel) maatschappelijk ontwrichtende gebeurtenissen komt de overheid in beeld.

Een probleem hierbij is echter dat vaak niet al meteen helder is wie of wat de oorzaak is van een incident en – in het geval van een moedwillige verstoring – welke motieven daarbij een rol spelen.[173] Dientengevolge is onduidelijk of nu Defensie, het NCSC, de politie of de inlichtingendiensten aan zet zijn. Elk van deze instanties dient bovendien andere belangen en heeft eigen bevoegdheden. De aanpak van incidenten kan daardoor verschillen vertonen. Terwijl de politie op zoek gaat naar daders zodat het OM vervolging in kan stellen, zullen de inlichtingendiensten geneigd zijn hun informatiepositie te beschermen. Het NCSC zal daarentegen herstelwerkzaamheden centraal stellen, uitgaande van zijn missie om een veilige, open en stabiele informatiesamenleving te waarborgen. Ook de politie heeft de bevoegdheid om hulp te verlenen en escalatie te voorkomen, maar dan moet wel de openbare orde en publieke veiligheid concreet in het geding zijn.[174] Het NCSC is niet aan deze voorwaarde gebonden.

Concluderend stellen we vast dat er voor het digitale domein geen duidelijke en voldoende ingekaderde bevoegdheid bestaat om ontwrichtende gebeurtenissen

169 Zie hierover Kortmann 2009.
170 De Officier van Justitie zou om poolshoogte te kunnen nemen een beroep kunnen doen op de doorzoekingsbevoegdheid conform art. 96c Sv. Zie hiervoor Prins 2019: 721.
171 Commissie modernisering opsporingsonderzoek in het digitale tijdperk 2018: 64.
172 Voor een soortgelijke redenering, zie Prins 2012: 44-45.
173 Prins 2012: 45.
174 Prins 2019: 578.

te bestrijden. Het accent ligt nu op het adviseren en ondersteunen van organisaties binnen de vitale infrastructuur. Wanneer organisaties weigeren mee te werken, is onduidelijk welke middelen de overheid heeft om in te grijpen en op welke gronden dat dient te gebeuren. Daar waar in het verleden is ingegrepen, vond dat min of meer 'op de bluf' plaats. Deze ad hoc handelswijze hangt sterk samen met de beperkte en op technische expertise en bijstand gerichte bevoegdheid van het NCSC en diens voorganger GovCert.

GRENSOVERSCHRIJDENDE CRISES BESTRIJDEN

In een digitaliserende samenleving houdt ontwrichting zich niet netjes aan landsgrenzen. Grensoverschrijdende crises opvangen is per definitie lastig, zo blijkt uit onderzoek.[175] Toch zijn er internationaal wel enkele stappen gezet. Zo heeft de EU verschillende voorzieningen voor crisismanagement, waarvan een deel specifiek is voor cybersecurity.[176]

Box 4.8 Europese en internationale voorzieningen

Het belangrijkste initiatief is de Cyber Security Strategie van de Europese Unie uit 2013, met als concreet uitvloeisel de NIB-richtlijn uit 2016 en de Cybersecurity Act uit 2018. De NIB-richtlijn verplicht de lidstaten tot instelling van een nationaal centrum voor cybersecurity en Europese samenwerking daartussen. Een belangrijk element uit de Cybersecurity Act is de versterking van ENISA, het EU-agentschap voor cybersecurity.

De EU kent een aantal gespecialiseerde organisaties op het terrein van cybersecurity, met als belangrijkste voorbeelden ENISA, het Europese Centrum voor Cyber Crime Centrum (EC3) dat valt onder Europol, het European Defence Agency (EDA), en het Europese Computer Emergency Response Team (CERT-EU).

Een aantal landen, waaronder Nederland, heeft een intentieverklaring getekend voor een EU Cyber Rapid Response Force, om bij een grootschalig digitaal incident snel te kunnen reageren.[177]

Het Forum of Incident Response and Security Teams (FIRST) is een wereldwijd samenwerkingsverband voor CERT's. Hierbij zijn vanuit Nederland onder meer de CERT van het ministerie van Defensie en diverse teams uit het bankwezen en SIDN aangesloten.[178]

175 Boin en Lodge 2018.
176 Backman en Rhinard 2018.
177 Zie https://eeas.europa.eu/topics/eu-international-cyberspace-policy/47525/new-tool-address-cyber-threats-eus-rapid-response-force_en. Vergelijk het voorstel voor een Europees cyberagentschap in CEPS 2018b. Dit agentschap kent ook de bevoegdheid om aanvallen te attribueren.
178 Hamer et al. 2019: 67.

De afgelopen jaren is de capaciteit van deze voorzieningen uitgebreid.[179] Ook zijn er grensoverschrijdende initiatieven in gang gezet gericht op het vergroten van de cyberveiligheid in kritieke sectoren, zoals de energie- en transportsector.[180] De huidige mechanismen om grensoverschrijdende crises op te vangen, zijn echter versnipperd over diverse instituties. Bovendien is hun functie niet altijd even scherp gedefinieerd en volgens experts functioneren ze op z'n best middelmatig.[181] De NIB-richtlijn brengt hierin enige verbetering, maar voorziet desondanks niet in een samenwerkingskader op het niveau van de Unie in het geval van grootschalige cyberincidenten.[182] De lidstaten hebben de Europese Commissie daarom verzocht plannen te ontwikkelen voor de afwikkeling van een groot cyberincident waarbij meerdere lidstaten zijn betrokken. Inmiddels is daarvoor een 'blauwdruk' gepubliceerd[183], waarmee is uitgetekend hoe tijdig en effectief gereageerd kan worden op incidenten. Met deze blauwdruk zal echter wel geoefend moeten worden. En omdat hij geen nieuwe bevoegdheid in het leven roept, komt de bestrijding hoe dan ook neer op nationale mechanismen voor crisisbeheersing, waarvan de vraag is of ze voldoende zijn toegesneden op de nieuwe situatie.

PRIORITEITEN STELLEN

De laatste kwestie die we in relatie tot bestrijding bespreken is het stellen van prioriteiten. Niet alle instrumenten zijn immers tegelijk in te zetten en sommige voorzieningen zullen wellicht ten koste van andere zoveel mogelijk in de lucht gehouden moeten worden. Het hiervoor besproken belang van een duidelijk omschreven bevoegdheid toont zich ook bij de keuzes die nodig zijn bij het bestrijden van een ontwrichting. Om te beginnen speelt de vraag wanneer de overheid welke instrumenten dient in te zetten. In diverse landen werkt men aan een nadere categorisering van cyberincidenten (zie box 4.9). Interessant aan deze initiatieven is de koppeling tussen de signalering en bestrijding van cyberincidenten enerzijds en bevoegdheid anderzijds, bijvoorbeeld wettelijke opsporing en vervolging. Een belangrijk doel is tevens een effectievere inzet van middelen en daarmee uiteindelijk betere hulp aan slachtoffers.

---

179 www.enisa.europa.eu/news/enisa-news/csirts-and-incident-response-capabilities-in-europe

180 Europese Commissie 2016.

181 Boin en Lodge 2018. Zie ook Europese Commissie 2016: 2.

182 In Nederland geïmplementeerd met de Wet beveiliging netwerk- en informatiesystemen (Wet van 17 oktober 2018, Stb. 2018, 387). https://wetten.overheid.nl/BWBR0041515/2018-11-09

183 Zie http://ec.europa.eu/transparency/regdoc/rep/3/2017/NL/C-2017-6100-F1-NL-MAIN-PART-1.PDF. . Bij het document is ook een blauwdruk gevoegd, zie daarvoor: http://ec.europa.eu/transparency/regdoc/rep/3/2017/NL/C-2017-6100-F1-NL-ANNEX-1-PART-1.PDF

Enkele voorbeelden:

Box 4.9 Categorisering cyberincidenten

Frankrijk overweegt een classificatie van cyberaanvallen, gekoppeld aan specifieke respons-mogelijkheden.[184] De Verenigde Staten kennen al sinds 2014 een dergelijk systeem. Het wordt door het National Cybersecurity and Communications Integration Center (NCCIC) gebruikt voor het rapporteren van incidenten en stelt de organisatie naar eigen zeggen in staat om objectieve nationale risicobeoordelingen te doen, beter te prioriteren en tijdig te reageren op de behoeften van de deelnemende partijen. Het NCCIC werkt met een score van 1 tot 100 gebaseerd op 8 criteria:

- feitelijke impact op een organisatie;
- geobserveerde activiteit;
- plaats van detectie;
- betrokken actoren;
- type informatie dat is kwijtgeraakt, gecompromitteerd of gecorrumpeerd;
- herstelmogelijkheden;
- intersectorale afhankelijkheden;
- mate van maatschappelijke ontwrichting.[185]

Het Verenigd Koninkrijk heeft recent een systeem van 6 categorieën incidenten ontwikkeld, waarbij het gehele spectrum van mogelijke incidenten is gedekt, van lokale incidenten tot nationale noodtoestanden. Het Britse National Cyber Security Centre koppelt elke categorie aan een partij die verantwoordelijk is voor de afwikkeling daarvan, en een specifiek antwoord op het incident geeft.[186]

In aansluiting op de blauwdruk voor incidentbestrijding op het vlak van de Europese Unie heeft de Europese NIB-samenwerkingsgroep[187] een 'taxonomie' van grootschalige cyberincidenten opgesteld.[188] De samenwerkingsgroep richt zich daarbij op een brede set van incidenten door naast kwaadwillende handelingen ook het spontaan falen van systemen, natuurlijke fenomenen als branden, overstromingen of aardbevingen, menselijke fouten en uitval van derde partijen op te nemen als oorzaken. De bedoeling is de taxonomie te koppelen aan de geïntegreerde EU-regeling politieke crisisrespons (IPCR).

184 Secrétariat général de la défense nationale 2018: 140.
185 www.us-cert.gov/NCCIC-Cyber-Incident-Scoring-System en https://grants.nhisac.org/BackgroundData/Cyber_Incident_Severity_Schema.pdf
186 www.ncsc.gov.uk/news/new-cyber-attack-categorisation-system-improve-uk-response-incidents
187 De NIB-samenwerkingsgroep bestaat uit vertegenwoordigers van de Europese lidstaten, ENISA en de Europese Commissie. Hij is ingesteld op basis van artikel 11 van NIB-richtlijn.
188 http://ec.europa.eu/information_society/newsroom/image/document/2018-30/cybersecurity_incident_taxonomy_00CD828C-F851-AFC4-0B1B416696B5F710_53646.pdf

In Nederland is de beoordeling van de ernst van incidenten gekoppeld aan de lijst met vitale infrastructuur. Bovenstaande voorbeelden maken duidelijk welk nut aanvullende criteria kunnen hebben voor de bestrijding van digitale incidenten. Een belangrijk voordeel is dat de nationale overheid niet bij elk incident hoeft te worden aangesproken. Een gedifferentieerdere classificatie van incidenten kan de basis vormen voor een scherper afgebakende verantwoordelijkheidsverdeling, zowel binnen de verschillende overheidslagen (denk aan NCSC, departementen, veiligheidsregio's en de informatiebeveiligingsdienst voor de gemeenten) als tussen overheidsdiensten en het bedrijfsleven. Ook kan een dergelijke classificatie een effectievere aanpak van cyberincidenten mogelijk maken, doordat deze aanpak op rijksniveau niet langer een op een gekoppeld hoeft te zijn aan incidenten met vitale infrastructuur.

Prioriteren is ook ter plekke nodig, zoals blijkt bij de brandbestrijding. Bij een grote brand kan de brandweer ervoor kiezen om de brand te blussen, maar ook voor het zoveel mogelijk beperken van de gevolgen, bijvoorbeeld door belendende panden nat te houden. Die panden lopen dan weliswaar waterschade op, maar blijven in ieder geval behouden. Een soortgelijke situatie speelt bij de afkoppeling van digitale systemen, die vergt dat de kosten van een acute bedrijfsonderbreking worden afgezet tegen het risico dat de problemen zich verder verspreiden, met mogelijk nog grotere schade tot gevolg. Omdat veel digitale systemen in handen zijn van private partijen moet vooraf duidelijk zijn met welke overwegingen de overheid ingrijpt.

Aan prioriteren zit zowel een technische als een inhoudelijke kant. Bij de technische kant speelt de logica van de systemen, die op een bepaalde manier zijn gekoppeld. Dit betekent dat het af- en aankoppelen een bepaalde volgorde veronderstelt. Het is van groot belang om te weten hoe de verschillende systemen en organisaties in een netwerk van elkaar afhankelijk zijn en in het vizier te hebben welke keuzes zich daarbij aandienen. Bij de inhoudelijke kant speelt de vraag welke maatschappelijke processen het langste in de lucht gehouden moeten worden en bij uitval als eerste weer moeten worden opgestart. De keuzes die hier door de overheid worden gemaakt, zullen voor lang niet alle betrokken partijen vanzelf spreken. Private partijen kunnen bijvoorbeeld eerst de eigen systemen en die van hun klanten veilig willen stellen in plaats het publieke belang voorop te stellen.

Een speciale positie bij prioriteren geldt voor de vitale processen. Duidelijk is dat de continuïteit van vitale processen voorrang krijgt bij incidenten. Processen die vallen onder categorie A krijgen daarbij voorrang boven processen onder categorie B (zie hoofdstuk 2). Digitalisering zet deze categorisering onder druk. De huidige opsomming van vitale infrastructuren focust wat betreft digitale voorzieningen vooral op traditionele telecommunicatiediensten en het belang daarvan voor onder

meer de inzet van hulpdiensten en de communicatie tussen hulpverleners. De sector telecom/ICT wordt echter geschaard onder categorie B. Of deze ordening houdbaar is valt te betwijfelen, zeker gezien aanwijzingen dat de uitval van digitale processen na de elektriciteitsvoorziening de grootste cascade-effecten heeft. Voor de elektriciteitsbedrijven bestaan mede om die reden gedetailleerde afschakel- en herstelplannen, waarbij herstel van de openbare orde en veiligheid prioriteit krijgen. Voor digitale processen ontbreken dergelijke plannen, wat nogmaals benadrukt hoe belangrijk het is om de afbakening en ordening van vitale processen opnieuw te doordenken.

4.5 HERSTEL EN WEDEROPBOUW

De laatste fase in de omgang met digitale ontwrichting heeft betrekking op herstel en wederopbouw. Wanneer het normale maatschappelijke leven ernstig is verstoord, zijn verschillende acties nodig om dat weer op de rails te krijgen. Vaak wordt het daarbij nooit meer 'zoals vroeger', omdat mensen en organisaties leren van het incident. Veel bedrijven en organisaties die zijn getroffen door een computervirus, ransomware of om andere redenen te maken kregen met uitval van systemen en processen, blijken hun beleid daarna aan te passen. Welbekend is de maatregel dat het personeel alleen nog onder strenge voorwaarden gebruik mag maken van USB-sticks. Om te kunnen leren, is het belangrijk te analyseren wat er is misgegaan en met welke oorzaak.
Verder dienen voor herstel en wederopbouw faciliteiten voorhanden te zijn.
Dit betekent onder meer dat slachtoffers gecompenseerd worden voor de schade die ze hebben geleden. Leren en compenseren houden overigens deels verband met elkaar. Immers, wie kernprocessen in de samenleving opnieuw en op een betere wijze wil vormgeven, zal daartoe wel de middelen moeten hebben.

EVALUEREN EN LEREN

De fase van herstel en wederopbouw dient benut te worden voor een heroriëntatie op de nieuw op te bouwen digitale voorzieningen. Bijvoorbeeld door onevenwichtigheden te adresseren tussen enerzijds economische macht over de inrichting van de digitale samenleving en anderzijds de politiek-bestuurlijke zeggenschap daarover. Een heroriëntatie kan ook betekenen: het ontwikkelen van voorzieningen gericht op veiligheid in plaats van primair op snelheid, efficiëntie en lage prijzen.

Maar het kan niet uitsluitend bij een heroriëntatie blijven. Er zullen ook concrete lessen getrokken moeten worden. De kunst is bovendien om ervoor te zorgen dat deze lessen ook daadwerkelijk tot lering leiden.[189] Dat gebeurt nog maar weinig, zo blijkt, ook niet naar aanleiding van grote incidenten als NotPetya en WannaCry.[190] Om te beginnen maakt maar 7% van de bedrijven in Nederland melding van incidenten bij

189 Van Vollenhoven 2018.
190 Van Tiel 2019.

de politie, de bank of de Autoriteit Persoonsgegevens.[191] Historische gegevens over cyberincidenten zijn bovendien beperkt beschikbaar en vooralsnog ontbreekt een algemeen aanvaarde definitie van incidenten.[192] Een bijkomend probleem is dat het overgrote deel van de incidentdata niet gaat over kwetsbaarheden die tot maatschappelijke ontwrichting kunnen leiden. Ook zijn de publieke data over incidenten vooralsnog vrij eenzijdig gericht op datalekken, omdat hierop de meldplichten en eisen ten aanzien van openbaarmaking overwegend zijn gericht.[193] De NIB-richtlijn brengt hierin verandering, door een meldplicht te introduceren voor problemen die te maken hebben met de continuïteit van 'essentiële diensten'. In aanvulling hierop moeten ook betaaldiensten volgens de Europese betalingsrichtlijn melding doen van grote incidenten die de financiële belangen van hun gebruikers dreigen te schaden. Beide meldplichten zijn echter dermate recent dat hieruit nog onvoldoende betrouwbare lessen zijn te trekken.

Een tweede observatie betreft het toezicht op digitale veiligheid.[194] Er is geen specifieke toezichthouder. Wel zijn er verscheidene organisaties actief op deelterreinen, zoals de Autoriteit Persoonsgegevens, die datalekken registreert, en De Nederlandsche Bank die een rol speelt bij het waarborgen van de continuïteit van het elektronisch betalingsverkeer. Een andere belangrijke partij is Agentschap Telecom, dat toezicht houdt op netwerkproviders en waar ook digitale dienstverleners hun continuïteitsproblemen moeten melden. Daarnaast spelen verscheidene departementen een rol, aangezien de vitale sectoren tot hun werkterrein behoren. De incidentdata die elk van deze instanties verzamelt, worden maar zeer beperkt gedeeld en lang niet altijd geanalyseerd, laat staan in samenhang.[195] Dit is een gemiste kans. Juist bij digitale ontwrichting zijn meerdere organisaties en sectoren betrokken, waardoor het nuttig kan zijn om incidentdata op elkaar te betrekken.

COMPENSEREN

Een belangrijk onderdeel van herstel en wederopbouw is tot slot de compensatie van slachtoffers, via aansprakelijkheid, verzekerbaarheid dan wel tegemoetkoming door de overheid. Adequate compensatieregelingen bevorderen de risico- en

---

191 Centraal Bureau voor de Statistiek 2018b. Tegelijkertijd geeft 50% van de grotere bedrijven aan met ICT-veiligheidsincidenten te maken te hebben.

192 Valeriano en Maness 2018.

193 OECD 2017: 34. Voor een indicatie van aantallen datalekken zie https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken/cijfers-datalekken-2018. De Autoriteit Persoonsgegevens ontving in 2018 ruim 20.000 meldingen van een datalek. In 2017 betrof het 10.009 meldingen en in 2016 in totaal 5849 meldingen.

194 Overigens is dit een meer algemeen probleem: zie Van Vollenhoven 2019.

195 Een uitzondering vormt het NCSC dat in een bijlage van het Cybersecuritybeeld Nederland een overzicht biedt van afgehandelde meldingen en incidenten. Zie hiervoor NCTV 2019: 43-46.

schadereductie in de maatschappij[196] en dragen bij aan het herstel van de economie, sociale stabiliteit en vertrouwen in instituties.[197] Ook cyberrisico's zijn in principe te verzekeren.[198] Sterker nog: de markt voor cyberverzekeringen is maar een fractie van de markt voor andere risico's en kan derhalve flink groeien.

Risico's zijn verzekerbaar wanneer ze te kwantificeren zijn in termen van waarschijnlijkheid en impact. Ook moet er een voldoende grote groep samengesteld kunnen worden die door dit risico wordt geraakt en die het derhalve kan delen. Tot slot moeten risico's optreden op onvoorspelbare tijdstippen en plekken, en buiten de wil van de verzekerde om. Anders zou elke partij zich daar namelijk individueel voor kunnen verzekeren.

Cyberrisico's zijn vanwege een gebrek aan historische data vooralsnog lastig te kwantificeren. Daarbij komt het al eerder gesignaleerde probleem dat een duidelijke classificatie van incidenten ontbreekt, evenals inzicht in de weerbaarheid van bedrijven en typen verliezen.[199] Cyberrisico's zijn bovendien permanent aan verandering onderhevig, wat het lastig maakt ze goed te beprijzen.

Hiernaast kunnen verzekeraars te maken krijgen met massale verliezen als gevolg van risicoaccumulatie.[200] Wanneer veel partijen afhankelijk zijn van dezelfde infrastructuur of toeleverancier of gebruikmaken van dezelfde algemene software, is het lastig om het risico van de verstoring of uitval daarvan per sector of regio te delen (veelal wordt de term 'poolen' gehanteerd). In een scenario van Lloyd's en Cyence, gebaseerd op een softwarefout bij clouddiensten, resulteert een dergelijke ontwrichting in een bedrag van tussen de $4,6 miljard en $53,05 miljard schade, afhankelijk van de duur van de uitval.[201]

Risicoaccumulatie is een belangrijke reden waarom de markt voor cyberverzekeringen maar langzaam groeit. De omvangrijke schade (zie tabel 4.1) en schadeclaims als gevolg van NotPetya waren voor enkele grote verzekeraars bovendien aanleiding om de dekking van hun verzekeringen verder te beperken.

196 Bruggeman en Faure 2018: 11; WRR 2011b: 16, 53.
197 Kuipers en Tjepkema 2017.
198 OECD 2017; Biener et al. 2015.
199 OECD 2017; ENISA 2017; Nieuwesteeg et al. 2017. Veel verzekeringen richten zich op het verlies van klantgegevens en niet op herstelkosten van digitale infrastructuur en verliezen als gevolg van bedrijfsonderbreking.
200 OECD 2017: 123.
201 Lloyd's en Cyence 2017.

Tabel 4.1 Commerciële impact van bedrijfsonderbreking door NotPetya[202]

Organisatie	Commerciële impact	Type financiële schade
A.P. Moller – Maersk	$ 250-300 miljoen	Winstdaling
Beiersdorf ag	Beperkte gevolgen voor omzet € 15 miljoen	€ 35 miljoen aan omzet van Q2 naar Q3 doorgeschoven Extra kosten
FedEx (TNT-express)	$ 400 miljoen	Winstdaling
Merck & Co.	$ 410 miljoen $ 380 miljoen	Omzetdaling in 2017 en 2018 Extra kosten
Mondelez International	-$ 104 miljoen $ 84 miljoen	Omzetdaling in 2017 Extra kosten
Nuance Communications	$ 68 miljoen $ 31,2 miljoen	Omzetdaling in 2017 Extra kosten
Reckitt Benckiser	-£ 114 miljoen	Omzetdaling van 2% in Q2 en in Q3
Saint-Gobain	-€ 220-250 miljoen € 80 miljoen	Omzetdaling in 2017 Winstdaling in 2017

Zij voelden zich daarbij gesterkt door de Amerikaanse toeschrijving van de cyberaanval aan Rusland.[203] Ook alternatieve dekkingen, bijvoorbeeld via aansprakelijkheid of schade aan bedrijfsapparatuur (zgn. *silent cyber*) sluiten zij inmiddels expliciet uit in hun polissen.

Schade als gevolg van gewapende conflicten mag bij wet niet worden verzekerd, vanwege het te grote financiële risico. Dit levert nauwelijks problemen op als oorlog ver weg is en er een duidelijke definitie is van wat een gewapend conflict behelst. Cyberaanvallen laten zich niet zo gemakkelijk in dit keurslijf dwingen. Ze stellen landen in staat om over de grens schade aan te richten, zonder daar ooit een voet te zetten. Ook is de vraag in hoeverre code als wapen valt te beschouwen, zeker gezien de snelle evolutie van malware. Het meest problematisch is echter dat onduidelijk is wanneer cyberaanvallen dermate veel impact hebben dat ze om vergelding vragen. Internationale regels en definities om dit te kunnen vaststellen ontbreken.[204] Nu verzekeraars cyberaanvallen als gewapend conflict beschouwen, en bedrijven daar protest tegen aantekenen, is het aan de rechter om te bezien in hoeverre een door een staat uitgevoerde cyberaanval een oorlogsdaad is.[205]

---

202 Bron AON 2019: 8. De in de tabel genoemde bedragen zijn gebaseerd op kwartaalcijfers van de desbetreffende bedrijven.

203 www.nytimes.com/2019/04/15/technology/cyberinsurance-notpetya-attack.html

204 Mačák 2017.

205 Verschillende bedrijven voeren momenteel rechtszaken tegen verzekeraars, waardoor rechters zich mogelijk zullen moeten uitspreken over de vraag of cyberaanvallen als gewapend conflict gelden.

De omgang met verschillende andere omvangrijke schadevoorvallen en daarmee verbonden risico's laat zien dat deze situatie niet onoplosbaar is. Ook na de watersnoodramp van 1953 en de aanslagen van 9/11 trokken verzekeraars zich terug, omdat zij dergelijke verliezen niet langer wilden compenseren. Het overstromingsrisico is Nederland nog altijd grotendeels onverzekerd maar voor de verzekering van het terrorismerisico is een publiek-private constructie gecreëerd, waarbinnen de overheid optreedt als laatste toevlucht, en verzekeraars niet alle verliezen hoeven te compenseren.[206] Deze constructie stelt verzekeraars in staat om verzekeringsproducten aan te bieden zonder al te grote financiële risico's te lopen. Toegepast op digitale ontwrichting zou een dergelijke constructie betekenen dat de overheid de kosten van digitale ontwrichting compenseert, wanneer deze kosten boven een bepaalde grens uitkomen. Met deze garantie op zak kunnen verzekeraars vervolgens de markt voor cyberveiligheid verder ontwikkelen en kunnen verzekeraars en bedrijven de kosten van kleinere voorvallen in principe zelf financieel afwikkelen.

4.6 CONCLUSIE

Altijd al hebben de overheid en andere partijen maatregelen genomen om voor allerlei risico's de gevolgen van een eventuele maatschappelijke ontwrichting zoveel mogelijk te beperken. Digitalisering voegt aan het bekende rijtje risico's een nieuw type maatschappelijke ontwrichting toe. Dit hoofdstuk draaide om de voorbereidende maatregelen die met het oog op dit type ontwrichting genomen kunnen worden.
De voornaamste conclusie die we trekken is dat deze maatregelen nog onvoldoende zijn genomen, zodat de overheid en andere partijen momenteel onvoldoende zijn voorbereid op digitale ontwrichting. Om hier verandering in te brengen is een aantal stappen nodig ten aanzien van de volgende observaties:

– Er is geen coherent beleid aangaande terugvalopties, het isoleren van ketens en netwerken, het doen van oefeningen en de informatievoorziening over hoe te handelen tijdens calamiteiten. Niet alleen is dit per sector en per organisatie anders geregeld, ook zijn tegenovergestelde ontwikkelingen waarneembaar. Om te beginnen vermindert het aantal terugvalopties doordat analoge alternatieven verdwijnen en organisaties voorzieningen uitbesteden aan derde partijen. De onderlinge verwevenheid van processen en sectoren neemt hierdoor toe.

206 Voor een uitgebreide bespreking van zowel pogingen het overstromingsrisico te verzekeren als de terrorismepool, zie Bruggeman en Faure 2018: 61-62, 70-72.

– De afgelopen jaren is de informatie-uitwisseling sterk verbeterd en meer dekkend geworden. De organisatie daarvan wordt echter bemoeilijkt door sectorale scheidslijnen en een deels achterhaald onderscheid tussen vitale aanbieders en niet-vitale aanbieders, waardoor signalen niet of te laat bij de juiste partijen terechtkomen. Ook is een breder perspectief nodig op het verzamelen en delen van kennis. De focus ligt momenteel op het delen van kennis en informatie over digitale veiligheidsmaatregelen, kwetsbaarheden en incidenten. Er is aanzienlijk minder inzicht in ketens en netwerken en de afhankelijkheden daarbinnen, voor vitale aanbieders en ook de overheid zelf. Dergelijke kennis is van groot belang om de ernst van incidenten te kunnen duiden en invloed uit te kunnen oefenen op de wijze waarop een digitale ontwrichting zich voltrekt.

– De overheid is bij digitale ontwrichting in hoge mate afhankelijk van de informatie en medewerking van (buitenlandse) private partijen maar ontbeert een duidelijk omschreven bevoegdheid om in te grijpen, gekoppeld aan verschillende categorieën digitale incidenten en publieke instanties die deze incidenten kunnen bestrijden. Meer bevoegdheid voor de overheid dient gepaard te gaan met een voldoende beschermingsniveau voor private partijen, omdat ingrijpen met dwang gepaard gaat en financiële consequenties kan hebben.

– Een digitale ontwrichting kan de landsgrenzen overschrijden. Dit noopt tot internationale coördinatie en instrumenten. De huidige aanpak leunt op – deels ontoereikende – nationale mechanismen, wat vooral risicovol is bij spillovereffecten naar kritieke infrastructuur elders in Europa en aanvallen op Europese instituties. De toenemende geopolitieke dynamiek rondom digitale ontwrichting maakt Europese en internationale samenwerking buitengewoon urgent.

– Herstel en wederopbouw zijn vooralsnog lastig te realiseren. De middelen voor herstel drogen op, nu verzekeraars zich lijken terug te trekken uit de markt voor cyberverzekeringen. Tegelijkertijd laten andere omvangrijke schadevoorvallen zien dat er oplossingen mogelijk zijn. Voor een goede wederopbouw is een breed georganiseerde reflectie op incidenten nodig. Die reflectie stuit momenteel op een geïsoleerde verwerking van incidentdata door verschillende toezichthoudende instanties, wat mogelijke leereffecten niet ten goede komt.

5 CONCLUSIES EN AANBEVELINGEN

5.1 INLEIDING

Op 24 juni 2019 vond een urenlange storing plaats van zowel het noodnummer 112 als 0900-8844, het landelijke servicenummer van de politie. Bovendien waren ook ziekenhuizen, gemeenten en bedrijven lange tijd onbereikbaar. Behalve het primaire systeem van KPN – de betrokken telecomprovider – bleken ook drie back-upsystemen niet te functioneren. Het voorval – volgens KPN vermoedelijk veroorzaakt door een softwarefout – toont hoe kwetsbaar voorzieningen in de fysieke wereld zijn als het digitaal misgaat. Het illustreert daarmee bij uitstek de centrale boodschap van dit rapport: de noodzaak van een betere voorbereiding op incidenten met een digitale dimensie. Zeker als deze incidenten niet beperkt blijven tot het digitale domein, maar ook potentieel ontwrichtende consequenties hebben voor de fysieke wereld en het vertrouwen in maatschappelijke instituties.

Het voorval maakt ook pijnlijk duidelijk hoezeer de overheid voor de continuïteit van vitale processen afhankelijk is van private partijen, die op hun beurt weer gebruikmaken van de diensten en voorzieningen van externe toeleveranciers. Nog verontrustender was dat de betrokken instanties, waaronder de rijksoverheid, onvoldoende voorbereid waren op deze situatie. Een duidelijk noodplan voor uitval van 112 lag niet op de plank. Ten slotte bleken de betrokken partijen niet in staat om elkaar tijdig te vinden en de aanpak van de storing te coördineren. Tekenend is dat het vijf kwartier duurde alvorens een alternatief noodnummer werd verspreid, aanvankelijk een verkeerd nummer werd doorgegeven en niet iedereen op z'n mobiel een melding van NL-Alert ontving. Overigens haperde ook in 2012 het noodnummer al eens. Dit mocht en zou niet meer gebeuren, aldus de toenmalige bewindspersoon. Maar het gebeurde toch – 100% veiligheid valt immers niet te garanderen. Zelfs een redelijk identiek incident blijkt kennelijk niet uit te sluiten.

In de voorgaande hoofdstukken hebben wij allereerst onderzocht in hoeverre onze samenleving is voorbereid op de omgang met een digitale ontwrichting. Vervolgens hebben we geanalyseerd waarom het bestaande instrumentarium niet voldoet om een dergelijke ontwrichting adequaat aan te pakken. In dit slothoofdstuk geven we een voorzet voor de stappen die de voorbereiding op een digitale ontwrichting kunnen verbeteren. Daarbij richten we ons tot de overheid, in het bijzonder de rijksoverheid. In paragrafen 5.2 en 5.3 geven we de voornaamste conclusies weer, die tonen dat we door de groeiende digitalisering van onze economie en samenleving te maken krijgen met een nieuw type ontwrichting. Het hierboven beschreven voorval is daarvoor exemplarisch. In de paragrafen daarna presenteren

we de aanbevelingen, die we ordenen aan de hand van de in het voorgaande hoofdstuk geïntroduceerde stadia van paraatheid, signalering, bestrijding en ten slotte herstel en wederopbouw.

5.2 EEN NIEUW TYPE ONTWRICHTING

Maatschappelijke ontwrichting is van alle tijden en kan verschillende oorzaken hebben. De verstoring of uitval van digitale voorzieningen is in toenemende mate een van die oorzaken. In dit rapport zijn we welbewust voorbijgegaan aan de vraag hoe groot de kans is op digitale verstoringen en welke impact zij naar verwachting zullen hebben. Dergelijke risicobeoordelingen zijn reeds voorhanden. Bovendien is er, getuige diverse incidenten in binnen- en buitenland, voldoende aanleiding om een digitale ontwrichting onder ogen te zien en de aanpak daarvan te doordenken. Behalve om de groeiende schaal, verspreiding en impact van incidenten, de stijgende kosten die daarmee gepaard gaan en de economische implicaties, gaat het ook om het vertrouwen dat burgers, organisaties en bedrijven hebben in digitale technologie.

Door de afhankelijkheid van geavanceerde digitale technologie over de volle breedte van onze samenleving en economie, ontstijgen de gevolgen van verstoringen en uitval in toenemende mate het domein van 'klassieke' ICT en cybersecurity. Dit resulteert in een nieuwe type ontwrichting, dat we in hoofdstuk 2 kortweg 'digitale ontwrichting' hebben genoemd. Door digitalisering is het onderscheid tussen 'de digitale' wereld en 'de fysieke' wereld sterk vervaagd. Bovendien zijn de grenzen tussen bedrijven en organisaties diffuus geworden. Zij zijn onderling verbonden door talloze systemen en netwerken. Een digitale verstoring behelst dientengevolge veel meer dan alleen de uitval van geïsoleerde digitale systemen. Deze realiteit staat echter onvoldoende scherp op het netvlies van bedrijven, organisaties, de overheid en politiek verantwoordelijken.

Overduidelijk is dat steeds meer maatschappelijke en economische processen zijn gebaseerd op dergelijke verknoopte informatiestromen. Door ontwikkelingen als dataficatie, toegenomen rekenkracht en de complexe verbindingen tussen systemen wereldwijd zijn het digitale domein en het fysieke domein intens met elkaar verweven geraakt. Vrijwel alle kernprocessen in de samenleving, zoals de stroomvoorziening, het betalingsverkeer, waterkeringen en de zorg, zijn afhankelijk van informatie-uitwisseling en digitale systemen, en gekoppeld aan grotere netwerken of zelfs het internet. Verwevenheid is daarmee een cruciaal aspect om rekening mee te houden, zowel bij de voorbereiding op als de daadwerkelijke bestrijding van incidenten waarbij digitale infrastructuur in het spel is. Het voldoet bijvoorbeeld niet langer om de invulling van beschermingsmaatregelen aan individuele organisaties over te laten en cyberoefeningen te houden in eigen kring. De zwakste schakel kan zich immers vrijwel overal ter wereld bevinden.

Digitalisering verandert ook de schaal en dynamiek van verstoringen. Dit hangt behalve met het sterk verknoopte karakter van digitale infrastructuur ook samen met onveilige, generieke software en hardware, netwerkafhankelijkheid en de lang niet altijd adequate beveiliging van systemen en data. Een belangrijke reden zijn tevens de complexe, veelal ondoorzichtige en grensoverschrijdende toeleverings- en productieketens, die kwaadwillende partijen veel mogelijkheden bieden om maatschappelijke en economische processen te verstoren of zelfs geheel stil te leggen. Een digitale ontwrichting kan hierdoor razendsnel optreden en een groot aantal organisaties en sectoren verspreid over de wereld treffen, maar ook het gevolg zijn van sluimerende processen die lang onopgemerkt blijven of onduidelijk zijn qua reikwijdte. In beide gevallen kan ook het vertrouwen in de democratische rechtstaat op het spel staan. Partijen in de samenleving kunnen immers de indruk krijgen dat de overheid onvoldoende grip heeft op de digitale wereld. Een extra complicatie hierbij is dat bij incidenten niet bij voorbaat duidelijk is of de overheid aan zet is en zo ja, welk onderdeel van de overheid. Tegelijkertijd kan het wel noodzakelijk zijn om vroegtijdig in te grijpen, met als doel schade te beperken.

Ook speelt dat met digitalisering de relevantie van geografische grenzen onder druk is komen te staan. Talloze incidenten tonen dat verstoringen vrijwel tegelijkertijd in meerdere landen tot ontwrichtende situaties kunnen leiden. Digitale ontwrichting is daarmee een dossier dat agendering binnen internationale gremia vereist, waaronder de Europese Unie. Anderzijds impliceert het grenzeloze karakter van digitalisering zeker niet dat de aanpak uitsluitend internationaal moet zijn. Sommige verstoringen blijven beperkt tot ons eigen land, zoals de hierboven genoemde storing in het telefoniesysteem van KPN. Minstens zo belangrijk is dat een digitale ontwrichting – hoe abstract zij ook lijkt – uiteindelijk altijd lokale gevolgen heeft. Door de intensieve verwevenheid met de fysieke wereld zal een digitale ontwrichting vitale processen op Nederlandse bodem treffen. Tot slot is Nederland bij een groot aantal maatregelen, zoals het realiseren van terugvalopties, scenario's voor afschakelen maar ook compensatie van schade en verzekeren, nauwelijks afhankelijk van andere landen. De voorbereiding op digitale ontwrichting zal kortom een combinatie zijn van nationale maatregelen en internationale samenwerking. De aanbevelingen die wij later in dit hoofdstuk uitwerken zijn daar een illustratie van.

5.3 CENTRALE NORMSTELLING EN COÖRDINATIE DOOR DE OVERHEID

Op het terrein van het veiligheidsbeleid verlangen we van de overheid dat zij inzichtelijk maakt welke belangen in het geding zijn. Ook zal zij duidelijk moeten maken hoe de verdeling van lusten, lasten en risico's dient te zijn bij het beharti-

gen van deze belangen en welke partijen waarvoor verantwoordelijk zijn.[207] Deze lijn volgend en de conclusies van het voorgaande hoofdstuk indachtig, dient de overheid ten aanzien van het digitale domein en de daaraan verbonden risico's een grotere rol te vervullen.

Welke rol vergt nadere toelichting. Centrale sturing is onrealistisch op het complexe en grotendeels door private partijen bevolkte terrein van cybersecurity, internet governance en vitale infrastructuur. De overheid kan echter ook op andere manieren een rol op zich nemen. Cybersecurity is in het afgelopen decennium uitgegroeid tot een serieus beleidsterrein met belangrijke internationale elementen. Publiek-private samenwerkingsverbanden zijn hierbij een onmisbaar instrument, zeker nu het overgrote deel van de digitale infrastructuur in handen is van private partijen. Deze samenwerking kenmerkt zich echter door een grote mate van vrijblijvendheid. Zo bepalen aanbieders van vitale processen in belangrijke mate zelf welke beschermingsmaatregelen ze nemen en hoe ze hun terugvalopties inrichten, met als gevolg dat ze verschillend zijn voorbereid op digitale ontwrichting. Ook hebben ze veel vrijheid in de keuze welke incidenten ze melden en actieve deelname aan de Information Sharing Analysis Centers (ISAC's) blijft voornamelijk beperkt tot een voorhoede van organisaties die het belang van informatie-uitwisseling erkent.

Van private bedrijven en organisaties kan niet worden verwacht dat zij de volledige verantwoordelijkheid voor digitale ontwrichting op zich nemen. Wel zullen zij in een dergelijke situatie alles moeten doen wat in hun vermogen ligt om erger te voorkomen. De overheid is de partij bij uitstek om het nakomen van deze verantwoordelijkheid af te dwingen, net als bij andere vormen van maatschappelijke ontwrichting het geval is. Zij heeft hiertoe momenteel echter een beperkt instrumentarium ter beschikking. Als private organisaties en bedrijven bij (dreigende) ontwrichting hun medewerking weigeren, heeft de centrale overheid relatief weinig bevoegdheden om hen daartoe te dwingen. Voor de Europese Unie geldt dit in nog grotere mate, omdat zij zich beperkt tot een adviserende rol en de strategische en operationele aspecten van cyber overlaat aan de lidstaten. In deze leemte kan worden voorzien door op het niveau van de rijksoverheid zowel bevoegdheid als normstelling te verhelderen en te verstevigen.[208] Dit zou het handelingsvermogen van de overheid in ontwrichtingssituaties aanzienlijk kunnen vergroten.

Tegelijkertijd moet het uitgangspunt zijn dat de 'lokale brandweer' lokale 'branden' blust en dat gespecialiseerde 'brandweerkorpsen' de meer complexe 'branden' voor hun rekening nemen, op lokaal, regionaal of landelijk niveau. Per domein zullen immers vaak verschillende maatregelen genomen moeten worden. Wanneer digi-

207 WRR 2011.
208 Zie ook Boeke 2016.

tale ontwrichting dreigt, kan opschaling plaatsvinden naar een hoger bestuurlijk niveau en kan de rijksoverheid de leiding over de crisisbeheersingsoperatie op zich nemen. Een voorbeeld van een dergelijk mechanisme is te vinden in de Wet op de veiligheidsregio's, die de mogelijkheid biedt om de crisisbeheersing en rampenbestrijding te adresseren op het meest geschikte bestuurlijke niveau en in de juiste functionele keten.[209] De verantwoordelijkheidsverdeling bij 'digitale' branden is vooralsnog onhelder en een opschalingsmechanisme is niet voorhanden, mede omdat criteria ontbreken om categorieën van incidenten te onderscheiden.

Ook constateren we dat digitale ontwrichting vraagt om een beter gecoördineerd optreden door de overheid. Door zowel de dynamiek van netwerkeffecten als de wisselwerking tussen de digitale en de fysieke wereld, overstijgt de voorbereiding op digitale ontwrichting per definitie het vermogen van individuele organisaties. Voor een organisatie, bedrijf of veiligheidsregio is het vrijwel onmogelijk om een overkoepelend beeld te krijgen, laat staan om vanuit de eigen context de juiste keuzes te maken wat betreft afschakelen, opschalen en tal van andere maatregelen. Voor inzicht in de samenhang van processen en te nemen maatregelen is gecoördineerde actie door de overheid nodig. Deze opdracht ziet niet alleen op het verkrijgen van het bredere beeld van processen en afhankelijkheden. Coördinatie is ook noodzakelijk met het oog op een effectieve voorlichting aan het publiek als er iets misgaat. De overheid blijft hierbij vanzelfsprekend verantwoordelijk voor de bestaande middelen op het terrein van cybersecurity.[210]

Van groot belang is tot slot dat een betere voorbereiding op digitale ontwrichting door de overheid geen vrijbrief is voor andere partijen om onverantwoorde risico's te nemen. Ook bedrijven en organisaties hebben de verantwoordelijkheid om zich op digitale ontwrichting voor te bereiden. Wanneer zij die verantwoordelijkheid ontlopen is dat schadelijk voor het vertrouwen van burgers in digitale processen, wat op termijn nadelig uitpakt voor het functioneren van samenleving, markt en overheid. Bovendien: wanneer een van hen achteroverleunt en nalaat om voorbereidende maatregelen te treffen, heeft iedereen daar last van op het moment dat het misgaat.

---

209 Zie ook Muller 2014: 15. Momenteel worden her en der in het land - mede gefaciliteerd door projectsubsidies vanuit het ministerie van Justitie en Veiligheid – initiatieven ontwikkeld die als invulling van lokale en domeinspecifieke (zoals voor de Rotterdamse haven) 'brandweercapaciteit' zijn te beschouwen.

210 Zoals de publieksvoorlichting via https://crisis.nl/wees-voorbereid/cyberaanval/. De op deze pagina genoemde suggesties m.b.t. een cyberaanval blijven overigens beperkt tot 'digitale' maatregelen. Echter, bij een meerdaagse landelijke pinstoring hebben burgers meer aan het advies om enig contant geld op zak te hebben dan hun wachtwoord te veranderen of nieuwe antivirussoftware te installeren.

Er bestaat reeds een aantal maatregelen om de voorbereiding op een digitale ontwrichting te coördineren. Partijen die de nadelige effecten – slachtoffers en schade – niet of onvoldoende beperken, kunnen daarvoor in sommige gevallen bijvoorbeeld aansprakelijk worden gesteld.[211] Tegelijkertijd moet worden geconstateerd dat er voor deze partijen nog een wereld te winnen is. Er kan onder meer worden geoefend met een ontwrichtingsscenario gericht op vernetwerking en afhankelijkheden van externe partijen. Ook zouden bedrijven en organisaties verplicht kunnen worden gesteld een cyberparagraaf in hun jaarverslag op te nemen, waarin zij aandacht besteden aan voorbereidende maatregelen bij digitale verstoringen. Hoe dan ook zal een aantal van de hieronder te presenteren aanbevelingen doorwerken in de private sector.

5.4 PARAATHEID: MEER AANDACHT VOOR VOORBEREIDING

Sinds jaar en dag beschermen overheden de infrastructuren die belangrijk zijn voor de continuïteit van de samenleving. Dit vergt inzicht in de wijze waarop deze infrastructuren kwetsbaar zijn voor verstoring, uitval of vernietiging. Wie deze kwetsbaarheden kent, kan immers vooraf maatregelen nemen om de gevolgen van ontwrichtende gebeurtenissen zoveel mogelijk te beperken. Dat gebeurt momenteel onvoldoende.

Dit rapport komt voort uit de zorg dat de mogelijkheid van een digitale ontwrichting onvoldoende aandacht krijgt, in tegenstelling tot preventie en beschermingsmaatregelen. De huidige beperkte focus in het beleid is niet zonder gevolgen. De consequentie is dat een publiek en politiek debat ontbreekt over de vraag welke voorzieningen Nederland nodig heeft om een effectieve aanpak tijdens een digitale ontwrichting te waarborgen. Onze eerste aanbeveling luidt dan ook:

Voer een publiek debat over de toerusting van de Nederlandse samenleving met het oog op de mogelijkheid van een digitale ontwrichting.

De kwetsbaarheid van kernprocessen in de samenleving wordt steeds meer door digitalisering bepaald. Daarom is een discussie nodig over welke mate van 'strategische autonomie' wenselijk en haalbaar is voor Nederland. Digitalisering maakt processen sneller en efficiënter maar heeft als keerzijde dat incidenten al snel meerdere organisaties, sectoren en landen kunnen raken. Welke balans tussen deze voor- en nadelen willen we nastreven? En als het onverhoopt misgaat, welke terugvalopties dienen er dan te zijn? Hoe lang mag een verstoring duren en wat vinden we een acceptabele hersteltijd?

211 Van Dam 1995; Keirse 2017.

Ook ontwikkelingen in de markt kunnen de mate van de paraatheid van de Nederlandse samenleving en overheid sterk beïnvloeden. Investeringsbeslissingen, overnames en de netwerkeffecten in de digitale wereld, kunnen resulteren in grote en lastig te corrigeren afhankelijkheden. Deze afhankelijkheden kunnen de overheid belemmeren bij de uitvoering van haar veiligheidstaak en ontwrichtingsaanpak. Een belangrijke vraag is daarom welke voorzieningen of bedrijven we in Nederland willen houden, teneinde nationale belangen te beschermen. Het goede nieuws is dat de discussie hierover intussen voorzichtig op gang is gekomen – denk aan de overwegingen rond de aanleg van 5G en de overnameplannen bij Fox-IT, kabelproducent Draka en KPN. De implicaties van afhankelijkheden van buitenlandse partijen voor een effectieve aanpak van een digitale ontwrichting moeten binnen deze discussie meer gewicht krijgen.

Meer dan nu het geval is zal de overheid dus moeten beschikken over de noodzakelijke kennis om de risico's van de nieuwe werkelijkheid vroegtijdig te kunnen duiden en 'ontwrichtingsbeleid' te kunnen formuleren. Een belangrijk onderdeel van dit beleid zal een beredeneerde afweging moeten zijn over de mate waarin we als land willen beschikken over terugvalopties, de mogelijkheid om systemen te isoleren en over voorzieningen die ook offline kunnen functioneren.[212]

5.5 SIGNALERING: EEN BETER BEELD VAN AFHANKELIJKHEDEN

Paraatheid en signalering hangen nauw met elkaar samen. Zo impliceert de bovenstaande aanbeveling dat met name de afhankelijkheden tussen de digitale en fysieke wereld en binnen maatschappelijke sectoren beter in beeld gebracht dienen te worden. Wij bepleiten daarom een extra inspanning van de overheid op dit vlak. Ook is een andere benadering en operationalisering nodig van de lijst met vitale infrastructuur, omdat deze nog onvoldoende is toegesneden op het type verbindingen dat een digitaliserende wereld met zich meebrengt. In het verlengde hiervan zal ook de prioritering van vitale processen opnieuw moeten worden bezien.

AFHANKELIJKHEIDSBEELD

Om digitale ontwrichting vroegtijdig op het spoor te kunnen komen, is inzicht nodig in de verbindingen tussen cyber en fysieke sectoren en in de ketens en netwerken waarbinnen de Nederlandse en internationale organisaties functioneren die onmisbaar zijn voor kernprocessen in de samenleving. Daarbij is het belangrijk kennis te hebben van kwesties als: wie bezitten de aandelen in deze organisaties, dan wel mogen deze bezitten; wie hebben de formele en feitelijke zeggenschap over deze aandeelhouders?[213] Ook zal er voor verschillende sectoren

212 Vergelijk WRR 2017a: 67-77, 186.
213 Bulten et al. 2017.

een overkoepelend beeld moeten zijn van de eventuele dominantie en daarmee sterke afhankelijkheid van bepaalde dienstenaanbieders. Verder valt te denken aan kennis over de vestigingslanden van belangrijke aanbieders en andere spelers, met het oog op internationaal overleg als snel maatregelen genomen dienen te worden. Ontbreekt dergelijke kennis, dan zijn risico's niet goed in te schatten, is informatie over incidenten niet goed te duiden en blijft de voorbereiding op digitale ontwrichting in feite gemankeerd in zijn aanpak. Onze tweede aanbeveling is daarom:

Stel in aanvulling op het huidige Cybersecuritybeeld een Cyberafhankelijkheidsbeeld op, dat inzichtelijk maakt van welke partijen, digitale processen en diensten het functioneren van vitale processen in de Nederlandse samenleving afhankelijk is.

Een dergelijk 'afhankelijkheidsbeeld' verstevigt de praktische en strategische functie van het reeds bestaande Cybersecuritybeeld Nederland, dat jaarlijks de belangrijkste incidenten, dreigingen, belangen en de weerbaarheid op het gebied van cybersecurity inventariseert.[214] Dit afhankelijkheidsbeeld kan evenwel niet in detail openbaar gemaakt worden gezien het gevoelige karakter van veel informatie. Belangrijk is dat deze informatie gebruikt wordt om een betere duiding te geven aan incidenten en beslissingen, zowel voorafgaand als tijdens een ontwrichting. Ook kan de informatie worden benut bij de strategische discussies en keuzes over de mate waarin maatschappelijke en economische voorzieningen in ons land afhankelijk kunnen zijn van bepaalde partijen.

De aanbeveling tot het opstellen van een Cyberafhankelijkheidsbeeld is in dit rapport specifiek gericht op vitale processen. Maar het ligt voor de hand dat ook bedrijven en organisaties die niet bij vitale processen zijn betrokken een dergelijk beeld opstellen. Zeker wanneer zij een belangrijke functie in de samenleving vervullen, zoals ziekenhuizen, pakketdiensten (denk aan medicijnen) of betalingsplatforms. Het ontwikkelen van meer kennis van afhankelijkheden is in eerste instantie de verantwoordelijkheid voor private bedrijven, publieke diensten en individuele organisaties. Deze kennis zullen zij bovendien met een zekere regelmaat moeten actualiseren vanwege de economische en technologische dynamiek. Oefenen met scenario's voor digitale ontwrichting is daarbij een voor de hand liggend instrument, dat echter nog lang niet overal gangbaar is en daarom wellicht vaker een verplicht karakter dient te krijgen, zeker binnen de vitale infrastructuur.

Tegelijkertijd ontstijgt de voorbereiding op digitale ontwrichting per definitie het vermogen van individuele organisaties, vanwege de dynamiek van netwerkeffecten.

214 Meest recent: www.ncsc.nl/onderwerpen_a_z/csbn/index.aspx

Zelfs wanneer individuele partijen zicht hebben op de eigen afhankelijkheden, dan nog ontbreekt het bredere beeld voor de sector en de samenhang met andere domeinen. Voor dit bredere beeld is de overheid nodig. Zo is bekend dat talloze bedrijven en organisaties zeer afhankelijk zijn van de clouddiensten van slechts twee grote Amerikaanse aanbieders, Microsoft en Amazon. Hetzelfde geldt voor de afhankelijkheid van leveranciers van industriële controlesystemen, elektronische patiëntendossiers of geldautomaten. Maar de optelsom van deze afhankelijkheden en de precieze betekenis daarvan voor een dienst, een sector of zelfs ons land is onvoldoende bekend. Dat geldt evenzeer voor de vraag welke processen dan precies in het geding zijn. Bovendien zal de bredere context bekend moeten zijn om in de voorbereiding op of tijdens een ontwrichting de risico's te kunnen duiden en op basis daarvan maatregelen te nemen (zoals de keuze tussen wel of niet volledig afschakelen van externe verbindingen en op 'eilandvoorziening' overgaan).

ANDERE BENADERING EN OPERATIONALISERING LIJST VITALE INFRASTRUCTUUR

Een afhankelijkheidsbeeld biedt ook een beter zicht op organisaties waarvoor een hoger beschermingsniveau nodig is en die op assistentie door de overheid moeten kunnen rekenen, waaronder het delen van informatie over risico's. Welke organisaties dit zijn, volgt op dit moment uit de lijst met vitale infrastructuur. Deze lijst is van grote waarde voor de voorbereiding en bestrijding van digitale ontwrichting. De precieze samenstelling van deze lijst is daarmee van belang voor de mate waarin Nederland op een dergelijke situatie is voorbereid.

De selectie van vitale processen is een lastig politiek proces, onder meer omdat de bescherming van deze processen kostbaar is en de overheid over de daarbij betrokken partijen meestal geen directe zeggenschap heeft. Het huidige 'systeem' werkt bovendien vooral ten behoeve van de rijksoverheid en organisaties die als vitale aanbieders zijn aangemerkt. Organisaties daarbuiten zijn op zichzelf aangewezen, mocht het misgaan. In een vernetwerkte wereld heeft dit niet mis te verstane consequenties, zowel nationaal als internationaal en niet in het minst ook voor de partijen binnen de vitale infrastructuur zelf.

Een eerste reden voor een andere benadering en operationalisering van de huidige lijst met vitale infrastructuur is het sterk toegenomen belang van digitale processen. Hierbij gaat het zowel om op zichzelf staande digitale processen zoals het elektronische berichtenverkeer en authenticatiediensten, als om processen die ondersteunend zijn aan andere vitale processen zoals de elektriciteitsvoorziening of het betalingsverkeer. Een aantal van deze processen is de afgelopen jaren reeds toegevoegd aan de lijst met vitale infrastructuur maar de vraag is of dit voldoende is. Door de snelle ontwikkeling en brede adaptatie van digitale toepassingen in tal van maatschappelijke domeinen, kunnen onverwacht nieuwe en omvangrijke kwetsbaarheden ontstaan, die vragen om opname van nieuwe organisaties als

aanbieders van vitale diensten. Een voorbeeld is de betalingsdienst die Facebook van plan is te lanceren.

Ten tweede is de vraag in hoeverre het nog zinvol is om vitale processen aan individuele aanbieders te koppelen. Er is alle aanleiding om in kaart te brengen door welke ketens en netwerken vitale processen worden ondersteund en daarmee van welke andere partijen de aanbieders van die processen afhankelijk zijn. Dit inzicht kan ertoe leiden dat ook andere partijen dan de aanbieders van vitale processen onder de vitale infrastructuur dienen te vallen. Het beleid gericht op vitale processen zal kortom duidelijk moeten maken hoe als 'vitaal' aan te merken aanbieders functioneren binnen ketens en netwerken, met als uitgangspunt dat sommige onderdelen daarvan onmisbaar zijn voor de continuïteit van de vitale processen. Het voorbeeld van de elektriciteitsvoorziening in hoofdstuk 4 laat zien dat ook incidenten die beginnen bij partijen die niet als vitale aanbieder zijn aangemerkt, door cascade-effecten kunnen bijdragen aan de ontwrichting van vitale processen. Met andere woorden, indien een incident buiten de vitale sectoren niet tijdig wordt aangepakt, kan ook de vitale infrastructuur worden geraakt.

Tot slot heeft het grensoverstijgende karakter van veel ketens en netwerken ook implicaties voor de Europese harmonisatie van de bescherming van vitale infrastructuur. Enerzijds zal er ook op Europees niveau meer aandacht moeten komen voor de wijze waarop aanbieders van als vitaal aangemerkte processen verbonden zijn, zowel onderling als met externe partijen. Anderzijds is een minder vrijblijvende opstelling van de lidstaten noodzakelijk. De uiteenlopende manieren waarop de Europese lidstaten invulling geven aan de in de Netwerk- en informatiebeveiliging richtlijn (NIB-richtlijn) genoemde vitale sectoren en diensten bemoeilijkt namelijk een gezamenlijke signalering en bestrijding van grensoverschrijdende incidenten en van incidenten die de Europese netwerken en instituties raken. Zo omvat de NIB-richtlijn maatregelen voor de zorgsector, maar ons land heeft die sector bij de implementatie van de richtlijn in de Wet beveiliging netwerk- en informatiesystemen (Wbni) niet opgenomen. Dit betekent concreet dat er op het terrein van de zorg voor de lidstaten geen gemeenschappelijk aanspreekpunt bestaat in het geval van een incident. Dergelijke uitzonderingen belemmeren de totstandkoming van een Europees dekkend stelsel voor de gehele vitale infrastructuur.

Besteed bij het beleid voor vitale infrastructuur meer aandacht aan de ketens en netwerken die vitale processen ondersteunen.

Onderzoek bovendien of digitalisering het nodig maakt de prioritering van vitale processen aan te passen (digitale triage).

DIGITALE TRIAGE

De lijst met vitale infrastructuur bevat eveneens criteria voor het stellen van prioriteiten bij de aanpak van een ontwrichting. In 2014 heeft een herijking van deze lijst plaatsgevonden. Aan de hand van diverse impactcriteria is toen, zoals besproken in hoofdstuk 2, ook een onderscheid gemaakt tussen twee categorieën vitale processen. De processen met de grootste impact bij uitval, bijvoorbeeld door cascade-effecten, krijgen voorrang tijdens crisissituaties. Immers, niet alle problemen kunnen tegelijkertijd worden aangepakt. Bovendien kan prioriteren dienstbaar zijn aan het beperken van de schade en een spoedig herstel. De digitalisering maakt het noodzakelijk om de categorisering van vitale processen opnieuw tegen het licht te houden. Het proces van prioriteitstelling noemen we 'digitale triage'.[215]

Om te beginnen is de vraag of de huidige indeling nog volstaat, gegeven de groeiende afhankelijkheid van digitale technologie. Het ligt voor de hand dat hierdoor ook gevolgen van een digitale ontwrichting een grotere omvang zullen hebben. De eerdergenoemde kosten van de verstoring en uitval van digitale voorzieningen zijn hiervoor een belangrijke indicatie. Ook zijn kanttekeningen te plaatsen bij de keuze om impact leidend te maken voor de prioritering van vitale processen. In crisissituaties kunnen namelijk heel andere processen het belangrijkst zijn voor een snel herstel van de samenleving. En heel andere processen kunnen (technisch) onmisbaar zijn voor de uitvoering van noodzakelijke herstelwerkzaamheden. Zo is de continuïteit van veel vitale processen inmiddels afhankelijk van talloze digitale voorzieningen. Sommige van deze voorzieningen verdienen wellicht voorrang bij de respons op incidenten, omdat ze het herstel van andere belangrijke maatschappelijke functies faciliteren. Digitale communicatievoorzieningen verdienen mogelijk meer voorrang omdat ze een bepalende rol spelen bij de informatievoorziening aan burgers en de aanpak van maatschappelijke onrust.

Aandacht voor digitale triage vanuit dit dubbele perspectief van zowel impact als herstelmogelijkheden, biedt bewindslieden de mogelijkheid om tijdens een crisis beslissingen te nemen die vooraf beredeneerd en politiek bediscussieerd zijn. Tijdens ontwrichtende gebeurtenissen is daarvoor geen tijd. Een dergelijke triage heeft ook als voordeel dat de betrokken partijen van tevoren op de hoogte wor-

---

215 Het begrip 'triage' stamt af van het Franse woord trier, wat rangschikken betekent. De betekenis kan worden teruggeleid naar het werk van een verpleger in het leger van Napoleon, die een methode ontwikkelde om verwondingen te evalueren en de evacuatie van patiënten in gang te zetten tijdens de strijd (Baker 2007). In het digitale domein wordt het begrip triage gebruikt in relatie tot het werk van cybersecurityanalisten, die zich bezighouden met detectie en monitoren van netwerken (Ben-Asher en Gonzalez, 2015; Zhong, Lin, Liu, Yen en Chen, 2018). Digitale triage zoals voorgesteld in dit rapport reikt echter verder dan enkel het digitale domein. De focus is gericht op het identificeren van prioriteiten met betrekking tot het herstel van vitale onderdelen in een digitaliserende samenleving.

den gesteld, zodat zij niet voor verrassingen komen te staan en maatregelen kunnen nemen. Dit proces verhoogt uiteindelijk de weerbaarheid van vitale functies in een samenleving.[216]

Tegelijkertijd is het een illusie om te denken dat de overheid hier als enige aan de knoppen zit – zoals destijds de afhankelijkheid van Microsoft bij Diginotar al toonde. In veel gevallen zullen ook andere partijen een rol spelen bij de keuzes die nodig zijn om digitale ontwrichting te bestrijden en herstel mogelijk te maken. Een goed zicht op en contact met deze partijen is van groot belang om tijdens een crisis het functioneren van de Nederlandse samenleving te kunnen blijven waarborgen. Het eerder besproken afhankelijkheidsbeeld moet hiertoe dienstbaar zijn.

5.6 BESTRIJDING: MEER BEVOEGDHEID, CATEGORISERING VAN INCIDENTEN EN EUROPESE COÖRDINATIE

Als het onverhoopt misgaat, dan dient de overheid een 'digitale brand' meester te kunnen worden. Zeker wanneer als gevolg daarvan maatschappelijke ontwrichting dreigt op te treden. De overheid ziet zich daarbij voor een aantal problemen gesteld. Allereerst ontbreekt voor de nieuwe werkelijkheid een adequaat toegerust equivalent van de welbekende hulpdiensten. Ten tweede is er geen duidelijke categorisering van incidenten om te kunnen bepalen wanneer de bevoegde hulpdiensten ingeschakeld worden. Een derde probleem is dat ontwrichtende gebeurtenissen met een grensoverschrijdende of Europese dimensie niet goed zijn op te vangen, omdat er op dat vlak nog nauwelijks coördinatie is.

BEVOEGDHEID

Wanneer de kans bestaat dat digitale verstoringen een ontwrichtend effect hebben op de samenleving, dan moet de overheid inzicht hebben in de situatie en waar nodig sturend optreden. Die sturing kan vergaand zijn. Van het bedrijf Diginotar nam de overheid in 2011 het bewind over, omdat onduidelijkheid bestond over de omvang van de problemen en het vertrouwen in de digitale overheid op het spel stond. In de nasleep van Diginotar is deze ingreep helaas niet expliciet geëvalueerd. De noodzakelijke bevoegdheden van de overheid zijn daardoor nooit goed bediscussieerd. Het is belangrijk dat alsnog te doen, omdat de overheid op dit moment wettelijk gezien uitsluitend facultatief advies en bijstand kan leveren. Dit betekent dat organisaties en bedrijven de digitale hulpdiensten buiten de deur kunnen houden bij de aanpak van digitale verstoringen en prioriteiten kunnen stellen die strijdig zijn met het publiek belang. Wanneer organisaties en bedrijven bovendien niet behoren tot de vitale infrastructuur staat de overheid min of meer machteloos.

216 Verner, Petit en Kim 2017.

De overheid heeft in het kader van de bestaande crisiswetgeving weliswaar verschillende mogelijkheden om in te grijpen, maar deze ontberen een heldere toespitsing op de omgang met incidenten in een digitaliserende samenleving. Bovendien is de huidige crisisbesluitvorming georganiseerd langs functionele lijnen of gekoppeld aan een gemeente, de regio of het Rijk. De rijksoverheid kan in noodsituaties altijd ingrijpen. Maar het is wenselijk dat dit gebeurt op een voorspelbare en controleerbare wijze. Dit geldt vooral als opsporingsinstanties als de politie en de Officier van Justitie interveniëren. Een cruciale vraag hierbij is of een dergelijke interventie gerechtvaardigd is als deze geen opsporings- of vervolgingsdoel dient. Van de brandweer verwachten we dat zij de brand blust en niet ook de inboedel confisqueert. In een digitale wereld is dat onderscheid veel lastiger te maken omdat gegevens niet van hun plek hoeven te komen om voor andere doelen te worden hergebruikt. Onze aanbeveling is daarom:

Creëer een helder afgebakende wettelijke bevoegdheid voor digitale hulptroepen ten dienste van de bestrijding van digitale storingen die een maatschappelijk ontwrichtend effect kunnen hebben. Onderzoek in dat kader de noodzaak van een aparte regeling voor overheidshandelen gericht op het tegengaan van verdere escalatie. Een categorisering van incidenten kan hierbij behulpzaam zijn.

Een generieke, wettelijk verankerde bevoegdheid en daarbij horende inkadering geeft de overheid de ruimte om digitale ontwrichting te bestrijden. Maar het doel daarvan is ook om burgers en bedrijven te vrijwaren van buitenproportionele, ongecontroleerde of arbitraire handelingen van de overheid.[217] Een dergelijke inkadering is in het bijzonder van belang wanneer ontwrichting dreigt te ontstaan maar feitelijk nog niet waarneembaar is.

NAAR EEN CATEGORISERING VAN INCIDENTEN

Bij het uitwerken van de hiervoor bepleite bevoegdheid verdient het de voorkeur de inzet daarvan te specificeren aan de hand van verschillende categorieën digitale incidenten, zoals bijvoorbeeld de Verenigde Staten, Frankrijk en het Verenigd Koninkrijk die inmiddels hanteren.[218] Lang niet alle digitale incidenten en categorieën raken aan de nationale veiligheid of hebben betrekking op verstoringen van vitale processen. Een nadere categorisering maakt een betere afweging mogelijk over de proportionaliteit van de inzet van bijzondere bevoegdheden en de keuze voor verschillende organisaties om ze te bestrijden enerzijds en de te verwachten gevolgen van een incident anderzijds. Door te differentiëren naar de ernst van de

217 WRR 2016: 97.
218 Zie p. 68 van dit rapport.

situatie kan bovendien een te vanzelfsprekend beroep op de centrale overheid worden voorkomen. Tegelijkertijd biedt een dergelijke categorisering wel degelijk handvatten voor bestuurlijke en politieke opschaling. Ook bij een brand bijvoorbeeld is de bestrijding in principe decentraal belegd, maar is opschaling mogelijk als de omvang van het incident daar aanleiding toe geeft.

EUROPESE COÖRDINATIE

Gegeven de kenmerken van digitale ontwrichting verdient het sterk de voorkeur de bovenstaande aanbevelingen ten aanzien van de bestrijding van incidenten ook internationaal te agenderen. De Europese Unie is daarbij een voor de hand liggend aangrijpingspunt, nu er met de NIB-richtlijn meer uniformiteit komt in de bescherming van aanbieders van vitale processen. Om digitale ontwrichting op een zinvolle manier te kunnen bestrijden is de Nederlandse overheid immers vaak ook afhankelijk van buitenlandse overheden, vooral van hun vermogen om een ontwrichtende gebeurtenis tijdig een halt toe te roepen of bijstand te verlenen. En andersom zullen andere landen Nederland om assistentie kunnen vragen.

Nederland kan aan een beter gecoördineerde Europese aanpak bijdragen door versterking van de NIB-samenwerkingsgroep[219] na te streven. Deze samenwerkingsgroep is opgericht in het kader van de NIB-richtlijn en wordt gesteund door de nationale Computer Security Incident Response Teams (CSIRT's), de Europese Commissie en agentschap ENISA. Naar analogie van de Europese Artikel 29-werkgroep, die inmiddels is opgevolgd door de wettelijk verankerde European Data Protection Board[220], zou dit samenwerkingsverband op termijn als opstap kunnen dienen voor een organisatie met meer bevoegdheid op het niveau van de Europese Unie. Deze bevoegdheid zou zich daarbij onder meer moeten richten op de bestrijding van incidenten die de Europese instituties raken of de capaciteit van individuele lidstaten dermate overstijgen dat dit een risico is voor vitale infrastructuur elders in Europa.[221]

5.7 HERSTEL EN WEDEROPBOUW: EEN CYBERPOOL ONDERZOEKEN EN INCIDENTDATA BETER BENUTTEN

Na een ontwrichtende gebeurtenis breekt er doorgaans ook weer een periode van herstel en wederopbouw aan. Een variëteit aan zaken vraagt dan om aandacht, van slachtofferhulp en schadevergoeding tot de evaluatie van wat er zoal misging. Specifiek met het oog op een digitale ontwrichting agenderen wij dan ook een tweetal kwesties die samenhangen met de noodzaak om na een grootschalig incident weer op te krabbelen en – waar mogelijk – de situatie te benutten om van de ontwrichting te leren en

219 Zie https://ec.europa.eu/digital-single-market/en/nis-cooperation-group
220 Zie https://edpb.europa.eu/
221 Vergelijk het voorstel voor een Europees cyberagentschap in CEPS 2018. Dit agentschap kent ook de bevoegdheid om aanvallen te attribueren.

verbeteringen door te voeren. Het betreft onderzoek naar de haalbaarheid van een cyberpool en een betere benutting van incidentdata.

CYBERPOOL

Een belangrijk onderdeel van herstel en wederopbouw is de compensatie van slachtoffers, via aansprakelijkheid, schadevergoeding, verzekerbaarheid dan wel tegemoetkoming door de overheid.[222] Het oogmerk van deze instrumenten is om benadeelden zoveel mogelijk in staat te stellen de draad weer op te pakken en bij voorkeur hun eerdere positie weer in te laten nemen. De realiteit is veelal anders, al is het maar omdat talloze vragen rijzen over toerekening van de schade, causaliteit of bijvoorbeeld het moment waarop de schade wordt vastgesteld.[223]

Zeker in een digitaliserende wereld zijn aansprakelijkheid, schadevergoeding en verzekerbaarheid lastig vorm te geven. Bovendien spelen cascade-effecten, de complexe wisselwerking tussen informatieprocessen en daarmee verband houdende causaliteitsvragen. Ook is de dader veelal niet te traceren en is er grote onbekendheid met zowel de risico's als het type kosten dat daaraan is verbonden. Met name verzekerbaarheid is, zoals in hoofdstuk 4 aangegeven, momenteel een urgent vraagstuk. Verzekeren is in principe een zaak voor de markt. Maar wanneer de markt er niet in slaagt om mogelijkheden te bieden om risico's voldoende af te dekken, kan de overheid zekerheid proberen te bieden.

De overheid kan verzekeringen wettelijk verplicht stellen – wat vaak een lang en ingrijpend traject is – maar ook met verschillende partijen een herverzekeringsfonds organiseren om risico's te (her)verzekeren. In dit verband wordt veelal de term *pool* gehanteerd. Een dergelijke pool wordt onder meer gebruikt voor de verzekering van grote of technisch ingewikkelde risico's. Elke partij deelt met een vooraf vastgesteld percentage mee in de verzekering. Een poolconstructie is voor digitale ontwrichting zeker een te onderzoeken optie, nu verzekeraars zich terug lijken te trekken uit de markt voor cyberverzekeringen uit angst voor te grote schadeclaims. Ter inspiratie voor deze 'cyberpool' kan bijvoorbeeld naar de Nederlandse Herverzekeringsmaatschappij voor Terrorismeschaden worden gekeken, die alle sectoren tegen schade verzekert tot een bedrag van 1 miljard euro per kalenderjaar, opgebracht door nationale verzekeraars, internationale herverzekeraars en de Nederlandse staat.[224] Met deze constructie liep Nederland in 2003 internationaal voorop.

---

222 Afgezien van compensatie van benadeelden kan civielrechtelijke aansprakelijkheid ook dienstbaar zijn aan (en soms ook een alternatief vormen voor) publiekrechtelijke maatregelen gericht op een betere voorbereiding. Immers, wie zelf de rekening moet betalen, zal geneigd zijn de kosten te minimaliseren en zal zich dus beter voorbereiden.

223 Hartlief 2014.

224 Bruggeman en Faure 2018: 70-72, 82.

Stimuleer onderzoek naar de haalbaarheid van een Nederlandse of Europese cyberpool om financiële dekking mogelijk te maken voor schade als gevolg van digitale ontwrichting.

Bij dit onderzoek verdienen het identificeren en kwantificeren van zogenoemde systeemrisico's bijzondere aandacht. Verzekeraars, grote nutsbedrijven, banken, multinationals en overheden wereldwijd maken in toenemende mate gebruik van kwantitatieve modellen om cyberrisico's beter te beheersen. Hoewel dit een stap in de goede richting is, ontbreken vooralsnog betrouwbare methoden om systeemrisico's in kaart te brengen. Deze risico's zijn te veranderlijk en complex, en overstijgen bovendien het niveau van individuele organisaties. De overheid kan aan de ontwikkeling van meer betrouwbare methoden een bijdrage leveren, bijvoorbeeld door de binnen de overheid reeds voorhanden kennis en data beschikbaar te stellen.

Tevens is het belangrijk om vast te stellen of, in hoeverre en welk type cyberaanvallen onder internationaal recht als gewapend conflict zijn te beschouwen. Dit gegeven is immers, zoals we bespraken in hoofdstuk 4, beslissend voor de verzekerbaarheid van schade als gevolg van cyberaanvallen. Nederland speelt op het vlak van de regulering van cyberspace een voortrekkersrol. Door zijn bijdrage aan de doorontwikkeling van de Tallinn Manual ondersteunt Nederland het daarin opgenomen verbod op aanvallen op civiele infrastructuur.[225] Hiernaast draagt Nederland internationaal uit dat de publieke kern van het internet bescherming behoeft en gevrijwaard moet blijven van bemoeienis door nationale overheden.[226] Dit zijn belangrijke stappen op de lange weg naar de regulering van cyberspace. Om op de kortere termijn de totstandkoming van een volwassen markt voor cyberverzekeringen niet onnodig te belemmeren, is van de Nederlandse overheid een terughoudende opstelling vereist wat betreft de typering van cyberaanvallen als oorlogshandelingen.

INCIDENTDATA BETER BENUTTEN

Herstel en vooral wederopbouw bieden de mogelijkheid om een volgende keer beter voorbereid te zijn en opnieuw te wegen welke belangen voorrang dienen te krijgen. Leren van eerdere keuzes en eventueel gemaakte fouten speelt daarbij een belangrijke rol. Met leren van kleine incidenten valt mogelijk een veel groter en ontwrichtend incident te voorkomen.

225 Deel IV van de *Tallinn Manual 2.0* bevat bepalingen over het verbod om cyberaanvallen te richten op civiele doelen, waaronder medische systemen. Deze doelen overlappen in belangrijke mate met vitale infrastructuur. Zie hiervoor Schmitt et al. 2017.

226 WRR 2015.

Het faciliteren van het collectieve leervermogen kan op talloze manieren, maar in ieder geval is intern en extern toezicht hierbij nuttig.[227] Externe toezichthouders beschikken over waardevolle data nu zij meldingen van incidenten ontvangen en verwerken, waaronder meldingen over problemen met de continuïteit van kernprocessen. Deze meldingen over datalekken, verstoringen en continuïteitsproblemen komen momenteel echter bij verschillende toezichthoudende instanties terecht. De data die met meldingen beschikbaar komen worden mede hierom nog lang niet altijd op systematische wijze geanalyseerd. Hierdoor ontzeggen toezichthouders zichzelf en de partijen waarop zij toezicht houden waardevolle informatie voor een betere voorbereiding op digitale ontwrichting. Bij dergelijke informatie valt te denken aan bijvoorbeeld inzichten in type daders in relatie tot de specifieke kenmerken van een aanval.

Zorg op nationaal en op Europees niveau voor een meer systematische ontsluiting van incidentdata, benut deze data beter en realiseer een effectieve terugkoppeling naar de betrokken partijen om het collectieve leervermogen te versterken.

De Cyber Security Raad onderzoekt momenteel de mogelijkheid om data van de Autoriteit Persoonsgegevens afkomstig uit de meldplicht voor datalekken beter te benutten. Evenzeer belangrijk is het benutten van data afkomstig uit de meldplichten in de NIB-richtlijn. Omdat deze richtlijn nadrukkelijk ten doel heeft om meer samenhang aan te brengen in het cybersecuritybeleid van de Europese lidstaten, is het belangrijk dat Nederland zich inspant om incidentdata ook in Europees verband beter gedeeld en geanalyseerd te krijgen. Deze taak zou eveneens belegd kunnen worden bij de eerder genoemde NIB-samenwerkingsgroep.

5.8 SLOT

Nederland is een van de meest gedigitaliseerde landen ter wereld. Digitale infrastructuur is – soms zonder dat we ons ervan bewustzijn – intens verweven met processen waarvan de continuïteit van groot belang is voor de samenleving, economie en wdemocratische rechtstaat. De komende jaren zal deze verbondenheid nog intensiever worden, met ontwikkelingen als artificiële intelligentie, cloud computing en het 'Internet of Things'. Daarom is het goed dat er steeds meer aandacht is voor de bescherming van digitale infrastructuur. Tegelijkertijd valt een 100% veilige situatie nooit te garanderen. In aanvulling op het bestaande beleid, pleit dit rapport daarom voor een betere voorbereiding op situaties waarin digitale

227 WRR 2013: 150, 155.

infrastructuur verstoord raakt of uitvalt en maatschappelijke ontwrichting dreigt te ontstaan.

Er staat inmiddels te veel op spel om de voorbereiding op en aanpak van een digitale ontwrichting op zijn beloop te laten. De grote afhankelijkheid van digitale infrastructuur noopt tot het nemen van maatregelen om schade te beperken en betrokken partijen in staat te stellen zo snel mogelijk weer op te krabbelen. De analyse in dit rapport laat zien dat de overheid een digitale ontwrichting momenteel maar beperkt tegemoet kan treden binnen de bestaande kaders, omdat het klassieke instrumentarium voor de omgang met maatschappelijke ontwrichting hierop onvoldoende is toegesneden. De aanbevelingen in dit hoofdstuk verschaffen daarom alternatieve handelingsmogelijkheden. Helder is dat het gebruik van deze mogelijkheden om een grondige doordenking vraagt van de rol en verantwoordelijkheid van de overheid in een digitaliserende wereld.

GESPROKEN PERSONEN

Vermelding organisatie ten tijde van gesprek

L.F.M. van den Aarsen, ministerie van Infrastructuur en Waterstaat
J.C.J.H. Aerts, Vrije Universiteit Amsterdam
E.S.M. Akerboom, Nationale Politie
A.J. Akkermans, Vrije Universiteit Amsterdam
N. Aland, Nationaal Coördinator Terrorismebestrijding en Veiligheid
J. van Alphen, Deltacommissaris
P. Antenbrink, Algemene Rekenkamer
H. Arnold, Centrum voor Criminaliteitspreventie en Veiligheid
H. Backx, GGD GHOR Nederland
R. Bakker, Gemeente Rotterdam
E. Beekman, Academisch Medisch Centrum
A.J.M. van Bellen, ECP, Platform voor de InformatieSamenleving
R. Bening, ING
R.A. Boin, Universiteit Leiden
W.H. van Boom, Universiteit Leiden
M.P. Boots, ministerie van Algemene Zaken
P.L.J. Bos, Veiligheidsregio Utrecht
T. Brinkman, Verbond van Verzekeraars
E. Bronsdijk, Gemeente Rotterdam
V. Bruggeman, Milieu Law and Policy Consulting
G.W. van der Burg, Openbaar Ministerie
M. Coenders, Gemeente Rotterdam
M.T.A. Coenders, Universiteit Utrecht
C. Contino, Fonds Slachtofferhulp
F. Dezeure, Freddy Dezeure BVBA
M. van Dorssen, Berenschot BV
H.L. Duijnhoven, TNO
J.F.E. Farwerck, KPN
M. Faure, Universiteit Maastricht
P. van der Feltz, Google Nederland
E. Fledderus, SURF
M. Groenendijk, Evides Waterbedrijf
I.M. Haisma, Sim-ci/Alliander
T. Hartlief, Universiteit Utrecht
P. Hartman, Riskfit Innovation
E. van den Heuvel, Cyber Security Raad
L. Holterman, Cyberveilig Nederland

B.P.F. Jacobs, Radboud Universiteit Nijmegen
O. Janssen, Aon
H. de Jong, Nationale Politie
T.H.J. Joustra, Onderzoeksraad voor Veiligheid
M. Jutte, Hudson Cybertec
E. Kamps, Crossyn Automotive BV
N. Kastelein, ministerie van Financiën
S. Kewal, ministerie van Binnenlandse Zaken en Koninkrijksrelaties
R. Kleijmeer, De Nederlandsche Bank NV
J. Knops, Nationaal Coördinator Terrorismebestrijding en Veiligheid
O. Koeroo, KPN
H.C.D. Korvinus, ministerie van Algemene Zaken
M. Krom, PostNL
L.W. van der Laan, D66
A.C.A.P. van Lammeren, Planbureau voor de Leefomgeving
M. Leenaars, NLnet
M.J. van Leeuwen, Verbond van Verzekeraars
T. van Lieshout, Veiligheidsregio Midden West Brabant
H.A.M. Luiijf, Luiijf Consultancy
N. Mallens, VNO-NCW
E. Medendorp, Onderzoeksraad voor Veiligheid
R. Miedema, Gemeente Rotterdam
E.M.L. Moerel, Tilburg Law School
A. Molenaar, Gemeente Rotterdam
E.R. Muller, Onderzoeksraad voor Veiligheid
A.A. Muntslag – Bakker, Cyber Security Raad
T. Netelenbos, ECP, Platform voor de InformatieSamenleving
W.J.K. Nierstrasz, Gemeente Rotterdam
B. Nieuwesteeg, Erasmus Universiteit Rotterdam
J.A. Nijhuis, Schiphol Group
D.G.M. O'Floinn, Nationaal Coördinator Terrorismebestrijding en Veiligheid
A.M. Ottolini, Evides Waterbedrijf
A.K.J. van Petersen, Nationaal Cyber Security Centrum
S. van der Pijnse van der Aa, Onderzoeksraad voor Veiligheid
A.C. Pleyte, Nationaal Coördinator Groningen
M. Postma, Fox-IT
I. Quist, Nationaal Coördinator Terrorismebestrijding en Veiligheid
H.J. Reinders, De Nederlandsche Bank NV
S.J.G. Reyn, ministerie van Defensie
S. Riedstra, ministerie van Justitie en Veiligheid
G.N. Roes, Raad van State
Y.C.M.T. van Rooy, Nederlandse Vereniging van Ziekenhuizen

R. Roozendaal, ministerie van Volksgezondheid, Welzijn en Sport
U. Rosenthal, Adviesraad voor wetenschap, technologie en innovatie
C. van Ruijven, Instituut Fysieke Veiligheid (IFV)
T. van Ruijven, TNO
H. Schrijvers, Sim-ci/Alliander
B. Sluijter, Nationaal Coördinator Terrorismebestrijding en Veiligheid
F. Soeteman, Verbond van Verzekeraars
J.W.E. Spies, Gemeente Alphen aan den Rijn
W.W. Stevens, ministerie van Algemene Zaken
C. Stuurman, Tilburg University
I. Sybesma, Fonds Slachtofferhulp
J.J. Sylvester, Nationale Ombudsman
J. van Tol, ministerie van Economische Zaken en Klimaat
M. in 't Veld, Nationaal Coördinator Groningen
P.G. van der Velden, CentERdata
K. Verhoeven, D66
A.C. Vervooren, Gemeente Rotterdam
M.F. Verweij, Wageningen University & Research
F.W. Vijselaar, ministerie van Economische Zaken en Klimaat
P. van Vollenhoven, Stichting Maatschappij en Veiligheid
G.H. de Vries, Universiteit van Amsterdam
H. de Vries, Nationaal Cyber Security Centrum
R. de Vries, Port of Rotterdam
R.H. van Wanroij, Nationaal Coördinator Terrorismebestrijding en Veiligheid
R. Wenselaar, Menzis
D. Wielenga, Raad voor de Leefomgeving en Infrastructuur
M. van Wieren, Aon
G.W.P.J. Wismans, Nationaal Coördinator Terrorismebestrijding en Veiligheid
M. Zannoni, COT Instituut voor Veiligheids- en Crisismanagement
P.M. Zorko, Nationaal Coördinator Terrorismebestrijding en Veiligheid
R.F.B. van Zutphen, Nationale Ombudsman
R. van Zwol, Raad van State

AFKORTINGEN

AIVD	Algemene Inlichtingen- en Veiligheidsdienst
AMS-IX	Amsterdam Internet Exchange
BGP	Border Gateway Protocol
CERT	Computer Emergency Response Team
CERT-EU	Computer Emergency Response Team Europese Unie
CPB	Centraal Planbureau
CSIRT	Computer Security Incident Response Team
CSR	Cyber Security Raad
DDoS	Distributed Denial of Service
DNB	De Nederlandse Bank
DNS	Domain Name System
DTC	Digital Trust Center
DVM	Dynamisch Verkeersmanagement
EC3	European Cyber Crime Centre
EDA	European Defense Agency
ENISA	European Union Agency for Network and Information Security
EPSC	European Political Strategy Centre
FIRST	Forum of Incident Response and Security Teams
ICT	Informatie en Communicatietechnologie
IMF	Internationaal Monetair Fonds
IoT	Internet of Things
IP	Internet Protocol
IPCR	Integrated Political Crisis Response
IRB	ICT Response Board
ISAC	Information Sharing Analysis Center
MIVD	Militaire Inlichtingen- en Veiligheidsdienst
NAFIN	Netherlands Armed Forces Integrated Network
NAVO	Noord-Atlantische Verdragsorganisatie
NCCIC	National Cybersecurity and Communications Integration Center
NCSC	Nationaal Cyber Security Centrum
NCTV	Nationaal Coördinator Terrorismebestrijding en Veiligheid
NDN	Nationaal Detectie Netwerk
NHC	Nationaal Handboek Crisisbesluitvorming
NHS	National Health Service
OECD	Organisation for Economic Cooperation and Development
OM	Openbaar Ministerie
PBL	Planbureau voor de Leefomgeving
PKI	Public Key Infrastructure
RIVM	Rijksinstituut voor Volksgezondheid en Milieu

RLI	Raad voor de Leefomgeving en Infrastructuur
SIDN	Stichting Internet Domeinregistratie Nederland
TIBER	Threat intelligence-based ethical red teaming
WODC	Wetenschappelijk Onderzoek en Documentatiecentrum
WRR	Wetenschappelijke Raad voor het Regeringsbeleid

LITERATUUR

Algemene Inlichtingen en Veiligheidsdienst (2019) *Jaarverslag 2018*, Den Haag: AIVD.

Algemene Rekenkamer (2019) *Digitale dijkverzwaring: cybersecurity en vitale waterwerken*, Den Haag.

Analistennetwerk Nationale Veiligheid (2010) *Nationale risicobeoordeling 2011*, Den Haag.

Analistennetwerk Nationale Veiligheid (2011) *Nationale risicobeoordeling 2011*, Den Haag.

Analistennetwerk Nationale Veiligheid (2012) *Nationale risicobeoordeling 2012*, Den Haag.

Analistennetwerk Nationale Veiligheid (2016) *Nationaal Veiligheidsprofiel 2016. Een All Hazard overzicht van potentiële rampen en dreigingen die onze samenleving kunnen ontwrichten*, Den Haag.

Analistennetwerk Nationale Veiligheid (2018) *Horizonscan nationale veiligheid 2018*, Den Haag. Beschikbaar op: www.thehaguesecuritydelta.com/media/com_hsd/report/216/document/ANV-Horizonscan-Nationale-Veiligheid-2018.pdf

AON (2019) *Cyber perils in a growing market. Helping EMEA organisations better understand the interconnectivity among multiple lines of insurance*. Beschikbaar op: www.aon.com/unitedkingdom/insights/cyber-perils-in-a-growing-market.jsp

Backman, S. en Rhinard, M. (2018) 'The European Union's capacities for managing crises', *Journal of contingencies and crisis management* 26, 2: 261-271.

Baker, M.S. (2007) 'Creating order from chaos: part I: triage, initial care, and tactical considerations in mass casualty and disaster response', *Military medicine* 172, 3: 232-236.

Bakker, S. (2017) *From luxury to necessity: what the railways, electricity and the automobile teach us about the IT revolution*, Amsterdam: Boom Uitgevers.

Ben-Asher, N. en C. Gonzalez (2015) 'Effects of cyber security knowledge on attack detection', *Computers in Human Behavior* 48: 51-61.

Bergström J., C. Uhr en T. Frykmer (2016) 'A Complexity Framework for Studying Disaster Response Management', *Journal of Contingencies and Crisis Management* 24, 3.

Bharosa, N., Lee, J. en M. Janssen (2010) 'Challenges and obstacles in sharing and coordinating information during multi-agency disaster response: Propositions from field exercises', *Information Systems Frontiers* 12, 1: 49-65.

Biener, C., M. Eling en J.H. Wirfs (2015) 'Insurability of Cyber Risks: An Empirical Analysis', *The Geneva Papers 2015* 40: 131-158.

Boeke, S. (2016) *First Responder or Last Resort? The role of the Ministry of Defence in national cyber crisis management in four European countries*, Den Haag: Universiteit Leiden.

Boin, R.A. (2017) *De Grenzeloze Crisis: Uitdagingen voor Politiek en Bestuur*, oratie Universiteit Leiden.

Boin, R.A. en M. Lodge (2018) *Enhancing the* EU's *transboundary crisis management capacity: recommendations for practice*, Londen: TransCrisis.

Bolhuis, M. (2018) 'Cybersecurityregulering in de praktijk. Van wetgeving naar technoregulering', www.recht.nl/vakliteratuur/ict/artikel/441678/cybersecurityregulering-in-de-praktijk-van-wetgeving-naar-technoregulering/

Bovens, M.A.P. (1998) *De digitale rechtstaat. Beschouwingen over informatiemaatschappij en rechtstaat*, oratie Utrecht, Alphen aan den Rijn: Samsom.

Broeders, D. (2017) 'Aligning the international protection of 'the public core of the internet' with state sovereignty and national security', *Journal of Cyber Policy* 2, 3: 366-376. Beschikbaar op: https://doi.org/10.1080/23738871.2017.1403640

Bruggeman, V. en Faure M. (2018) 'Compensation for victims of disaster in Belgium, France, Germany and the Netherlands', WRR Working Paper 30, Den Haag.

Bruijne, M. de, M. van Eten, Carlos Hernández Gañán, Wolter Pieters (2017) *Towards a new cyber threat actor typology. A hybrid method for the* NCSC *cyber security assessment,* TU Delft. Beschikbaar op: www.wodc.nl/binaries/2740_Volledige_Tekst_tcm28-273243.pdf

Brundage, M. et al. (2018) *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation.* Beschikbaar op: http://img1.wsimg.com/blobby/go/3d82daa4-97fe-4096-9c6b-376b92c619de/downloads/1c6q2kc4v_50335.pdf

Bulten, C., B. de Jong, E. Breukink en A. Jettinghoff (2017) *Vitale vennootschappen in veilige handen*, Nijmegen: Onderzoekscentrum onderneming & recht. Beschikbaar op: www.wodc.nl/binaries/2609_Volledige_Tekst_tcm28-250320.pdf

Carr, N. (2015) *De glazen kooi. Wat automatisering met ons doet*, Amsterdam: Maven Publishing.

Cassa, C.A., R. Chunara, K. Mandl en J.S. Brownstein (2013) 'Twitter as a sentinel in emergency situations: lessons from the Boston marathon explosions', *PLoS Currents, Disasters* 2 juli, editie 1. doi: 10.1371/currents.dis.ad70cd1c8bc585e9470046cde334ee4b.

Centraal Bureau voor de Statistiek (2018a) *ICT, kennis en economie*, Den Haag: Centraal Bureau voor de Statistiek.

Centraal Bureau voor de Statistiek (2018b) *Cybersecuritymonitor 2018. Een verkenning van dreigingen, incidenten en maatregelen*, Den Haag: Centraal Bureau voor de Statistiek.

Centraal Planbureau (2018) *Risicorapportage cyberveiligheid economie 2018*, Den Haag: Centraal Planbureau. Beschikbaar op: www.cpb.nl/sites/default/files/omnidownload/CPB-Notitie-15okt2018-Risicorapportage-Cyberveiligheid-Economie-2018.pdf

Centre for European Policy Studies (2018) *Strengthening the* EU's *Cyber Defence Capabilities. Report of a* CEPS *Task Force,* Brussel: Centre for European Policy Studies (CEPS).

Choo, K. (2011) 'The cyber threat landscape: Challenges and future research directions', *Computers & Security* 30,8: 719-731.

Clearfield, C. en A. Tilcsik (2018) *Meltdown: Why our systems fail and what we can do about it*, New York: Penguin.

Commissie modernisering opsporingsonderzoek in het digitale tijdperk (2018) *Regulering van opsporingsbevoegdheden in een digitale omgeving*. Beschikbaar op: www.rijksoverheid.nl/documenten/rapporten/2018/06/26/rapport-commissie-koops---regulering-van-opsporingsbevoegdheden-in-een-digitale-omgeving

Cyber Security Raad (2017) *Naar een landelijk dekkend stelsel van informatieknooppunten, advies inzake informatieuitwisseling met betrekking tot cybersecurity en cybercrime*, Den Haag.

Cyber Security Raad (2018) *Naar een open, veilig en welvarend digitaal Nederland, advies inzake de Nederlandse Cybersecurity Agenda*, Den Haag.

Dam, C.C. van (1995) 'Aansprakelijkheid voor nalaten', *Preadvies voor de Nederlandse Vereniging voor Rechtsvergelijking,* Deventer: Kluwer.

DeNardis, L. (2014) *The global war for internet governance,* Yale: Yale University Press.

Donahue, A.K., C.C. Eckel en R.K. Wilson (2014) 'Ready or not? How citizens and public officials perceive risk and preparedness', *The American Review of Public Administration* 44, 4: 89-111.

Douglas, M. en A. Wildavsky (1982) Risk and Culture, Berkeley, CA: University of California Press.

Dreyer, P., T. Jones, K. Klima, J. Oberholtzer, A. Strong, J. W. Welburn en Z. Winkelman (2018) *Estimating the global cost of cyber risk. Methodology and examples,* Santa Monica, CA: RAND Corporation.

Duin, M. van, V. Wijkhuis en W. Jong (red.) (2017) *Lessen uit crises en mini-crises 2016*, Den Haag: Boom.

Dunn Cavalty, M. (2007) 'Critical information infrastructure: vulnerabilities, threats and responses', ICTS *and international security*, 3. Beschikbaar op: www.peacepalacelibrary.nl/ebooks/files/UNIDIR_pdf-art2643.pdf.

Eeten, M. van, A. Nieuwenhuijs, E. Luiijf, M. Klaver en E. Cruz (2011) 'The state and the threat of cascading failure across critical infrastructures: the implications of empirical evidence from media incident reports', *Public Administration* 89, 2: 381-400.

Eeten, M. van en M. Bauer (2012) 'Mega-crises and the internet: risks, incentives, and externalities', blz. 356-370 in I. Helsoot, A. Boin, B. Jacobs en L. Comfort (red.), *Mega-crises. Understanding the prospects, nature, characteristics and the effects of cataclysmic events*, Springfield: Charles C. Thomas.

Elsberg, M. (2012) *Black out. Morgen is het te laat*, Amsterdam: Meulenhoff Boekerij B.V.

ENISA (2015) *The 2015 report on national and international cyber security exercises. Survey, analysis and recommendations,* Heraklion: ENISA.

ENISA (2017) *Commonality of risk assessment language in cyber insurance. Recommendations on cyber insurance.* Beschikbaar op: www.enisa.europa.eu/publications/commonality-of-risk-assessment-language-in-cyber-insurance

ENISA (2018a) ENISA *threat landscape report 2017. 15 top cyberthreats and trends*, Heraklion: ENISA.

ENISA (2018b) *Good practices on interdependencies between* OES *and* DSPS, Attiki: ENISA.

ENISA (2019) ENISA *threat landscape report 2018. 15 top cyberthreats and trends*, Heraklion: ENISA.

European Political Strategy Centre (2017) *Building an effective European Cyber Shield. Taking* EU *coorperation to the next level*, nr. 24. Beschikbaar op: https://ec.europa.eu/epsc/publications/strategic-notes/building-effective-european- cyber-shield_en#h-1

Europese Commissie (2016) *Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions: Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry*, COM 410 final.

Frerks, G. (2018) 'Citizen engagement and resilience in Dutch disaster management: a black hole in policy and practise?', blz. 140-155 in J. Bohland, J. Harrald en D. Brosnan (red.). *The disaster resiliency challenge*, Chicago: Charles C. Thomas.

Geer, D., R. Bace, P. Gutmann, P. Metzger, C. Pfleeger, J. Querterman en B. Schneier (2003) *CyberInsecurity: The cost of monopoly–how the dominance of Microsoft's products poses a risk to security,* Computer & Communications Industry Association port. Beschikbaar op: www.schneier.com/essays/archives/2003/09/cyberinsecurity_the.html

Gompel, M. van (2018) 'Softwarefout en winkeldief oorzaak van grote treinstoring Amsterdam', *SpoorPro Vakblad voor de spoorsector*. Beschikbaar op: www.spoorpro.nl/materieel/2018/08/22/grote-treinstoring-in-amsterdam-door softwarefout-en-winkeldief/?gdpr=accept

Greenberg, A. (2018) 'The Untold Story of NotPetya, the Most Devastating Cyberattack in History'. Geraadpleegd van www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Hamer, J., R. van Est en L. Royakkers m.m.v. N. Alberts (2019) *Cyberspace zonder conflict. Op zoek naar de-escalatie van het internationale informatieconflict,* Den Haag: Rathenau Instituut.

Hartlief, T. (2014) 'Privaatrecht in nood – Over de beperkte betekenis van het privaatrecht bij rampen en crises en een rechtsgebied onder toenemende druk van het publiekrecht', blz. 65-194 in *Crises, rampen en recht. Preadviezen Nederlandse Juristen-Vereniging*, Kluwer.

Hathaway, M. en F. Spidalieri (2017). The Netherlands cyber readiness at glance. Geraadpleegd van: www.thehaguesecuritydelta.com/media/com_hsd/report/139/document/CRI-Netherlands-Profile-PIPS.pdf

Hausken, K. (2007) 'Information sharing among firms and cyber attacks', *Journal of Accounting and Public Policy* 26, 6: 639-688.

Hebly, M.R. en S.D. Lindenbergh (2016) 'Schadebegroting en tijdsverloop', *Preadvies Vereniging voor de Vergelijkende Bestudering van het Recht van België en Nederland*, Den Haag: 301-361.

Helsloot, I. en A. Ruitenberg (2004) 'Citizen response to disasters: a survey of literature and some practical implications', *Journal of contingencies and crisis management* 12, 3: 98-111.

HM Government (2016) *National cyber security strategy 2016-2021*. Beschikbaar op: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

Hon, W.K. en C. Millard (2018) 'Banking in the Cloud: Part 2 –regulation of cloud as 'outsourcing'', *Computer Law & Security Review*, 34: 337–357.

Hood, C. (1998) *The art of the state. Culture, rethoric and public management*, Oxford: Oxford University Press.

House of Lords (2018) *Cyber Security of the* UK's *Critical National Infrastructure.* Beschikbaar op: https://publications.parliament.uk/pa/jt201719/jtselect/jtnatsec/1708/1708.pdf

Inspectie Veiligheid en Justitie (2012) *Evaluatie van de rijkscrisisorganisatie tijdens de DigiNotar-crisis*, Den Haag.

Internet Society (2017) *Global internet report 2017. Paths to our digital future.* Beschikbaar op: https://future.internetsociety.org/2017/wp-content/uploads/sites/3/2017/09/2017-Internet-Society-Global-Internet-Report-Paths-to-Our-Digital-Future.pdf

Jalali, M.S., J.P. Kaiser, M. Siegel en S. Madnich (2017) 'The Internet of Things promises new benefits – and risks: a systematic analysis of adoption dynamics of IoT products', MIT *Sloan School Working paper*: 5249-17.

Janczewski, J. en W. Caelli (red.) (2016) *Cyber conflicts and small states*, Farnham: Ashgate.

Jocqué, G. (2016) 'Tijdsverloop en schadevergoeding', *Tijdschrift voor Privaatrecht 4*: 1375-1434.

Kamerstukken II 2014/2015 30 821, nr. 23. https://zoek.officielebekendmakingen.nl/kst-30821-23.html.

Kamerstukken II 2015/2016 30 821, nr. 32. https://zoek.officielebekendmakingen.nl/kst-30821-32.html.

Keirse, A.L.M. (2017) 'Rechtsvergelijkend perspectief: staatsaansprakelijkheid voor onrechtmatige rechtspraak in de lidstaten', *Overheid en Aansprakelijkheid* 2: 81-90.

Kitchin, R. (2014). *The data revolution: Big data, open data, data infrastructures and their consequences*, Londen: Sage.

Klaver, M.H.A., B. Verheesen en H.A.M. Luiijf (2013) *Intersectorale afhankelijkheden: buitenlandse methoden en mogelijke toepasbaarheid in Nederland*, Den Haag: TNO.

Koepke, P. (2017) 'Cybersecurity Information Sharing Incentives and Barriers', *Working paper,* MIT *Management Sloan School* web. mit. edu/smadnick/www/wp/2017-13. pdf.

Kortmann, C.A.J.M. (2009) *Staatsrecht en raison d'Etat.* Afscheidscollege op 27 februari 2009, Deventer: Kluwer.

Kuipers G.M. en M.K.G. Tjepkema (2017), 'Publieke regie' in Groningen. Publiekrechtelijke schadeafhandeling en het vertrouwen in de overheid, *Nederlands Juristenblad* 29, 1576: 2058-2067.

Lawson, S. (2013) 'Beyond cyber-doom: assassing the limits of hypothetical scenario's in the framing of cyber-threats', *Journal of Information Technology and Politics* 10: 86-103.
Lin, H. (2016) 'Attribution of Malicious Cyber Incidents: From Soup to Nuts', *Columbia Journal of International Affairs*. Beschikbaar op: https://ssrn.com/abstract=2835719
Lloyd's en Cyence (2017) *Counting the cost: Cyber exposure decoded*, Lloyd's: Londen.
Luiijf, E. en A. Kernkamp (2015) *Sharing cyber security information: Good practice stemming from the Dutch public-private-participation approach*, Den Haag: TNO.
Luiijf, H.A.M. en M.H.A. Klaver (2015) 'Governing Critical ICT: Elements that Require Attention', *European Journal of Risk Regulation* 2, 6: 263-270.
Mačák, K. (2017) 'From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers', *Leiden Journal of International Law* 30, 4: 877-899.
McAfee (2017) *McAfee Labs Threats Report June 2017*. Beschikbaar op www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-jun-2017.pdf
Meulen, N. van der (2013) 'DigiNotar: dissecting the first dutch digital disaster', *Journal of strategic security* 6, 2: 44-58.
Michels, J.D. en I. Walden (2018) 'How safe is safe enough? Improving cybersecurity in Europe's critical infrastructure under the NIS Directive', *Queen Mary School of Law Legal Studies Research Paper* No. 291/2018. Beschikbaar op: https://ssrn.com/abstract=3297470
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (2018) *Brief inzake verhogen informatieveiligheid bij de overheid*, 16 oktober, Den Haag.
Ministerie van Economische Zaken en Klimaat en ministerie van Justitie en Veiligheid (2018) *Roadmap Veilige Hard- en Software*, Den Haag.
Ministerie van Justitie en Veiligheid (2019) *Nationale Veiligheid Strategie 2019*, Den Haag.
Ministerie van Veiligheid en Justitie (2012) *Nationaal Crisisplan* ICT, Den Haag. Beschikbaar op https:///zoek.officielebekendmakingen.nl/blg-193555
Muller E.R. (red.) (2011) *Crises in Nederland: Rampen, rellen, gijzelingen en andere crises*, Leiden: Kluwer.
Muller, E.R. (2014) 'Crisis en recht: Naar een integrale Crisisbeheersingswet?' (preadvies), blz. 163 in E.R. Muller, T. Hartlief, B.F. Keulen en H. Kummeling (red.) *Crises, rampen en recht*, Handelingen Nederlandse Juristen-Vereniging nr. 2014-1, Deventer: Kluwer.
Mueller, M. (2017) *Will the internet fragment? Sovereignty, globalization and cyberspace*, Cambridge: Polity Press.
Munnichs, G. M., M. Kouw en L. Kool (2017) *Een nooit gelopen race: over cyberdreigingen en versterking van weerbaarheid*, Den Haag: Rathenau Instituut.
Nationaal Coördinator Terrorismebestrijding en Veiligheid (2016) *Nationaal handboek crisisbesluitvorming*, Den Haag.
Nationaal Coördinator Terrorismebestrijding en Veiligheid (2017) *10 jaar Risico- en Crisisbarometer. Analyse van decennium onderzoek naar risico-, crisis- en angstbeleving*, Den Haag.
Nationaal Coördinator Terrorismebestrijding en Veiligheid (2018a) *Cybersecuritybeeld Nederland 2018*, Den Haag.

Nationaal Coördinator Terrorismebestrijding en Veiligheid (2018b) *Nationale veiligheid bij overnames en investeringen of inkoop en aanbesteding*, geraadpleegd van: www.nctv.nl/binaries/WEB_113154_NCTV_Veiligheid_bij_overnames_tcm31-334520.pdf

Nationaal Coördinator Terrorismebestrijding en Veiligheid (2018c) *Quickscan nationale veiligheid bij inkoop en aanbesteden*, geraadpleegd op: http://content.rp.rijksweb.nl/cis/content/media/rijksportaal/bzk_1/organisatie_21/bzk_2/dg_overheids_organisatie__dgoo_/mediastore_kerntaken_organisatie_en_bedrijfsvoeringsbeleid/inkoop_3/nationale_veiligheid_bij_inkoop_en_aanbesteden/Quickscan_DEF.pdf

Nationaal Coördinator Terrorismebestrijding en Veiligheid (2019) *Cybersecuritybeeld Nederland 2019*, Den Haag.

Nationaal Cyber Security Centrum (2015) *Zicht op risico's van legacysystemen*, Den Haag.

National Audit Office (2017, 27 oktober) *Investigation: WannaCry cyber attack and the* NHS. Beschikbaar op: www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/#

Nieuwesteeg, B., L. Visscher en B. de Waard (2017) 'De rechtseconomie van cyberverzekeringen', *Het Verzekerings-archief* 3: 155-160.

NIS Cooperation Group (2018) 'Cybersecurity Incident Taxonomy', CG *Publication* 04/2018. Beschikbaar op: http://ec.europa.eu/information_society/newsroom/image/document/2018-30/cybersecurity_incident_taxonomy_00CD828C-F851-AFC4-0B1B416696B5F710_53646.pdf

OECD (2003) *Emerging Risks in the 21stCentury. An agenda for action*, Parijs: OECD Publishing.

OECD (2017) *Enhancing the Role of Insurance in Cyber Risk Management*, Parijs: OEC Publishing.

Onderzoeksraad voor Veiligheid (2012) *Het DigiNotar-incident. Waarom digitale veiligheid de bestuurstafel te weinig bereikt*, Den Haag.

Overvest, B., A.M. Braam, R. Windig en E. Bartels (2018) 'Knelpunten op de markt voor Cyberveiligheid', CPB *Policy Brief* 2018/01, Den Haag: CPB.

Perrow, C. (1983) 'The organizational context of human factors engineering', *Administrative Science Quarterly* 28, 4: 521-541.

Planbureau voor de Leefomgeving (2014) *Maatschappelijke ontwrichting en overstromingen*, Den Haag.

Pras, A. (2014) *Alle dagen internet. Beheersen door beheren*, oratie 13 november 2014, Universiteit Twente.

Prins, J.E.J. (2019) Digitaal binnentreden om escalatie te voorkomen, *Nederlands Juristenblad* 578.

Prins, J.E.J. (2010) "Digital Tools: Risks and Opportunities for Victims. Explorations in e-victimology", in J. van Dijk, R. Letschert (red.), *Globalisation, Victims and Empowerment*, Springer.

Prins, J.E.J. (2011) 'Een Hack bij DigiNotar', *Nederlands Juristenblad* 86, 30: 1585.

Prins, J.E.J. (2017) 'Schadelijke beestjes', *Nederlands Juristenblad* 92, 8: 507.

Prins, R. (2012) 'Een veilige cyberwereld vraagt nieuw denken', *Veiligheid in cyberspace. Justitiële verkenningen* nr. 38, 1: 40-51.

Pupillo, L. (2018) 'EU Cybersecurity and the paradox of progress', CEPS *Policy Insights* no. 2018/06.

Pupillo, L., A. Ferreiora en G. Varisco (2018) *Software vulnerability disclosure in Europe. Technology, policies and legal challenges*, Brussel: Centre for European Policy Studies. Beschikbaar op: www.ceps.eu/wp-content/uploads/2018/06/CEPS%20TFRonSVD%20with%20cover_0.pdf

Raad voor de Leefomgeving en Infrastructuur (2018) *Stroomvoorziening onder digitale spanning,* Den Haag; Raad voor de leefomgeving en infrastructuur.

Romanosky, S. (2016) 'Examining the costs and causes of cyber incidents', *Journal of Cybersecurity* 2, 2: 121-135.

Ruijven, Th. van en H. Duijnhoven (2018) *Verkenning ten behoeve van de risicocategorie aantasting functioneren internet,* Den Haag: TNO.

Ruijven, Th van en B. Keijser (2017) *Ketenweerbaarheid tegen cyberdreigingen: uitgangspunten, good practices en een stappenplan voor het vergroten van cyber-ketenweerbaarheid*, Den Haag: TNO.

Sanger, D.A. (2018) *The perfect weapon. War sabotage and fear in the cyber age*, New York; Crown.

Schmitt, M.N., L. Vihul, D. Akande, G.D. Brown en P. Ducheine (2017) *Tallin Manual 2.0 on The International Law Applicable to Cyber Operations. Prepared by the International Groups of Experts at the Invitation of the* NATO *Cooperative Cyber Defence Centre of Excellence*, Cambridge: Cambridge University Press.

Schneier, B. (2015) *Data and Goliath. The hidden battles to collect your data and control your world,* New York: W.W. Norton & Company.

Schneier, B. (2018) *Click Here To Kill Everybody: Security and Survival in a Hyper-connected World*, W.W. Norton & Company.

Schwab, K. (2016) *The Fourth Industrial Revolution*, New York: Crown Publishing.

Scott, J. en D. Spaniel (2016) *Rise of the machines. The Dyn attack was just a practice run*, Institute for Critical Infrastructure Technology.

Secrétariat général de la défense nationale (2018) *Revue stratégique de cyberdéfense*, 12 février 2018. Beschikbaar op: www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf

Settanni, G., F. Skopik, Y. Shovgenya, R. Fiedler, M. Carolan, D. Conroy, K. Boettinger, M. Gall, G. Brost, C. Ponchel, H. Kaufmann, K. Theuerkauf, P. Olli en M. Haustein (2017) 'A collaborative cyber incident management system for European interconnected critical infrastructures', *Journal of Information Security and Applications* 34: 166-182.

Sharma, M. (2017) *Securing critical information infrastructure. Global perspectives and practices*. Idsa monograph series nr. 60. Beschikbaar op: https://idsa.in/system/files/monograph/monograph60.pdf

Simon, T., A. Goldberg en B. Adini (2015) 'Socializing in emergencies – A review of the use of social media in emergency situations', *International Journal of Information Management* 35, 5: 609-619.

Snyder, C. (2017) *Too connected to fail. How attackers can disrupt the global internet, why it matters and what we can do about it, Paper*, Cyber Security Project, Belfer Center.

Sommer, P. en I. Brown (2011) *Reducing systemic cybersecurity Risk*, OECD: Parijs.

Stratix (2017) *Telekwetsbaarheid. Handelingsperspectief voor huishoudens bij uitval van telecomdiensten door stroomstoring*, Hilversum.

Tiel, B. van (2019) *Kritische waakhond, vergeet de digitale veiligheid niet*. Beschikbaar op: www.pwc.nl/nl/themas/blogs/kritische-waakhond-vergeet-de-digitale-veiligheid-niet.html

Tran, D. (2018) The Law of Attribution: Rules for Attributing the Source of a Cyber-Attack. *20 Yale Journal of Law & Technology* 376.

Valeriano, B. en R.C. Maness (2018) 'How we stopped worrying about cyber doom and started collecting data', *Politics and governance* 6, 2: 49-60.

Van den Hoven van Genderen, R. (2017) "Is de verkoop van Fox-IT aan een buitenlandse partij (de 'FOXIT') een bedreiging voor de nationale veiligheid?', *Tijdschrift voor Internetrecht* 2, 3.

Verner, D., F. Petit en K. Kim (2017) 'Incorporating Prioritization in Critical Infrastructure Security and Resilience Programs', *Homeland Security Affairs* 13, artikel 7 (oktober 2017). www.hsaj.org/articles/14091

Vollenhoven, P. van (2019) *Oproep van een waakhond,* Amsterdam: Balans.

West, G. (2017) *Scale: The Universal Laws of Growth, Innovation, Sustainability, and the Pace of Life in Organisms, Cities, Economies, and Companies*, New York: Penguin.

Wetenschappelijke Raad voor het Regeringsbeleid (1998) *Staat zonder land: een verkenning van bestuurlijke gevolgen van informatie- en communicatietechnologie,* Den Haag: Sdu Uitgevers.

Wetenschappelijke Raad voor het Regeringsbeleid (2008) *Onzekere veiligheid. Verantwoordelijkheden rond fysieke veiligheid*, Amsterdam: Amsterdam University Press.

Wetenschappelijke Raad voor het Regeringsbeleid (2011a) *iOverheid*, Amsterdam: Amsterdam University Press.

Wetenschappelijke Raad voor het Regeringsbeleid (2011b) *Evenwichtskunst. Over de verdeling van verantwoordelijkheid voor fysieke veiligheid*, Amsterdam: Amsterdam University Press.

Wetenschappelijke Raad voor het Regeringsbeleid (2012) *Publieke zaken in de marktsamenleving*, Amsterdam: Amsterdam University Press.

Wetenschappelijke Raad voor het Regeringsbeleid (2013) *Toezien op publieke belangen. Naar een verruimd perspectief op rijkstoezicht,* Amsterdam; Amsterdam University Press.

Wetenschappelijke Raad voor het Regeringsbeleid (2015) *De publieke kern van het internet. Naar een buitenlands internetbeleid*, Amsterdam: Amsterdam University Press.

Wetenschappelijke Raad voor het Regeringsbeleid (2016) *Big data in een vrije en veilige samenleving*, Amsterdam: Amsterdam University Press.
Wetenschappelijke Raad voor het Regeringsbeleid (2017a) *Veiligheid in een wereld van verbindingen*, Den Haag.
Wetenschappelijke Raad voor het Regeringsbeleid (2017b) *Weten is nog geen doen. Een realistisch perspectief op zelfredzaamheid*, Den Haag.
World Economic Forum (2017) *2017 Global Risks Report*, januari.
Zhong, C., T. Lin, P. Liu, J. Yen en K. Chen (2018) 'A cyber security data triage operation retrieval system', *Computers & Security* 76: 12-31.
Zuboff, S. (2019) *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, New York: PublicAffairs.
Zwan, E. van der en M. Spit (2015) 'De internationale stand van zaken in de bescherming van vitale infrastructuur', *Magazine nationale veiligheid en crisisbeheersing* 3: 32-33.

VOORBEREIDEN OP DIGITALE ONTWRICHTING

Digitale infrastructuur is – vaak zonder dat we het merken – intens verweven met processen die van groot belang zijn voor de samenleving, de economie en de democratische rechtstaat. De overheid en andere belangrijke partijen zijn onvoldoende voorbereid op verstoringen of uitval van deze infrastructuur.

Voor fysieke ontwrichting zijn er goed toegeruste hulpdiensten. Maar wie te bellen als er een 'digitale brand' uitbreekt? Welke middelen heeft een 'digitale brandweer' nodig om effectief te kunnen blussen? Deze vragen zijn in het bijzonder relevant als de 'brand' niet beperkt blijft tot het digitale domein, maar ook ontwrichtende consequenties heeft voor de fysieke wereld en het vertrouwen in de democratische rechtstaat.

De Wetenschappelijke Raad voor het Regeringsbeleid adviseert daarom een betere voorbereiding op wat hij 'digitale ontwrichting' noemt. Nodig zijn onder meer inzicht in afhankelijkheden, een nieuwe benadering van vitale infrastructuur, adequate bevoegdheden om escalatie te voorkomen en inspanningen op het terrein van cyberverzekeringen.

ISBN 978-94-90186-77-7

WRR

WETENSCHAPPELIJKE RAAD VOOR HET REGERINGSBELEID