WRR

WETENSCHAPPELIJKE RAAD VOOR HET REGERINGSBELEID

Samenvatting van WRR-rapport

101

VOORBEREIDEN OP DIGITALE ONTWRICHTING

SAMENVATTING

Voorbereiden op digitale ontwrichting

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.

Wetenschappelijke Raad voor het Regeringsbeleid
Buitenhof 34
Postbus 20004
2500 EA Den Haag
Telefoon 070-356 46 00
E-mail info@wrr.nl
Website www.wrr.nl

WRR

WETENSCHAPPELIJKE RAAD VOOR HET REGERINGSBELEID

Voorbereiden op digitale ontwrichting

SAMENVATTING VAN WRR-RAPPORT 101

Wetenschappelijke Raad voor het Regeringsbeleid, Den Haag 2019

Verantwoording
Deze publicatie is een samenvatting van WRR-rapport 101 *Voorbereiden op digitale ontwrichting*. Voor een onderbouwing van de in deze publicatie gepresenteerde conclusies en aanbevelingen wordt verwezen naar de uitvoerige analyses van het beleid en de wetenschappelijke literatuur die in dat rapport te vinden zijn.

Het rapport *Voorbereiden op digitale ontwrichting* (ISBN 978-94-90186-77-7) is op 9 september 2019 door de raad aangeboden aan de regering. Het rapport kan in pdf-formaat gratis worden gedownload op www.wrr.nl.

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

WRR Den Haag

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.

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.

WRR

WETENSCHAPPELIJKE RAAD VOOR HET REGERINGSBELEID