Instituut
Fysieke
Veiligheid

Cybergevolgbestrijding

Lessen uit recente Nederlandse casus

Instituut Fysieke Veiligheid
Kennisontwikkeling en onderwijs
Postbus 7010
6801 HA Arnhem
Kemperbergerweg 783, Arnhem
www.ifv.nl
info@ifv.nl
026 355 24 00

Colofon

Instituut Fysieke Veiligheid (2020). *Cybergevolgbestrijding: lessen uit cyberverstoringen in Nederland*. Arnhem: IFV.

Titel:	Cybergevolgbestrijding: lessen uit cyberverstoringen in Nederland
Datum:	27 november 2020
Status:	Definitief
Auteurs:	Laurens van der Varst, Daan Heijmen, Emily Berger, Thomas van der Sleen, Emma Bosman
Projectleider:	Laurens van der Varst
Review:	Menno van Duin
Eindverantwoordelijk:	Menno van Duin

Abstract

As a result of developments in technology, demography et cetera, society is confronted with various new risks, one of which is cyber. In the modern world, the dependency on digital systems is such, that problems with these systems can cause serious disruptions. Between 2017 and 2020, the Netherlands was confronted by various cyber-attacks and cyber-related problems: the cyber-attack on Rotterdam harbour (June 2017); the cyber-attack on the municipality of Lochem (June 2019); the disruption of the Dutch telephone network (June 2019); the cyber-attack on Maastricht University (December 2019) and the problems with the Citrix-software (January 2020). By discussing these cyber-attacks and cyber-related problems together in one report, we aim to get more insight in the way they can be characterized, in the challenges society is confronted with and in the lessons we can learn. The aim is to build a knowledge base that can help Dutch safety regions to better prepare for and respond to cyber related crises.

Samenvatting

De samenleving krijgt onder meer door ontwikkelingen op het gebied van technologie, demografie en klimaat te maken met allerlei nieuwe risico's, die met onzekerheid zijn omgeven en voor nieuwe uitdagingen voor de crisisbeheersing zorgen. Een van die risico's wordt gevormd door cyber en digitale verstoringen. De afhankelijkheid van digitale systemen is zó groot geworden, dat aantasting van deze systemen kan leiden tot een ontwrichting van de samenleving. Tussen 2017-2020 hebben zich diverse cyberaanvallen en digitale verstoringen voorgedaan in Nederland. Door deze verschillende cybercasus in onderlinge samenhang in kaart te brengen en te bundelen, kunnen we meer inzicht krijgen in de wijze waarop verstoringen kunnen worden getypeerd, welke (bestuurlijke) uitdagingen er spelen rondom cyber en welke lessen we uit deze casus kunnen trekken. Het doel van dit onderzoek is dan ook het volgende:

Het vergroten van het praktisch inzicht over cyberverstoringen en de (bestuurlijke en organisatorische) crisisrespons, teneinde kennis op te bouwen voor een veerkrachtige voorbereiding en respons van veiligheidsregio's en crisispartners op cyberverstoringen.

Enkele vragen die hierbij spelen en die bij de bespreking van de afzonderlijk cyberincidenten die in dit rapport centraal staan aan bod komen, zijn:

1. Welke partijen waren bij de respons betrokken en hoe verliepen de onderlinge afstemming en de coördinatie? Was er een rol voor de veiligheidsregio en zo ja, welke?
2. Welke uitdagingen en (bestuurlijke) dilemma's deden zich bij die respons voor?
3. Wat waren de gevolgen van de verstoringen?
4. Hoe werd er over de verstoringen naar het publiek gecommuniceerd?

In dit rapport worden de volgende casus besproken: de cyberaanval op de Rotterdamse haven (27 juni 2017); de cyberaanval op de gemeente Lochem (6 juni 2019); de KPN-storing (24 juni 2019); de cyberaanval op Universiteit Maastricht (23 december 2019) en de kwetsbaarheid in de Citrix-software (januari 2020). Deze casus zijn beschreven op basis van openbare bronnen. Daarnaast is een aantal interviews gehouden met personen die betrokken waren bij de casus.

Het zwaartepunt van dit rapport ligt bij cybergevolgbestrijding, waaronder alle activiteiten worden verstaan die verricht worden in het kader van het bestrijden van de effecten van een incident, waarvan de oorzaak en/of het gevolg in het digitale domein ligt/liggen. In het eerste hoofdstuk wordt ingegaan op cyberverstoringen in algemene zin. Daarna volgen vijf hoofdstukken waarin steeds één van de casus wordt besproken. Het laatste hoofdstuk bevat een aantal overkoepelende observaties en aanbevelingen. Zo wordt vastgesteld dat de impact van cyberverstoringen op organisaties enorm kan zijn en niet moet worden onderschat, maar dat de maatschappelijke gevolgen in de meeste casus echter betrekkelijk beperkt blijven. Tevens is vastgesteld dat de rol van veiligheidsregio's in de besproken casus bescheiden was, maar dat deze in de toekomst kan veranderen (en zelfs groter worden). Ook wordt geconstateerd dat er weinig ervaring is met cybergevolgbestrijding en met het functioneren van het Landelijk Dekkend Stelsel, dat getroffen organisaties zélf verantwoordelijk zijn voor 'failure management' en dat cyberverstoringen zich kenmerken door onzichtbaarheid, complexiteit en onzekerheid. De grootste uitdaging wordt gezien in het vinden en uitvoeren van een effectieve responsstrategie, die organisaties en crisisteams zich

eigen kunnen maken door te oefenen en te leren. Daarnaast wordt geconcludeerd dat een snelle en accurate informatie-uitwisseling essentieel is voor de incidentrespons en het beheersen van de mogelijke gevolgen van cyberverstoringen, maar dat er zorgvuldig moet worden afgewogen welke informatie wanneer en met wie gedeeld kan worden. Ten slotte wordt gesteld dat voor een adequate cyberweerbaarheid een goede coördinatie en samenwerking tussen onder meer het CERT, de ICT-afdeling én de reguliere crisisstructuur van groot belang zijn.

Inhoud

Afkortingen

AIVD	Algemene Inlichtingen- en Veiligheidsdienst
BOB	Beeldvorming, Oordeelsvorming, Besluitvorming
CERT	Computer Emergency Response Team
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMT	Crisis Management Team
CTO	Chief Technology Officer
CvB	College van Bestuur
GRIP	Gecoördineerde Regionale Incidentbestrijdingsprocedure
IBD	Informatiebeveiligingsdienst
ICT	Informatie- en communicatietechnologie
IFV	Instituut Fysieke Veiligheid
IGJ	Inspectie Gezondheidszorg en Jeugd
ISAC	Information Sharing and Analysis Centre
IT	Informatietechnologie
JenV	Justitie en Veiligheid
LOCC	Landelijk Operationeel Coördinatiecentrum
MB	Megabyte
MCL	Medisch Centrum Leeuwarden
NCC	Nationaal CrisisCentrum
NCSC	Nationaal Cyber Security Centrum
NCTV	Nationaal Coördinator Terrorismebestrijding en Veiligheid
NFIR	Nederlands Forensisch Incident Response
ODG	Operationeel Draaiboek Generiek
OM	Openbaar Ministerie
RAV	Regionale Ambulancevoorziening
RDP	Remote Desktop Protocol
RvT	Raad van Toezicht
UM	Universiteit Maastricht
VNG	Vereniging van Nederlandse Gemeenten
VNOG	Veiligheidsregio Noord- en Oost-Gelderland
WRR	Wetenschappelijke Raad voor het Regeringsbeleid

Inleiding

Aanleiding: zorgen over cyberrisico's

De samenleving krijgt door ontwikkelingen op het gebied van technologie, demografie en klimaat te maken met nieuwe risico's. Die risico's zijn met onzekerheid omgeven, onder meer door het ontbreken van risicogegevens en door het grote aantal factoren dat van invloed is op het risico (OECD, 2003). Eén van die nieuwe en bovendien heel actuele risico's is cyber – een risico dat volgens diverse instanties en commissies hoger op de agenda moet komen. Zo pleitte de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) in 2019 voor meer digitale weerbaarheid door bijvoorbeeld een 'digitale brandweer', net zoals eerder de commissie-Verhagen had gedaan.

Op het gebied van cyber en digitale verstoringen liggen nieuwe uitdagingen voor de crisisbeheersing. Zo zijn tegenwoordig bijna alle vitale processen en diensten afhankelijk van ICT. De afhankelijkheid van digitale systemen is zó groot geworden, dat aantasting van deze systemen kan leiden tot een ontwrichting van de samenleving. Er zijn vrijwel geen analoge alternatieven meer om op terug te vallen (NCTV, 2019). Deze digitale kwetsbaarheid komt steeds verder aan het licht, onder andere door een stijging van het aantal digitale aanvallen en verstoringen. Om enkele recente voorbeelden te noemen: de cyberaanvallen op de gemeente Lochem (juni 2019) en de Universiteit Maastricht (december 2019) en het lek bij Citrix-systemen (januari 2020). De gijzelingssoftware waarmee Veiligheidsregio Noord- en Oost-Gelderland (VNOG) in september 2020 werd geconfronteerd, laat zien dat dit soort risico's ook voor veiligheidsregio's actueel zijn.

Het lectoraat Crisisbeheersing volgt deze ontwikkeling op de voet. In dat licht zijn het afgelopen jaar twee verkennende onderzoeken naar cyber uitgevoerd:

1. *Cyberrisico's en veiligheidsregio's* (IFV, 2020a), waarbij de focus lag op de manier waarop veiligheidsregio's cyberrisico's beoordelen.
2. *Versterken van veerkracht. Naar een gezamenlijke aanpak van veiligheidsrisico's* (IFV, 2020b), waarbij werd ingezoomd op digitale ontwrichting.

Hierbij zijn casus van cyberverstoringen of digitale ontwrichting wel in ogenschouw genomen, maar niet uitgebreid geanalyseerd.

Doel en vraagstelling

In de afgelopen periode, grofweg 2017-2020, hebben zich diverse cyberaanvallen en digitale verstoringen voorgedaan in Nederland (en daarbuiten). Die verstoringen zijn tot op heden niet in onderlinge samenhang beschreven en geanalyseerd. Door de verschillende cybercasus in onderlinge samenhang in kaart te brengen, kunnen we meer inzicht krijgen in de wijze waarop verstoringen kunnen worden getypeerd, welke (bestuurlijke) uitdagingen er spelen rondom cyber en welke lessen we uit deze casus kunnen trekken.

Het doel van dit onderzoek is dan ook het volgende:

Het vergroten van het praktisch inzicht over cyberverstoringen en de (bestuurlijke en organisatorische) crisisrespons, teneinde kennis op te bouwen voor een veerkrachtige voorbereiding en respons van veiligheidsregio's en crisispartners op cyberverstoringen.

Enkele vragen die hierbij spelen, zijn:
1. Welke partijen waren bij de respons betrokken en hoe verliepen de onderlinge afstemming en de coördinatie? Was er een rol voor de veiligheidsregio en zo ja, welke?
2. Welke uitdagingen en (bestuurlijke) dilemma's deden zich bij die respons voor?
3. Wat waren de gevolgen van de verstoringen?
4. Hoe werd er over de verstoringen naar het publiek gecommuniceerd?

Deze vragen zullen aan bod komen bij de bespreking van de afzonderlijk cyberincidenten die in dit rapport centraal staan.

Aanpak

Om het inzicht in cyberverstoringen te vergroten, worden in dit rapport verschillende recente casus besproken waarbij sprake was van digitale aanvallen of verstoringen.

Casus opgenomen in de publicatie zijn:
> de cyberaanval op de Rotterdamse haven (27 juni 2017)
> de cyberaanval op de gemeente Lochem (6 juni 2019)
> de KPN-storing (24 juni 2019)
> de cyberaanval op Universiteit Maastricht (23 december 2019)
> de kwetsbaarheid in de Citrix-software (januari 2020).

Deze casus zijn beschreven op basis van openbare bronnen, zoals nieuwsartikelen, evaluatierapporten en beleidsdocumenten. Daarnaast zijn zes interviews gehouden met personen die betrokken waren bij de casus. Een overzicht van de geïnterviewde personen is opgenomen in bijlage 1. Op 29 oktober hebben we tevens een bijeenkomst georganiseerd om het rapport met cyberexperts en andere betrokkenen bij cyberveiligheid en -gevolgbestrijding te bespreken (deelnemerslijst in bijlage 2). De inzichten die voortkwamen uit deze bijeenkomst zijn vervolgens verwerkt in het uiteindelijke rapport.

Afbakening

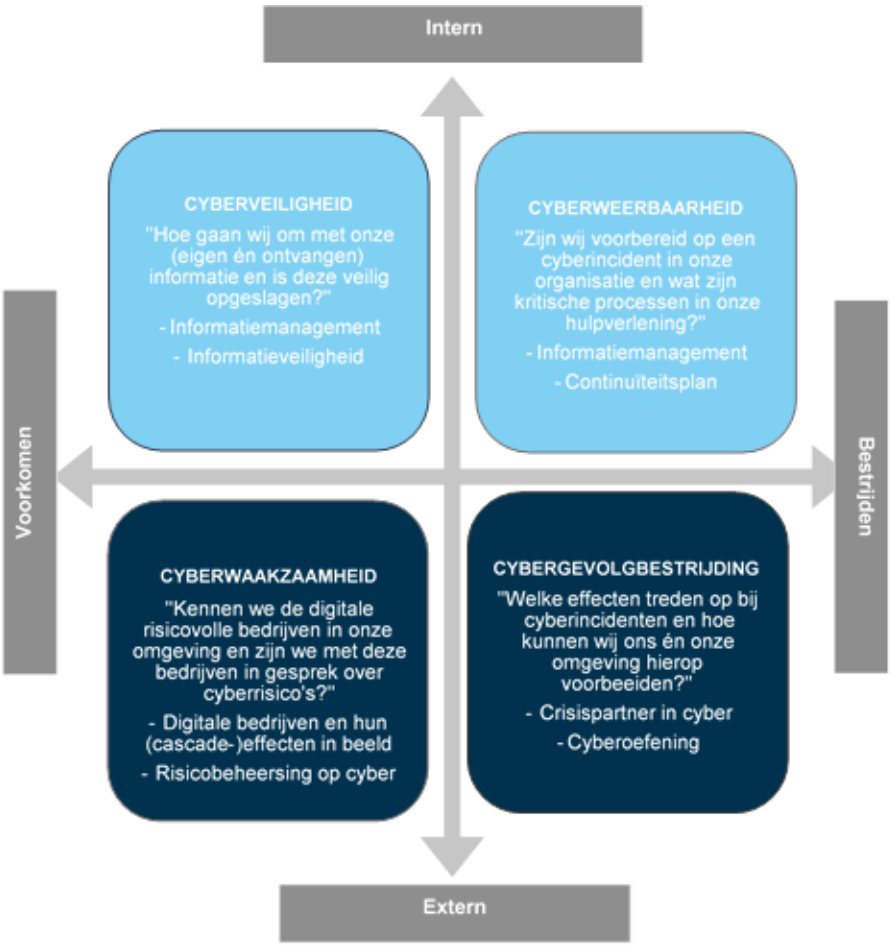
Bij het selecteren van casus voor dit onderzoek is voor een brede afbakening van digitale verstoringen gekozen. Zowel casus waarbij sprake was van een moedwillige als een niet-moedwillige verstoring (technisch falen) zijn meegenomen. Daarnaast zijn niet alleen casus opgenomen met gevolgen voor de interne organisatie, maar ook casus met externe gevolgen.

Een aantal casus in dit rapport kunnen worden geclassificeerd als *disrupties* (Oomes, 2020) Disrupties hebben volgens Oomes een eigen dynamiek, met onverwachte effecten en maatschappelijke verontwaardiging tot gevolg. Ze vragen niet om spoedeisende hulpverlening en sluiten mede daardoor niet automatisch aan bij de regionale opschaling. Volgens Oomes wordt bij een disruptie meestal niet de benodigde overheidsdrempel voor regionale opschaling overschreden. Mocht dat onverhoopt tóch gebeuren, "is de overheid

niet de bronbestrijder maar de effectbeheerser". De bron van een disruptie kenmerkt zich namelijk door problemen als stroomstoringen en de uitval van ICT-voorzieningen. Mogelijke gevolgen zijn bijvoorbeeld grote drukte, files en mensenmassa's. Volgens Oomes bestaat bij een dergelijke bronbestrijding "geen nood aan een peloton of een compagnie, maar aan een storingsdienst met vakbekwame techneuten" (Oomes, 2020). Bij dit soort disrupties speelt regelmatig een hoge mate van dreiging, zoals in de casus Maersk, Lochem en Maastricht. Zo'n disruptie kan door getroffen partijen natuurlijk wel worden gezien of ervaren als crisis – ook als daarbij geen vitale (veiligheids)belangen in het geding zijn.

Definities van cyberverstoringen stellen doorgaans dat door dergelijke verstoringen de veiligheid of openbare orde wordt bedreigd, of dat zij leiden tot maatschappelijke ontwrichting. We merken echter op dat dit zeker niet bij iedere cyberverstoring het geval is. Cyberverstoringen kunnen een grote impact hebben op getroffen organisaties, zónder de veiligheid of openbare orde te bedreigen of te leiden tot maatschappelijke ontwrichting, zoals we later in dit rapport zullen zien.

In december 2019 is door het Veiligheidsberaad het *Bestuurlijk routeboek digitale ontwrichting* vastgesteld. De bestuurlijke opgaven zijn geordend in onderstaand cyberkwadrant (zoals uitgewerkt door Veiligheidsregio IJsselland). Het zwaartepunt van dit rapport ligt bij cybergevolgbestrijding. Onder cybergevolgbestrijding worden alle activiteiten verstaan in het kader van het bestrijden van de effecten van een incident waarvan de oorzaak en/of het gevolg in het digitale domein ligt/liggen (IFV, 2019b).



Figuur I.1 Cyberkwadrant zoals uitgewerkt door Veiligheidsregio IJsselland

Leeswijzer

In het eerste hoofdstuk gaan we in op cyberverstoringen in algemene zin. Daarna volgen vijf hoofdstukken met de verschillende casus: de Rotterdamse haven, de gemeente Lochem, de KPN-storing, de Universiteit Maastricht en tot slot de kwetsbaarheid in de Citrix-software. Het laatste hoofdstuk bevat tien overkoepelende observaties uit deze casus.

Bijlage 1 bevat een lijst van de geïnterviewde personen en bijlage 2 van de deelnemers aan de expertsessie. In bijlage 3 is een overzicht opgenomen van relevante partijen op het gebied van cybersecurity en -gevolgbestrijding. Bijlage 4 bevat een overzicht van relevante publicaties op het gebied van cyberdreigingen en -gevolgbestrijding.

1 Veiligheidsregio's en cyber

In dit hoofdstuk reflecteren we bondig op cyberverstoringen in algemene zin: vormen zij een nieuw soort crisis? Verder wordt beschreven hoe veiligheidsregio's zich momenteel voorbereiden op cyberverstoringen. Tot slot behandelen we cyberdreigingen in 2020, waarbij ook de coronacrisis aan bod komt.

1.1 Cyber: een nieuw soort crisis?

Het Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) schetst in zijn jaarlijkse *Cybersecuritybeeld Nederland* de omvang, ernst en veelzijdigheid van de cyberdreigingen.[1] In 2019 waarschuwt de NCTV voor cyberverstoringen – verstoringen die in potentie kunnen leiden tot een (grote) mate van maatschappelijke ontwrichting (NCTV, 2019). Ook veiligheidsregio's krijgen in groeiende mate te maken met cyberrisico's. Cyber komt als thema dan ook nadrukkelijk terug in regionale risicoprofielen, vaak onder klassieke benamingen als 'uitval telecommunicatie en ICT' en 'uitval vitale voorzieningen' (IFV, 2020a).

Cyber in regionale risicoprofielen (IFV, 2020a)
In de meeste risicoprofielen wordt 'cyber' beschouwd als mogelijke oorzaak van een fysiek incident. De meeste risicoprofielen richten zich hierbij op de uitval van nutsvoorzieningen (vooral ICT en telecommunicatie), storingen bij ziekenhuizen en BRZO-bedrijven[2] en cascade-effecten. Uit een enquête onder veiligheidsregio's komt de volgende top-4 van risico's naar voren:

> uitval van vitale infrastructuur
> verstoring van de continuïteit van de eigen hulpverlening
> verstoring van BRZO-bedrijven
> hack van datacenters.

Sommige veiligheidsregio's identificeren digitale ontwikkelingen als algemeen aandachtspunt en trend voor de komende jaren – een trend met potentiële impact op verschillende veiligheidsdomeinen. Andere veiligheidsregio's berekenen kans en impact van specifieke (moedwillige) cyberscenario's.

Als voorbereiding op dit crisistype is het van belang te onderzoeken in hoeverre cyber een andersoortige crisis is dan de meer klassieke (mini)crises, zoals branden, overstromingen en ordeverstoringen. Uit crisisliteratuur blijkt dat nieuwe risico- en crisistypen duidelijk afwijken van de meer reguliere of routinematige crises (Comfort, Boin & Demchak, 2010). Die nieuwe of ongekende crises zijn moeilijk kenbaar, beperken zich niet tot één bepaalde sector en kunnen razendsnel escaleren (Boin, 2017). Tevens leiden nieuwe technologische risico's bij burgers en overheden tot meer angst en onzekerheid, zo weten we uit de risicopsychologie (Slovic & Weber, 2002).

[1] De NCTV stelt dit dreigingsbeeld samen met het Nationaal Cyber Security Centrum (NCSC) op.
[2] BRZO staat voor Besluit Risico's en Zware Ongevallen.

Hierin speelt mee dat veiligheidsregio's nog betrekkelijk weinig ervaring hebben opgedaan met cyberverstoringen. Dat alleen al roept vragen op over het functioneren van het responsnetwerk: over rollen, taken en bevoegdheden, de werking van procedures en wat de betrokken actoren van elkaar (kunnen) verwachten (IFV, 2020b).

Hoe onderscheidt digitale ontwrichting zich van reguliere crises? (IFV, 2020a)

1. Cyberincidenten zijn vaak niet (of minder direct) zicht- en tastbaar dan klassieke fysieke incidenten en crises. Bij fysieke incidenten met een digitale oorzaak is de bron vaak moeilijk te identificeren.
2. Het verloop van een cyberincident is aan de voorkant nagenoeg onvoorspelbaar.
3. Cyberincidenten houden zich niet aan grenzen en kunnen meerdere domeinen betreffen.
4. Dit heeft tot gevolg dat men met andere partners moet afstemmen en samenwerken dan bij klassieke incidenten.
5. Er spelen veelal andere dilemma's. Zo kan het herstel van ICT-voorzieningen van getroffen bedrijven of organisaties op gespannen voet staan met opsporingsbelangen van de politie.
6. Een cyberincident kan daardoor een langer herstel- en nazorgtraject tot gevolg hebben.
7. Al met al vergen cyberincidenten meer flexibiliteit en improvisatievermogen van een crisisorganisatie dan klassieke incidenten.

Duidelijk is dat er niet één soort cyberverstoring bestaat; de verschijningsvormen van cyberverstoringen zijn divers (IFV, 2020b). Alleen al uit de verschillende casus uit dit onderzoek blijkt die verscheidenheid: van gijzelingssoftware tot problemen met software-updates. Gevolgen van cyberverstoringen kunnen optreden bij een breed scala aan organisaties, overheidsdiensten en vitale infrastructuren. Vele scenario's zijn denkbaar. Er zijn heel veel 'threat agents' en 'failure paths' waardoor het feitelijk onmogelijk is te voorzien waar een verstoring zal ontstaan en welke gevolgen precies zullen optreden in diverse technische systemen (IFV, 2020b).

Naast de 'stroming' binnen de literatuur en praktijk die wijst op de onderscheidende kenmerken van cyberverstoringen, staan deskundigen die een nuchterder visie hebben op cyberverstoringen. Eén van die deskundigen is hoogleraar cybersecurity Van Eeten (2019). Hij stelt dat veel organisaties dagelijks te maken hebben met ICT-verstoringen, waardoor zij over de nodige veerkracht beschikken. Organisaties doen ervaring op met dit soort incidenten, leren ervan en kunnen veelal terugvallen op bestaande crisisplannen en -structuren. Bovendien zijn de fysieke gevolgen door digitale verstoringen minder erg dan we veelal denken. De veiligheidsregio's hebben juist uitgebreide ervaring met het beheersen van de fysieke gevolgen van crises. Hoewel instanties als de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) en de WRR waarschuwen voor digitale ontwrichting van de samenleving, is er volgens deze hoogleraar niet zoiets als digitale ontwrichting. De ontwrichting zélf is niet zozeer digitaal, als wel de oorzaak ervan. Naarmate cyberverstoringen ons meer fysiek raken, zijn we er dus beter op voorbereid (Van Eeten, 2019). Ook het ontbreken van een digitale brandweer (die de WRR zou willen invoeren) is volgens Van Eeten niet per se zorgelijk. Dergelijke digitale hulpdiensten bestaan namelijk al in de vorm van commerciële aanbieders van incidentresponsdiensten.

Minstens zo belangrijk als de specifieke aanleiding en oorzaak van crises is de collectieve reactie van mensen in de samenleving op (de gevolgen van) een cyberverstoring. Of de aanleiding van een crisis nu een cyberverstoring of een brand is, de maatschappelijke

gevolgen en mogelijke ontwrichting worden veroorzaakt door de wijze waarop mensen erop reageren. We spreken pas van ontwrichting als een grote groep burgers op de verstoring reageert door haar dagelijks handelen aan te passen en daardoor de situatie verergert (IFV, 2020b). Dit hoeft natuurlijk niet het geval te zijn: er kan ook sprake zijn van veerkracht, wanneer mensen samenwerken om een bedreigende situatie het hoofd te bieden. Veerkracht kan dus bijdragen aan het tegengaan van maatschappelijke ontwrichting.

Concluderend kunnen we wel stellen dat cyberverstoringen een betrekkelijk nieuw fenomeen zijn en dat dit type crisis een aantal specifieke uitdagingen met zich meebrengt. In die zin zijn cyberverstoringen anders dan de meer routinematige ongevallen en rampen. Niet alles is echter nieuw. Veiligheidsregio's hebben namelijk meer ervaring met de bestrijding van de fysieke en sociale gevolgen van crises. De opgedane ervaring van veiligheidsregio's met cyberverstoringen is zeer gering. Hoe bereiden veiligheidsregio's zich eigenlijk op cyberverstoringen voor? Op deze vraag wordt in de volgende paragraaf een antwoord gegeven.

1.2 De voorbereiding op cyberverstoringen door veiligheidsregio's

Veiligheidsregio's bereiden zich op verschillende manieren voor op cyberverstoringen, zo blijkt uit onderzoek van het IFV (2020a). Deze voorbereiding gebeurt door deel te nemen aan regionale / landelijke netwerken (86% van de veiligheidsregio's), het opbouwen van cyberkennis en -expertise (81%) en het oefenen met cyberscenario's (67%). Wel is er nog onduidelijkheid over en onbekendheid met de rollen, taken en bevoegdheden van betrokken actoren, de procedures rond alarmering, opschaling en besluitvorming en de benodigde eigen expertise op het vlak van cybergevolgbestrijding. Over de bestrijding van de fysieke effecten van een cyberincident maakt men zich over het algemeen weinig zorgen binnen de veiligheidsregio's. De reguliere crisisbeheersingsstructuren en procedures zijn naar verwachting ook voor digitale verstoringen behulpzaam. Wel kunnen de specifieke aanpak, rol en verantwoordelijkheid van de veiligheidsregio per incident verschillen (TNO, 2019).

Minder zicht hebben veiligheidsregio's op de bestrijding van de oorzaken van digitale verstoringen (bronbestrijding) en op de taken en bevoegdheden van landelijke, regionale en lokale actoren bij een cyberincident (IFV, 2020a). Overigens is, mede door de afwezigheid van een Computer Emergency Response Team (CERT), momenteel niet bekend hoeveel cyberincidenten er jaarlijks plaatsvinden bij veiligheidsregio's zelf.

In de voorbereiding op cyberverstoringen kunnen vier domeinen worden onderscheiden: cyberveiligheid, cyberweerbaarheid, cyberwaakzaamheid en cybergevolgbestrijding (zie figuur 1.1 op pagina 10). In al deze domeinen worden momenteel door veiligheidsregio's maatregelen genomen en acties ondernomen.[3] Hieronder lichten we er enkele toe.

Veiligheidsregio's en cyberweerbaarheid

Om de voorbereiding op en omgang met cyberverstoringen te versterken, is in juni 2020 het zogeheten VR-ISAC (Veiligheidsregio-Information Sharing and Analysis Center) ingericht. Hiermee zijn veiligheidsregio's formeel aangesloten op het vertrouwelijke informatie-uitwisselingsysteem van het NCSC (POI, 2020a).

[3] De vakgroep Informatieveiligheid richt zich op cyberveiligheid en -weerbaarheid (informatieveiligheid, privacy, bedrijfscontinuïteit van de veiligheidsregio's, waaronder de meldkamer). De werkgroep Digitale ontwrichting en cyber concentreert zich op de rol van veiligheidsregio's bij cyberverstoringen (cyberwaakzaamheid en gevolgbestrijding).

Het VR-ISAC biedt veiligheidsregio's een vertrouwelijke omgeving waarin informatie kan worden uitgewisseld met betrekking tot cyberkwetsbaarheden, -dreigingen, -maatregelen en -verstoringen én waarin best practices en leerpunten kunnen worden besproken en gedeeld. Het is een frequent geformaliseerd overleg over cybersecurity voor het uitwisselen van kennis en expertise op het gebied van cyberdreigingen en -verstoringen waar informatiespecialisten uit de veiligheidsregio's en van het IFV aan deelnemen. Dit platform kan worden beschouwd als een 'early warning system' voor de koude fase. Veel (vitale) sectoren beschikken over een ISAC.

Het platform moet veiligheidsregio's in staat stellen zich beter voor te bereiden op cyberverstoringen door versterking van de eigen informatiepositie, uitwisseling van best practices, oefenen, alarmering over dreigingen en het vergroten van de bewustwording ten aanzien van potentiële incidenten die de interne bedrijfsvoering van de veiligheidsregio's kunnen ontwrichten (POI, 2020a). Momenteel is de VR-ISAC bezig met een verkennend onderzoek naar de mogelijkheid om de veiligheidsregio's aan te laten sluiten op een sectorale CERT. Een dergelijke CERT houdt zich in het bijzonder bezig met de (coördinatie van de) incidentrespons.

Veiligheidsregio's en cybergevolgbestrijding

Veiligheidsregio's zijn zoekend naar de rol die zij moeten vervullen bij de voorbereiding op en de omgang met cyberverstoringen. In opdracht van de Raad Directeuren Veiligheidsregio (de huidige RCDV) werkt een landelijke werkgroep sinds juni 2018 dan ook aan kennisvergroting en -deling en aan praktische hulpmiddelen voor cybergevolgbestrijding. Doel is het delen van kennis, ervaring en best practices door de regio's. In de werkgroep Digitale Ontwrichting en Cyber zijn vertegenwoordigers namens de veiligheidsregio's actief, onder wie adviseurs crisisbeheersing, planvorming of operationele voorbereiding. De resultaten van een uitgebreide vraagarticulatie, een verkenning van het onderwerp cyber en de (rol van de) veiligheidsregio daarin hebben geresulteerd in het *Whitepaper digitale ontwrichting en cyber* (IFV, 2019b). Dit whitepaper doet suggesties voor veiligheidsregio's bij de voorbereiding op en de omgang met cyberverstoringen.

1.3 Cyberdreigingen 2020

In het *Cybersecuritybeeld Nederland 2020* wordt door de NCTV (2019) benadrukt dat cybersecurity nog niet overal op orde is. Dit laat ruimte voor cyberverstoringen – verstoringen die in potentie kunnen leiden tot een (grote) mate van maatschappelijke ontwrichting. De dreiging die uitgaat van statelijke actoren als Rusland en China en door statelijke actoren gesteunde groeperingen is groot; deze dreiging groeit en is uitermate veelzijdig.

Nederland heeft tot op heden niet te maken gehad met een cyberverstoring die leidde tot grote maatschappelijke ontwrichting. Toch laten de in dit rapport behandelde cyberaanvallen zien hoe groot de gevolgen kunnen zijn voor organisaties, hun medewerkers en burgers. Ook de NCTV benadrukt de grote gevolgen van deze en andere recente cybercasus in Nederland (NCTV, 2019). Volgens de NCTV is alertheid van organisaties en medewerkers van belang; een cyberverstoring met maatschappij-ontwrichtende gevolgen valt volgens de NCTV namelijk niet uit te sluiten.

Cybersecurity vergroten blijft een lastige opgave, niet in de laatste plaats omdat digitale diensten en processen onderling stevig met elkaar zijn verweven. ICT-systemen bestaan doorgaans uit vele componenten van zowel hard- als software en zijn in groeiende mate verbonden met tal van andere, externe systemen. Hierdoor kunnen actoren die hun cybersecurity wél op orde hebben alsnog in de problemen komen door cyberverstoringen bij actoren waarbij dit niet het geval is. De in dit rapport behandelde Citrix-casus is, zoals we in hoofdstuk 6 zullen zien, illustratief voor deze kwetsbaarheden die veroorzaakt worden door de digitale verbondenheid tussen organisaties, hun medewerkers en burgers (NCTV, 2019).

Om cyberrisico's te beheersen, is het dus van belang om cybersecurity over de hele breedte te vergroten. Het gaat over veiligheid én weerbaarheid, over cyberwaakzaamheid én gevolgbestrijding. Cyber is, zoals de casus aantonen, naast een technisch vraagstuk ook een vraagstuk van 'governance' en risicomanagement voor bestuurders (NCTV, 2019). Er moeten namelijk technische, procedurele en organisatorische maatregelen worden genomen, op zowel ICT- als bestuurlijk gebied. Daarnaast ontbreekt het (nog steeds) aan een compleet en scherp beeld van de cybersecurity van vitale processen en bijbehorende systemen (NCTV, 2019).[4]

Het zetten van dergelijke stappen is van essentieel belang voor de (fysieke) veiligheid van Nederland. Als land vertrouwen we namelijk veelal op digitale diensten en processen. Zo zijn bedrijven en organisaties er mede dankzij ICT-voorzieningen in geslaagd om tijdens de coronacrisis zowel commerciële, educatieve als sociale activiteiten (gedeeltelijk) doorgang te laten vinden (NCTV, 2019). Mensen zijn massaal vanuit huis gaan werken – een trend die zich in de toekomst naar alle waarschijnlijkheid zal voortzetten én een trend met de nodige cyberrisico's als gevolg. Cybercriminelen spelen namelijk snel en listig in op ontwikkelingen in de samenleving door hun werkwijze aan te passen en hun aandacht en inspanningen te verleggen. Zo hebben cybercriminelen de toepassing(en) van hun mal- en ransomware aangepast tijdens de coronacrisis. In maart 2020 was het aantal cyberaanvallen al gestegen ten opzichte van vóór de coronacrisis en sprak Europol de verwachting uit dat deze stijging zich in de daaropvolgende maanden voort zou zetten (Europol, 2020).

Een combinatie van een grootschalige cyberverstoring en de coronacrisis zou grote gevolgen hebben gehad (NCTV, 2019). Gelukkig hebben er tot op heden geen noemenswaardige cyberverstoringen plaatsgevonden – op enkele ongelukkig uitgelekte Zoom-vergaderingen na.[5] De Lochem- en Maastricht-casus tonen, zoals we later zullen zien, echter aan dat hackers vaak nauwgezet te werk gaan en maanden de tijd nemen om tot diep in de ICT-systemen van hun slachtoffers te geraken. Eventuele effecten van dergelijke hacks, zoals het daadwerkelijk uitrollen van de ransomware en de gijzeling van data, worden daardoor pas in een later stadium zicht- en voelbaar. Of we goed genoeg zijn voorbereid op een dergelijke verstoring, is op basis van huidige kennis niet goed vast te stellen. Met dit rapport hopen we een bijdrage te leveren aan de daarvoor benodigde kennisopbouw.

[4] Vanzelfsprekend zijn verschillende actoren bezig dit in beeld te krijgen. Zo is VR-ISAC momenteel bezig met het in kaart brengen van deze processen en systemen.

[5] De Britse premier Boris Johnson deelde op Twitter een screenshot van de eerste Britse digitale kabinetsvergadering met daarin per ongeluk het Zoom ID-nummer en de gebruikersnamen van enkele ministers.

2 De cyberaanval op de Rotterdamse haven (2017)

2.1 Inleiding

Het is 27 juni 2017 als plotseling een deel van het vrachtverkeer in de Rotterdamse haven tot stilstand komt. De malware NotPetya heeft de computers van het Deense bedrijf APM Terminals, onderdeel van scheepvaart- en transportgigant Maersk, vergrendeld. Niet alleen Maersk en het Rotterdamse havengebied zijn getroffen, over de hele wereld zijn bedrijven slachtoffer geworden van de cyberaanval. Waar in sommige landen hele steden werden lamgelegd, werden in de zee voor Hoek van Holland tal van vrachtschepen opgehouden. Als gevolg daarvan zagen sommige schepen zich genoodzaakt om dagenlang stil te liggen; andere schepen weken uit naar nabijgelegen havens. Op wegen naar het havengebied ontstonden files van te laden vrachtwagens en het Rotterdamse havenbedrijf had zijn handen vol aan het beheersen van al het opgehoopte vrachtverkeer. Uiteindelijk leed Maersk voor enkele honderden miljoenen dollars aan schade. Tegelijkertijd werd tijdens de verstoring over de hele wereld geprobeerd de cyberaanval te doorgronden. Wat was hier gebeurd (Van Duin & Maan, 2018; Modderkolk, 2019)?

De cyberaanval op Maersk wordt veelal gebruikt als een referentiecasus in veel cyberpublicaties. Huib Modderkolk gebruikt de casus bijvoorbeeld in zijn boek *Het is oorlog maar niemand die het ziet* (2019) om de noodzaak van digitale beveiliging te benadrukken. Immers, “één zwakke plek kan de maatschappij ontwrichten” (Modderkolk, 2019). De WRR (2019) refereert ook veelvuldig aan de casus, onder andere om de maatschappij-ontwrichtende gevolgen van een cyberverstoring te illustreren. Van Eeten daarentegen grijpt de casus aan om te wijzen op de bekende gedaante die cyberverstoringen aannemen op het moment dat ze fysieke gevolgen hebben – een gedaante waar we al omgangsvormen mee hebben en dus op zijn voorbereid. Volgens hem is er dan ook een stuk minder reden tot paniek (Van Eeten, 2019).

De casus is eerder, in 2018, verschenen in het boek *Lessen uit crises en mini-crises 2017* (Van Duin & Wijkhuijs, 2018). Omdat er zulke waardevolle lessen uit de casus te leren zijn, is besloten om de casus ook in dit rapport op te nemen.

2.2 Feitenrelaas

Het is vroeg in de ochtend als in Oekraïne op 27 juni 2017 computersystemen van zowel overheidsinstellingen als bedrijven massaal beginnen vast te lopen. Door een op dat moment nog onbekende reden worden computers vergrendeld. De bestanden van de gebruikers worden pas ontgrendeld als ze 300 dollar aan Bitcoins betalen, zo stelt het bericht dat gebruikers te zien krijgen. Bij elektriciteitscentrales, telecomproviders, banken en ziekenhuizen in heel Oekraïne worden verstoringen gemeld. In de hoofdstad Kiev zorgt de cyberaanval voor hinder bij zowel de metro als op het vliegveld. “Voor even komt in Oekraïne het maatschappelijke leven tot stilstand” (Van Duin & Maan, 2018). Maar hoewel

Oekraïne uiteindelijk met afstand het zwaarst wordt getroffen, blijft het niet bij dit land. De cyberaanval raakt namelijk ook tal van andere landen, zoals Rusland, Duitsland, de Verenigde Staten, het Verenigd Koninkrijk, Frankrijk, Denemarken en Nederland (Emerce, 2017).

Afbeelding 2.1 De melding die getroffen organisaties te zien krijgen op hun computerscherm[6]

Als reactie op de wereldwijd gevoelde cyberaanval doen zowel private beveiligings(bedrijven) – zoals Talos, Symantec, Eset en Kaspersky – als overheidsinstanties onderzoek naar de aanval. Middels blogs houden onderzoekers elkaar en de rest van de wereld op de hoogte van de ontwikkelingen en hun bevindingen. Na een analyse van de malware blijkt het niet om ransomware, maar om wiperware te gaan (Van Duin & Maan 2018; Emerce, 2017). Waar bij ransomware computers of bestanden worden 'gegijzeld' met als doel losgeld te eisen voor het ontgrendelen van de vergrendelde systemen of data, worden deze bij wiperware onherstelbaar beschadigd. Het gaat dus om een cyberaanval van een (nog) destructievere aard. In dit geval geeft Kaspersky Labs de wiperware, vanwege het overeenkomstige uiterlijk met het in 2016 opgedoken Petya, de naam NotPetya (later door anderen ook wel Nyetya, ExPetr of New Petya genoemd) (Van Duin & Maan 2018; Emerce, 2017).

De start van de cyberaanval is te herleiden naar het Oekraïense boekhoudprogramma M.E.Doc.[7] De hackers verantwoordelijk voor de wiperware blijken al sinds april van dat jaar ongemerkt toegang te hebben tot het moederbedrijf van M.E.Doc, Intellect Service (TalosIntelligence.com 2017). Intellect Service ontwikkelt de software voor het boekhoudprogramma M.E.Doc. Door malware te verstoppen in het updateproces van de software van het boekhoudprogramma, weten de hackers in een paar maanden tijd ongemerkt de ICT-systemen van tal van bedrijven die het programma gebruiken, te besmetten met NotPetya. In Oekraïne wordt veelvuldig gebruikgemaakt van het boekhoudprogramma, bijvoorbeeld om gegevens uit te wisselen met de belastingdienst. Maar ook in vele andere landen wordt de software van M.E.Doc gebruikt. Op 27 juni activeren de hackers uiteindelijk NotPetya en maakt de wereld kennis met de destructieve

[6] Bron: https://www.security.nl/posting/521411/Containerterminals+Rotterdam+getroffen+door+ransomware.
[7] Zie voor de beschrijving van deze casus bijvoorbeeld NCTV, 2018, p. 15.

aard van de wiperware die overal ICT-systemen heeft geïnfecteerd (Van Duin & Maan, 2018).

Ondanks het feit dat verreweg de meeste infecties in Oekraïne plaatsvinden, worden in zeker 65 landen infecties geregistreerd (Emerce, 2017). NotPetya heeft middels de software-updates van het boekhoudprogramma M.E.Doc ook het ICT-netwerk van Maersk besmet. Via het interne netwerk van de scheepvaart- en transportgigant bereikt NotPetya 17 van de 76 terminals van Maersk, waaronder het in de Rotterdamse haven gelegen APM Terminals (Greenberg, 2018). Op 27 juni om 13.15 uur komen de kranen van APM Terminals door de wiperware tot stilstand. Van het ene op het andere moment ligt een derde van de goederenoverslag van de Rotterdamse haven stil (Van Duin & Maan, 2018). De fysieke gevolgen van de cyberaanval zijn groot. De infrastructuur van APM Terminals is namelijk volledig geautomatiseerd en zodoende is het niet mogelijk om schepen te laden en lossen. Ondanks het feit dat delen van de doorgaans geautomatiseerde activiteiten handmatig kunnen worden overgenomen, zien vrachtschepen zich genoodzaakt dagenlang stil te blijven liggen in de zee bij Hoek van Holland of uit te wijken naar andere, nabijgelegen havens. Door de doorgaans continue aanloop van vrachtwagens ontstaan er tevens grote files in en rondom het havengebied (Van Duin & Maan, 2018; Logistiek.nl, 2017). Aan boord van de opgehouden schepen bevinden zich doorgaans honderden tot duizenden containers gevuld met elektronica, grondstoffen voor fabrieken, onderdelen, kleding en fruit. Spullen waar klanten lang(er) op zullen moeten wachten door de verstoring (Bremmer & Van Heel, 2017).

Officieel geldt er in juni 2017 voor individuele bedrijven zoals APM Terminals geen meldplicht voor cyberaanvallen. Omdat de verstoring van het vrachtverkeer dermate groot is, doet het bedrijf toch melding van het voorval. Circa één uur nadat NotPetya de kranen van APM Terminals tot stilstand heeft gebracht, wordt de Rotterdamse havenmeester telefonisch op de hoogte gebracht van de verstoring. De havenmeester is verplicht om melding te maken van deze en andere ernstige ICT-verstoringen. De Rotterdamse haven maakt namelijk onderdeel uit van de Nederlandse vitale infrastructuur. Zodoende wordt direct het NCSC op de hoogte gesteld. Het NCSC volgt de cyberaanval op de voet en staat in nauw contact met buitenlandse autoriteiten (Bremmer & Van Heel, 2017). Namens de overheid zoekt de dienst uit of andere organisaties in Nederland zijn geraakt, specifiek rijksoverheidsorganisaties en vitale aanbieders, en bewaakt het de effecten van de aanval op Nederland zijn vitale infrastructuur (NCSC, 2019). De volgende dag, op 28 juni, krijgen bedrijven een handelingsperspectief voor en gedetailleerde informatie over de cyberaanval van het Rotterdamse havenbedrijf. Om kwetsbaarheden tegen nieuwe aanvallen te beperken, wordt onder andere geadviseerd om updates te installeren (Van Duin & Maan, 2018; FERM-Rotterdam.nl, 2017).

In de hierop volgende week werkt men bij Maersk met man en macht om de volledige ICT-infrastructuur opnieuw op te bouwen: 4000 servers, 45.000 computers en 2500 applicaties worden opnieuw geïnstalleerd (Lalkens, 2018). Omdat veel digitale voorzieningen niet voorhanden zijn, werken werknemers van Maersk in de tussentijd met de middelen die zij wel tot hun beschikking hebben. Over de hele wereld worden in de terminals papieren documenten op te verschepen containers geplakt en bestellingen worden via persoonlijke Gmail-accounts, Whatsapp en Excel-bestanden geboekt (Greenberg, 2018). Uiteindelijk slaagt Maersk in ongekend tempo in zijn taak: tien dagen na de activatie van de wiperware zijn de getroffen terminals, waaronder APM Terminals, deels weer operationeel. Gelukkig voor de scheepvaart- en transportgigant lijken de hackers geen klantgegevens te hebben buitgemaakt en lijkt de schade voornamelijk financieel van aard. Mede dankzij het feit dat men tijdens de verstoring op kundige en veerkrachtige wijze is overgeschakeld naar

handmatige administratie is de omvang van het verkeer bij het bedrijf met ‘slechts’ 20 procent gedaald (TheRegister.co.uk, 2018). Uiteindelijk wordt de financiële schade van de cyberaanval bij Maersk geraamd op 250 tot 300 miljoen dollar. Wereldwijd loopt de totale schade op tot meer dan 10 miljard dollar (Greenberg, 2018).

2.3 Beschouwing

In deze casus behandelen we vier relevante thema’s. Allereerst is dat de rol van de overheid en verantwoordelijkheid van de getroffen organisatie. Wie is aan zet bij een cyberverstoring? Vervolgens komen de fysieke gevolgen van een cyberverstoring aan de orde. Hoe gaan we om met dergelijke gevolgen? Ten derde gaan we in op het belang van digitale beveiliging. Tot slot bespreken we de typologie van een cyberverstoring: waar hebben we het precies over?

2.3.1 De rol van de overheid en verantwoordelijkheid van de getroffen organisatie

In 2018 schreven Van Duin en Maan het volgende over de verstoring:
“Het is evident dat bij deze cyberaanval eerst en vooral Maersk (APM Terminals) actie moest ondernemen. […] Omdat Maersk de computer en informatieveiligheid kennelijk niet voldoende op orde had, moest het bedrijf zelf aan de bak (computers aanpassen en software vervangen) om weer operationeel te kunnen worden. Toch is daarmee niet het hele verhaal verteld. Op verschillende manieren waren ook overheden betrokken en de vraag is of in de toekomst, bij een vergelijkbare casus, de rol van de overheid wellicht zelfs groter zal (moeten) zijn.”

Circa twee jaar na dato is de vraag wie de verantwoordelijkheid heeft bij cybergevolgbestrijding en welke rol de overheid hierbij is toebedeeld nog steeds onverminderd relevant. In eerste instantie is de getroffen organisatie aan zet. Ook in deze casus was Maersk, als getroffen organisatie, daarom zelf hoofdverantwoordelijk voor de incidentrespons (Van Duin & Maan, 2018). De benodigde stappen om de digitale omgeving weer operationeel te krijgen, moest het bedrijf hoofdzakelijk zelf doorlopen. En dit deed het met succes: APM Terminals en Maersk herstelden in ongekend tempo de ICT-problemen. Het Rotterdamse havenbedrijf was – mede omdat de havenmeester van dienst sinds enkele maanden tevens ‘port cyber resilience officer’ was – intensief betrokken bij de cyberverstoring en haar fysieke gevolgen. Wederom met succes: het havenbedrijf loste bijvoorbeeld de verkeersproblemen op het water op.

Het NCSC bewaakte namens de overheid de effecten van de aanval op de vitale infrastructuur, maar de verdere rol van de overheid bleef in deze casus relatief beperkt. Desalniettemin zijn actoren zoals het NCSC, de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de NCTV wel degelijk betrokken bij dergelijke cyberverstoringen. Ze komen bijvoorbeeld veelal in beeld om informatie op te halen en houden zich, overwegend achter de schermen, bezig met verstoringen, onder andere om te voorkomen dat deze effect hebben op Nederlands vitale infrastructuur. Tot daadwerkelijke bijstand tijdens de incidentrespons komt het meestal niet, ook niet in deze casus. Zoals gesteld, is de getroffen organisatie hoofdzakelijk zélf verantwoordelijk voor de gevolgbestrijding. Pas op het moment dat de getroffen organisaties binnen de doelgroep (rijksoverheidsorganisaties en vitale aanbieders) van het NCSC vallen, kan de dienst vanuit zijn wettelijk taak bijstand verlenen en kunnen de organisaties rekenen op deze bijstand, bijvoorbeeld in de vorm van incidentrespons (NCSC, 2019).

2.3.2 Fysieke gevolgen

Cyberverstoringen kunnen ook fysieke gevolgen hebben. Als gevolg van NotPetya vielen wereldwijd systemen in 65 landen uit en in sommige landen waren de fysieke gevolgen een stuk ernstiger dan in Nederland. Zo gingen in Oekraïne banken plat, was pinnen niet meer mogelijk en vielen het metronetwerk, vliegvelden en de kerncentrale van Tsjernobyl uit (Modderkolk, 2019). Cyberverstoringen kunnen dus zeker grote fysieke gevolgen hebben, gevolgen die een heel land kunnen raken. En ondanks het feit dat de fysieke gevolgen in Nederland meevielen vergeleken met bijvoorbeeld die in Oekraïne, waren ze er wel degelijk. Doordat de terminals stilvielen, zagen vrachtschepen zich genoodzaakt dagenlang stil te liggen in de zee bij Hoek van Holland of uit te wijken naar andere, nabijgelegen havens. Door de continue aanloop van vrachtwagens ontstonden er tevens grote files in en rondom het havengebied. Bij dergelijke fysieke gevolgen neemt de (cyber)verstoring echter een voor hulpdiensten en crisisorganisaties bekende gedaante aan. Op het moment dat er grootschalige files ontstaan, treden er bijvoorbeeld allerlei bekende processen in werking. We hebben immers al jarenlange ervaring (en manieren van omgang) met een dergelijke verstoring (Van Eeten, 2019). Van Eeten verwoordt het als volgt: “Zodra je het woord digitaal of cyber weghaalt uit het verhaal van Maersk, wordt het een bijna banale aangelegenheid. Storing bij groot bedrijf, dus files.”

De fysieke gevolgen van de cyberverstoring en de daaruit voortkomende problemen werden dan ook effectief en relatief snel verholpen door de betrokken actoren. En ondanks de op het eerste oog gigantische financiële schade (250 tot 300 miljoen dollar), bleek deze achteraf mee te vallen. De aanval had dan wel een reductie van 20 procent van de omvang van het vrachtverkeer bij APM Terminals tot gevolg gehad, tot een totale disruptie van de bedrijfsvoering was het, mede dankzij de effectieve responscapaciteit en veerkrachtig handelen, niet gekomen. Het bedrijf schreef als gevolg van de verstoring de enkele honderden miljoenen euro’s af en behield zonder enig probleem zijn positie als marktleider (Van Eeten, 2019).

2.3.3 Digitale beveiliging

De fysieke gevolgen van de cyberverstoring waren in deze casus duidelijk zichtbaar. Zoals inmiddels duidelijk moge zijn, waren er landen en bedrijven die nog veel harder werden geraakt dan Nederland en Maersk. Maar bij het overgrote deel van getroffen bedrijven werden alleen de computers met software van M.E.Doc geraakt door de aanval, terwijl APM Terminals daarentegen volledig uitviel. Hoe kwam dat? Van Duin en Maan concludeerden in 2017 al dat de computer- en informatieveiligheid kennelijk niet voldoende op orde was. Volgens Modderkolk (2019) is dit een opmerkelijk gegeven, gezien de cruciale rol die het bedrijf vervult in het mondiale scheepsverkeer. Hij wijdt de impact aan het gebrek aan een gevoelde noodzaak bij APM tot digitale beveiliging. Waar aan fysieke beveiliging geen gebrek was (“stevige hekken, 24 uur bewaking en enkel toegang na een aanmeldingsprocedure met vingerafdruk”) zou het bedrijf zijn digitale beveiliging simpelweg niet goed voor elkaar hebben gehad.

Deze casus is dan ook illustratief voor een terugkerend probleem: organisaties die hun digitale beveiliging niet goed (genoeg) op orde hebben. Dit kan komen doordat zij basismaatregelen niet in acht nemen (het Terminal Operation System van APM Terminals had tot 2015 bijvoorbeeld geen antivirussoftware), maar ook doordat zij updates ondanks herhaaldelijk en dringend verzoek van softwareleveranciers niet of te laat uitvoeren (Modderkolk, 2019). Niet alleen de incidentrespons is hoofdzakelijk de verantwoordelijkheid van de getroffen partij, (het op peil houden van) een goede digitale beveiliging is dat zeer zeker ook.

2.3.4 Een (cyber)disruptie

De omschrijving van een digitale verstoring uit het *Whitepaper digitale ontwrichting en cyber* (IFV, 2019b) is niet toepasbaar op deze casus. Het gaat immers niet om een verstoring van een digitaal systeem die de veiligheid of openbare orde in een veiligheidsregio bedreigt. Het gaat echter wel degelijk om een verstoring van een digitaal systeem die een grote impact heeft op de getroffen organisatie.

De aanval op Maersk kan tevens worden gezien als een exemplarisch voorbeeld van een disruptie uit de typologie van Oomes. Net zoals bij een disruptie was er namelijk geen regionale opschaling nodig en wist de getroffen organisatie als voornaamste bronbestrijder de verstoring te verhelpen en de fysieke gevolgen te beheersen. De overheid, in dit geval voornamelijk in de vorm van het NCSC, hield zich met name bezig met het beheersen van de effecten van de aanval op de vitale infrastructuur. Aan de situatie zelf lag een ICT-uitval ten grondslag en de uitval had onder andere files tot gevolg. Daarnaast was er met name behoefte aan zogenaamde storingsdiensten met vakbekwame technici die de verstoring verhielpen, namelijk ICT'ers.

2.4 Tot slot

De cyberaanval in de Rotterdamse haven figureert nadrukkelijk in allerlei rapportages over cybersecurity. De aanval is een illustratief voorbeeld van een cyberverstoring waar autoriteiten regelmatig voor waarschuwen en die terugkomt in tal van (cyber)dreigingsbeelden (NCTV, 2019). De wereldwijd gevoelde cyberaanval met wiperware NotPetya wordt door sommigen zelfs de meest verwoestende in de geschiedenis genoemd (Greenberg, 2018). En dit alles is niet geheel ten onrechte. De aanval trof landen en bedrijven over de hele wereld, leidde tot verstoringen in verschillende productieketens, werd breed uitgemeten in de media en veroorzaakte maar liefst 10 miljard dollar aan schade. De getroffen organisaties in de Rotterdamse haven moesten alle zeilen bijzetten om de ontstane problemen op te lossen. Een dergelijk incident had zich in de haven niet eerder voorgedaan, zo blijkt ook uit een illustratief citaat uit het boek van Modderkolk (2019):

> "Havenmeester René de Vries is een ervaren politieman. Hij heeft allerlei soorten incidenten meegemaakt. Steekpartijen, op heterdaad betrapte dieven en bedreigingen. Maar op dinsdag 27 juni 2017 heeft hij geen idee wat er gebeurt. Een brand op een schip of een lek van vervuilende stoffen is voor hem overzichtelijk. Een afgebakend probleem. Maar wat de haven nu overkomt, is ongrijpbaar".

De cyberaanval was er dus een met een ongekend karakter. Toch leert de casus Maersk ons ook dat enige nuance op zijn plaats is. De cyberaanval was dan misschien een van de meest verwoestende ooit, wereldwijd werden de verstoringen relatief snel en op veerkrachtige wijze verholpen en in Nederland werden de fysieke gevolgen, niet door de overheid maar door de getroffen bedrijven, effectief beheerst. Een dergelijke reactie vergt voorbereiding in de koude fase en slagkracht en capaciteit in de warme fase – zaken die APM Terminals en de Rotterdamse haven goed op orde hadden. We kunnen dus concluderen dat we er zelfs bij een cyberaanval van deze omvang in slagen om de gevolgen te beperken.

Waar organisaties naast de incidentrespons ook zelf hoofdverantwoordelijk voor zijn, is hun digitale beveiliging. De reden voor een cyberverstoring, zoals een succesvolle hack, zijn maar al te vaak kwetsbaarheden in de digitale beveiliging. Hierbij is, zoals Van Duin en Maan terecht opmerkten, de keten zo sterk als de zwakste schakel. Het succesvol

verstoppen van malware in software-updates van het Oekraïense boekhoudprogramma M.E.Doc heeft mede daardoor gevolgen gehad voor organisaties aan de andere kant van de wereld, waaronder de haven van Rotterdam. Dat is op zijn beurt weer verontrustend. Malware in software die door veel partijen wereldwijd wordt gebruikt, kan razendsnel leiden tot problemen, zoals we die in de Rotterdamse haven zagen.

Belangrijkste bevindingen

1. Getroffen organisaties zijn bij cyberverstoringen zelf hoofdverantwoordelijk voor de incidentrespons. De overheid bewaakt voornamelijk de effecten van de aanval op de vitale infrastructuur.
2. Cyberverstoringen kunnen (grote) fysieke gevolgen hebben. Bij dergelijke fysieke gevolgen nemen cyberverstoringen echter een voor hulpdiensten en crisisorganisaties bekende gedaante aan. Mede hierdoor kunnen de fysieke gevolgen vaak effectief worden beheerst.
3. Het hebben en op peil houden van goede digitale beveiliging is essentieel én de eigen verantwoordelijkheid van organisaties.
4. De cyberaanval op Maersk resulteerde in een verstoring van een digitaal systeem zonder bedreiging van de veiligheid of openbare orde in een veiligheidsregio, maar met wel een grote impact op de getroffen organisatie(s). De aanval op Maersk is daarnaast een exemplarisch voorbeeld van een cyberdisruptie.

3 De cyberaanval op de gemeente Lochem (2019)

3.1 Inleiding

In juni 2019 werd de gemeente Lochem geconfronteerd met een cyberaanval op het gemeentelijke ICT-netwerk. Daarmee was Lochem een van de eerste gemeenten in Nederland die met een dergelijke aanval te maken kreeg. Eerder waren er weliswaar incidenten met virusbesmettingen van ICT-voorzieningen en datalekken, maar een moedwillige cyberaanval op een gemeente had voor zover bekend niet eerder plaatsgevonden.

De detectie van de aanval op 6 juni was voor de gemeente aanleiding om een crisisteam bijeen te roepen om de schade zoveel mogelijk te beperken. Er werd forensisch onderzoek gedaan, melding gedaan bij de Autoriteit Persoonsgegevens en afstemming gezocht met (externe) experts. Ondanks dat het niet tot een daadwerkelijke gijzeling van data kwam, zag de gemeente zich op 12 juni toch genoodzaakt haar dienstverlening gedeeltelijk op te schorten voor het uitvoeren van herstelwerkzaamheden. De gevolgen van het incident lijken achteraf gelukkig mee te vallen, maar volgens ICT-expert Brenno de Winter is de gemeente door het oog van de naald gekropen (De Winter, 2019). De schade had vele malen groter kunnen zijn. De aanval past in de trend van toenemende cyberverstoringen en een groeiend besef van de kwetsbaarheden van vitale ICT-voorzieningen.

In dit hoofdstuk beschrijven we de casus op basis van openbare bronnen en gesprekken met betrokken sleutelfunctionarissen. In dit kader is gesproken met de burgemeester van Lochem en de Chief Information Security Officer (CISO), tevens teamleider van de ICT-dienst van de gemeente. We gaan vervolgens in op de gemeentelijke crisisstructuur en het principe van besluitvorming tijdens onzekerheid.

3.2 Feitenrelaas

Op donderdag 6 juni wordt omstreeks 15.15 uur een van de systeembeheerders van de gemeente Lochem gebeld door het landelijke Team High Tech Crime van de politie. De melding luidt dat er verdacht internetverkeer vanuit gemeentelijke servers wordt gesignaleerd (De Winter, 2019). De politie vraagt de systeembeheerder actie te ondernemen en geeft de gemeente vervolgens enkele IP-adressen waar het verdachte verkeer vandaan komt en/of naartoe gaat. Met deze IP-adressen in zijn bezit gaat de ICT-dienst van de gemeente aan de slag. De ICT-dienst doorloopt vervolgens het standaard protocol. Er wordt gebeld met de leverancier en beheerder van de firewall van de gemeentelijke ICT-omgeving om in beeld te brengen waar het verdachte internetverkeer vandaan komt en waar het naartoe gaat. Het verkeer lijkt via een ‘client-computer’ in een virtuele desktopomgeving – een thuiswerkserver – te lopen. Vervolgens wordt deze virtuele computer digitaal verwijderd, wordt de toegang voor de desbetreffende IP-adressen geblokkeerd en worden enkele controles uitgevoerd. De genomen stappen worden uiteindelijk teruggekoppeld aan de

politie.[8] Rond 18.00 uur neemt de politie echter wederom contact op met de gemeente; de genomen maatregelen zijn in haar ogen onvoldoende. Hierom neemt de CISO contact op met de Informatiebeveiligingsdienst (IBD) (Groet, 2019; De Winter, 2019). Vertegenwoordigers van de IDB en het NCSC (Nationaal Cyber Security Centrum) reizen nog diezelfde avond af naar Lochem. Ondertussen stelt de CISO, Remko Gelmers, rond 21.30 uur de burgemeester Van 't Erve op de hoogte. Vanaf circa 23.00 uur worden door de IBD, het NCSC, de politie en de gemeente Lochem corrigerende werkzaamheden en onderzoek verricht. In de loop van de avond en nacht wordt duidelijk dat er sprake is geweest van onbevoegde toegang tot het gemeentelijke ICT-netwerk (IBD 2019). Omstreeks 09.00 uur de volgende ochtend, op vrijdag, vertrekken de medewerkers van de IBD, het NCSC en de politie. Op deze dag doet de gemeente Lochem melding van een (mogelijk) datalek van bedrijfsgegevens bij de Autoriteit Persoonsgegevens (Gemeente Lochem, 2019a).

Hoewel de detectie pas op 6 juni plaatsvindt, heeft dit incident een langere aanloop. Hackersgroepen hebben namelijk al enige tijd onrechtmatig toegang tot de gemeentelijke ICT-omgeving. Doordat het zogeheten 'Remote Desktop Protocol' (RDP) op onverklaarbare wijze aan staat, kunnen hackers in de ICT-systemen van de gemeente komen (De Winter, 2019). Waarom deze poort open staat, is niet meer te achterhalen; wel is bekend dat de hackers, nadat de RDP-poort op 14 december 2018 is opengezet, gedurende een periode van meer dan vijf maanden tientallen keren inloggen in het systeem (NFIR, 2019). Hierbij trachten zij steeds verder het systeem te penetreren en meer rechten te bemachtigen. Het uiteindelijke doel is een vorm van ransomware te installeren en zo bestanden te versleutelen in ruil voor losgeld. De hackers hebben een poging gedaan tot digitale gijzeling (IBD, 2019), maar zijn niet tot een daadwerkelijke gijzeling van data gekomen.

De hackers zijn dan wel niet geslaagd in hun gijzelingspoging, wel wordt er een zogenoemde 'ransomnote' gevonden en lijkt er sprake te zijn van een datalek. Een ransomnote is een digitale (gijzelings)brief waarin wordt gesteld dat een digitale transactie dient te worden uitgevoerd om weer toegang te krijgen tot de versleutelde data (NFIR, 2019). Deze ransomnote was alvast geplaatst in voorbereiding op de aanstaande gijzeling. De gemeente lijkt met de schrik vrij te zijn gekomen. Toch wordt de aanval uiterst serieus genomen.[9] Op vrijdagochtend 7 juni roept de burgemeester om 10.00 uur dan ook het gemeentelijke crisisteam bijeen.[10] De betrouwbaarheid van het gemeentelijke ICT-netwerk kan namelijk nog niet worden gegarandeerd en mogelijke gevolgen van de hack kunnen niet worden uitgesloten. In het eerste crisisoverleg besluit het crisisteam om het Nederlands Forensisch Incident Response (NFIR) te vragen om forensisch bewijs te verzamelen en uitvoerig onderzoek te verrichten naar de aard van het (mogelijke) datalek. Ook besluit het crisisteam het incident aan te wenden als leermoment. Er wordt dan ook besloten maximale openheid te betrachten, proactief te communiceren over het incident naar de buitenwereld en proactief om te gaan met het voorval (De Winter, 2019). Gedurende het verdere verloop van de crisis wordt gewerkt op basis van deze standaard crisisstructuur en wordt de gebruikelijke besluitvormingsprocedure aangehouden (beeld, oordeel, besluit; de BOB-structuur). Dezelfde dag wordt het eerste nieuwsbericht verspreid via de website van de gemeente Lochem (zie onderstaand kader). In dit nieuwsbericht wordt vermeld "dat hackers

[8] Het besluit aangifte te doen is al vrij snel genomen, maar de daadwerkelijke aangifte laat nog even op zich wachten. Er wordt gekozen om eerste de onderzoeksresultaten af te wachten zodat men weet *waarvan* precies aangifte moet worden gedaan.

[9] Achteraf blijkt sprake van een 'Advanced Persistent Threat' (APT): een langdurige en doelgerichte cyberaanval waarbij onbevoegden (zoals staten of door staten ondersteunde groeperingen) onopgemerkt en langdurig toegang krijgt tot een netwerk. Het doel is om continu toegang te krijgen en gegevens te stelen.

[10] Het crisisteam bestaat uit de gemeentesecretaris, de ambtenaar Openbare Orde en Veiligheid, een communicatieadviseur en het hoofd ICT (en tevens CISO). De burgemeester zit het overleg van het crisisteam voor.

een aanval hebben uitgevoerd op het IT-netwerk van de gemeente". Ook wordt aangegeven dat de aanval inmiddels is gestopt en dat er onderzoek wordt verricht naar het incident, "omdat een geslaagde inbraakpoging via het netwerk bij de overheid uitzonderlijk is" (Gemeente Lochem, 2019b). Bij het opmaken van dit en het hierop volgende persbericht heeft de gemeente rekening te houden met het feit dat door het inmiddels gestarte strafrechtelijke onderzoek geen dadergevoelige informatie openbaar mag worden gemaakt.

Hackers breken in op ICT- netwerk gemeente Lochem, 7 juni 2019[11]
Op 6 juni is ontdekt dat hackers een aanval hebben uitgevoerd op het ICT-netwerk van de gemeente Lochem. We hebben de aanval gestopt. Er is nog geen aanleiding om te vermoeden dat er persoonsgegevens zijn gestolen. Uit voorzorg melden we de aanval bij de Autoriteit Persoonsgegevens. Ook doen we aangifte bij de politie.

Omdat een geslaagde inbraakpoging via het netwerk bij de overheid uitzonderlijk is, doen we samen met de Informatiebeveiligingsdienst voor Gemeenten (IBD) en het Nationaal Cyber Security Centrum (NCSC) onderzoek naar het incident. De burgemeester laat ook een extern onderzoek doen.

We zetten alles op alles om gegevens te beveiligen. We kunnen op dit moment in het belang van het onderzoek geen mededelingen over het incident doen.

In het aansluitende pinksterweekend, zondag 9 en maandag 10 juni, worden de herstelwerkzaamheden en het forensisch onderzoek voortgezet door het NFIR. Hierbij worden in het kader van het onderzoek kopieën gemaakt van alle relevante gemeentelijke ICT-systemen. Door de omvangrijke taak worden de desbetreffende werkzaamheden uiteindelijk pas op 18 juni afgerond. Tevens worden, zonder dat dit tot een melding leidt, het interne netwerk en de internetverbinding intensief gemonitord om een eventuele nieuwe poging tot een hack te voorkomen (Alert Online, 2019; De Winter, 2019).

Hoewel de crisis aanvankelijk beslecht lijkt, doet zich op dinsdagmiddag 11 juni een onvoorziene ontwikkeling voor. Het vermoeden ontstaat namelijk, dat de hackers zijn doorgedrongen tot een database met gegevens van medewerkers van de gemeente Lochem. Door dit mogelijke lek kan niet langer worden uitgesloten dat hackers beheerdersrechten (een zogenaamd 'golden ticket') hebben verkregen of zouden kunnen verkrijgen en valt de betrouwbaarheid van het gemeentelijke ICT-netwerk definitief niet langer te garanderen. Het crisisteam kiest er vervolgens voor om, na een geplande raadsvergadering op dinsdagavond 11 juni, over te gaan tot een ingrijpende maatregel: het offline halen van het geheel aan ICT-systemen. Hierdoor zal de gemeentelijke dienstverlening die afhankelijk is van ICT de volgende dag (12 juni) niet beschikbaar zijn (De Gezonde Digitale Organisatie, 2019).[12] In de nacht wordt dit offline halen doorgevoerd en vervolgens worden alle wachtwoorden gewijzigd. Zo wordt het bezit van beheerdersrechten voor de hackers uitgesloten en kan de betrouwbaarheid van de ICT-systemen opnieuw worden gegarandeerd (De Winter, 2019; Groet, 2019). Op de website van de gemeente wordt een nieuwsbericht geplaatst waarin een update wordt gegeven van de stand van

[11] https://www.lochem.nl/laatste-nieuws/nieuwsbericht/gemeentenieuws/hackers-breken-in-op-ict-netwerk-gemeente-lochem-2367

[12] De internetverbinding wordt gedurende tien uur voor alle systemen volledig verbroken (dit is de tijdsduur waarna het golden ticket van de hackers is verlopen). In de tussentijd worden alle wachtwoorden van alle systemen gewijzigd, krijgen alle gebruikers een nieuw wachtwoord en wordt een procedure opgezet om die wachtwoorden aan iedereen uit te reiken. Hierdoor zijn na de eerdergenoemde tien uur niet alle systemen direct operationeel. Sommige (delen van) systemen blijken daarnaast te zijn verstoord. In de loop van de woensdag 12 juni zijn alle systemen weer (bijna volledig) in de lucht. Hierop was geanticipeerd, zodat vooraf was aangegeven dat (een deel van) de dienstverlening op woensdag niet mogelijk zou zijn.

zaken (zie onderstaand kader). Hierin wordt gesteld dat als gevolg van het incident “de gemeente is genoodzaakt om een deel van de dienstverlening op woensdag 12 juni te staken” (Gemeente Lochem, 2019b).[13]

Gemeente Lochem digitaal niet bereikbaar vanwege herstel na hack, 11 juni 2019[14]
Na een dergelijke aanval is het gebruikelijk om met een schone ICT omgeving te beginnen. Daarmee wordt herstel in gang gezet van de systemen. Om dit goed te kunnen doen is het noodzakelijk om een aantal systemen van de gemeente Lochem opnieuw te installeren, waardoor ze tijdelijk niet beschikbaar zijn. De gemeente is genoodzaakt om een deel van de dienstverlening op woensdag 12 juni te staken. Wel zullen de website en de social media kanalen beschikbaar blijven. Ook huwelijken gaan gewoon door. Het gebouw blijft open, medewerkers van de receptie kunnen uw vragen beantwoorden.

Het tijdelijk stil leggen van het systeem heeft alleen invloed op zaken die digitale ondersteuning behoeven, zoals het maken van een online afspraak, aanvragen van paspoorten, het registreren van een verhuizing en het aangeven van geboortes.

Deze maatregel wordt genomen, omdat de gemeente alles op alles wil zetten om de gegevens van haar burgers te beveiligen. Natuurlijk betreuren we de hinder die hierdoor ontstaat. Lopende het onderzoek is nog niet helder waardoor dit heeft kunnen gebeuren en of de aanvallers iets hebben buitgemaakt. In het belang van het onderzoek kunnen we nog niet met verdere details naar buiten treden. Zodra dat wel kan, zullen we u uiteraard informeren.

In de loop van 12 juni komen de verschillende ICT-systemen (deels) weer online en worden de gemeentelijke diensten die afhankelijk zijn van ICT weer hervat. In de loop van de dag is een groot deel van de ICT-infrastructuur weer operationeel. Doordat het wijzigen van wachtwoorden niet helemaal soepel is verlopen, werken niet alle applicaties naar behoren. Hierdoor zijn extra inspanningen noodzakelijk, zoals de hulp van een leverancier of het herstarten van de systemen. Ook moeten afspraken worden verplaatst en nieuwe wachtwoorden worden aangemaakt. Vervolgens voert beveiligingsbedrijf NFIR op verzoek van de burgemeester een penetratietest uit om de getroffen maatregelen te testen en de verbeterpunten van de ICT-systemen in kaart te brengen (Groet, 2019; De Kluis, 2019; De Winter, 2019). Op 13 juni doet de IBD op verzoek van de gemeente Lochem een bijstandsverzoek aan omliggende gemeenten. Zo wordt getracht de druk op de eigen ICT-medewerkers van Lochem te verminderen (Groet, 2019), aangezien deze vrijwel voortdurend bezig zijn met het ondersteunen van het forensisch onderzoek van het NFIR. De gemeenten Enschede en Hengelo leveren daarop ondersteunende ICT-capaciteit, die op 17 juni kan worden ingezet.

Uiteindelijk lijkt de gemeente Lochem relatief goed met de cyberaanval te zijn weggekomen. Er zijn ‘slechts’ 32 megabyte (MB) aan data verkregen door de hackers. Wel is als gevolg van de verrichte onderzoeken, de herstelacties en additionele kosten de financiële schade opgelopen tot meer dan 2 ton (De Gezonde Digitale Organisatie, 2019). Deze incidentele, niet-begrote kosten hadden echter vele malen hoger kunnen zijn, als de data ook daadwerkelijk zouden zijn gegijzeld (IBD, 2019). Het onderzoek en alle onderliggende

[13] Met betrekking tot het offline halen van de ICT-systemen van de gemeente Lochem spreekt De Winter in zijn rapportage van 12, 13 en 14 juni. Uit de communicatie van de gemeente Lochem zélf blijkt echter dat het gaat om respectievelijk 11, 12 en 13 juni. In dit hoofdstuk is daarom uitgegaan van de data zoals gecommuniceerd door de gemeente Lochem.

[14] Het originele bericht is door de Gemeente Lochem verwijderd van haar website. Het bericht is echter terug te vinden via: https://drimble.nl/regio/gelderland/zutphen/60707844/gemeente-lochem-digitaal-niet-bereikbaar-vanwege-herstel-na-hack.html

documenten die zijn uitgebracht naar aanleiding van het incident worden in september door de gemeente openbaar gemaakt (IBD, 2019). De gemeente kiest bewust voor het actief openbaar maken van de rapportages over de cyberaanval, omdat zij hiermee wil bijdragen aan het vergroten van de bewustwording over cyberrisico's onder gemeenten en burgemeesters. In de media pleit burgemeester Van 't Erve naderhand voor een betere voorbereiding op cyberdreigingen: "Voor dijkdoorbraken en gif-emissies liggen draaiboeken klaar, is coördinatie minutieus geregeld en kent ieder zijn taak; een situatie die bij ICT-rampen node wordt gemist".[15]

3.3 Beschouwing

In deze casus zien we twee centrale thema's: de ondersteuning van gemeenten bij een cyberaanval en besluitvorming in onzekerheid. Omdat cyberincidenten een relatief nieuw risico vormen, is het voor gemeenten nog zoeken naar de crisisrespons en welke partijen hen kunnen ondersteunen bij de incidentbestrijding. Verder gaan cyberincidenten gepaard met onzekerheid, waaronder ook besluiten genomen moeten worden: wat is de oorzaak, welke effecten treden er mogelijk nog op en hoe lossen we dit op? Beide kwesties hebben in deze casus gespeeld en worden nu achtereenvolgens besproken.

3.3.1 Crisisrespons en benodigde expertise

Regelmatig hebben gemeenten te maken met allerlei (mini-)crises, van een incident in het sociaal domein tot maatschappelijke onrust. Soms wordt daarbij in regionaal verband opgeschaald, maar niet altijd is de inzet van politie en brandweer nodig. Gemeenten kiezen dan niet voor formele opschaling volgens de GRIP-procedure, maar schalen intern op en werken in lijn met generieke procedures van besluitvorming (gestructureerd overleg, beeld-, oordeels- en besluitvorming). Binnen de crisisbeheersing wordt dan ook wel gesproken van GRIP-0 (Van Duin & Wijkhuijs, 2015). Al naargelang de situatie worden externe partijen als het Openbaar Ministerie (OM) uitgenodigd voor het overleg. Rond nieuwe risico's zoals cyberaanvallen dringt de vraag zich op welke crisisstructuur nodig is voor bron- en gevolgbestrijding. Juist omdat het nieuwe risico's betreft (waarmee nog relatief weinig ervaring is opgedaan en beperkt is geoefend), is het voor gemeenten en veiligheidsregio's in de praktijk nog zoeken welke responsstructuur en expertise zijn vereist.

Bij de aanpak van de cyberaanval koos de gemeente Lochem zoals gezegd voor een interne opschaling en crisisstructuur; er werd een crisisteam ingericht onder leiding van de burgemeester. Volgens CISO Remko Gelmers functioneerde deze generieke crisisstructuur bijzonder goed. De verschillende disciplines aan tafel gaven updates over de voortgang, acties en knelpunten, er werd gestructureerd gewerkt en er was één centrale plek waar alle informatiestromen samenkwamen. Een cyberaanval vraagt echter veel van een organisatie, niet alleen op organisatorisch en bestuurlijk gebied, maar ook ICT-technisch. De benodigde inspanningen op dat laatstgenoemde terrein vroegen, zeker voor een relatief kleine gemeente als Lochem, dan ook veel van de ICT-dienst.

Meerdere partijen (onder andere IBD, NCSC, NFIR en de politie) die de gemeente op bepaalde momenten van kennis en kunde voorzagen, raakten bij het incident betrokken. Desalniettemin liet met name de mate van praktische bijstand ruimte voor verbetering. Zoals Gelmers het verwoordde: "Het zou fijn dat als er iets gebeurt en je belt, dat er direct mensen

[15] iBestuur Magazine 34, Cyberaanval Lochem gaat de hele overheid aan, 20 mei 2020.

in de auto springen om te komen helpen."[16] Mede daardoor werd de benodigde expertise gezocht in de vorm van een externe specialist, van gemeentelijke bijstand en van het NFIR voor forensisch onderzoek. Alleen al het begeleiden en coördineren van dat onderzoek en het afhandelen van het aanbod aan bijstand was volgens Gelmers een dagtaak op zichzelf. Die externe specialist was Brenno de Winter. Burgemeester Van 't Erve had op 6 juni toevalligerwijs al contact gehad met deze ICT-specialist. Zodoende belde hij De Winter met het verzoek om de gemeente van een afstand als adviseur bij te staan. Volgens de burgemeester fungeerde hij als een essentiële schakel tussen de ICT-dienst en het bestuur van de gemeente Lochem, en voor de CISO was De Winter een sparringpartner en klankbord.

Voor de betrokken functionarissen in het crisisteam was het volop pionieren en improviseren op onbekend terrein. De gemeente en ook de veiligheidsregio hadden niet eerder geoefend met vergelijkbare scenario's. Het crisisteam moest de benodigde expertise en capaciteit voor de respons zelf mobiliseren. Burgemeester Van 't Eve verwoordde het treffend: "We kregen van iedereen begrip, maar niemand kon wat doen. Uiteindelijk moet je het toch zelf doen." Dat de gemeente kon terugvallen op de interne crisisstructuur en procedure vormde een belangrijke basis om gestructureerd tot oplossingen te komen. Waar de gemeente ook op terug kon vallen, was de IBD. Ondanks dat een deel van de gebruikelijke rol van het IBD werd vertolkt door Brenno de Winter, was er meermaals contact tussen de CISO en de IBD, dacht de dienst mee met de gemeente, had contact met het NCSC en de politie en waren werknemers van de dienst op sommige momenten ter plaatse aanwezig. De IBD had zeker een toegevoegde waarde. Toch zou het in de ogen van de gemeente lonen om als gemeente bijstand te kunnen krijgen van een landelijk incidentresponsteam voor cyberincidenten.

3.3.2 Besluiten in onzekerheid

Cyberrisico's zijn omgeven met de nodige onzekerheid: over achterliggende oorzaken van verstoringen, over mogelijke keteneffecten en over noodzakelijke beheersmaatregelen (IFV, 2020b). Die onzekerheid speelde ook in deze casus. Welke effecten heeft de cyberaanval op de gemeentelijke ICT-voorzieningen en diensten, wanneer zijn systemen weer veilig en betrouwbaar en wie of wat gaat schuil achter de ransomware? Hoe ga je als gemeente om met deze onzekerheden en dilemma's? Dilemma's die hierbij speelden hadden betrekking op de betrouwbaarheid van getroffen systemen en de omvang van de aanval.

De eerste vraag die volgens de burgemeester speelde, was of de betrouwbaarheid van de getroffen systemen kon worden gegarandeerd. Op welk moment valt met zekerheid te zeggen dat de hackers géén toegang meer hebben tot de ICT-omgeving van de gemeente en dat de voorzieningen weer veilig zijn? Wat deze kwestie lastig maakt, is dat een volledig veilig systeem eigenlijk nooit kan worden gegarandeerd; in elk systeem zitten namelijk onvermijdelijk kwetsbaarheden. De gemeente koos niettemin voor de strategie van maximale zekerheid: zij zou niet rusten zolang de vraag naar de betrouwbaarheid van ICT-systemen niet positief kon worden beantwoord en er dus nog aanwijzingen waren die wezen op kwetsbaarheden. Dit leidende principe resulteerde onder meer in grondig forensisch onderzoek, een uitgebreid verbeterprogramma en penetratietesten.

De tweede vraag die speelde, was de omvang van de cyberaanval. Hoe ernstig is de aanval, hoe hard zijn we getroffen en hoe groot is de mogelijke schade? Vragen die hieruit voortkomen zijn: hoe groot schaal je op? Wat is een passende crisisstructuur? Wanneer ben je aan het overreageren of onder-reageren? Dat is onvermijdelijk ingewikkeld, omdat in de

[16] Normaliter vervult de IBD (als sectoraal Computer Emergency Response Team) deze rol richting gemeenten. De IBD helpt bij het inschatten van de aard en omvang van cyberincidenten en adviseert over maatregelen.

eerste uren en dagen veel onduidelijk is en heldere antwoorden ontbreken. In feite weet je niet wat proportioneel is; dat blijkt pas in de evaluatie achteraf. Daarbij speelt tevens – zeker in relatie tot nieuwe en specialistische risico's – het gevaar van onderschatting: 'het zal zo'n vaart niet lopen'. Gelukkig voor de gemeente had de burgemeester affiniteit met digitalisering. Hij zag de mogelijke ernst van de zaak tijdig in en schaalde vervolgens daadkrachtig op. Ook werd extern advies ingeschakeld. Hierbij hanteerde de burgemeester het principe 'liever te groot opschalen en dan weer afschalen, dan andersom'.

3.4 Tot slot

Op 6 juni werd Lochem geconfronteerd met een serieuze poging tot digitale gijzeling ('advanced persistent threat'). Het voorbereidende werk van de hackers bleef voor de gemeente onopgemerkt; pas achteraf bleek dat zij al enkele maanden toegang tot gemeentelijke ICT-systemen hadden gehad. Uiteindelijk wees de politie de gemeente op verdacht internetverkeer op gemeentelijke servers – wat ons betreft een illustratie van hoe lastig het detecteren van en beveiligen tegen dit soort dreigingen voor gemeenten is. Bovendien kan zo'n aanval in feite elke gemeente of organisatie treffen. Zoals de CISO van Lochem het stelde: "Je moet goed beveiligd zijn om een inbraak te voorkomen. Maar een digitale inbraak valt vrijwel niet te voorkomen. Je moet dus voorbereid zijn op die inbraak." Dit citaat duidt op een mooie manier de noodzaak om als organisatie te kunnen reageren op een cyberincident. Cyberaanvallen zullen in de komende jaren alleen maar toenemen en ondanks dat voorkomen beter is dan genezen, moeten we voldoende oog hebben voor cybergevolgbestrijding.

Tijdens de cyberaanval lijkt de generieke crisisstructuur van de gemeente goed bruikbaar. De principes van crisisbeheersing (gestructureerd overleg; de BOB-structuur) bleken effectief voor de probleemanalyse en voor het treffen van maatregelen. Aandachtspunten zijn er zeker ook. Zowel de burgemeester als de CISO gaven aan dat een ICT-specialist (bij voorkeur iemand die deze kennis kan koppelen aan de bestuurlijke praktijk) in de vorm van een adviseur en/of klankbord over waardevolle expertise beschikt op het gebied van de omgang met een cyberaanval. De gemeentelijke ICT-dienst had daarnaast niet alle expertise en mankracht in huis om de cyberaanval zelfstandig door te komen. Aanvullende kennis en kunde was dus gewenst. Hier kan bijvoorbeeld vorm aan gegeven worden door het vooraf afsluiten van een contract met een cybersecuritybedrijf. De daarmee samenhangende kosten zijn hier uiteraard een nadeel van, maar gemeenten kunnen dit ook collectief regelen, zoals zij via de Vereniging van Nederlandse Gemeenten (VNG) het IBD hebben. De casus in Lochem leert ons dat dergelijke ondersteuning aan de voorkant beter vastgelegd moet worden. Anders blijven gemeenten genoodzaakt om tijdens de aanval dergelijke kennis en kunde grotendeels zelf te mobiliseren. In dit geval ging dat goed, maar het had zomaar anders kunnen aflopen.

Bij een cyberaanval wordt niet altijd forensisch onderzoek verricht. In deze casus werd op aanraden van De Winter wel een dergelijk onderzoek uitgevoerd, en wel door het NFIR. Ondanks het feit dat het NFIR dit onderzoek uitvoerde, vroegen het onderzoek en de implementatie van mitigerende maatregelen de inspanningen van gemiddeld twee ICT'ers van de gemeente. Voor een relatief kleine gemeente is dat best veel. Anticipeer hierop en reserveer daarom mankracht voor dergelijk forensisch onderzoek. Mankracht reserveren is echter niet voor elke organisatie even gemakkelijk of überhaupt mogelijk. Daarnaast is praktische ondersteuning voor veel relatief kleine organisaties snel(ler) wenselijk. Uiteindelijk werd in Lochem bijstand in de vorm van extra mankracht uit andere gemeenten gevonden. Het kost momenteel echter nog (te) veel tijd om dergelijke bijstand te realiseren; in het geval

van Lochem vier dagen. Daarnaast kost het veel tijd en energie om de desbetreffende mensen bij te praten, te instrueren en dergelijke. In de toekomst zou dit beter moeten worden geregeld.

De casus toont aan dat Nederlandse gemeenten voor verschillende opgaven staan wat betreft cyberverstoringen. Er is bijvoorbeeld geen landelijk draaiboek voor gemeenten en veiligheidsregio's bij cyberincident en er is geen systeem voor opschaling van de (incident)respons dat voldoet aan de behoeften van gemeenten. De strategie om de verantwoordelijkheid voor cybersecurity en de incidentrespons bij individuele gemeenten te leggen, schiet tekort. Het is noodzaak om de voorbereidingen gemeenschappelijk te treffen (gemeenten, veiligheidsregio's, IBD, NCSC). Dit kan bijvoorbeeld aan de hand van scenario's en het Nationaal Crisisplan Digitaal[17] of door de inzet van een variant van het Nationaal Respons Netwerk.[18] Het helpt om preventief te investeren in dergelijke netwerken. Wat dan nodig is, is specifieke kennis, van mitigatie tot (forensisch) onderzoek. Dat is wat anders dan een paar extra handen. Vragen die bij deze opgaven spelen, zijn: Willen we dit met elkaar organiseren? Wie gaat dat trekken? Wie gaat dat betalen en wie is er voor verantwoordelijk? En wie is bepalend in geval van een incident?

Belangrijkste bevindingen

1. De reguliere crisisstructuur en werkwijzen bieden ook bij cyberverstoringen het nodige houvast. Wel is andere expertise nodig voor het oplossen en herstel van ICT-problemen, en die expertise is niet beschikbaar binnen de bestaande crisisstructuur.
2. Voor organisaties zoals gemeenten, blijft het een uitdaging om eventueel aanvullende expertise te mobiliseren tijdens een cyberverstoring.
3. De betrouwbaarheid van getroffen systemen valt lastig te garanderen, ook nadat de verstoring is verholpen. Die onzekerheid zorgt voor bestuurlijke dilemma's: wanneer zijn systemen weer veilig genoeg?
4. Cyberverstoringen zijn relatief nieuw en vragen om de inspanningen van nieuwe, andersoortige actoren. In de koude fase moet dit 'nieuwe' crisisnetwerk (beter) in kaart worden gebracht en moet er meer worden geoefend met het functioneren van dit netwerk.

[17] Het Nationaal Crisisplan Digitaal helpt de vertaalslag te maken van de crisisaanpak op nationaal niveau naar operationeel uitgewerkte plannen voor onder meer overheden. Zie voor meer informatie hierover: https://www.ncsc.nl/documenten/publicaties/2020/februari/21/nationaal-crisisplan-digitaal.

[18] Het Nationaal Respons Netwerk (NRN) is een convenant met afspraken over samenwerking bij de oplossing van cybersecurityincidenten. Het is ondertekend door het IBD, de Belastingdienst, SURF, Defensie, Rijkswaterstaat en het NCSC. Zie voor meer informatie hierover: https://www.ncsc.nl/actueel/nieuws/2020/februari/7/nrn.

4 De KPN-storing (2019)

4.1 Inleiding

Op maandag 24 juni 2019 vond er in de middag een cyberverstoring plaats in het KPN-netwerk, waardoor het alarmnummer 112 in het hele land onbereikbaar was. Ook het telefoonnummer voor niet-spoedeisende gevallen werkte niet meer. In alle 25 veiligheidsregio's werd opgeschaald naar GRIP-2 en naast regionale NL-Alerts werd er voor het eerst een landelijke NL-Alert verstuurd. Het onhandige toeval was, dat er bij KPN tegelijkertijd een storing van NL-Alert via 4G was, waardoor een deel van de gebruikers geen NL-Alert-berichten kon ontvangen. Om de onbereikbaarheid van het noodnummer op te vangen, werden politieagenten, brandweerauto's en ambulances preventief de straat op gestuurd. Ook konden burgers in geval van nood bij brandweerkazernes en politiebureaus terecht. De storing was aan het begin van de avond weer verholpen en duurde bijna 3,5 uur. Gelukkig heeft de storing niet tot grote maatschappelijke impact geleid.[19] Wel vormde zij een unieke gebeurtenis met de afzonderlijke opschaling van alle veiligheidsregio's. In de draaiboeken van de politie was dan ook geen rekening gehouden met een dergelijk scenario.

Het feitenrelaas van dit hoofdstuk is grotendeels gebaseerd op het eerder verschenen door het IFV uitgebrachte rapport over de KPN-storing (IFV, 2019c). Deze informatie is aangevuld met behulp van het later verschenen gezamenlijke inspectierapport, opgesteld door de Inspectie Justitie en Veiligheid (JenV), het Agentschap Telecom en de Inspectie Gezondheidszorg en Jeugd (IGJ) (Gezamenlijke Inspecties, 2020).

4.2 Feitenrelaas

Op maandagmiddag 24 juni 2019 wordt om 15.32 uur in het monitoringscentrum van KPN een eerste afname van verkeersstromen duidelijk, waarna steeds meer meldingen binnenkomen. KPN start daarom en op basis van signalen van klanten en de eigen organisatie de calamiteitenprocedure op (Gezamenlijke Inspecties, 2020). Diverse bedrijven en gemeenten blijken niet langer telefonisch bereikbaar te zijn. Al snel wordt duidelijk dat mensen ook geen contact kunnen krijgen met de alarmlijn 112 en dat daarnaast het nummer van de politie voor niet-spoedeisende gevallen, 0900-8844, niet werkt (IFV, 2019c).

Storingen bij het alarmnummer
De storing op 24 juni waardoor 112 onbereikbaar was, was niet de eerste. Eerdere storingen betroffen echter niet alle bellers in het hele land. Bovenop de algehele storing kwam op de 24ste bovendien de storing van NL-Alert.

Eerdere voorbeelden van onbereikbaarheid van het alarmnummer 112 zijn de (regionale) 112-storingen in 2012, de stroomstoring in Noord-Holland in 2015 en die in Amsterdam en

[19] Bij de Inspectie Gezondheidszorg en Jeugd zijn drie sterfgevallen gemeld die tijdens de storing plaatsvonden. Het is niet zeker of deze personen nog hadden geleefd als er geen storing bij 112 was geweest.

omgeving in 2017. Deze storingen zijn ook door de inspecties onderzocht. Een belangrijk aandachtspunt dat uit deze onderzoeken naar voren is gekomen, is dat organisaties op tijd een handelingsperspectief moeten aanbieden aan burgers en betrokken organisaties (Gezamenlijke Inspecties, 2020).

Ook storingen van de niet-spoedeisende telefoonnummers komen voor. Zo waren er, heel recent in september 2020, twee keer in één week problemen met het politietelefoonnummer voor niet-spoedeisende zaken (0900-8844). Door een landelijke storing was dit nummer niet bereikbaar; ook de 088-nummers waren niet goed te bereiken. Het alarmnummer 112 werkte wel gewoon (NOS, 2020a).

Rond 16.30 uur activeert de politie een Nationale Staf Grootschalig en Bijzonder Optreden (NSGBO). Alle veiligheidsregio's schalen op naar GRIP-2 en stellen hun noodplannen in werking; meldkamers roepen extra personeel op (IFV, 2019c). De politie handelt volgens scenario vier van het Operationeel Draaiboek Generiek (ODG), waarin wordt uitgegaan van een onbereikbare 112-alarmcentrale door een storing in de openbare infrastructuur of de technische 112-voorziening, maar waarbij het landelijke servicenummer van de politie nog wel bereikbaar is. De maatregelen die bij dit scenario horen, zijn dat alle politiebureaus en brandweerkazernes worden bemenst, zodat burgers daar een melding kunnen doen. Daarbij hoort een landelijke uniforme mediaboodschap die door het ministerie van JenV wordt opgesteld en in elk geval de volgende informatie bevat: de 112-dienstverlening is tijdelijk onbereikbaar, bel eventueel 0900-8844 en wanneer er geen telefoon beschikbaar is, zoek het/de dichtstbijzijnde politiebureau of brandweerkazerne. De minister van JenV, geadviseerd door de korpschef politie en politiechef Landelijke Eenheid, neemt het besluit tot deze communicatie. De situatie strookt nu echter niet met dit scenario, omdat het landelijke servicenummer ook niet bereikbaar was. De politie brengt de situatie in kaart en informeert de regionale meldkamers. Daarnaast adviseert zij het ministerie van JenV om een landelijk NL-Alert-bericht te versturen (Gezamenlijke Inspecties, 2020). Hier wordt niet gelijk voor gekozen, maar enige tijd later wordt toch door het Nationaal Crisiscentrum (NCC) in Den Haag besloten om voor het eerst sinds het bestaan van NL-Alert een landelijk waarschuwingsbericht te versturen om de bevolking op de hoogte te stellen van de uitval van 112. Rond 17.20 uur blijkt dat er vanuit het NCC in verband met technische problemen geen landelijk bericht kan worden verstuurd. Uiteindelijk kan het bericht pas om 18.12 uur worden verzonden via het Managing en Monitoring Centre van de politie in Utrecht. Hierbij gaat wat mis met de verwijzing naar het alternatieve noodnummer; in het bericht wordt namelijk verwezen naar de tiplijn van *De Telegraaf*. In het uur daarna komen daar rond de 600 Whatsappberichten binnen, waarvan uiteindelijk negentien serieuze berichten worden doorgezet naar de meldkamer in Driebergen. Om 19.12 uur wordt middels een tweede landelijke NL-Alert het juiste nummer gedeeld (IFV, 2019c). Regionaal worden weer andere alternatieve telefoonnummers gecommuniceerd om hulpdiensten te kunnen bereiken (Gezamenlijke Inspecties, 2020).

Storing van NL-Alert bij KPN
Na het eerste regionale en het eerste landelijke NL-Alert-bericht komen signalen binnen dat NL-Alert-berichten via het KPN-netwerk niet worden ontvangen. Gelijktijdig met de telefoniestoring blijkt er bij KPN een storing van NL-Alert via 4G te zijn, die los staat van de telefoniestoring. Vanaf 12.00 uur kan geen enkele gebruiker verbonden met het 4G-netwerk van KPN NL-Alert-berichten ontvangen. De volgende dag om 11.30 uur wordt geconstateerd dat er een probleem is als gevolg van een eerdere 'configuration change', die om 11.40 uur ongedaan wordt gemaakt. Daarna kunnen KPN-gebruikers op 4G weer NL-Alert-berichten ontvangen (Gezamenlijke Inspecties, 2020).

Ondertussen worden ook in de veiligheidsregio's op allerlei manieren bypasses gelegd om ervoor te zorgen dat de hulpdiensten bereikbaar zijn voor noodmeldingen. Zo zijn er vier veiligheidsregio's die nog vóór het landelijke bericht een regionale NL-Alert versturen, met daarin informatie over de uitval van 112 en lokale telefoonnummers waarmee burgers in geval van nood de hulpdiensten kunnen bereiken. Twee veiligheidsregio's sturen aanvullend op het landelijke bericht een eigen NL-Alert uit. Daarnaast worden agenten, brandweerauto's en ambulances preventief de straat op gestuurd voor het geval iemand hulp nodig heeft. Ook zetten brandweerkazernes, politiebureaus en – in een aantal regio's – gemeentehuizen hun deuren open voor het publiek. In de loop van de middag en avond melden kleine aantallen mensen zich hier met hulpverzoeken (IFV, 2019c).

In de (sociale) media gaat de gehele middag en avond veel aandacht uit naar deze zogenoemde 112-storing. Burgers uiten klachten over met name NL-Alert: een deel van de mensen ontvangt een reeks berichten (deels van verschillende veiligheidsregio's, met daarin verschillende handelingsperspectieven), terwijl andere geen bericht ontvangen en via hun partner, collega's of buren van de storing op de hoogte raken. Daarnaast ontstaat er commotie over het verkeerde telefoonnummer in de landelijke NL-Alert (IFV, 2019c). Tot slot blijven door de vele verstuurde NL-Alerts (regionaal en landelijk) berichten hangen in het centrale NL-Alert-systeem, waardoor deze berichten vertraagd naar de mobiele netwerkoperators worden verstuurd. Veel mensen ontvangen deze NL-Alerts daardoor pas (veel) later (Gezamenlijke Inspecties, 2020).

Om 17.45 uur vindt het onderzoeksteam van KPN de oorzaak van de KPN-storing. Het blijkt te gaan om een technische (ver)storing, en niet om een cyberaanval zoals in de media en op sociale media enige tijd wordt gespeculeerd. Het zou gaan om "een aaneenschakeling van fouten waaronder een routeringsprobleem en het niet werken van de back-up" (Kerssenberg, 2019). Om 18.30 uur wordt het eerste systeem succesvol herstart (Gezamenlijke Inspecties, 2020). De telefoniestoring is om 18.52 uur voorbij; de meldkamers zijn dan weer via 112 bereikbaar. Om 21.00 uur zijn alle crisisorganisaties afgeschaald (Gezamenlijke Inspecties, 2020) en om 21.29 uur wordt een laatste landelijke NL-Alert verstuurd met de informatie dat de noodnummers 112 en 0900-8844 weer bereikbaar zijn (IFV, 2019c).

Tijdens de cyberverstoring is ongeveer 40.000 keer geprobeerd om 112 te bellen, waarbij in veel gevallen sprake geweest zal zijn van 'testtelefoontjes' door functionarissen en burgers – normaal komen er gemiddeld circa 1600 telefoontjes binnen in dit tijdsbestek. Ongeveer zestien procent van de meldingen betrof een echte noodhulpaanvraag (IFV, 2019c). Bij de IGJ zijn drie meldingen binnengekomen over mensen die zijn overleden tijdens de 112-storing, maar het is door de IGJ niet vast te stellen of zij nog hadden geleefd als er geen storing was geweest (Gezamenlijke Inspecties, 2020; IFV, 2019c).

4.3 Beschouwing

In dit hoofdstuk staan drie thema's centraal. Als eerste gaan we in op de voorbereiding van een incident versus de werkelijkheid: in hoeverre kun je je voorbereiden op een dergelijk scenario? En hoe zat het met de voorbereiding in deze casus? Vervolgens bespreken we de gezamenlijke beeldvorming. De KPN-storing betrof het hele land; hoe zorg je dan voor een gezamenlijk beeld en wie pakt de regie? Tot slot komt het thema analoge alternatieven aan bod. Er wordt vaak gezegd dat er geen analoge alternatieven zijn voor digitale systemen (zie bijvoorbeeld NCTV, 2019), maar bleek dat in deze casus ook het geval te zijn geweest? Waren er toch analoge alternatieven voorhanden en zo ja, welke dan?

4.3.1 Voorbereiding versus werkelijkheid

Naar aanleiding van de 112-storingen in 2012 is op basis van een onderzoek een brief door de minister van JenV naar de Tweede Kamer gestuurd, waarin onder andere een handelingsperspectief en de afspraken aangaande de communicatie naar burgers bij uitval van 112 zijn geformuleerd. Daarna heeft het ministerie van JenV in juni 2013 een brief gestuurd aan de korpschef van de politie, de voorzitters en directeuren veiligheidsregio's, de regionaal brandweercommandanten en directeuren van de Regionale Ambulancevoorziening (RAV). Het beschreven handelingsperspectief bevat drie mogelijkheden voor gevallen dat het alarmnummer tijdelijk niet of minder goed bereikbaar is:

> Wanneer er wordt gebeld met een vast toestel en er geen contact volgt, dient te worden gebeld met een mobiele telefoon
> Wanneer er wordt gebeld met een mobiele telefoon en er geen contact volgt, dient te worden gebeld met een vast toestel
> Indien alle telefoonvoorzieningen zijn uitgevallen, dient de burger naar het dichtstbijzijnde bureau/station van hulpverlening te gaan.

De politie en veiligheidsregio's moeten van het handelingsperspectief de te nemen maatregelen afleiden, waarbij het onduidelijk is welke stations van hulpverlening zij open moeten stellen. De veiligheidsregio's zijn niet betrokken geweest bij het opstellen van het handelingsperspectief en in de ODG en de genoemde brief staan geen afspraken over communicatie en de rolverdeling tussen het ministerie van JenV, de politie en de veiligheidsregio's. Het is echter van groot belang om hier afspraken over te maken, hebben de inspecties aangegeven, omdat het ministerie van JenV over de communicatie gaat, terwijl de andere organisaties verantwoordelijk zijn voor de uitvoering van de maatregelen. Ook zijn de uitvoeringsmaatregelen die bij het handelingsperspectief horen niet of nauwelijks geoperationaliseerd in afspraken en/of procedures voor de crisisorganisaties. Tot slot is niet geverifieerd door het ministerie van JenV of organisaties vervolg hebben gegeven aan de brief. Veiligheidsregio's hebben de brief van JenV van juni 2013 niet of nauwelijks in hun plannen verwerkt. Twee derde van de veiligheidsregio's heeft wel het risico op onbereikbaarheid van 112 in de risicoprofielen opgenomen, maar de daaropvolgende planvorming is per regio erg divers. Bij dit risico gaat het veelal om onbereikbaarheid van de regionale meldkamer; het niet bereikbaar zijn van de landelijke 112-alarmcentrale is niet of nauwelijks in de plannen van veiligheidsregio's opgenomen (Gezamenlijke Inspecties, 2020).

Op basis van de storing van 24 juni 2019 en de eerdere 112-storingen stellen de inspecties dat de incidenten de feilbaarheid van de techniek aantonen en dat "uitval van telecommunicatie zich altijd kan voordoen ondanks genomen maatregelen" (Gezamenlijke Inspecties, 2020). Op basis van het onderzoek van de Inspectie JenV kwamen zij tot de conclusie dat het bij het ministerie van JenV en veel veiligheidsregio's ontbrak aan kennis van richtinggevende documenten die gaan over de aanpak van een crisis veroorzaakt door onbereikbaarheid van 112. Verder bleek dat deze beleidsdocumenten niet zijn geïmplementeerd en geoperationaliseerd (Gezamenlijke Inspecties, 2020). Hoewel in de ODG scenario's waren opgesteld met bijbehorende maatregelen, erop gericht om meldingen zo snel mogelijk aan de betreffende hulpdienst door te geven, was niet de situatie opgenomen zoals die zich voordeed op 24 juni. Dan is het natuurlijk ook lastig om te handelen volgens een draaiboek. Desalniettemin werden genoemde maatregelen getroffen, zoals het openstellen van brandweerkazernes.

Verder bleken niet alle veiligheidsregio's op dezelfde manier te handelen tijdens de telefoniestoring. Zo informeerde de politie burgers via Twitter over de mogelijkheid om (nood)meldingen bij brandweerkazernes te kunnen doen, in overeenstemming met scenario vier van de ODG. Omdat echter niet alle veiligheidsregio's over plannen en/of procedures en een bijbehorend handelingsperspectief beschikten in relatie tot onbereikbaarheid van 112,

hadden enkele veiligheidsregio's de brandweerkazernes niet bezet, maar boden andere alternatieven aan. Een voorbeeld hiervan is het aanbieden van een regionaal telefoonnummer om in contact met de regionale meldkamer te komen. Uiteindelijk namen veiligheidsregio's wel enkele maatregelen onder meer zoals beschreven in de ODG en informeerden burgers over de storing en alternatieve mogelijkheden om hulpdiensten te bereiken (Gezamenlijke Inspecties, 2020). Deze casus laat zien dat de werkelijkheid zich altijd net even anders voordoet dan waarop is gerekend in de voorbereide plannen en scenario's. Ondanks dat hebben de veiligheidsregio's de plannen over het algemeen flexibel weten toe te passen zoals de ODG en de brief van het ministerie van 2013 beschrijven.

4.3.2 Gezamenlijke beeldvorming en de vraag wie de regie heeft

Bij de KPN-storing was het zo dat er geen duidelijk bron- en effectgebied was. Het betrof in die zin een 'gebiedsontbonden crisis', waarbij het gebied waarop de crisis betrekking had niet geheel duidelijk was, evenmin als de relatie tussen het domein en de oorsprong. Wanneer een incident betrekking heeft op verschillende regio's spreken we van het bovenregionale niveau[20], waarvoor juridisch weinig zaken specifiek zijn geregeld. Vooral de afstemming en crisiscommunicatie zijn dan belangrijke thema's: wie neemt de regie? Wat is de kernboodschap? Tijdens de KPN-storing namen de veiligheidsregio's, de RAV'en en de politie elk afzonderlijke maatregelen – dat terwijl de storing heel Nederland trof: was een landelijke aanpak dan niet logischer geweest (IFV, 2019c)?

Omdat naast het noodnummer ook het servicenummer 0900-8844 onbereikbaar was, wilde het ministerie van JenV burgers een breder handelingsperspectief bieden. Het ontbrak het ministerie echter aan regie over de aanpak van de crisis, doordat het wachtte met het versturen van een snelle en eenduidige boodschap. Aangezien een landelijke uniforme boodschap uitbleef, werden er veel verschillende regionale NL-Alert-berichten verstuurd (Gezamenlijke Inspecties, 2020). Menno van Duin stelde in het IFV-rapport naar de KPN-storing dat er sprake was van "een zeker gat tussen centrale aansturing die bij een nationale ramp of crisis in de rede ligt en de regionale aansturing die bij een lokale of regionale crisis gebruikelijk is". Bij een (dreigende) overschrijding van de regiogrens bij een ramp of crisis is er vaak sprake van onduidelijkheid en terughoudendheid, wat het lastig maakt om een goede samenwerking te bewerkstelligen of de regie (operationeel of bestuurlijk) bij een van de partijen te leggen (IFV, 2019c). Bij de KPN-storing kwam de afstemming tussen het Rijk en de veiligheidsregio's niet vanzelfsprekend en soepel tot stand. Meer eenduidigheid in de aanpak en vooral meer eenheid in de communicatie waren wenselijk geweest. Een gedeeld beeld was noodzakelijk om de handelingsperspectieven op elkaar af te kunnen stemmen, het GRIP-niveau overeen te laten komen en af te stemmen over crisiscommunicatie en over mogelijke scenario's. Om tot dit gedeelde beeld te komen, zou het goed geweest zijn als er meer onderlinge afstemming en afstemming met het Rijk was geweest (IFV, 2019c).

4.3.3 Geen analoge alternatieven?

Ondanks dat er geen draaiboeken waren die exact aansloten bij de situatie zoals die zich voordeed, zijn er geen grote incidenten voorgevallen tijdens de 112-storing. Met name het niet functioneren van het noodnummer 112 leidde tot de aantasting van een vitaal belang, maar aan de hand van eerder opgestelde plannen (zie voorgaande paragraaf) is geïmproviseerd om zo goed en zo kwaad als het ging toch burgers in nood te kunnen helpen. Hier is veelvuldig over gecommuniceerd via de verschillende kanalen van de veiligheidsregio's en via NL-Alerts (die al dan niet en met wisselende informatie aankwamen). Ondanks het feit dat er wat verwarring ontstond over de gecommuniceerde

[20] Zie voor een uitgebreide beschrijving van de verschillende niveaus, opschaling en coördinatiestructuren het rapport *KPN-storing: hoe bestuurlijk omgaan met gebiedsontbonden crises?* (IFV, 2019c).

boodschap, hebben burgers de betreffende alternatieve telefoonnummers en opengestelde brandweerkazernes en dergelijke weten te bereiken. Vaak wordt gesproken van de afwezigheid van analoge alternatieven bij uitval of verstoring van digitale vitale processen en systemen (zie bijvoorbeeld NCTV, 2019), maar enige nuchterheid is hier op zijn plaats. Er zijn zaken die beter of anders hadden gekund of zelfs anders hadden gemoeten, maar tijdens de 112-storing van 24 juni 2019 kon zonder werkend systeem toch aardig teruggevallen worden op alternatieven, zoals het openstellen van brandweerkazernes. De gevolgen bleven relatief beperkt en er werden al snel veel maatregelen genomen.

4.4 Tot slot

Tijdens de KPN-storing van 24 juni 2019 was het noodnummer enkele uren onbereikbaar. In tegenstelling tot de meeste andere casus in dit rapport, betrof dit een puur technische, niet-moedwillige verstoring, met de pech dat er tegelijkertijd een technische storing bij NL-Alert plaats had. Op een scenario waarbij zowel het noodnummer 112 als het servicenummer 0900-8844 onbereikbaar waren, was men bij de politie en de rijksoverheid niet voorbereid. Ook waren de veiligheidsregio's niet voorbereid op een dergelijke gebiedsontbonden crisis en ontbrak het aan centrale regie. Om beter voorbereid te zijn op de uitval van een (in dit geval telefonie)systeem, zou het natuurlijk helpen als er ook rekening wordt gehouden met een scenario als zodanig. Hierbij moet wel worden opgemerkt, dat de praktijk bijna altijd anders is dan de plannen, en dat de voorbereiding dus maar tot op zekere hoogte zinvol zal zijn. Het gaat erom dat veiligheidsregio's veerkrachtig te werk gaan en de plannen flexibel toe kunnen passen. Vooropgesteld moet worden dat, ondanks de gebrekkige voorbereiding en afstemming, hard is gewerkt door alle partijen om de effecten van de storing te ondervangen. Daarbij valt de creativiteit van de veiligheidsregio's op om toch beschikbaar te blijven voor de bevolking. De gevolgen zijn dan ook beperkt gebleven.

Belangrijkste bevindingen

1. Er wordt vaak gesteld dat er bij uitval van een digitaal systeem geen alternatieven zijn om op terug te vallen. Dit blijkt niet altijd op te gaan. Veiligheidsregio's en hulpdiensten bleken in deze casus behoorlijk vindingrijk.
2. De praktijk is bijna altijd anders dan die waar middels draaiboeken op is voorbereid. Bestaande plannen kunnen desalniettemin flexibel en op veerkrachtige wijze worden toegepast.
3. De KPN-storing laat zien dat ook niet-moedwillige cyberverstoringen hun weerslag op de samenleving kunnen hebben, al viel de maatschappelijke impact mee.
4. Veiligheidsregio's en crisispartners zijn vaak niet goed voorbereid op een gebiedsontbonden crisis, waarbij het niet altijd duidelijk is welke partij een regierol heeft. Bij crises waarbij de oorzaak bij een cyberverstoring ligt, lijkt dit nog sterker te gelden.

5 De cyberaanval op Universiteit Maastricht (2019)

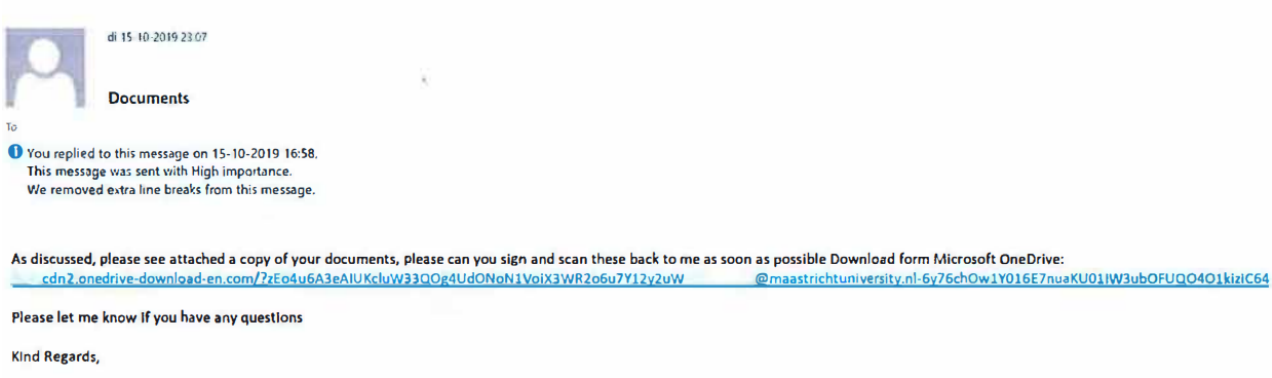
5.1 Inleiding

In dit hoofdstuk staat de cyberaanval op de Universiteit Maastricht (UM) in december 2019 centraal. Op kerstavond 2019 plaatste de universiteit een bericht op haar website met de melding dat de universiteit was getroffen door een “serieuze cyberaanval”. In het bericht stond dat vrijwel alle Windows-systemen waren geraakt. Om wat voor soort aanval het ging, werd niet vermeld. Wel werd gemeld dat er sprake was van een moedwillige aanval. Of de aanvallers toegang hadden tot onderzoeksgegevens werd op dat moment nog onderzocht door de UM. Met uitzondering van enkele laboratoria werden alle UM-gebouwen tot en met zondag 29 december gesloten (Maastricht University, 2019a). Deze cyberaanval bleek echter al iets meer dan drie maanden eerder te zijn begonnen doordat iemand op een phishing-link had geklikt.

Het hoofdstuk is gebaseerd op openbare bronnen en onderzoeksrapporten; daarnaast zijn twee interviews gevoerd. Ten eerste is gesproken met (zelfstandig) bestuurs- en communicatieadviseur Fons Elbersen, tevens voormalig directeur Marketing en Strategie van de Universiteit Maastricht. Tijdens het incident was hij als woordvoerder, adviseur van het College van Bestuur en lid van het Crisismanagement Team verantwoordelijk voor de communicatiestrategie van de universiteit. Verder is gesproken met Wim Biemolt, die als voorzitter van SURFcert betroken was bij de incidentrespons.

5.2 Feitenrelaas

Op 15 oktober klikt een student of medewerker met een account op het UM-netwerk op de ‘phishing-link’ in onderstaande e-mail (zie afbeelding 5.1). Via deze link wordt een Excel-document geopend dat malware bevat die de hackers toegang tot het netwerk van de UM geeft. Eén dag later klikt nog een student of medewerker op een vergelijkbare link. Via de infecties van deze twee systemen verkrijgen de aanvallers voor het eerst toegang tot een deel van het netwerk van de UM.


di 15-10-2019 23:07

Documents

To

You replied to this message on 15-10-2019 16:58.
This message was sent with High importance.
We removed extra line breaks from this message.

As discussed, please see attached a copy of your documents, please can you sign and scan these back to me as soon as possible Download form Microsoft OneDrive:
cdn2.onedrive-download-en.com/?zEo4u6A3eAIUKcluW33QOg4UdONoN1VoiX3WR2o6u7Y12y2uW @maastrichtuniversity.nl-6y76chOw1Y016E7nuaKU01IW3ubOFUQO4O1kiziC64

Please let me know if you have any questions

Kind Regards,

Afbeelding 5.1 De 'phishing-mail' die de hackers de eerste toegang tot het netwerk van de UM heeft verleend

In de weken na 15 oktober dringen de aanvallers handmatig het digitale netwerk verder binnen. De technische infrastructuur van de UM bestaat uit 1647 Linux- en Windows-servers; uiteindelijk worden 267 servers uit het Windows-domein door de aanvallers versleuteld. Het gaat om kritieke systemen voor de bedrijfsvoering van de universiteit, waaronder de e-mailservers, bestandsservers met onderzoeks- en bedrijfsvoeringgegevens én een aantal back-upservers (Maastricht University, 2020a). Deze versleutelingen waren mogelijk door de aanwezigheid van verouderde software – op enkele van de servers waren enkele updates niet uitgevoerd. Uiteindelijk weten de hackers op 21 november de volledige controle over het UNIMAAS-domein (het digitale UM-netwerk) te krijgen. Op 19 december, als de aanvallers bezig zijn met de voorbereidingen op de daadwerkelijke digitale gijzeling, merkt de antivirussoftware van de UM de hack op. De hackers krijgen hier een melding van en de-installeren snel de desbetreffende antivirussoftware; dit voorkomt dat de melding van de antivirussoftware de UM bereikt en stelt de hackers in staat tot het uitrollen van de Clop-ransomware. Die ransomware-aanval vindt in de avond van 23 december plaats.

De UM merkt de aanval vrijwel direct op en onderneemt actie. In de vroege nacht van 24 december wordt het gerenommeerde cybersecuritybedrijf Fox-IT ingeschakeld. Vanaf 16.00 uur is Fox-IT, dat zichzelf omschrijft als een 'digitale brandweer' (Delft.Business, 2020), op locatie aanwezig. Het UM-netwerk wordt 'op slot gegooid' door alle ICT-systemen offline te halen. Fox-IT biedt de universiteit ondersteuning op het gebied van crisismanagement, verricht forensisch onderzoek naar de toedracht en adviseert het crisisteam over het herstel van de ICT-systemen. In de avond van 23 december is het sectorale Computer Emergency Response Team (CERT), het SURFcert, al ingelicht door de UM.[21] Mede omdat de UM de hulp inschakelt van Fox-IT blijft de rol van SURFcert gedurende de casus relatief beperkt. Wel is SURFcert, dat de gehele crisis vanaf afstand opereert, in staat om het netwerkverkeer van en naar de universiteit te analyseren en vervolgens te kijken of dergelijke patronen ook bij andere onderwijsinstellingen zichtbaar zijn. Daarnaast zoekt SURFcert contact met andere CERT's voor aanvullende informatie. Er is bijvoorbeeld contact met het CERT dat betrokken is geweest bij de soortgelijke aanval op de Universiteit Antwerpen. Al deze informatie wordt vervolgens gedeeld met de UM. SURFcert ontvangt tevens informatie van de UM met betrekking tot de (technische) kenmerken van de aanval, zoals over de plaatsen in het netwerk waar de door de hackers gebruikte kwetsbaarheden zich bevinden. Deze informatie zet SURFcert vervolgens door in zijn netwerk met andere instellingen, die met deze informatie hun voordeel kunnen doen door bijvoorbeeld de desbetreffende kwetsbaarheden te versterken.

[21] Dit is het netwerk van aangesloten onderzoeks- en onderwijsinstellingen zoals universiteiten en hogescholen.

De UM besluit een multidisciplinair crisismanagementteam (CMT) in te richten, inclusief een crisiscommunicatieadviseur, mede op aanraden van Fox-IT. Omdat de woordvoerder van de UM op dat moment in het buitenland verblijft, geeft oud-medewerker Elbersen vanaf 26 december invulling aan deze functie. Uiteindelijk bestaat het CMT uit de vicevoorzitter van het College van Bestuur (CvB), de directeur ICT, de Chief Information Officer (CIO), de CISO, de directeur Bestuurlijk-Juridische Zaken (en tevens secretaris van het CvB), de adjunct-Bestuurlijk-Juridische Zaken, drie medewerkers van marketing en communicatie in afwisselende samenstelling en drie medewerkers van het 'quick-response team' van Fox-IT. Zo ontstaat een crisisteam dat specifiek is toegerust op de cybercrisis.

Op 27 december meldt de UM in een tweede update dat zij sinds maandag 23 december het slachtoffer is van een cyberaanval met 'gijzelsoftware' (de Clop-ransomware gemaakt door Grace_RAT/TA505). De UM heeft aangifte gedaan van de aanval bij de politie. Het CvB geeft aan de situatie te betreuren en stelt dat er op korte termijn zal worden gekeken of door de aanval benadeelde studenten of medewerkers tegemoet kunnen worden gekomen (Maastricht University, 2020b). De UM geeft vanaf 27 december dertien dagen lang dagelijks updates over de cyberaanval. Op 30 december werkt een team aan decryptie en herstel van het UM-netwerk. De eerste dagen worden de werkzaamheden georganiseerd rond drie thema's: (1) organisatie; (2) onderzoek en (3) herstel. De UM geeft voornamelijk invulling aan het organisatie- en het herstelteam. Het onderzoeksteam bestaat uit een combinatie van werknemers van de UM en experts van Fox-IT (Maastricht University, 2020a). Bij het herstel wordt prioriteit gegeven aan de voor studenten cruciale systemen, zodat hun onderwijs en toetsing zo spoedig mogelijk weer doorgang kunnen vinden. Op 30 december kondigt de universiteit in een update aan dat het onderwijs op 6 januari weer zal kunnen worden hervat. De circa 4000 herkansingen die in deze week staan gepland, zullen gewoon door gaan. Wel geeft de UM aan dat er een extra herkansingsmogelijkheid komt én dat men werkt aan een 'coulance-regeling' voor studenten die aantoonbaar zijn benadeeld door de aanval. De volgende dag treedt deze regeling in werking. Studenten kunnen zich hiervoor wenden tot een speciaal opgerichte commissie (Maastricht University, 2019b; 2019c).

Oost-Europese hackersgroepering Grace_RAT/ TA505
Naar alle waarschijnlijkheid zitten hackers van de Oost-Europese groepering Grace_RAT, ook wel bekend als TA505 achter de aanval, zo blijkt op 30 december. Deze groepering zou eerder de digitale systemen van de Universiteit Antwerpen en een Frans ziekenhuis plat hebben gelegd en is hoogstwaarschijnlijk verantwoordelijk voor de beruchte 'Clop-ransomware' die in minder dan één jaar tijd al meer dan 150 succesvolle cyberaanvallen heeft veroorzaakt (Pols, 2019).

Vlak na de jaarwisseling, op 2 januari, meldt universiteitsblad *Observant* dat de UM losgeld zou hebben betaald om de getroffen systemen weer werkend te krijgen (Observant, 2020). De UM reageert met de boodschap dat het voorlopig géén informatie zal verstrekken over de communicatie met de aanvallers; het onderzoek loopt nog en men is voornemens dit onderzoek op geen enkele wijze te schaden. Wel wordt aangekondigd dat de resultaten van het onderzoek zullen worden gedeeld in de vorm van een symposium genaamd 'lessons learnt' (Maastricht University, 2020g). Tijdens dit symposium op 5 februari blijkt dat het CvB van de UM op 29 december inderdaad heeft besloten losgeld te betalen aan de 'gijzelnemers van het UM-netwerk'. Over de eis van de aanvallers wordt lang en uitvoerig nagedacht en de overwegingen die spelen worden bij partijen zoals de politie en Fox-IT getoetst. Ook de Raad van Toezicht (RvT) wordt in deze afweging meegenomen; het Ministerie van Onderwijs, Cultuur en Wetenschap en de Onderwijsinspectie worden in kennis gesteld van het besluit. Om zeker te weten dat de UM ook daadwerkelijk contact heeft met de hackers, worden versleutelde bestanden opgestuurd naar de hackers met de

vraag om deze onversleuteld weer terug te sturen. Daarnaast wordt een klein bedrag aan Bitcoins overgemaakt om meer inzicht te krijgen in deze (voor de UM nieuwe) vorm van betaling.

Nadat deze stappen succesvol zijn doorlopen, besluit het CvB op 29 december om over te gaan op betaling. Het zou gaan om dertig Bitcoins, die op het moment van betaling een waarde van 197.000 euro vertegenwoordigen. Na deze betaling ontvangt de UM op 30 december de decryptie-sleutel van de hackers en kunnen de versleutelde servers weer worden vrijgegeven (Maastricht University, 2020a). De belangrijkste onderwijs-gerelateerde computersystemen zijn daardoor vanaf 2 januari, zij het in beperkte vorm, weer beschikbaar (Maastricht University, 2020g). Het OM is inmiddels een strafrechtelijk onderzoek gestart. Op 6 januari komen meerdere systemen weer online en wordt een groot deel van de normale werkzaamheden hervat. Tevens geeft de UM aan dat studenten en medewerkers in het algemeen begripvol en ontspannen hebben gereageerd op de situatie. Tweedejaarsstudenten psychologie zouden zelfs hebben geapplaudisseerd toen zij werden bijgepraat over de situatie tijdens hun college (Maastricht University, 2020b, 2020c, 2020g).

De crisis is in een fase gekomen waarin geen dagelijkse updates meer zullen worden gegeven, zo meldt de universiteit op 10 januari. Achter de schermen werken medewerkers nog steeds aan het operationeel krijgen van getroffen systemen, waarbij de prioriteit bij de belangrijkste centrale systemen ligt (Maastricht University, 2020d). Tijdens de eerstvolgende update, op 13 januari, geeft de universiteit aan dat steeds meer systemen worden vrijgegeven, maar dat het nog enkele weken kan duren voordat dit voor alle systemen geldt (Maastricht University, 2020e). Op 13 januari maakt de UM de datum voor het symposium 'lessons learnt' bekend. De bijeenkomst van 5 februari heeft, naast en in het verlengde van het delen van de recente ervaringen, als doel om een publieke discussie te starten over "de spanning die in de universitaire sector bestaat tussen de openheid en toegankelijkheid die de academie vraagt en de geslotenheid die de bescherming tegen cybercrime veronderstelt" (Maastricht University, 2020f). Tijdens het symposium wordt uitgebreid ingegaan op het verloop van de crisis, presenteert Fox-IT zijn bevindingen en beantwoordt vicevoorzitter dr. Nick Bos van het CvB vragen van aanwezige belangstellenden uit de academische en cybersecurity-wereld, alsmede vragen van journalisten. Met dit symposium is de crisis officieel ten einde, bijna vijf maanden na het moment waarop de hackers voor het eerst toegang weten te krijgen tot het digitale netwerk van de UM.

5.3 Beschouwing

In deze casus speelden verschillende kwesties een rol. Communiceren met door het incident gedupeerden, het delen van informatie via CERT's en het dilemma wel of geen losgeld te betalen om de systemen weer vrij te krijgen, stonden volgens ons centraal. Deze thema's zullen hieronder dan ook worden behandeld.

5.3.1 Communicatie over een cybercrisis

Goede communicatie met gedupeerden en de bredere bevolking behoort tot de kerntaken van crisismanagers (Boin et al., 2016). Die communicatie is 'a hell of a job', waarbij het lijkt alsof crisisbestrijders het eigenlijk nooit goed kunnen doen. Verwachtingen over de communicatie zijn hooggespannen; het oordeel luidt al snel dat er te weinig is gecommuniceerd of dat het ontbreekt aan duidelijk handelingsperspectief.

Eén van de vragen die speelt, is of de communicatie over een cybercrisis anders is dan communicatie over reguliere crises. Woordvoerder Fons Elbersen geeft aan dat de crisiscommunicatie bij de cyberaanval niet verschilde van de communicatie tijdens meer reguliere crises. De patronen zijn in essentie hetzelfde en zodoende is sprake geweest van een ‘normale’ communicatiestrategie, waarin generieke communicatieprincipes werden toegepast, zoals het bepalen van communicatiedoelen en het maken van een stakeholderanalyse. De UM wilde in de externe communicatie graag zelf de regie houden over het informatieproces. Dat deed zij door periodieke updates te geven en relevante doelgroepen te bedienen met statusupdates en handelingsperspectief. Daarbij was het streven volgens woordvoerder Elbersen: “Zorgen dat je niet door externe factoren in een reactieve modus terecht komt. Je moet zelf proactief regie proberen te houden op de informatievoorziening. Anders word je een speelbal.”

Ook koos de UM doelbewust voor een open, eerlijke en transparante manier van communiceren. Die aanpak was gebaseerd op de overtuigingen en waarden van de Maastrichtse universiteit, waaronder het belang van een open en transparante cultuur, haar publieke functie en maatschappelijke taak. Het trouw blijven aan die kernwaarden vormde de basis voor alle in- en externe communicatie. Het zou zorgen voor herkenbaarheid en volgens Elbersen leiden tot meer acceptatie en begrip van het publiek. Dat bleek, na wat initiële argwaan van de media (‘als ze zo open zijn, dan zal er wel iets mis zijn’), goed te werken.

Hoewel de cyberaanval was omgeven door veel inhoudelijke en technische (ICT-) onzekerheden, was er volgens de woordvoerder genoeg om wél over te communiceren. Er was namelijk “geen onzekerheid over het feit dat de digitale systemen plat lagen en geen onzekerheid over wie dat allemaal trof en in welke mate.” Mede daardoor koos de UM ervoor om vanaf het eerste moment open en eerlijk te zijn en het publiek mee te nemen in het proces. Wel bleek het nog een hele uitdaging om deze communicatieboodschappen de wereld in te krijgen. Benodigde systemen, zoals e-mail en het Intranet, waren door de aanval immers niet meer beschikbaar. De website van de UM was echter niet in handen gevallen van de hackers en was daardoor wel online gebleven. Zodoende heeft het CMT deze site, in combinatie met het wijdvertakte en fijnmazige sociale medianetwerk van de UM, als communicatie(distributie)kanaal kunnen inzetten (Inspectie van het Onderwijs, 2020).

De universiteit heeft tussen 24 december 2019 en 27 januari 2020 maar liefst 22 updates op haar website geplaatst, waarin uitgebreid werd gecommuniceerd over de verstoring(en), de getroffen maatregelen en de gevolgen voor studenten en medewerkers. Uiteindelijk werd tijdens een afsluitend symposium, waarbij zowel de directie van de UM, Fox-IT als andere externe actoren aan het woord kwamen, uitgebreid verslag gedaan van de crisis. Hier werden ook aanvullende vragen van de media beantwoord. Deze benadering pakte uitzonderlijk goed uit. De dagelijkse persvragen waarmee de universiteit tot dan toe werd bestookt, droogden na het symposium vrijwel volledig op.

5.3.2 Het delen van informatie via CERT’s

De UM koos zogezegd voor een open, eerlijke en transparante manier van communiceren. Een dergelijke strategie is niet alleen van belang voor de communicatie naar de buitenwereld, maar ook voor de communicatie over de (technische) kenmerken van de aanval. Bij dit incident vond dit contact plaats tussen de UM en haar CERT en het sectorale SURFcert, dat op zijn beurt weer contact had met het NCSC en met andere onderwijs- en onderzoeksinstellingen in binnen- en buitenland. Het delen van dergelijke technische informatie is belangrijk, omdat de instellingen waarmee de kennis wordt gedeeld, er vervolgens hun voordeel mee kunnen doen. Dit proces van informatiedeling staat of valt bij

de mate waarin en de snelheid waarmee de informatie openlijk wordt gedeeld. Gedurende een crisis kan echter druk komen te staan op deze informatiedeling,[22] en dat was ook het geval in deze casus. Tijdens de aanval bleek het voor SURFcert namelijk lastiger dan gehoopt om alle benodigde informatie tijdens het incident los te krijgen van de UM. Om dergelijke vertrouwelijke informatie ook tijdens de crisis te blijven delen, volstaat kennelijk niet alleen een netwerk met afspraken over het delen van informatie.

5.3.3 Losgeld betalen of niet

In elke crisis doen zich voor bestuurders en andere crisisfunctionarissen lastige dilemma's voor (Van Duin & Wijkhuijs, 2018). Een terugkerend dilemma bij cyberverstoringen, in het bijzonder bij (geslaagde) ransomware-aanvallen waarbij een poging wordt gedaan tot digitale gijzeling, gaat over het al dan niet betalen van losgeld. Hoe ging de universiteit hiermee om? De UM noemde de keuze om wel of niet te betalen zelf een 'duivels dilemma'. Hierbij speelden twee tegengestelde wensen: enerzijds de wens om criminelen niet te betalen (en een verdienmodel in stand te houden), en anderzijds de wens om de continuïteit van de universiteit te waarborgen. Dit is een dilemma waarbij het leidend principe doorgaans is: 'gij zult niet betalen aan criminelen' (hoewel vaak onduidelijk blijft wat er nu eigenlijk achter de schermen gebeurt). Daarnaast kleeft er altijd een risico aan het betalen van losgeld; er is bijna geen vorm van garantie of de encryptie-sleutel daadwerkelijk wordt geleverd na betaling én of de versleutelde data nog integer zijn na decryptie. Uiteindelijk heeft het dilemma ruim een week op tafel gelegen bij het CMT en het CvB. Over de eis van de aanvallers werd lang en uitvoerig nagedacht en de overwegingen die speelden werden bij partijen zoals de politie en Fox-IT getoetst. Volgens Elbersen koos de universiteit ervoor om dit dilemma niet als een puur zakelijke transactie te benaderen, maar eerder vanuit een ethisch perspectief. Hoe gaan we ons hier als universiteit toe verhouden? Welke waarden staan op het spel? Welke belangen vertegenwoordigen wij als universiteit?

In dit proces speelden de volgende aspecten een rol:

> de wens om de omvang en duur van verstoring van essentiële voorzieningen en diensten, zoals onderwijs- en onderzoeksactiviteiten, te beperken
> de omvang en duur van herstelwerkzaamheden aan geïnfecteerde systemen (de verwachte duur van herstel is enkele weken tot meerdere maanden)
> de kosten
> de wens om gemaakte keuzes transparant en open toe te lichten.

Uiteindelijk koos de UM na intern beraad en externe toetsing voor het betalen van het gevraagde losgeld van dertig Bitcoins (op dat moment 197.000 euro). Het betalen van het losgeld bood de grootste kans op spoedige hervatting van het onderwijs aan 19.000 studenten. De woordvoerder van de UM verwoordde het aldus: "Op het moment dat iemand je kind gijzelt en een pistool tegen zijn of haar hoofd houdt, is het lastig om vast te houden aan dat principe en te zeggen dat je niet gaat betalen". Tevens besloot het CvB op advies van het CMT om, op een moment dat de universiteit daar de regie over zou hebben, de gemaakte keuze toe te lichten. Uiteindelijk gebeurde dit tijdens het symposium. Door op een open en transparante manier te communiceren, wilde de UM de publieke discussie over het belonen van criminelen uit de taboesfeer halen en een debat opstarten over de dilemma's rond cybersecurity in het hoger onderwijs.

[22] Zie ook: https://www.scienceguide.nl/2020/01/maastricht-university-gaat-niet-uit-van-gerichte-aanval/.

5.4 Tot slot

De Universiteit Maastricht kreeg in december te maken met een serieuze cyberaanval; het soort risico waarvoor al enige tijd de nodige aandacht bestond in het hoger onderwijs (SURF, 2019). Zo werken hogescholen en universiteiten op het vlak van informatiebeveiliging en incidentrespons met elkaar samen en organiseren zij jaarlijks een cyberoefening. Al die inspanningen konden de cyberaanval op de universiteit echter niet voorkomen. Deze aanval kan beschouwd worden als een echte wake-up call: iets dergelijks kan elke organisatie in Nederland treffen. Op digitaal vlak gebeuren continu incidenten en in die zin is het haast onvermijdelijk dat het je een keer overkomt.

Het vinden van een goede balans tussen openheid en weerbaarheid is voor onderwijsinstellingen een permanente uitdaging. Iedereen (medewerkers, onderzoekers, studenten) heeft baat bij een snelle en laagdrempelige uitwisseling van data en eenvoudige toegang tot data en ICT-voorzieningen. Beveiligingsmaatregelen belemmeren de gewaardeerde openheid, toegankelijkheid en het gebruiksgemak. Bovendien valt niet alles te controleren. De circa 19.000 studenten en 4500 medewerkers van de UM gebruiken niet alleen computers van de universiteit, maar ook zelf meegenomen laptops en tablets. Op de computers van de universiteit heeft de UM controle (bijvoorbeeld als het gaat om de geïnstalleerde antivirussoftware en het uitvoeren van updates); die controle is er niet op de eigen laptops en tablets van medewerkers en studenten. Dit geldt waarschijnlijk voor de meeste hoger onderwijsinstellingen. Hoe ver reikt je verantwoordelijkheid voor informatiebeveiliging als universiteit? Wat mag je van medewerkers en studenten verwachten? Dit zijn ingewikkelde vragen waarop geen eenvoudige antwoorden zijn en die vrijwel permanent aandacht en bewustzijn vergen.

Organisaties zoals universiteiten die geen onderdeel zijn van de vitale infrastructuur hebben geen landelijk vastgelegde richtlijnen voor hun digitale informatieveiligheid. De verantwoordelijkheid voor een goede bedrijfsvoering en informatieveiligheid ligt bij de instelling zelf (Inspectie van het Onderwijs, 2020). Doordat universiteiten geen vitale sector zijn, kunnen zijn niet rekenen op bijstand van partijen zoals het NCSC. Het NCSC kwam tijdens de aanval wel op de radar, maar dan voornamelijk om informatie op te halen. De veiligheidsregio speelde in deze casus geen rol van betekenis. Vanuit de universiteit werd primair samengewerkt met politie en justitie. Belangrijke beslissingen, zoals die over het betalen van losgeld of de communicatiestrategie, zijn uiteindelijk allemaal door het CvB op voorspraak van het CMT genomen. De universiteit kon na de aanval terugvallen op haar generieke crisisorganisatie, maar schakelde ook het gerenommeerde adviesbureau Fox-IT in voor het doen van forensisch onderzoek en geven van advies over informatiebeveiliging.

De impact van de verstoring concentreerde zich op studenten en medewerkers van de UM. Zij kregen te maken met de nodige onzekerheid. ‘Gaan mijn tentamens nog door?’, ‘Kan ik straks nog bij mijn bestanden?’ en ‘Wat als ik hierdoor studievertraging op loop?’ waren vragen die veelvuldig werden gesteld. Wat opviel, was de open en transparante communicatie door de universiteit. Daarbij waren de eigen kernwaarden van de universiteit een belangrijke leidraad. Zo legde het CMT in een afsluitend symposium uitgebreid verantwoording af over gemaakte keuzes, inclusief het betalen van losgeld. Hoewel er de nodige kritiek op dat besluit was, kreeg de universiteit veel goodwill voor de afhandeling van het incident. De wijze van communiceren is er dan ook een uit het handboek crisiscommunicatie: proactief, voorspelbaar, open en strak geregisseerd (Seeger, 2006). Het laat zien dat de wijze waarop organisaties reageren op crises hen niet alleen kan breken, maar ook kan maken.

Belangrijkste bevindingen

1. De aanval op de Universiteit Maastricht kan worden beschouwd als een echte wake-up call: een dergelijke cyberaanval kan elke organisatie in Nederland treffen.
2. Ook bij cybercrises is goede crisiscommunicatie van belang. Een duidelijke strategie is daarbij waardevol – een open en transparante manier van communiceren over cyberverstoringen wordt zeer gewaardeerd én maakt het mogelijk om te leren van dergelijke casus. Daarbij blijft het onverminderd van belang relevante stakeholders van begin tot eind mee te nemen in dilemma's en afwegingen, zoals de Universiteit Maastricht uitmuntend deed.
3. Bij (geslaagde) ransomware-aanvallen waarbij een poging wordt gedaan tot digitale gijzeling, speelt het dilemma over het betalen van losgeld. Dit is een 'duivels dilemma' waarbij het doorgaans leidende principe 'gij zult niet betalen aan criminelen' onder druk kan komen te staan. Dat onderstreept het belang van goede communicatie: transparant blijven uitleggen en verantwoorden van gemaakte keuzes.
4. Tijdens cyberverstoringen is het delen van informatie binnen de eigen branche, bijvoorbeeld via sectorale CERT's, van belang. Het stelt andere organisaties in staat tijdig extra beveiligingsmaatregelen te nemen. Dit proces van informatiedeling kan tijdens een crisis echter onder druk komen te staan.
5. Het vinden van een goede balans tussen digitale openheid (gebruikersgemak, toegankelijkheid van ICT voorzieningen) en digitale weerbaarheid is voor organisaties zoals onderwijsinstellingen een permanente uitdaging.

6 Kwetsbaarheid in Citrix-software (2020)

6.1 Inleiding

Begin december 2019 ontdekte het bedrijf Citrix dat er sprake was van een kwetsbaarheid in zijn software. Deze software wordt door bedrijven en overheden in Nederland gebruikt om op afstand te kunnen werken. Het NCSC adviseerde op 18 december aan organisaties die Citrix gebruiken om de software uit te schakelen. Tegen die tijd waren de gevolgen van de kwetsbaarheid reeds zichtbaar bij het Medisch Centrum Leeuwarden en de gemeente Zutphen. Bij beide organisaties had een hackpoging plaatsgevonden en konden medewerkers niet meer thuiswerken. Citrix kwam nog diezelfde maand december met een tijdelijke oplossing, die echter niet afdoende bleek. In januari 2020 werd namelijk een zogeheten exploit-code openbaar gemaakt, waardoor hackers de kwetsbaarheid in de Citrix-systemen alsnog konden uitbuiten.

In dit hoofdstuk wordt de Citrix-casus beschreven en geanalyseerd op basis van openbare bronnen. Tevens heeft een uitvraag plaatsgevonden onder veiligheidsregio's via de landelijke werkgroep digitale ontwrichting en cyber. Aanvullend zijn er interviews afgenomen met twee functionarissen die betrokken waren bij de casus: de programmaleider informatie en innovatie van Veiligheidsregio Fryslân en een beleidsmedewerker crisisbeheersing van Veiligheidsregio Brabant-Zuidoost.

6.2 Feitenrelaas

Op 6 december 2019 informeert het beveiligingsbedrijf Positive Technologies het Amerikaanse bedrijf Citrix over een kwetsbaarheid in twee softwarepakketten (Netscaler ADC en Gateway server) (NOS, 2020a). Deze software wordt door organisaties wereldwijd gebruikt om vanaf afstand in te kunnen loggen op systemen van het werk. In Nederland wordt het ook veel gebruikt door verschillende bedrijven, overheden en organisaties. Door de kwetsbaarheid in de Citrix-software kunnen hackers inloggen op computersystemen die er gebruik van maken en deze systemen binnendringen, bijvoorbeeld voor het stelen van vertrouwelijke gegevens of het afpersen van de gebruikers / eigenaren van de systemen (NOS, 2020a). Elf dagen later, op 17 december, maakt Citrix de kwetsbaarheid publiekelijk bekend. Dit is ook het eerste moment dat het NCSC kennisneemt van de kwetsbaarheid (Nieuwsuur, 2020a). Bij het bekendmaken van de kwetsbaarheid adviseert Citrix zijn gebruikers om een aantal wijzigingen aan te brengen in de softwarepakketten om de kans op misbruik te verkleinen (Digital Trust Centrum, 2020). Het betreft een tijdelijke oplossing, waarvan later blijkt dat die niet voor elke versie van de Citrix-software effectief is (Wassens, 2020b). De volgende dag publiceert het NCSC op zijn website een eerste beveiligingsadvies voor de Citrix-software met het label 'medium/high'.[23] Dit geeft aan dat er een reële kans is

[23] Het NCSC stelt beveiligingsadviezen voor kwetsbaarheden en dreigingen op basis van twee elementen op: de kans op misbruik en de impact van mogelijk misbruik. Zowel de kans als de impact worden gecategoriseerd als low, medium of

op misbruik met een hoge impact. Wanneer Positive Technologies op 23 december bekend maakt dat 80.000 bedrijven in 158 landen risico lopen om te worden gehackt, wordt het advies door het NCSC op 24 december aangescherpt naar ‘high/high’, oftewel een grote kans op misbruik met een grote impact (Grapperhaus & Knops, 2020b).

Begin januari blijkt dat 700 Nederlandse bedrijven met Citrix-systemen gevaar lopen, doordat een zogeheten exploitcode openbaar zal worden gemaakt (NOS, 2020c).[24] Het NCSC informeert organisaties binnen de rijksoverheid en vitale partners over de ontwikkelingen en adviseert om de tijdelijke maatregelen van Citrix over te nemen. Daarnaast verzoekt het NCSC de CIO-Rijk om de Chief Technology Officers (CTO) en CISO binnen alle departementen aanvullend te informeren. Twee dagen later, op 11 januari 2020, wordt de exploitcode daadwerkelijk openbaar. Het NCSC adviseert opnieuw de maatregelen van Citrix op te volgen (Grapperhaus & Knops, 2020a) en constateert op 13 januari dat er nog steeds kwetsbare Citrix-systemen zijn in Nederland (Grapperhaus and Knops 2020b). Het NCSC plaatst op zijn website en sociale media (zie afbeelding 6.1) een waarschuwing die wordt gedeeld door de NCTV. Op dat moment neemt de aandacht voor de Citrix-kwetsbaarheid in de landelijke media toe.

Afbeelding 6.1 Tweet van Pieter-Jaap Aalbersberg (NCTV) over het beveiligingslek bij Citrix

Op 15 januari doen de gemeente Zutphen en het Medisch Centrum Leeuwarden (MCL) melding van een hackpoging op hun netwerken. Door beperkte capaciteit bij het systeembeheer, het op korte termijn vervangen van Netscaler en het feit dat de kwetsbaarheid nog niet actief werd misbruikt, besloot de gemeente Zutphen om de tijdelijke maatregelen pas op 13 januari door te voeren. Een dag later voerde de gemeente een controle uit om de effectiviteit van de maatregelen te testen (Gemeente Zutphen, 2020), waaruit op 15 januari bleek dat de Netscaler was gehackt.

Vanaf het bekendmaken van de kwetsbaarheid in december, informeert het Z-CERT (het expertisecentrum op het gebied van cybersecurity in de zorg) zorgaanbieders actief over de Citrix-kwetsbaarheid, inclusief het handelingsperspectief. De zorgaanbieders blijven echter zelf verantwoordelijk voor hun ICT en daarbij ook voor het doorvoeren van de tijdelijke maatregelen van Citrix (Bruins, 2020). Net als de gemeente Zutphen heeft ook het MCL de tijdelijke maatregelen van Citrix niet tijdig doorgevoerd. Op 15 januari maakt het MCL bekend dat ook daar een hackpoging heeft plaatsgevonden (Bruins, 2020). Zowel de gemeente Zutphen als het MCL leggen de Citrix-systemen stil naar aanleiding van de

high. In totaal kunnen er dus negen verschillende beveiligingsadviezen worden gegeven. Zie ook https://www.ncsc.nl/actueel/beveiligingsadviezen.

[24] Een exploitcode is software die kwaadwillenden kunnen creëren om kwetsbare systemen te detecteren en deze uit te buiten voor hun eigen belang.

hackpoging (Nieuwsuur, 2020b). Daarmee is het systeem niet meer beschikbaar voor medewerkers, wat betekent dat de artsen en patiënten van het MCL niet bij elektronische patiëntendossiers kunnen en dat het dataverkeer met andere ziekenhuizen wordt gehinderd (Nieuwsuur, 2020b). Het MCL geeft aan dat er geen toegang is verkregen tot de interne systemen en dat de patiëntveiligheid niet in gevaar is geweest (Bruins, 2020). Ook de gemeente Zutphen (2020) geeft aan dat er geen persoonsgegevens buit zijn gemaakt.

Op 16 januari zijn er nog 240 Nederlandse organisaties met Citrix-systemen die geen maatregelen hebben genomen (Wassens, 2020b). Op dat moment is er nog steeds geen sluitende oplossing aangedragen door Citrix en is het onduidelijk of de tijdelijke maatregen helpen. De NCTV schaalt interdepartementaal op (Grapperhaus & Knops, 2020b) en het NSCS adviseert op 17 januari, op aanraden van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD), de rijksoverheid en andere vitale organisaties om de Citrix-systemen uit te schakelen tot er een definitieve oplossing is (Grapperhaus & Knops, 2020b). Door het uitschakelen van Citrix kan personeel voorlopig niet thuiswerken (Wassens, 2020a), waarop men massaal naar het kantoor gaat om te kunnen werken. Volgens een nieuwsbericht is zelfs sprake van ‘Citrix-files’ op Nederlandse snelwegen (NU.nl, 2020b).

Op 20 januari, meer dan een maand na de bekendmaking van de kwetsbaarheid, stelt Citrix beveiligingspatches beschikbaar voor een deel van de kwetsbare softwarepakketten en adviseert op zijn website deze door te voeren (Grapperhaus & Knops, 2020a). Op 20 januari voeren de gemeente Zutphen en het MCL deze definitieve oplossing door en kunnen daarmee hun Citrix-systemen weer inschakelen (Bruins, 2020; Gemeente Zutphen, 2020). Daarnaast publiceert het NCSC (2020b) op 20 januari een stroomschema dat kan worden gebruikt om een risicoafweging te maken. Organisaties die de tijdelijke maatregelen van Citrix niet vóór 9 januari hebben doorgevoerd, wordt geadviseerd een herstelplan op te stellen, omdat er een grote kans is dat kwaadwillenden toegang hebben gekregen tot hun systemen. Wanneer de tijdelijke maatregelen wel zijn ingevoerd voor 9 januari, wordt het advies gegeven de patches te installeren (NCSC, 2020b). Nog niet voor elke versie van Citrix zijn dan patches beschikbaar, maar op 25 januari is dat wel het geval (Grapperhaus & Knops, 2020b).

In totaal blijken er 29 datalekken te zijn gemeld bij de Autoriteit Persoonsgegevens (Metselaar, 2020). Daarnaast zijn er in februari nog zeventig organisaties die hun Citrix-systemen niet (juist) hebben geüpdatet en daardoor kwetsbaar zijn voor digitaal misbruik (RTL Z, 2020). Uit de evaluatie van het COT (2020) blijkt dat de impact van de Citrix-kwetsbaarheid voor de meeste organisaties beperkt is gebleven. Er zijn geen meldingen dat er daadwerkelijk systemen zijn gehackt en gegevens zijn gestolen. Door het afsluiten van de Citrix-systemen kon er echter niet meer worden thuisgewerkt, met files op de Nederlandse autowegen tot gevolg. Daarnaast waren (delen van) systemen van verschillende organisaties tijdelijk niet toegankelijk, waardoor de informatie-uitwisseling binnen sommige organisaties was verhinderd. Zo was bijvoorbeeld het elektronisch patiëntendossier niet langer inzichtelijk voor patiënten van het MCL (NU.nl, 2020a). Ook andere zorginstellingen zoals ambulancediensten en de GGD ervoeren problemen, doordat systemen niet toegankelijk waren of medewerkers niet bij noodzakelijke informatie konden, zoals blijkt uit de uitvraag onder veiligheidsregio’s.
Het is echter nauwelijks uit te sluiten dat hackers daadwerkelijk gebruik hebben gemaakt van de kwetsbaarheid in het systeem, bijvoorbeeld door onopgemerkt ‘backdoors’ te plaatsen waarmee zij ongezien toegang hebben tot bepaalde systemen. Op 1 juli publiceert De Volkskrant dan ook een artikel met de titel: “Half jaar na Citrix-crisis zijn 25 Nederlandse organisaties gehackt. En ze weten zelf van niets” (Modderkolk, 2020). In het artikel wordt op basis van onderzoek van Fox-IT geconcludeerd dat hackers en/of spionagegroepen ondanks

de patch van Citrix nog steeds toegang hebben tot de interne systemen van zeker 25 Nederlandse organisaties. Volgens Fox-IT waren hackers, waaronder Iraanse en Chinese spionagegroepen, in staat een ‘extra sleutel van de voordeur’ te maken, waardoor zij (onbevoegd) toegang tot interne systemen konden houden. En omdat de hackers de sleutel hebben, helpt het niet om de deur op slot te doen middels het doorvoeren van beveiligingsupdates.

6.3 Beschouwing

De casus is voor instanties als het ministerie van Justitie en Veiligheid (JenV), de IBD en VNG aanleiding geweest om nader onderzoek te doen. Mede op basis van deze onderzoeken focussen we ons in onze beschouwing op de volgende thema’s: de maatschappelijke impact, de verantwoordelijkheden van betrokken organisaties en de rol van de veiligheidsregio.

6.3.1 Maatschappelijke impact

Nederland staat in de top vijf van landen die Citrix het meest gebruiken; begin januari liepen dan ook ruim 700 Nederlandse organisaties gevaar door de kwetsbaarheid bij Citrix (NOS, 2020c). Volgens IT-expert Ralph Moonen betrof dit een “dwarsdoorsnede van BV Nederland en de overheid” en liepen onder andere de servers van een regionale luchthaven, beursgenoteerde bedrijven, overheden en ziekenhuizen gevaar (Nieuwsuur, 2020b). Succesvolle hacks bij dergelijke organisaties kunnen op diverse terreinen impact hebben, waaronder dat van de bedrijfscontinuïteit, de economie en de maatschappij. Via kwetsbaarheden in software kunnen hackers inbreken op de interne systemen van organisaties en zo belangrijke gegevens buitmaken, zoals persoons- of financiële gegevens.

De Citrix-kwetsbaarheid stelde hackers in principe ook in staat om ransomware te installeren (Kerstens & Mol, 2020), maar voor zover bekend is dat in Nederland niet gebeurd. Naast de ongemakken van het niet thuis kunnen werken en de verhindering van informatie-uitwisseling lijkt de impact van de Citrix-kwetsbaarheid dan ook mee te vallen. Wél heeft zich in deze casus nog het gevolgrisico voorgedaan van onbevoegde toegang tot ICT-voorzieningen en data, waardoor hackers en spionagegroepen ondanks de beveiligingspatch van Citrix toegang hebben tot in elk geval 25 Nederlandse organisaties.

6.3.2 Betrokken partijen

Burgers, bedrijven en (overheids)instanties hebben verschillende rollen op het gebied van cybersecurity. Het ontbreekt deze partijen veelal aan een overzicht van de verdeling van de verantwoordelijkheden op dit gebied (Veiligheidsberaad, 2018). Aan de hand van deze casus schetsen we een beeld van de betrokken partijen, de rol die zij speelden en hun verantwoordelijkheden.

Bij de Citrix-casus werd de complexiteit mede bepaald door het grote aantal betrokken actoren. Daarom bespreken we nu de (belangrijkste) partijen die een rol speelden:

> Citrix: een Amerikaanse softwareleverancier.
> Private cybersecuritybedrijven, zoals Positive Technologies en Fox-IT. Deze bedrijven merkten kwetsbaarheden in Citrix-software op en waarschuwden onder andere de softwareleverancier over de risico’s.

- NCSC: Het Nationaal Cyber Security Centrum is hét centrale informatieknooppunt en expertisecentrum voor cybersecurity in Nederland.[25] Het NCSC informeert en adviseert overheden en met name de vitale infrastructuur over dreigingen of incidenten in informatiesystemen en ondersteunt deze in het treffen van maatregelen. Alleen het bevoegd gezag (bijvoorbeeld een departementale toezichthouder) kan echter toezichthouden en handhaven ten aanzien van aanbieders van essentiële diensten en digitale dienstverleners. Het NCSC kan organisaties dus niet dwingen hun systemen te updaten. In deze casus hield het NCSC, conform zijn wettelijke taak, zich bezig met monitoring en advisering; zo hield men contact met de rijksoverheid en vitale partners om adviezen en updates te geven.
- CIO-Rijk: de CIO-Rijk van het ministerie van Binnenlandse Zaken stelt kaders voor het bevorderen en vormgeven van informatisering en ICT binnen de rijksoverheid en zelfstandige bestuursorganen. In deze casus verzocht de CIO-Rijk om de CTO en CISO's binnen het Rijk aanvullend te informeren over de Citrix-kwetsbaarheid (Grapperhaus & Knops, 2020b).
- Landelijk Operationeel Coördinatiecentrum (LOCC): het LOCC levert operationeel advies op bovenregionaal en nationaal niveau ten behoeve van bestuurlijke besluitvorming. In deze casus heeft het LOCC via de vakgroep Informatieveiligheid de veiligheidsregio's gevraagd om de gevolgen van de Citrix-kwetsbaarheid in kaart te brengen.
- Getroffen organisaties: gebruikers van Citrix- software hebben een eigen verantwoordelijkheid voor het up-to-date houden van software en zijn daarnaast verantwoordelijk voor de incidentrespons (eventueel bijgestaan door instanties als de IBD of Z-CERT).

Uit de casus komt naar voren dat private partijen, zoals het beveiligingsbedrijf Positive Technologies, een rol hebben gespeeld in het achterhalen van de kwetsbaarheid in de software. Deze partijen trokken vervolgens aan de bel en waarschuwden de softwareleverancier – op eigen initiatief en niet vanuit een bepaalde formele verantwoordelijkheid. Citrix informeerde hierop zijn klanten en trad met hen in overleg om het probleem te verhelpen. In Nieuwsuur gaf Citrix aan dat het een gangbare procedure is om de gebruikers van Citrix "zo snel mogelijk waarschuwen voor de kwetsbaarheid en hen helpen dit te verhelpen" (Nieuwsuur, 2020c). Ook nam Citrix naar eigen zeggen contact op met het NCSC. De tijdelijke oplossing van Citrix in december 2019 bleek niet toereikend te zijn (IBD, 2020a); doordat de kwetsbaarheid bekend was, konden kwaadwillenden een exploitcode creëren om de kwetsbaarheid uit te buiten (Nieuwsuur, 2020c).

Cybersecurityexpert Ronald Prins stelde dat het normaal is dat een bedrijf een afspraak maakt met de beveiligingsonderzoeker die de kwetsbaarheid probeert te achterhalen om een definitieve oplossing te kunnen vinden vóór de desbetreffende kwetsbaarheid bekendgemaakt wordt. In dit geval presenteerde Citrix een halve oplossing en maakte de kwetsbaarheid bekend, aldus Prins (IBD, 2020a; Nieuwsuur, 2020c). Daardoor waren klanten weliswaar op de hoogte van de kwetsbaarheid, maar waren ze daar slechts ten dele tegen beschermd. Bovendien bood het kwaadwillenden de gelegenheid er misbruik van te maken. Het softwarebedrijf heeft voor zo ver bekend géén formele verantwoordelijkheid voor het notificeren van klanten en/of de verplichting om klanten actief te wijzen op het doorvoeren van beveiligingsupdates. Eerder lijkt er sprake te zijn van gangbare procedures (waarover ook wisselend wordt gedacht, blijkens de uitspraken van Prins) en de opvattingen die de softwareonderneming aangaande de eigen verantwoordelijkheden heeft.

[25] De wettelijke taken van het NCSC op het gebied van cybersecurity worden sinds 9 november 2018 geregeld via de Wet beveiliging netwerk- en informatiesystemen (Wbni).

De problemen met de software troffen een groot aantal publieke en private organisaties. Zowel in de Pulsar Secure VPN als bij Citrix liepen eindgebruikers die niet tijdig de beveiligingsmaatregelen en -updates hadden doorgevoerd, gevaar. Al deze partijen zijn zelf verantwoordelijk voor informatieveiligheid en ICT-beveiliging, wat ook werd onderstreept door toenmalig minister Bruins van Medische Zorg en Sport (2020) tijdens het beantwoorden van Kamervragen naar aanleiding van de hack bij het MCL. Volgens de minister zijn zorginstellingen “onder alle omstandigheden” zelf verantwoordelijk voor hun ICT en informatieveiligheid: het is aan hen om afdoende maatregelen te treffen en noodzakelijke updates door te voeren. In de praktijk is dat uitermate weerbarstig, zo blijkt uit het Cybersecuritybeeld Nederland (2020).

COT Leerevaluatie respons Citrix (2020)
In opdracht van de NCTV voerde het COT een snelle evaluatie uit van de respons op Citrix. Hieruit blijkt dat bij veel organisaties de vraag leeft hoe het Landelijk Dekkend Stelsel functioneert, ook in relatie tot de verschillende rollen en de wettelijke mandaten. Daarbij spelen vooral vragen met betrekking tot:

> ‘het wel of niet mogen delen’ van informatie (met name buiten de vitale sector)
> de vraag wie de nationale regie voert en
> wat de rol is van de sectorale computercrisisteams.

De discussie gaat vooral over specifieke informatie, zoals de onderbouwing van de duiding, technische informatie en/of informatie over bedreigde / kwetsbare organisaties. Meer algemene risico-informatie kan volgens betrokkenen breed worden gedeeld.

Binnen sectoren zien organisaties graag een nauwere sectorale samenwerking tussen de verschillende ISAC’s en het NCSC. De verwachtingen van de verschillende onderdelen van het stelsel komen niet altijd overeen met de realiteit: het stelsel is in opbouw. De rol in de koude fase (voorbereiding) en lauwe fase (risico’s) is helder: respectievelijk het voorbereiden en opbouwen van een gemeenschap en het delen van (risico)informatie. Het is vooral belangrijk om duidelijk te zijn over de rol in de ‘warme’ fase: als er daadwerkelijk problemen zijn, wat mogen organisaties dan verwachten qua snelheid en type informatie en door wie wordt deze informatie gedeeld?

Uit de evaluatie blijkt tevens dat er vragen waren over de opschaling van de crisisstructuur bij een ICT-crisis. Op welke structuur dienen de organisaties terug te vallen? Was hier überhaupt sprake van een crisis en wie is verantwoordelijk voor deze duiding? Daarbij gebeurde het dat organisaties hun eigen crisisstructuur opschaalden en aansluiting zochten met andere crisisteams en anderen de Citrix-kwetsbaarheid als ‘business as usual’ afhandelden.

De media-aandacht werd daarbij als escalerende factor genoemd. De media zorgde er volgens velen voor dat de situatie rondom Citrix ‘groter’ werd dan dat zij feitelijk was. De ontstane dynamiek zorgde voor bestuurlijke druk binnen organisaties; er werd uitgeschakeld omdat men – ondanks eigen technische inschattingen – niet het risico durfde te nemen om achteraf uit te moeten leggen waarom een ‘advies van de overheid’ niet is opgevolgd.

De discussie richt zich in de casus ook op de rol van het NCSC: had deze partij niet meer kunnen doen, met name op het gebied van informatievoorziening en door bijstand te verlenen aan niet-vitale sectoren? Nadat het NCSC op de hoogte was gesteld van het risico, informeerde het weliswaar zijn eigen ‘wettelijke achterban’, maar die informatie werd niet gedeeld binnen andere CERT-netwerken, zoals de zorg en het onderwijs. Die sectoren

hadden mogelijk wel baat gehad bij dergelijke informatie. Uit de Kamerbrief van 23 januari 2020 van de ministers van JenV (Grapperhaus) en Binnenlandse Zaken (Knops) over de Citrix-kwetsbaarheid (Grapperhaus & Knops, 2020b) blijkt dat het NCSC vanaf 17 december permanent heeft gemonitord, technisch onderzoek heeft uitgevoerd, advies heeft uitgebracht en bijstand heeft verleend aan de rijksoverheid en vitale sectoren. Ook speelde het NCSC een rol in de verspreiding van beveiligingsadviezen onder organisaties buiten de doelgroep van het NCSC: dergelijke adviezen worden standaard op de website van het NCSC geplaatst voor een breder publiek. Daarmee lijkt het NCSC in elk geval te hebben voldaan aan zijn wettelijke verplichtingen, waaronder het informeren en adviseren over enerzijds dreigingen en incidenten en anderzijds over beveiligingsmaatregelen van de rijksoverheid en vitale partijen op het gebied van informatiesystemen. Het NCSC kan bedrijven en zorginstellingen echter niet dwingen hun systemen te updaten omwille van de informatieveiligheid. In de woorden van minister Grapperhaus: "Waar het mij om gaat, is dat het NCSC geen doorzettingsmacht heeft. Dus ze kunnen niet tegen bedrijf X, een heel groot bedrijf dat een rol speelt in de vitale infrastructuur, zeggen: en nu gaat u het doen, u krijgt een aanzegging en anders komen we het over een maand voor u doen. Die bevoegdheid moet er komen" (Tweede Kamer, 2019). Hiermee zinspeelt Grapperhaus op een uitbreiding van de bevoegdheden van het NCSC, in lijn met het pleidooi van de WRR (wat betreft de invoering van een digitale brandweer).

6.3.3 De vitale infrastructuur

Naar aanleiding van de gebeurtenissen in deze casus is discussie ontstaan over de vraag welke sectoren tot de vitale infrastructuur behoren. Elektriciteit, toegang tot internet, drinkwater en betalingsverkeer behoren tot de essentiële voorzieningen voor de samenleving en behoren tot de zogenoemde vitale infrastructuur.[26] Vitale sectoren staan in nauw contact met het NCSC en de NCTV; de betrokken publieke en private organisaties binnen de vitale infrastructuur wisselen met elkaar dreigingsinformatie en beveiligingsmaatregelen uit. Ook waarschuwen zij elkaar over kwetsbaarheden en bij acute dreigingen. In het overzicht van vitale processen van de NCTV ontbreken ziekenhuizen, zorginstellingen, universiteiten en grote bedrijven zoals Shell, Ahold, Heineken of Philips. Ook veiligheidsregio's worden niet gezien als vitale partners. De veiligheidsregio's hebben daardoor tijdens het Citrix-incident geen directe informatie gekregen van het NCSC.

Naast de veiligheidsregio's zijn ook andere instanties die buiten de vitale infrastructuur vallen, zoals gemeenten en ziekenhuizen, door het NCSC niet één op één benaderd en gewaarschuwd over de risico's in de Citrix-software. Waren zij wel onderdeel van de vitale infrastructuur geweest, dan waren zij eerder op de hoogte gesteld en in de gelegenheid geweest noodzakelijke maatregelen door te voeren, zo is nu de veronderstelling. Het zoveel mogelijk delen van relevante informatie binnen sectorale CERT-netwerken kan tijdwinst opleveren en partners in staat stellen passende maatregelen te treffen en/of gezamenlijk tot oplossingen te komen. Volgens IT-expert Ralph Moonen is het tijd om het begrip 'vitale infrastructuur' te gaan oprekken, zoals hij heeft verteld in Nieuwsuur. Volgens SP-Kamerlid Hijink kan de samenleving het zich niet veroorloven als afdelingen spoedeisende eerste hulp uitvallen doordat digitale systemen niet werken, dus "dan moet dat een vitale sector zijn" (Nieuwsuur, 2020b). In gesprek met een respondent van een veiligheidsregio wordt opgemerkt dat (digitale) ontwrichting van bedrijven ook maatschappelijke impact kan hebben. "De Citrix-problematiek maakte nogmaals duidelijk dat incidenten bij organisaties die niet als vitaal zijn aangemerkt tot overlast of onrust kunnen leiden" (Ministerie van Justitie en Veiligheid, 2020).

[26] De beoordeling wat vitale sectoren zijn wordt gemaakt door vakdepartementen.

Landelijk Dekkend Stelsel
Het Landelijk Dekkend Stelsel is een stelsel van samenwerkingsverbanden op het gebied van cybersecurity. De netwerken zijn ingericht voor het efficiënter en doeltreffender delen van informatie tussen publieke en private partijen. Denk aan: sectorale CERT's en het Digital Trust Center. Het NCSC treedt op als centraal informatieknooppunt. Het stelsel is onderdeel van het programma Nederland Digitaal Veilig.[27]

Inmiddels is per januari 2020 middels een ministeriële regeling onder de Wet beveiliging netwerk- en informatiesystemen (Wbni) een grondslag geboden voor intensievere informatiedeling tussen het NCSC en vier sectorale CERT's: zorg, gemeenten, waterschappen en onderwijs.

6.3.4 Wat doen veiligheidsregio's?

Meerdere veiligheidsregio's volgden zelf de berichtgeving op de websites van Citrix en het NCSC. Een aantal veiligheidsregio's gaf aan tevreden te zijn over de communicatie vanuit Citrix en het NCSC. Andere regio's vonden echter dat de berichten van het NCSC en van Citrix tegenstrijdig waren, met name over het wel of niet uitzetten van de Citrix-systemen. Een veiligheidsregio gaf ook aan dat zij tegenstrijdigheden ervoeren in de berichten van het NCSC. Daarnaast won een aantal veiligheidsregio's advies in bij andere cybersecurity-experts die wéér anders adviseerden. Een tweetal veiligheidsregio's heeft op basis van deze externe adviezen ervoor gekozen Citrix niet af te sluiten. Al deze verschillende adviezen leidden tot onduidelijkheid bij veiligheidsregio's en meerdere heroverwegingen van de te nemen acties. Veiligheidsregio's hebben ook onderling contact met elkaar gehad, bijvoorbeeld via de Whatsappgroep van de vakgroep informatieveiligheid. Maar, zo gaf een respondent aan: "elke regio pakt het op z'n eigen manier op of duidt de urgentie/vraag anders." Een andere respondent gaf aan dat er in kleine clubjes contact was geweest, maar dat er geen centrale informatie beschikbaar was.

In de Citrix-casus zijn een aantal veiligheidsregio's, doordat zij zelf gebruikmaken van de software, op hun hoede wat betreft de interne informatieveiligheid. Deze veiligheidsregio's gaven aan de berichtgeving van het NCSC standaard te monitoren. Hierdoor waren zij in staat adequaat te reageren op de Citrix-kwetsbaarheid. Andere veiligheidsregio's gebruiken géén Citrix en hoefden daarom intern geen actie te ondernemen. Er waren ook enkele veiligheidsregio's die aangaven dat zij pas in januari op de hoogte raakten van de kwetsbaarheid bij Citrix vanwege de media-aandacht die de zaak kreeg in Nederland. Veiligheidsregio's beschikten tijdens de gebeurtenissen niet over een gemeenschappelijk beeld van de situatie en over eventueel benodigde acties. Een dergelijk beeld, gevormd op basis van een gemeenschappelijke informatiepositie, kan waardevol zijn – juist in situaties die landelijk en bij een groot aantal publieke en private organisaties spelen. Het LOCC, maar ook het recent opgerichte Information Sharing and Analysis Center (ISAC) voor de veiligheidsregio's, kan hierin in de toekomst een rol vervullen.

Zoals uit de discussie omtrent vitale partners al blijkt, kunnen ook verstoringen in ICT-voorzieningen bij niet-vitale bedrijven en organisaties maatschappelijke effecten sorteren. Om als veiligheidsregio de cyberrisico's in beeld te hebben, is het nodig om vitale en niet-vitale organisaties zoals BRZO-bedrijven in de regio te kennen. De veiligheidsregio kan net als bij niet-digitale crises een platform zijn om crisispartners en essentiële informatie bijeen te brengen (IFV, 209b). De vraag is daarbij wel: ben je als veiligheidsregio proactief? Of vertrouw je erop dat (crisis)partners en bedrijven naar de veiligheidsregio toe komen wanneer er sprake is van een hack met maatschappelijke impact? In deze casus deed een

[27] https://magazines.ncsc.nl/ncscmagazine/2019/01/lds

aantal veiligheidsregio's een belronde langs de crisispartners en gemeenten in de regio om te inventariseren wat de effecten van de Citrix-kwetsbaarheid waren. Zo creëerden zij voor zichzelf een beeld van mogelijke gevolgen en effecten in hun regio. Andere regio's hebben dit (soms bewust) niet gedaan.

6.4 Tot slot

De problemen met de Citrix-software trof een groot aantal organisaties (bedrijven, gemeenten, departementen, ziekenhuizen). De kwetsbaarheden hadden niet alleen direct merkbare gevolgen, zoals een verstoring van bedrijfsprocessen en voorzieningen, maar ook niet direct zichtbare gevolgen, zoals spionage door onbevoegde toegang tot ICT-voorzieningen en data. In deze casus speelde nadrukkelijk de vraag wie, op het gebied van informatiebeveiliging en incidentrespons, nu eigenlijk waarvoor verantwoordelijk was. Duidelijk is dat de leverancier verantwoordelijk is voor betrouwbare software en updates en de gebruikers voor het doorvoeren van die updates. De gebruikers moeten zelf zorg dragen voor informatieveiligheid en beveiliging van ICT-voorzieningen. Minder duidelijk is het functioneren van het Landelijk Dekkend Stelsel in de 'warme fase'. Het is bijvoorbeeld nog niet zeker wat aangesloten partijen dan kunnen verwachten van informatieverstrekking (snelheid, type informatie) en regievoering (COT, 2020). Ook zijn de verhoudingen en verbindingen tussen sectorale netwerken voor cybersecurity en reguliere crisisstructuren in de acute fase niet helder.

Uit deze casus blijkt de bescheiden rol van veiligheidsregio's, zeker als er geen fysieke gevolgen voor de openbare orde optreden. Het monitoren en in beeld brengen van mogelijke (landelijke en regionale) effecten kan wel een rol zijn voor veiligheidsregio's in het kader van verhoogde waakzaamheid. Veiligheidsregio's beschikten niet over een gemeenschappelijk beeld van de situatie en over eventueel benodigde acties. Dergelijke beeldvorming, vanuit een deugdelijke informatiepositie, is echter essentieel – juist bij problemen die landelijk en bij veel organisaties tegelijkertijd spelen. Het LOCC, maar ook het recent opgerichte Information Sharing and Analysis Center (ISAC) voor de veiligheidsregio's, kunnen hier in de toekomst in voorzien. Tot slot blijken in de casus de beperkingen van de vitale infrastructuur, nadat organisaties die niet als vitaal zijn aangemerkt in problemen waren gekomen. Een ministeriële regeling heeft per januari 2020 in elk geval de mogelijkheid geboden voor een intensievere informatiedeling tussen het NCSC en Z-CERT, waterschappen, gemeenten en SURFcert.

Belangrijkste bevindingen

1. De verantwoordelijkheid van het hebben van betrouwbare software en het aanbieden van updates ligt bij de softwareleverancier. Het tijdig doorvoeren van die updates, en daarmee zorgdragen voor een goed beveiligde computer, is echter de verantwoordelijkheid van de gebruikers.
2. Op het gebied van informatieverstrekking en regievoering is het voor aangesloten partijen nog niet altijd duidelijk wat zij kunnen verwachten van het Landelijk Dekkend Stelsel in de warme fase.
1. De verhoudingen en verbindingen tussen sectorale netwerken voor cyberveiligheid en reguliere crisisstructuren zijn in de warme fase voor betrokkenen nog niet helder.
2. Veiligheidsregio's spelen tot op heden een beperkte rol in de gevolgbestrijding van cyberverstoringen. Mogelijk is er voor hen een grotere rol weggelegd, bijvoorbeeld op het gebied van gezamenlijke beeldvorming van de situatie en eventueel benodigde acties.

3. De huidige definitie van de vitale infrastructuur werkt beperkend. Niet als vitaal-aangemerkte sectoren vormen daardoor niet de primaire doelgroep van het NCSC, terwijl cyberverstoringen bij sommige van deze sectoren wel degelijk tot maatschappelijke effecten kunnen leiden.

7 Overkoepelende observaties en aanbevelingen

In dit hoofdstuk reflecteren we op de bestudeerde casus aan de hand van tien overkoepelende observaties. We trekken lessen voor veiligheidsregio's, gemeenten en andere crisispartners. Aan deze observaties hebben we ook enkele aanbevelingen gekoppeld, die we tussen de observaties door weergeven in kaders. Met deze aanbevelingen hopen we veiligheidsregio's en andere crisispartners handvatten te geven voor cybergevolgbestrijding.

7.1 Forse impact van cyberverstoringen op getroffen organisaties

De casus in dit rapport hadden zonder uitzondering een grote impact op de betrokken organisaties. De cyberincidenten leidden tot een verstoring van (vitale) bedrijfsprocessen en dienstverlening, hinder voor medewerkers en cliënten en financieel verlies door schade aan en herstel van ICT-voorzieningen, het betalen van losgeld en kosten voor de inhuur van externen. Ondanks dat de behandelde cyberverstoringen de veiligheid of openbare orde in een veiligheidsregio niet hebben bedreigd, hadden de verstoringen wel degelijk een grote impact op de getroffen organisatie(s). De impact van cyberverstoringen kan dus enorm zijn, en moet niet worden onderschat.

De gemeente Lochem, Universiteit Maastricht en Maersk werden geconfronteerd met complexe ransomware-aanvallen, waarachter serieuze hackerscollectieven schuilgingen. De dreiging van dergelijke aanvallen en de impact op de getroffen organisaties kunnen groot zijn. Dit soort cyberaanvallen zijn in de praktijk, ongeacht het niveau van beveiliging, lastig te voorkomen. Statelijke actoren en door staten gesteunde criminele groeperingen zorgen voor tal van organisaties voor een vrijwel permanente en hoge dreiging.

Cyberverstoringen met verstrekkende gevolgen, dat wil zeggen zogenaamde maatschappij-ontwrichtende verstoringen (waarvoor instanties als de NCTV en WRR waarschuwen), zijn tot op heden de uitzondering. In géén van de bestudeerde casus trad een langdurige verstoring van vitale voorzieningen op, er vielen geen doden of gewonden en de bevolking bleef niet verstoken van primaire levensbehoeften. In die zin is geen sprake geweest van een daadwerkelijke of dreigende maatschappelijke ontwrichting. Het dominante beeld is er een van relatief beheersbare cyberincidenten, waarop systemen geautomatiseerd en medewerkers en organisaties behoorlijk veerkrachtig reageren.

Dat betekent overigens niet, zo benadrukken we direct, dat dergelijke verstorende effecten bij toekomstige cyberverstoringen niet kunnen optreden. De digitalisering schrijdt voort en daarmee de potentiële kwetsbaarheden.

Overheden, bedrijfsleven en organisaties als ziekenhuizen en scholen hebben dagelijks te maken met cyberdreigingen – zoals gijzelingssoftware, phishing-mails en technische of menselijke fouten.[28] Dergelijke dreigingen kunnen zeker in de huidige tijd worden beschouwd als een vast onderdeel van het bedrijfsproces: ‘a fact of life’ en bijna ‘business as usual’. Gelukkig zijn niet al die dreigingen even ernstig en complex. Door goede ICT-voorzieningen, informatiebeveiliging en adequaat optreden van alerte CERT’s kunnen risico’s tijdig worden gedetecteerd en (meestal routinematig) worden verholpen, zoals ook Van Eeten (2019) terecht heeft opgemerkt.

7.2 Maatschappelijke gevolgen en vitale sectoren

Hoe vaak cyberincidenten plaatsvinden en met welke gevolgen, is feitelijk niet bekend (Centraal Planbureau, 2019). De casus in deze publicatie bleken, zeker voor de betrokken organisaties, forse gevolgen te hebben gehad: een verstoring van (vitale) bedrijfsprocessen en dienstverlening, hinder voor medewerkers en cliënten en financieel verlies door schade aan en herstel van ICT-voorzieningen, het betalen van losgeld en kosten voor de inhuur van externen. Afgezien van deze directe gevolgen waren de maatschappelijke gevolgen in de meeste casus echter betrekkelijk beperkt. Er trad geen langdurige verstoring van vitale voorzieningen op, er vielen geen doden of gewonden en de bevolking bleef niet verstoken van primaire levensbehoeften. In die zin is geen sprake geweest van een daadwerkelijke of dreigende maatschappelijke ontwrichting. Wel hadden de cyberverstoringen een grote impact op de getroffen organisatie(s) en was er sprake van zogenaamde (cyber)disrupties.

De NCTV heeft meerdere sectoren als vitaal aangemerkt.[29] Uit de Citrix-casus blijken de beperkingen van die afbakening, nadat organisaties die niet als vitaal zijn aangemerkt, in de problemen waren gekomen. In de lijst met vitale sectoren komen ziekenhuizen, zorginstellingen, universiteiten, chemische bedrijven en grote bedrijven zoals Shell niet voor. Formeel zijn ook veiligheidsregio’s tot op heden niet aangemerkt als vitale sector. In een brief van de minister gericht aan de Tweede Kamer wordt echter wel gesteld dat veiligheidsregio’s essentieel zijn voor de crisisbeheersing in Nederland (Grapperhaus, 2020). Zoals duidelijk moge zijn, kan een uitval van digitale voorzieningen binnen dergelijke niet-vitale organisaties eveneens tot grote (maatschappelijke) effecten leiden, bijvoorbeeld wanneer een ziekenhuis wordt getroffen en de afdeling spoedeisende hulp uitvalt. Inmiddels zijn daarom de formele voorwaarden voor het delen van informatie over cybersecurity tussen het Rijk en vier ‘nieuwe’ sectoren gecreëerd.

7.3 Bescheiden rol van veiligheidsregio’s bij cyberverstoringen (tot op heden)

Cyber is, naast overstromingen, pandemieën en klimaatverandering, een van de risico’s waar veiligheidsregio’s zich op voorbereiden. Hoewel cyberaanvallen een betrekkelijk nieuw en onbekend risico vormen, beschikken veiligheidsregio’s in de basis over het vermogen eventuele externe gevolgen van cyberverstoringen te bestrijden. Dat vermogen ligt in bestaande procedures en werkwijzen waarop regio’s kunnen terugvallen, ongeacht het type incident. Denk hierbij aan beeldvorming, leiding en coördinatie, en crisiscommunicatie.

[28] Zie ook: https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf.
[29] Zie ook https://www.nctv.nl/onderwerpen/vitale-infrastructuur/overzicht-vitale-processen.

In de bestudeerde casus in dit rapport was de rol van veiligheidsregio's bij cyberincidenten en -crises betrekkelijk klein. Veiligheidsregio's komen bij cyberverstoringen vooral in beeld als:

a. de veiligheidsregio zelf getroffen is, zoals bij de VNOG gijzelingssoftware en de KPN-storing
b. er sprake is van het optreden van mogelijke fysieke gevolgen van een cyberverstoring (en als er behoefte is aan monitoring, beeldvorming van effecten en vervolgrisico's, coördinatie en crisiscommunicatie), zoals bij de Citrix-casus en wederom de KPN-storing.

Bij fysieke gevolgen kan worden gedacht aan maatschappelijke onrust, uitval van essentiële voorzieningen (voedsel, water, elektriciteit) en collectieve gedragsreacties. Dan liggen er voor de veiligheidsregio's taken op het gebied van gevolgbestrijding en verhoogde waakzaamheid.

Hoewel de rol van veiligheidsregio's in de casus bescheiden was, kan die rol in de toekomst groter worden en zelfs veranderen. Hierbij kan gedacht worden aan:

1. het bevorderen van regionaal risicobewustzijn bij (BRZO-)bedrijven, vitale en andere maatschappelijke partners
2. kennisopbouw en -deling over cyberrisico's en dreigingen (middels VR-ISAC)
3. beeldvorming, duiding en monitoring
4. risico- en crisiscommunicatie
5. incidentrespons (middels VR-ISAC en VR-CERT).

De KPN-storing en recent de ransomware-aanval op de VNOG onderstrepen voor veiligheidsregio's evident de noodzaak om de eigen organisatiecontinuïteit op orde te hebben: welke vitale processen en voorzieningen moeten hoe dan ook blijven functioneren? Ook het delen van cybersecurity-informatie binnen de eigen sector door middel van een VR-ISAC en op termijn een VR-CERT kan bijdragen aan het vergroten van de cyberweerbaarheid van veiligheidsregio's.

Aanbeveling 1: Onderzoek naar cybergevolgbestrijding door veiligheidsregio's

Veiligheidsregio's kunnen worden geconfronteerd met diverse cyberscenario's. Het voorbereiden op al die specifieke scenario's is echter niet realistisch, en daarom zou het helpen om enkele *maatgevende cyberscenario's* beschikbaar te hebben. Hierbij valt te denken aan een set van vier of vijf voorstelbare scenario's die gezamenlijk het brede pallet aan mogelijke scenario's bestrijken.

Die maatgevende cyberscenario's kunnen vervolgens worden gebruikt voor nader onderzoek naar cybergevolgbestrijding door veiligheidsregio's (naar alarmering en opschaling, leiding en coördinatie, grensoverschrijdende samenwerking tussen het Rijk en de regio's)[30], voor het bevorderen van bestuurlijke bewustwording omtrent cybersecurity en om te oefenen.

[30] Functioneren van de keten voor cybergevolgbestrijding.

7.4 Weinig ervaring met cybergevolgbestrijding en het functioneren van het landelijk dekkend stelsel

De ervaring van veiligheidsregio's met cybergevolgbestrijding en het functioneren van het Landelijk Dekkend Stelsel is gering, zeker in vergelijking met klassieke (niet-digitale) incidenten. Die ervaring neemt wel toe als gevolg van daadwerkelijke incidenten als de Lochem-casus, de kwetsbaarheden in de Citrix-software en de ransomware-aanval op VNOG.

Een cyberresponsnetwerk, inclusief specialistische actoren (zoals het NCSC en sectorale CERT's) en planvorming (zoals het Nationaal Crisisplan Digitaal), is er feitelijk al. Ook is een Landelijk Dekkend Stelsel in opbouw. Boeke (2018) typeert de Nederlandse aanpak als een 'participant-governed network', waarbij publieke en private partijen op basis van vertrouwen en gelijkwaardigheid participeren. De NCSC fungeert daarbij als centrale spil die de samenwerking tussen partijen faciliteert, zonder daarbij al te dwingend te zijn. Toch blijft het voor gemeenten en veiligheidsregio's zoeken naar welke responsstructuur en expertise vereist zijn. De vraag is met name hoe het responsnetwerk bij cyberincidenten *functioneert:* hoe verlopen opschaling en alarmering, wie doet wat, wat kunnen partijen van elkaar verwachten? Een mogelijke verklaring betreft het feit dat risico's rondom cyber betrekkelijk nieuw zijn, en er zowel tijdens daadwerkelijke incidenten als in oefeningen nog weinig ervaring mee is opgedaan.

Het opbouwen van meer ervaring door oefenen kan het vertrouwen in het functioneren van dat nieuwe crisisnetwerk versterken (en zicht geven op zwakke schakels). Het opdoen en hebben van ervaring is namelijk een van de belangrijkste factoren voor succesvol crisismanagement (Van Duin, 2011). Open en transparante communicatie over cyberverstoringen biedt ook anderen dan de direct betrokkenen de gelegenheid om van dit soort incidenten te leren. Bijzondere aandacht is daarbij vereist voor de relaties tussen cybersecuritynetwerken (in de koude fase) en reguliere crisisbeheersing (in de warme fase).

Aanbeveling 2: Oefenen met cybergevolgbestrijding

Het opbouwen van ervaring met cybergevolgbestrijding en het functioneren van een Landelijk Dekkend Stelsel is voor veiligheidsregio's en andere crisispartners noodzakelijk. Ervaring kan niet alleen worden opgedaan middels het doorleven van cyberscenario's, maar ook door gemeenschappelijke oefeningen. Hierbij kan worden gedacht aan het:

> oefenen van 'inhoud en proces'
> oefenen van verschillende cyberscenario's
> oefenen van de gehele opschalingsketen (ISAC-CERT-crisisorganisatie)
> oefenen van rollen en taken tussen het Rijk en veiligheidsregio's.

Deelname van veiligheidsregio's aan de landelijke ISIDOOR-3-oefening waaraan ook het Rijk en vitale partners deelnemen, is een belangrijke stap om deze verschillende partijen aan elkaar te verbinden.

7.5 Getroffen organisaties zijn zelf verantwoordelijk voor ‘failure management’

Organisaties die geconfronteerd worden met gijzelingssoftware en andere ICT-problemen zijn zelf verantwoordelijk voor het oplossen van die problemen (eigen verantwoordelijkheid voor ‘failure management’) (Treurniet, Boersma & Groenewegen, 2019). Daarbij helpen reguliere crisisplannen maar tot op zekere hoogte. Om de problemen op te lossen en de eigen ICT-voorzieningen weer operationeel én betrouwbaar te krijgen, zijn onder andere nodig: een goed incidentresponsteam, forensisch onderzoek, expertise op het gebied van het veiligstellen van data en ICT-voorzieningen én herstel en beveiliging. Daarvoor wenden organisaties zich regelmatig tot externe experts en gespecialiseerde adviesbureaus (zie ook: Boeke, 2018). Zo zag de gemeente Lochem zich genoodzaakt om zelf ICT-expertise en mankracht te mobiliseren, onder meer voor het begeleiden van forensisch onderzoek, mitigerende maatregelen en duiding. De Universiteit Maastricht schakelde het bedrijf Fox-IT in om haar bij te staan in de bestrijding van de gevolgen van de cyberaanval, voor forensisch onderzoek en advies. Het is logisch dat benodigde expertise niet altijd in huis is en extern moet worden gemobiliseerd. Het is echter wel handig als daar in de koude fase afspraken over worden gemaakt.

7.6 Cyberverstoringen: complexiteit en onzekerheid leren accepteren

Cyberverstoringen kenmerken zich onder andere door onzichtbaarheid, complexiteit en onzekerheid (IFV, 2020a). Er is bijvoorbeeld geen rook, en oorzaak-gevolgrelaties zijn onduidelijk. Vaak bestaat er veel onzekerheid: wie gaan achter de aanval schuil, zijn er data gecorrumpeerd, is er een sluitende oplossing voor het probleem? Hierdoor ontstaat het gevaar op *onder-reageren* (door een gebrek aan ervaren urgentie: ‘het zal zo’n vaart wel niet lopen’) of juist *overreageren* (door de behoefte aan controle en zekerheid en het ontbreken van ervaring met dit type specialistisch risico). Dit is een klassiek dilemma, doordat in de eerste uren en dagen veel onduidelijk is (Treurniet et al., 2019). Vragen die met dit dilemma te maken hebben, zijn: hoe groot schaal je op? Wat is proportioneel? In feite weet je echter nooit wat proportioneel is; dat blijkt pas gaandeweg of bij de evaluatie achteraf.

Tijdens en in de nasleep van een cyberverstoring speelt vrijwel altijd de vraag of de betrouwbaarheid van systemen én data kan worden gegarandeerd. Dit kan mogelijk ook nog problemen opleveren nadat de verstoring (ogenschijnlijk) is verholpen. Bij de gemeente Lochem had dit bijvoorbeeld betrekking op de getroffen systemen: wanneer weet je zeker dat de aanvallers geen toegang meer hebben tot de systemen en dat je de betrouwbaarheid van deze systemen weer kunt garanderen? Ook bij de Universiteit Maastricht speelde dit vraagstuk tijdens de crisis, niet alleen met betrekking tot de systemen, maar ook zeker tot de door de hackers versleutelde (wetenschappelijke) data. Deze data kunnen immers, ook na betaling van het losgeld, door hackers zijn gekopieerd of zijn aangetast. Bij de Citrix-casus viel lastig te garanderen of het systeem na het installeren van de patches weer veilig was; er was (en is) een mogelijkheid dat hackers onontdekte ‘backdoors’ hadden geplaatst, waarmee zij ongezien het systeem konden penetreren. Op dit soort vragen is niet altijd een sluitend antwoord te geven. Het is aan bestuurders en crisisfunctionarissen om dergelijke complexiteiten en onzekerheden te accepteren.

7.7 Over het nut van plannen en de uitdaging van strategie

Reguliere crisisstructuren bieden ook bij cyberverstoringen een zekere basis voor crisisbeheersing. Uit diverse casus (zoals Lochem en Maastricht) wordt duidelijk dat organisaties bij cyberverstoringen terugvallen op hun generieke crisisorganisatie en -werkwijzen. In beide gevallen startten de instellingen met het organiseren en structureren op basis van bestaande afspraken en plannen. Dat is natuurlijk ook de achterliggende gedachte achter generieke planvorming: het bieden van structuur, houvast en beproefde werkwijzen, maar met ruimte voor improvisatie en flexibiliteit.

Een plan biedt – ook bij cybercrises – structuur en geeft zicht op actoren, bevoegdheden en procedures. Het is onontbeerlijk voor crisisteams om die plannen te kennen, maar niet voldoende (IFV, 2019a). De grootste uitdaging zien wij in het vinden en uitvoeren van een effectieve responsstrategie. Die strategie is niet zomaar te vinden in plannen, maar kunnen organisaties en crisisteams zich wel eigen maken door te oefenen en te leren. Een belangrijk aspect van die strategie is het accepteren van en leren omgaan met complexiteit (Weick & Sutcliffe, 2015). Dit is bij uitstek van belang bij cyberverstoringen.[31] Onderdelen van zo'n strategie zijn in onze ogen:

> zelfkennis: waar staan jij en jouw organisatie voor? Welke waarden hebben jullie?
> accepteren dat je niet alles zelf weet (en anderen nodig hebt om oplossingen te vinden)
> het nog niet weten (en dat durven toegeven)
> bereidheid tot leren en tussentijds bijstellen van de strategie
> in verbinding blijven met gedupeerden en belanghebbenden
> nieuwsgierig zijn en blijven: vragen stellen.

Op tal van gebieden (technologie, economie, samenleving) is de wereld namelijk dermate complex geworden dat we de werking ervan nauwelijks kunnen doorgronden.[32] Dat betekent dat er geen eenvoudige oplossingen zijn voor problemen, dat we de gevolgen van een bepaalde maatregel nauwelijks kunnen doorzien en dat controle en beheersing een illusie zijn. Daar zullen ook bestuurders en andere crisisbeheersers zich toe moeten verhouden. Dat vraagt, zeker in de respons op nieuwe risico's als cyberaanvallen, mogelijk een andere benadering en mindset dan we van oudsher in de traditionele crisisbeheersing gewend zijn.

Aanbeveling 3: Veerkrachtige cyberrespons

Cyberverstoringen zijn omgeven met complexiteit en onzekerheid. Het is lastig voorbereiden op dergelijke crises, die bovendien van bestuurders en crisisfunctionarissen een andere strategie vragen dan zij gewend zijn. Dit vraagt veerkracht van betrokken personen en organisaties. Het is daarom raadzaam te investeren in veerkracht, zoals veerkrachtig leiderschap. Daarvoor is binnen bestaande crisisopleidingen momenteel beperkt aandacht.

7.8 Informatiedeling is blijvend van belang

Snelle en accurate informatie-uitwisseling is essentieel voor de incidentrespons en het beheersen van de mogelijke gevolgen van cyberverstoringen. Op het gebied van

[31] Voor een interessante uitwerking van zo'n strategie zie het rapport: *Covid-19. Een analyse van de nationale crisisrespons* van Crisisplan (2020). Zie ook Weick en Sutcliffe (2015).
[32] Zie het werk van Nassim Nicholas Taleb, waaronder Antifragiliteit (2014).

cyberdreigingen vindt daarom vrijwel permanente informatie-uitwisseling plaats binnen sectoren (Bekkers, Van der Kleij & Leukfeldt, 2020). Die informatie is belangrijk om kwetsbaarheden snel te kunnen detecteren, partijen op risico's te attenderen en mogelijke beheersmaatregelen te kunnen treffen. Bij daadwerkelijke incidenten kan de uitwisseling van informatie in alle hectiek echter onder druk komen te staan. Daarnaast doen zich in het proces van informatiedeling diverse mogelijke vragen en dilemma's voor:

> Met welke partijen wordt (op welk moment) informatie gedeeld? Met welke sectoren niet?
> Wie zorgt voor duiding?
> Wie voert de regie over de informatie?

Hieraan gerelateerd is de verhouding tussen netwerken in de koude fase en reguliere crisisstructuren in de warme fase. Wanneer vindt informatiedeling (en alarmering) vanuit sectorale netwerken naar reguliere crisisstructuren plaats? Hoe gaan die netwerken in de acute fase met elkaar samenwerken?

7.9 Crisiscommunicatie

Crisiscommunicatie bij cybercrises is niet per definitie afwijkend van de communicatie bij reguliere crises. De patronen zijn, zoals ook de woordvoerder van de Universiteit Maastricht opmerkte, in essentie hetzelfde. Cruciaal zijn het bieden van een handelingsperspectief, het informeren (en geïnformeerd houden) van belanghebbenden en het geven van regelmatige statusupdates. Hoewel de cyberaanval op de Universiteit Maastricht was omgeven door de nodige inhoudelijke en technische onzekerheden, was er volgens de woordvoerder genoeg om wél over te communiceren. Zo was het bijvoorbeeld duidelijk dat de digitale systemen platlagen, wie daarvan last ondervonden en in welke mate. De open en transparante communicatie over de gijzelingssoftware door de Universiteit Maastricht en ook door de gemeente Lochem valt op. Beide organisaties deelden onderzoeksbevindingen, gaven regelmatig statusupdates en de universiteit organiseerde zelfs een symposium over de cyberaanval. Dat zien we als een best practice, die volgens ons navolging verdient. Zo kunnen anderen ook leren van de aanpak van bedrijven en instellingen die ervaringen met cyberincidenten hebben opgedaan.

Al te openlijk communiceren kan echter ook een risico zijn, omdat organisaties zo hun eigen kwetsbaarheden blootleggen. Maar zodra er fysieke gevolgen optreden (en mensen hinder van het incident ondervinden), zal communicatie over het incident onvermijdelijk zijn. Communicatie kan onder druk komen te staan als reguliere communicatiekanalen door een cyberaanval uitvallen, zoals duidelijk werd in Maastricht. In de meeste gevallen waren organisaties echter in staat via hun reguliere kanalen zoals de website, persberichten en sociale media te communiceren. Ook kan het openlijk delen van gegevens over incidenten lastig blijken in de hectiek van de crisis, bijvoorbeeld omdat dan andere belangen gaan meespelen (zoals opsporing en vervolging, reputatie, herstel van de interne bedrijfsvoering). De prioriteit ligt toch vaak eerst bij het verhelpen van het probleem en dan pas bij het informeren van de eigen sector.

Aanbeveling 4: Blijf leren en evalueren

Er is beperkte ervaring bij veiligheidsregio's en crisispartners met cybergevolgbestrijding, zeker in vergelijking met klassieke calamiteiten en flitsrampen. Het is daarom van belang te kunnen (blijven) leren van cyberverstoringen. Hiervoor is het noodzakelijk om door open

communicatie elkaar in staat te stellen van elkaar te leren, zodat kennis kan worden opgebouwd. Ook het bespreken en delen van lessen van andere organisaties, bijvoorbeeld in leerarena's, kan bijdragen aan gemeenschappelijke kennisopbouw. Het leren van daadwerkelijke cyberverstoringen was een van de redenen om dit onderzoek uit te voeren.

7.10 Samenspel tussen preventie, incidentrespons én crisisbeheersing

Organisaties zijn verantwoordelijk voor de beveiliging van hun eigen informatie- en ICT-voorzieningen. Die beveiliging biedt geen volledige veiligheidsgarantie, maar is wel essentieel. Een gebrekkige beveiliging maakt organisaties namelijk kwetsbaar voor cyberaanvallen, en daar maken hackers maar al te graag gebruik van, zoals duidelijk werd in de Maersk-casus. Digitale beveiliging werpt, naar analogie van woninginbraakpreventie (Keurmerk Veilig Wonen), simpelweg barrières voor misbruik op. Een goed slot op je deur sluit niet uit dat inbrekers alsnog binnen (kunnen) komen, maar het maakt de kans wél veel kleiner. Ditzelfde geldt voor digitale systemen, temeer daar hackers zelden gericht een specifieke organisatie of specifiek bedrijf proberen te hacken. Ze richten zich veelal op die organisaties en bedrijven die hun beveiliging niet goed op orde hebben. Hoe kwetsbaarder de digitale beveiliging is (bijvoorbeeld door het niet tijdig uitvoeren van updates), hoe groter de kans dat een bedrijf slachtoffer wordt.

Een cyberverstoring valt echter nauwelijks uit te sluiten, ook niet met een adequate digitale beveiliging. Daarom is, naast preventie, het tijdig verhelpen van cyberverstoringen een belangrijk aspect van cyberweerbaarheid. De ICT-afdeling van veel organisaties, zoals universiteiten, gemeenten en zorginstellingen, werken daarvoor (samen) met zogeheten CERT's. Als deze 'lines of defence' niet voldoende blijken en voorzieningen door een cyberaanval of ICT-storing (ernstig) verstoord raken, zal opschaling aan de orde zijn om de bredere gevolgen te beheersen. De opgave is dan te zorgen voor benodigde coördinatie en samenwerking tussen onder meer het CERT, de ICT-afdeling én de reguliere crisisstructuur.

Aanbeveling 5: Ketens versterken

Binnen het brede cyberdossier werken diverse actoren (elk op hun eigen deelterrein en hoofdzakelijk binnen hun eigen kolom) aan een betere cyberweerbaarheid en -gevolgbestrijding. Het beter aan elkaar verbinden van die actoren lijkt zinvol. Het is simpelweg handig om van elkaar te weten wat je doet en hoe je elkaar kunt helpen.

De taal en het begrippenkader van informatiebeveiliging / incidentrespons komen niet noodzakelijk overeen met de taal en het begrippenkader van de reguliere crisisbeheersing en het referentiekader van bestuurders. Oefenen en over de grenzen van de eigen sector en kolom samenwerken, kunnen bijdragen aan gemeenschappelijke begripsvorming en een gemeenschappelijke taal en gemeenschappelijk begrippenkader – wat cruciaal is voor cybergevolgbestrijding.

Onze aanbeveling is derhalve om manieren te verkennen om betrokken actoren en overlegstructuren met elkaar in verbinding te brengen, zoals nu al gebeurt tussen de vakgroep Informatieveiligheid en werkgroep Cybergevolgbestrijding.

Vanuit het perspectief van cybergevolgbestrijding zou de prioriteit moeten liggen op het verbinden van de voor cyber specifieke crisisstructuur (informatieveiligheid / incidentrespons) met de generieke crisisstructuren – bijvoorbeeld door digitale verbindingsofficieren, een OvD-Digitaal, de ontwikkeling van cyberexpertise en kennisopbouw over het functioneren van de keten voor cybergevolgbestrijding.

Literatuurlijst

Alert Online (2019). *Gemeente Lochem: "We zijn letterlijk door het oog van de naald gekopen"*. Geraadpleegd van https://www.alertonline.nl/nieuws/2019/gemeentelochem.

Bekkers, L., Kleij, R. van der & Leukfeldt, R. (2020). *Verkenning best practices cybersecurity informatiedeling*. Den Haag: Haagse Hogeschool.

Boeke, S. (2018). National cyber crisis management: Different European approaches. *Governance*, *31*(3), 449-464.

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

Boin, A., Hart, P. 't, Stern, E. & Sundelius, B. (2016). *The Politics of Crisis Management. Public Leadership under Pressure.* 2nd ed. Cambridge (UK): Cambridge University Press.

Bremmer, D. & Heel, L. van (2017). 'Wereldwijde hack legt bedrijven en Rotterdamse terminal plat'. *Algemeen Dagblad*. Geraadpleegd van https://www.ad.nl/rotterdam/wereldwijde-hack-legt-bedrijven-en-rotterdamse-terminal-plat~a60dd307/.

Bruins, B. (2020, 10 februari). Beantwoording Kamervragen over het stilleggen van het dataverkeer door het Medisch Centrum Leeuwarden naar aanleiding van een hackpoging [Kamerbrief]. Geraadpleegd van https://www.rijksoverheid.nl/documenten/kamerstukken/2020/02/10/beantwoording-kamervragen-over-het-bericht-stilleggen-van-het-dataverkeer-door-het-medisch-centrum-leeuwarden-naar-aanleiding-van-een-hackpoging.

Centraal Planbureau (2019). *Risicorapportage cyberveiligheid economie 2019*. Den Haag: Centraal Planbureau.

Comfort, L.K., Boin, A. & Demchak, C.C. (2010). *Designing Resilience: Preparing for Extreme Events*. Pittsburgh: University of Pittsburgh Press.

COT (2020). *Samenvatting indrukken en leerpunten leerevaluatie respons Citrix.* Geraadpleegd van https://www.rijksoverheid.nl/documenten/rapporten/2020/03/20/tk-bijlage-ii-samenvatting-indrukken-en-leerpunten-leerevaluatie-respons-citrix.

De Gezonde Digitale Organisatie (2019). *ICT-systeem Gemeente Lochem gehackt.* Geraadpleegd van https://degezondedigitaleorganisatie.nl/ict-systeem-gemeente-lochem-gehackt/.

Delft.Business (2020). *Binnen zonder kloppen*. Geraadpleegd van https://delft.business/kennis-delen/binnen-zonder-kloppen/.

Digital Trust Centrum (2020). *UPDATE: Vele Nederlandse Citrix-servers kwetsbaar voor aanvallen*. Geraadpleegd van https://www.digitaltrustcenter.nl/nieuws/update-vele-nederlandse-citrix-servers-kwetsbaar-voor-aanvallen.

Duin, M. van (2011). *Veerkrachtige crisisbeheersing: nuchter over het bijzondere* [Lectorale rede]. Geraadpleegd van https://www.ifv.nl/kennisplein/Documents/lectorale_rede_m-_van_duin.pdf.

Duin, M. van & Maan, J. (2018). Cyberaanval op Maersk. In Van Duin, M. & Wijkhuijs, V. (Red.), *Lessen uit crises en mini-crises 2017* (pp. 119-129). Boom uitgevers: Den Haag.

Duin, M. van & Wijkhuijs, V. (2015). *De flexibiliteit van GRIP.* Arnhem: IFV.

Eeten, M. van (2019). *Blussen met nullen en enen: Cyber-rampen, cyber-exceptionalisme en de rol van de overheid* [Oratie]. De Van Slingelandt-lezing. Geraadpleegd van https://www.bestuurskunde.nl/2019/11/14/blussen-met-nullen-en-enen-cyber-rampen-cyber-exceptionalisme-en-de-rol-van-de-overheid/.

Emerce (2017). *'Nederland op vier na grootste slachtoffer Petya'.* Geraadpleegd van https://www.emerce.nl/nieuws/nederland-vier-na-grootste-slachtoffer-petya.

Europol (2020). *Pandemic profiteering how criminals exploit the COVID-19 crisis March 2020*. Den Haag: Europol.

FERM-Rotterdam.nl (2017). *Handelingsperspectief grootschalige ransomware-aanval.* Geraadpleegd van https://ferm-rotterdam.nl/nl/nieuws/handelingsperspectief-grootschalige-ransomware-aanval.

Gemeente Lochem (2019a). *Gemeente Lochem digitaal niet bereikbaar vanwege herstel na hack*. Geraadpleegd van https://www.lochem.nl/laatste-nieuws/nieuwsbericht/gemeentenieuws/gemeente-lochem-digitaal-niet-bereikbaar-vanwege-herstel-na-hack-2374.

Gemeente Lochem (2019b). *Hackers breken in op ICT-netwerk gemeente Lochem*. Geraadpleegd van https://www.lochem.nl/laatste-nieuws/nieuwsbericht/gemeentenieuws/hackers-breken-in-op-ict-netwerk-gemeente-lochem-2367.

Gemeente Zutphen (2020). *Beantwoording vragen over informatiebeveiligingsincident Citrix Netscaler*. Geraadpleegd van https://raad.zutphen.nl/data/schriftelijkevraag-raad/_XA8905E3017015CE4726C731206B86E9/2020-V0002 Antwoordbrief.pdf.

Gezamenlijke Inspecties (2020). *Onbereikbaarheid van 112 op 24 juni 2019*. Den Haag/Groningen/Utrecht: Inspectie Justitie en Veiligheid, Agentschap Telecom & Inspectie Gezondheidszorg en Jeugd.

Grapperhaus, F. (2020, 20 maart). Kamerbrief evaluatie Citrix-problematiek en kabinetsreactie WRR-rapport: voorbereiding op digitale ontwrichting [Kamerbrief]. Geraadpleegd van https://www.rijksoverheid.nl/documenten/kamerstukken/2020/03/20/tk-kamerbrief-evaluatie-citrix-problematiek-en-kabinetsreactie-wrr-rapport.

Grapperhaus, F. (2020, 7 oktober). Gijzelsoftware-aanval op Veiligheidsregio Noord- en Oost-Gelderland [Kamerbrief]. Geraadpleegd van https://www.rijksoverheid.nl/documenten/kamerstukken/2020/10/07/tk-gijzelsoftware-aanval-op-veiligheidsregio-noord-en-oost-gelderland-vnog.

Grapperhaus, F. & Knops, R. (2020a, 20 januari). Kwetsbaarheid in producten Citrix [Kamerbrief]. Geraadpleegd van https://www.rijksoverheid.nl/documenten/kamerstukken/2020/01/20/tk-kwetsbaarheid-in-producten-citrix.

Grapperhaus, F. & Knops, R. (2020b, 23 januari). Overzicht op hoofdlijnen Citrix-kwetsbaarheden [Kamerbrief]. Geraadpleegd van https://www.rijksoverheid.nl/documenten/kamerstukken/2020/01/23/tk-overzicht-op-hoofdlijnen-citrix-kwetsbaarheden.

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

Groet, V.R. (2019). *Notitie m.b.t. beschouwing incidentmanagement gemeente Lochem*. Den Haag: Informatiebeveiligingsdienst.

Instituut Fysieke Veiligheid (z.d.). *Kennisplein - Nationaal Cyber Security Centrum (NCSC).* Geraadpleegd op 1 september 2020 van https://www.ifv.nl/kennisplein/cybercrime/links/nationaal-cyber-security-centrum-ncsc.

Instituut Fysieke Veiligheid (2019a). *Doel en doelmatigheid van planvorming.* Arnhem: IFV.

Instituut Fysieke Veiligheid (2019b). *Whitepaper digitale ontwrichting en cyber.* Arnhem: IFV.

Instituut Fysieke Veiligheid (2019c). *KPN-storing: hoe bestuurlijk omgaan met gebiedsontbonden crises?* Arnhem: IFV.

Instituut Fysieke Veiligheid (2020a). *Cyberrisico's en veiligheidsregio's.* Arnhem: IFV.

Instituut Fysieke Veiligheid (2020b). *Versterken van veerkracht*. Arnhem: IFV.

Informatiebeveiligingsdienst (2019). *Leren van Lochem: lessen uit een informatiebeveiligingsincident*. Geraadpleegd van https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2019/09/20190830-Leren-van-Lochem-Definitief-TLP_WIT.pdf

Informatiebeveiligingsdienst (2020a). *Kwetsbaarheden in Citrix: Lessen voor gemeenten en de IBD.* Geraadpleegd van https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2020/03/20200310-Lessen-Citrix-Crisis-TLP_WIT.pdf.

Informatiebeveiligingsdienst (2020b). *Over de IBD*. Geraadpleegd van https://www.informatiebeveiligingsdienst.nl/over-de-ibd/.

Inspectie van het Onderwijs (2020). *Cyberaanval Universiteit Maastricht.* Den Haag: Inspectie van het Onderwijs.

Kerssenberg, D. (2019). KPN Topman: "Wij zijn niet gehackt". *Webwereld.* Geraadpleegd van https://webwereld.nl/nieuws/business/kpn-topman-wij-zijn-niet-gehackt-3775092/

Kerstens, B. & Mol, D. (2020). 'Ziekenhuis Leeuwarden legt dataverkeer met buitenwereld stil na cyberaanval'. *Algemeen Dagblad*. Geraadpleegd van https://www.ad.nl/tech/ziekenhuis-leeuwarden-legt-dataverkeer-met-buitenwereld-stil-na-cyberaanval~a45daf1e/.

Kluis, E. de (2019). *Gemeente Lochem ging door oog van de naald bij hack.* Geraadpleegd van https://www.binnenlandsbestuur.nl/digitaal/nieuws/gemeente-lochem-door-oog-van-de-naald-bij-hack.10713247.lynkx.

Lalkens, P. (2018). 'Maersk moest complete IT-systeem vernieuwen na cyberaanval'. *Financieel Dagblad*. Geraadpleegd van https://fd.nl/ondernemen/1239239/maersk-moest-complete-it-systeem-vernieuwen-na-cyberaanval.

Logistiek.nl (2017). *APM heeft weer 1 terminal open na cyberaanval*. Geraadpleegd van https://www.logistiek.nl/supply-chain/nieuws/2017/06/apm-heeft-weer-1-terminal-open-101157047?io_source=www.logistiek.nl&_ga=2.186930414.753753792.1601993678-1208615138.1601993678.

Maastricht University (2019a). *UM getroffen door cyberaanval.* Geraadpleegd van https://www.maastrichtuniversity.nl/nl/nieuws/um-getroffen-door-cyberaanval.

Maastricht University (2019b). *Update #5: cyberaanval UM.* Geraadpleegd van https://www.maastrichtuniversity.nl/nl/nieuws/update-5-cyberaanval-um.

Maastricht University (2019c). *Update #6 en 7: cyberaanval UM.* Geraadpleegd van https://www.maastrichtuniversity.nl/nl/nieuws/update-6-en-7-cyberaanval-um.

Maastricht University (2020a). Reactie Universiteit Maastricht op rapport FOX-IT.

Maastricht University (2020b). *Update #12: cyberaanval UM.* Geraadpleegd van https://www.maastrichtuniversity.nl/nl/nieuws/update-12-cyberaanval-um.

Maastricht University (2020c). *Update #13: cyberaanval UM.* Geraadpleegd van https://www.maastrichtuniversity.nl/nl/nieuws/update-13-cyberaanval-um.

Maastricht University (2020d). *Update #17: cyberaanval UM.* Geraadpleegd van https://www.maastrichtuniversity.nl/nl/nieuws/update-17-cyberaanval-um.

Maastricht University (2020e). *Update #18: cyberaanval UM.* Geraadpleegd van https://www.maastrichtuniversity.nl/nl/nieuws/update-18-cyberaanval-um.

Maastricht University (2020f). *Update #20: cyberaanval UM.* Geraadpleegd van https://www.maastrichtuniversity.nl/nl/updates-cyberaanval.
Maastricht University (2020g). *Update #9: cyberaanval UM.* Geraadpleegd van https://www.maastrichtuniversity.nl/nl/nieuws/update-9-cyberaanval-um-0.

Metselaar, D. (2020). '29 mogelijke datalekken gemeld na hackpoging Citrix-software'. *NRC*. Geraadpleegd van https://www.nrc.nl/nieuws/2020/01/22/29-mogelijke-datalekken-gemeld-na-hackpoging-citrix-software-a3987714.

Modderkolk, H. (2019). *Het is oorlog maar niemand die het ziet.* Amsterdam: Uitgeverij Podium.

Modderkolk, H. (2020). 'Half jaar na Citrix-crisis zijn 25 Nederlandse organisaties gehackt. En ze weten zelf van niets'*. De Volkskrant*. Geraadpleegd van https://www.volkskrant.nl/nieuws-achtergrond/half-jaar-na-citrix-crisis-zijn-25-nederlandse-organisaties-gehackt-en-ze-weten-zelf-van-niets~b26947bc/

Nationaal Cyber Security Centrum (NCSC) (2019). *NCSC Magazine Editie 1*. Geraadpleegd van https://magazines.ncsc.nl/ncscmagazine/2019/01/index.

Nationaal Cyber Security Centrum (NCSC) (2020a). *Effectief opereren in de CERT-gemeenschap.* Den Haag: NCSC.

Nationaal Cyber Security Centrum (NCSC) (2020b). *Stroomschema risicoafweging Citrix.* Geraadpleegd van https://www.ncsc.nl/documenten/publicaties/2020/januari/20/stroomschema-risicoafweging-citrix.

Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) (2019). *Cybersecuritybeeld Nederland 2020*. Den Haag: NCTV.

NFIR (2019). *Managementsamenvatting Security Incident Lochem.* Den Haag: NFIR.

Nieuwsuur (2020a). Nieuwsuur aflevering 17 seizoen 2020. Geraadpleegd van https://www.npostart.nl/nieuwsuur/18-01-2020/VPWON_1310681.

Nieuwsuur (2020b, januari 15). Nieuwsuur aflevering 14 seizoen 2020. Geraadpleegd van https://www.npostart.nl/nieuwsuur/15-01-2020/VPWON_1310678.

Nieuwsuur (2020c, januari 18). Nieuwsuur: schakel Citrix uit. Geraadpleegd van https://www.npostart.nl/nieuwsuur/18-01-2020/VPWON_1310681.

NOS (2020a). *Opnieuw storing bij politienummer, 112 wel bereikbaar.* Geraadpleegd van https://nos.nl/artikel/2348689-opnieuw-storing-bij-politienummer-112-wel-bereikbaar.html.

NOS (2020b). *Waarschuwing voor hacks bij Citrix-servers na beveiligingslek*. Geraadpleegd van https://nos.nl/artikel/2318528-waarschuwing-voor-hacks-bij-citrix-servers-na-beveiligingslek.html.

NOS (2020c). *Citrix: we volgden na lek standaardprocedure, gebeurt duizenden keren per jaar.* Geraadpleegd van https://nos.nl/nieuwsuur/artikel/2319236-citrix-we-volgden-na-lek-standaardprocedure-gebeurt-duizenden-keren-per-jaar.html.

NU.nl (2020a). *Hackpoging bij Medisch Centrum Leeuwarden, ziekenhuis sluit netwerk af.* Geraadpleegd van https://www.nu.nl/tech/6023960/hackpoging-bij-medisch-centrum-leeuwarden-ziekenhuis-sluit-netwerk-af.html.

NU.nl (2020b). *Verkeer moet rekening houden met mist, gladheid en Citrix-files.* Geraadpleegd van https://www.nu.nl/binnenland/6024912/verkeer-moet-rekening-houden-met-mist-gladheid-en-citrix-files.html.

Observant (2020). *Cyberhack: Universiteit Maastricht betaalt losgeld.* Geraadpleegd van https://www.observantonline.nl/Home/Artikelen/articleType/ArticleView/articleId/17789/Cyberhack-Universiteit-Maastricht-betaalt-losgeld.

Oomes, E. (2020). *Kleine taxonomie van de ongewenste gebeurtenis.* Geraadpleegd van https://www.rizoomes.nl/crisismanagement/kleine-taxonomie-van-de-ongewenste-gebeurtenis/.

Organisation for Economic Cooperation and Development (OECD) (2003). *Annual Report: 2003.* Parijs: OECD.

Pols, G. (2019). 'Russen zitten vermoedelijk achter hack Universiteit Maastricht'. *Trouw*. Geraadpleegd van https://www.trouw.nl/nieuws/russen-zitten-vermoedelijk-achter-hack-universiteit-maastricht~baa96b9d/?referrer=https%3A%2F%2Fwww.google.com%2F.

Programma Overleg Informatievoorziening (2020a). *Instellingsbesluit Veiligheidsregio-Information Sharing and Analysis Centre (VR-ISAC).* Arnhem: IFV.

Programma Overleg Informatievoorziening (2020b). *Lidmaatschapsreglement VR-ISAC.* Arnhem: IFV.

RTL Z (2020). *"Nog tientallen Citrix-servers lek in Nederland".* Geraadpleegd van https://www.rtlz.nl/tech/artikel/5009426/citrix-servers-nederland-lek-update-patch-beveiliging.

Seeger, M.W. (2006). Best Practices in Crisis Communication: An Expert Panel Process. *Journal of Applied Communication Research*, *34*(3), 232–244.

Slovic, P. & Weber, E.U. (2002). Perception of risk posed by extreme events. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2293086

SURF (2019). *Cyberdreigingsbeeld 2019/2020 onderwijs en onderzoek.* Utrecht: SURF.

TalosIntelligence.com (2017). *The MeDoc Connection.* Geraadpleegd van https://blog.talosintelligence.com/2017/07/the-medoc-connection.html?m=1.

TheRegister.co.uk (2018). *IT "heroes" saved Maersk from NotPetya with ten-day reinstallation blitz.* Geraadpleegd van https://www.theregister.com/2018/01/25/after_notpetya_maersk_replaced_everything/.

TNO (2019). *Factsheet: challenge regionale cybergevolgbestrijding Veiligheidsregio Zuid-Holland Zuid.* Den Haag: TNO.

Treurniet, W., Boersma, K., & Groenewegen, P. (2019). Configuring emergency response networks. *International Journal Emergency Management, 15*(4), 316–333.

Tweede Kamer. (2019). Vragenuur : Vragen Van Raak. Geraadpleegd van https://www.tweedekamer.nl/nieuws/kamernieuws/het-vragenuur-van-dinsdag-1-oktober.

Veiligheidsberaad (2018). *De rol van de veiligheidsregio's bij digitale ontwrichting.* Geraadpleegd van https://www.veiligheidsberaad.nl/?jet_download=1612.

Veiligheidsberaad (2019). *Bestuurlijk routeboek digitale ontwrichting.* Geraadpleegd van https://veiligheidscoalitie.nl/action/?action=download&id=2358

Wassens, R. (2020a). 'Maatregelen die lek in Citrix moeten dichten werken niet altijd'. NRC. Geraadpleegd van https://www.nrc.nl/nieuws/2020/01/16/maatregelen-die-lek-in-citrix-moeten-dichten-werken-niet-altijd-a3987128?utm_source=social&utm_medium=twitter&utm_campaign=twitter&utm_content=&utm_term=20200115.

Wassens, R. (2020b). 'Gemeenten schakelen Citrix-systemen uit op advies NCSC'. *NRC*. Geraadpleegd van https://www.nrc.nl/nieuws/2020/01/17/gemeenten-schakelen-citrix-systemen-uit-op-advies-ncsc-a3987218.

Weick, K.E. & Sutcliffe, K.M. (2015). *Managing the Unexpected. Sustained Performance in a Complex World (3th edition).* Wiley: New Jersey.

Wetenschappelijke Raad voor het Regeringsbeleid (WRR) (2019). *Voorbereiden op digitale ontwrichting.* Den Haag: WRR.

Winter, B. de. (2019). *Door het oog van de naald.* Geraadpleegd van https://www.lochem.nl/fileadmin/internet-doc/Bestuur-Organisatie-Nieuws/Nieuws/2019/hack/Duidingsrapportage_Lochem-WHITE.pdf.

Bijlage 1 Geïnterviewde personen

Naam	Functie
Dhr. W. Biemolt	Voorzitter SURFcert
Dhr. F. Elbersen	(Zelfstandig) bestuurs- en communicatieadviseur / woordvoerder Universiteit Maastricht
Dhr. S. van ’t Erve	Burgemeester gemeente Lochem
Dhr. R. Gelmers	CISO gemeente Lochem
Dhr. J. Haasjes	Programmaleider informatie en innovatie bij Veiligheidsregio Fryslân
Dhr. B. Oude Hengel	Beleids- en projectmedewerker Crisisbeheersing bij Veiligheidsregio Brabant-Zuidoost

Bijlage 2 Deelnemers expertsessie

Naam	Functie
Dhr. M. Bekker	Sr. adviseur crisisbeheersing, Nationaal Crisiscentrum en betrokken geweest bij het Nationaal Crisisplan Digitaal
Dhr. J. Brouwer	Privacy officer, Veiligheidsregio Twente & voorzitter VR ISAC en vakgroep Informatieveiligheid
Dhr. P. van Dijk	Coördinerend beleidsmedewerker Team Informatiesamenleving, Vereniging van Nederlandse Gemeenten
Dhr. D. Dijkstra	Sr. adviseur cyberveiligheid, Nationaal Cyber Security Centrum
Dhr. M. Dirriwachter	Projectleider vitale digitale overheid, ministerie van Binnenlandse Zaken
Dhr. J. Groenendaal	Lector risicobeheersing en cybersecurity, Haagse Hogeschool & consultant
Dhr. S. Hooymans	Beleidsadviseur (adviseur portefeuillehouder digitaal RCDV), IFV
Dhr. D. Jaspers	Sr. adviseur, Nationaal Cyber Security Centrum
Dhr. R. Kleijweg	Adviseur dienst informatievoorziening, IFV & secretaris VR-ISAC en vakgroep Informatieveiligheid
Dhr. M. Neef	Innovator, consultant en onderzoekscoördinator (cyber, weerbaarheid en crisisbeheersing), TNO Defensie en Veiligheid
Dhr. G. Wismans	Coördinator beleid nationale crisisbeheersing, Nationaal Crisiscentrum en betrokken geweest bij het Nationaal Crisisplan Digitaal

Bijlage 3 Belangrijke actoren

NCSC

Het Nationaal Cyber Security Centrum (NCSC) is hét centrale informatieknooppunt en expertisecentrum voor cybersecurity in Nederland. Het NCSC is sinds 1 januari 2019 een zelfstandig uitvoerend onderdeel van het ministerie van JenV, het coördinerend ministerie op het gebied van cybersecurity. De NCTV fungeert daarbij als opdrachtgever van het NCSC (Grapperhaus & Knops, 2020a). Binnen de nationale crisisstructuur cyberincidenten heeft het NCSC een coördinerende rol. Het NCSC informeert en adviseert overheden en het bedrijfsleven over dreigingen of incidenten in informatiesystemen en ondersteunt hen in het treffen van maatregelen (Grapperhaus & Knops 2020b; IFV, 2019b). Naast de rijksoverheid is de vitale infrastructuur de primaire doelgroep van het NCSC. Deze vitale sectoren zijn cruciaal voor het goed functioneren van de Nederlandse samenleving. Voorbeelden van vitale sectoren zijn de energie-, water- en telecomsector (IFV, z.d.).

IBD

Sinds 1 januari 2013 is op initiatief van alle Nederlandse gemeenten de Informatiebeveiligingsdienst (IBD) actief en kunnen alle gemeenten gebruik maken van de producten en de generieke dienstverlening van de IBD. De IBD:

> is het sectorale CERT/CSIRT voor alle Nederlandse gemeenten en onderdeel van de Vereniging Nederlandse Gemeenten (VNG)
> ondersteunt gemeenten op het gebied van informatiebeveiliging en privacy
> is voor gemeenten het schakelpunt met het NCSC
> draagt namens gemeenten bij aan de Baseline Informatiebeveiliging Overheid (BIO) en geeft regelmatig kennisproducten uit
> faciliteert kennisdeling tussen gemeenten onderling, met andere overheidslagen, met vitale sectoren en met leveranciers (IBD, 2020b).

Werkgroep digitale ontwrichting en cyber

De werkgroep digitale ontwrichting en cyber focust zich op het externe gedeelte van het cyberkwadrant, respectievelijk cyberwaakzaamheid- en gevolgbestrijding. Zij heeft als doel het delen van kennis, ervaring en best practices en vormt samen met de VR-ISAC als het ware de verbinding tussen Rijk en regio. De werkgroep komt momenteel circa vijf keer per jaar samen. Doorgaans zitten er adviseurs in van 23[33] veiligheidsregio's – dit zijn bijvoorbeeld adviseurs crisisbeheersing, planvorming of operationele voorbereiding. De werkgroep stelt zich op als ambassadeur voor het thema cybersecurity, zowel intern in de veiligheidsregio's als extern naar regionale en nationale partners. De werkgroep heeft het onderwerp cyber en de (rol van de) veiligheidsregio verkend, wat resulteerde in het *Whitepaper digitale ontwrichting en cyber* (IFV, 2019b).

[33] Er is nooit actief gepoogd om alle 25 regio's aan te laten haken. De werkgroep is dan ook organisch tot 23 regio's gegroeid.

Vakgroep informatieveiligheid

Complementair aan de werkgroep digitale ontwrichting en cyber bestaat de vakgroep informatieveiligheid. Deze vakgroep richt zich met name op het interne gedeelte van het cyberkwadrant: cyberweerbaarheid- en veiligheid. De vakgroep bestaat sinds 2015 en is door het Netwerk Informatiemanagement (NIM/NICT) in het leven geroepen. In de vakgroep nemen voornamelijk CISO's van veiligheidsregio's deel. Het doel van de vakgroep is om kennis uit te wisselen tussen alle 25 veiligheidsregio's op het gebied van informatieveiligheid, om samen te werken aan het versterken van bewustwording op het gebied van informatieveiligheid en om (gezamenlijk) stappen te zetten ter verbetering van de informatieveiligheid. De vakgroep komt zes keer per jaar samen, waarbij het voornemen is om minimaal twee keer per jaar samen met de werkgroep digitale ontwrichting en cyber te vergaderen. Daarnaast nemen de voorzitter en secretaris van de vakgroep ook zitting in de werkgroep.

De vakgroep voert een aantal activiteiten uit, zoals adviezen geven op een aantal dossiers, meewerken aan risicoanalyses, producten ontwikkelen (bijvoorbeeld de standaard verwerkersovereenkomst) en collegiale toetsing (audit). Een van de meest recente activiteiten van de vakgroep is de instelling van het VR-ISAC.

VR-ISAC

Op 25 juni 2020 werd na goedkeuring van de RCDV het VR-ISAC (Veiligheidsregio-Information Sharing and Analysis Center) ingesteld. Hiermee werden veiligheidsregio's formeel aangesloten op het vertrouwelijke informatie-uitwisselingsysteem van het NCSC.

Een ISAC voorziet actoren van een vertrouwelijke setting waarin informatie kan worden uitgewisseld met betrekking tot cyberkwetsbaarheden, -dreigingen, -maatregelen en -verstoringen én waarin best practices en leerpunten kunnen worden besproken en gedeeld. Als samenwerkingsverband voorziet het VR-ISAC de veiligheidsregio's van deze mogelijkheden; het is een geformaliseerd overleg over cybersecurity voor het uitwisselen van kennis en expertise op het gebied van cyberdreigingen en -verstoringen door informatiespecialisten uit de veiligheidsregio's en van het IFV.

Het VR-ISAC heeft tevens enkele vastgelegde taken en verantwoordelijkheden. Het VR-ISAC (1) adviseert over maatregelen ter versterking van de digitale weerbaarheid, met name op tactisch en strategisch niveau (onder andere het POI). Daarnaast (2) faciliteert het in de structurele uitwisseling van kennis en expertise tussen veiligheidsregio's, het IFV, het NCSC en andere ISAC's. In het verlengde hiervan (3) versterkt het de informatiepositie (op tactisch / strategisch niveau) bij de beheersing van cyberverstoringen (in tegenstelling tot een CERT dat zich op operationeel niveau richt op de bestrijding van een cyberverstoring) én (4) waarschuwt het voor actuele cyberdreigingen die de interne bedrijfsvoering van de veiligheidsregio's mogelijk kunnen ontwrichten (POI, 2020b).

CERT & VR-CERT

Binnen het cyberdomein wordt naast een ISAC ook veelvuldig gebruikgemaakt van een CERT: een Computer Emergency Response Team (ook wel CSIRT's of

computercrisisteams genoemd). Een CERT is “onder andere verantwoordelijk voor het voorkomen, isoleren en mitigeren van computer- en informatiebeveiligingsincidenten” en “wordt vaak opgericht door enkele partijen in een sector/regio die besluiten dat er behoefte is aan een verhoging van de gezamenlijke slagkracht en weerbaarheid, om informatiebeveiligingsincidenten of -crises het hoofd te bieden” (NCSC, 2020a). Het NCSC is bijvoorbeeld het CERT voor de rijksoverheid en voor aanbieders van vitale infrastructuren. Waar het VR-ISAC de functie van een early warning system heeft, zal een VR-CERT fungeren als een incidentresponssysteem. Momenteel zijn de veiligheidsregio’s niet aangesloten op een CERT. Wel wordt een haalbaarheidsstudie uitgevoerd naar een mogelijk VR-CERT.

Bijlage 4 Relevante cyberpublicaties

- Berenschot (2020). *Handreiking Cybergevolgbestrijding (CGB) G4-gemeenten. Deel 1: Warme fase. Praktische handvatten tijdens een cybercrisis*. Utrecht: Berenschot Groep B.V.
- Berenschot (2020). *Handreiking Cybergevolgbestrijding (CGB) G4-gemeenten. Deel 2: Koude fase. Naslagwerk cybergevolgbestrijding*. Utrecht: Berenschot Groep B.V.
- Instituut Fysieke Veiligheid (2019). *Whitepaper digitale ontwrichting en cyber*. Arnhem: IFV.
- Instituut Fysieke Veiligheid (2020). *Cyberrisico's en veiligheidsregio's*. Arnhem: IFV.
- Instituut Fysieke Veiligheid (2020). *Versterken van veerkracht*. Arnhem: IFV.
- Nationaal Coördinator Terrorismebestrijding en Veiligheid (2020). *Cybersecuritybeeld 2020*. Den Haag: Ministerie van Justitie en Veiligheid.
- Nationaal Cyber Security Centrum (2020). *Nationaal Crisisplan Digitaal*. Den Haag: Ministerie van Justitie en Veiligheid.
- Wetenschappelijke Raad voor het Regeringsbeleid (2019). *Voorbereiden op digitale ontwrichting*. Den Haag: WRR.