Instituut
Fysieke
Veiligheid

Whitepaper digitale ontwrichting en cyber

Instituut Fysieke Veiligheid
Bestuurs-, beleids- en
directieondersteuning
Postbus 7010
6801 HA Arnhem
Kemperbergerweg 783, Arnhem
www.ifv.nl
info@ifv.nl
026 355 24 00

Colofon

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

Opdrachtgever:	Raad Directeuren Veiligheidsregio (RDVR)
Contactpersoon:	Steven van de Looij
Titel:	Whitepaper digitale ontwrichting en cyber
Datum:	9 september 2019
Status:	Definitief
Versie:	1.0
Auteurs:	Sjoerd Hooymans
Eindverantwoordelijk:	Majken Cupido

Voorwoord

De digitale wereld en de fysieke wereld raken steeds meer vervlochten. Veiligheidsregio's zijn zoekende in hoe zij hierop in kunnen en moeten spelen. Daarom is in de Raad Directeuren Veiligheidsregio (RDVR) van juni 2018 opdracht gegeven tot het uitvoeren van een aantal activiteiten:

> Ontwikkelen van een Handreiking cybergevolgbestrijding.
> Ontwikkelen van een bestuurlijke netwerkkaart.
> Opzetten van een platform voor kennisuitwisseling.
> Investeren in de relatie met partners.
> Organiseren van een roadshow.

Vanwege de complexiteit van het onderwerp is niet sec aandacht besteed aan het ontwikkelen van bovenstaande producten, maar vooral aan uitgebreide vraagarticulatie. Voorliggend document is het resultaat van deze vraagarticulatie. Het document geeft daarnaast ontwikkelrichtingen aan voor veiligheidsregio's die zich verder willen voorbereiden op digitale verstoringen en ontwrichting.

De inhoud van dit document is ontwikkeld door de werkgroep Digitale ontwrichting, waarin verschillende veiligheidsregio's en het LOCC zitting hebben. Naast het ontwikkelen van dit document heeft de werkgroep ook contact gehad met het NCC/NCSC, heeft ze kennis en kunde gedeeld en heeft ze zich opgesteld als ambassadeur voor het thema. Omdat binnen het Veiligheidsberaad digitale ontwrichting ook een actueel thema is, heeft de werkgroep met haar activiteiten zoveel mogelijk aangesloten bij de bestuurlijke ontwikkelingen.

Het is belangrijk om te benoemen dat digitale ontwrichting en cyber een relatief nieuw thema is. Echter, uitgangspunt is altijd om te focussen op reguliere hulpverlening en reguliere structuren. De eigenschappen van 'cyber' moeten in dit reguliere werk als bijzondere impactcriteria meegenomen worden. Grote uitdagingen op dit vlak zijn het in beeld krijgen van de risico's, het hebben van een goede informatiepositie en het opbouwen van het juiste netwerk.

Ik heb het IFV gevraagd met dit document een eerste verkenning van de uitdagingen uit te voeren en hoop dat het helpt bij de zoektocht van veiligheidsregio's op het gebied van digitale ontwrichting. Aan het einde van het document geef ik aan wat ik als portefeuillehouder in ieder geval wil oppakken. Ik nodig eenieder die een bijdrage aan dit ontwikkelproces wil leveren uit contact met mij op te nemen!

Steven van de Looij
Algemeen directeur Veiligheidsregio Noord-Holland-Noord
RDVR-portefeuillehouder Digitale Ontwrichting en Cyber

Raad
Directeuren
Veiligheidsregio

Inhoud

Inleiding

Aanleiding

De digitale transformatie is één van de grootste veranderingen van deze tijd. Onze samenleving raakt steeds meer afhankelijk van en steeds meer vervlochten met digitale systemen. Deze ontwikkeling biedt veel voordelen, maar zorgt ook geregeld voor ongemak en hinder, bijvoorbeeld wanneer internetbankieren niet werkt vanwege een DDoS-aanval.[1] Of wanneer vluchten geannuleerd worden door een stroomstoring op Schiphol, waardoor het inchecksysteem beperkt beschikbaar is.[2]
Naast hinder hebben dit soort zaken ook impact op de fysieke veiligheid. Denk bijvoorbeeld aan de verkeerchaos die ontstond bij een grote storing op Schiphol waarbij mensen op de snelweg liepen.[2] Maar ook: kunnen hulpverleningsvoertuigen nog wel tanken als er niet betaald kan worden? Hoe zit het met de continuïteit van een ziekenhuis bij een langdurige stroomstoring?

Bovenstaande voorbeelden laten zien dat digitale verstoringen al snel gevolgen hebben voor ons dagelijks leven. Om ervoor te zorgen dat iedereen hetzelfde beeld heeft bij het begrip *digitale verstoringen*, zijn de volgende definities van belang.

Definitie digitale verstoringen
Iedere verstoring van een digitaal (ICT) systeem (moedwillig of door toeval, bedoeld of door een fout) die de (fysieke) veiligheid of openbare orde in een veiligheidsregio bedreigt. De oorzaak kan zowel in het digitale als fysieke domein liggen. In feite kan iedere verstoring een cybercomponent hebben. Ernstige en of langdurige digitale verstoringen kunnen tot maatschappelijke ontwrichting leiden; digitale ontwrichting. (Werkgroep Digitale ontwrichting).

Definitie cybersecurity (digitale veiligheid)
Het vrij zijn van gevaar of schade veroorzaakt door verstoring of uitval van ICT of door misbruik van ICT.

Definitie cybergevolgbestrijding
Alle activiteiten in het kader van bestrijden van de effecten van een incident waarvan de oorzaak en/of gevolg in het digitale domein ligt.

Cyber kan als vraagstuk spelen voor de eigen organisatie (continuïteit van eigen kritische processen; bedrijfscontinuïteit), de hulpverleningsketen (continuïteit van de hulpverlening) en de regionale crisisbeheersing (denk onder andere aan uitval van vitale infrastructuur: het beheersen van gevolgeffecten en het stimuleren van zelfredzaamheid en samenred-zaamheid).

[1] Zie voor meer informatie het artikel *Banken weer paar uur getroffen door DDoS-aanvallen* (NOS, 24 mei 2018).
[2] Zie voor meer informatie het artikel *Toegangswegen naar Schiphol tijdelijk gesloten om stroomstoring* (Blik Op Nieuws, 29 april 2018).

Figuur I.1 Verschillende soorten digitale verstoringen (COT, 2017)

Er zijn dus verschillende risicotypen die raken aan het digitale domein en die impact kunnen hebben op de fysieke veiligheid. Onderstaande tabel geeft enkele voorbeelden.

Tabel I.2 Voorbeelden van digitale verstoringen met impact op de fysieke veiligheid

Soort risico	Voorbeeld
Fysieke oorzaak, digitaal gevolg	> Brand bij een zendmast, die de telecommunicatie platlegt.[3] > Helikopter die in stroomleidingen vliegt, waardoor de elektriciteitsvoorziening uitvalt met consequenties voor telecommunicatie.[4]
Digitale oorzaak, fysiek gevolg	> Hack van een besturingsprogramma met invloed op waterkeringen. > Hack die betalingsverkeer platlegt met gevolgen voor de hulpverlening, zorg, openbare orde, etc. > Hack van een vuurwerkshow, met slachtoffers in publiek. > Verstoring van matrixborden die leidt tot verkeerschaos. > Telefoonstoring leidt tot onbereikbaarheid 112.
Digitale dynamiek, gevolgen voor openbare orde	> Oproep tot project X Haren. > Beïnvloeden van de verkiezingen. > Nepnieuws leidend tot rellen. > Zelfdoding door digitale chantage.
Openbare orde dynamiek, digitale gevolgen	> Maatschappelijke onrust zet hackcollectief aan tot het platleggen van overheidswebsites.
Informatie-incident (gecorrumpeerde data, datalek, privacy)	> Corrumpeerde ziekenhuisdata, die de kwaliteit van zorg onder druk zetten. > Gelekte gevoelige informatie, waardoor veiligheidssystemen in het geding komen.

[3] Zie voor meer informatie het artikel *Geen radio door brand in zendmast Rotterdam* (NOS, 30 maart 2016).
[4] Zie voor meer informatie het artikel *Telecomspecialist na stroomstoring: 'We zijn ons totaal niet bewust van onze kwetsbaarheid'* (Omroep Gelderland, 16 november 2017).

Digitale verstoringen kunnen (grote) gevolgen hebben voor de fysieke veiligheid in veiligheidsregio's. Veiligheidsregio's hebben als taak te zorgen voor continuïteit van een samenleving en inwoners goede hulpverlening te bieden. Daarom is het onontbeerlijk dat veiligheidsregio's zich goed voorbereiden op digitale verstoringen. Deze whitepaper kan veiligheidsregio's helpen op een goede manier in te spelen op digitale verstoringen.

Doel en doelgroep

Dit document heeft enerzijds tot doel het bewustzijn te vergroten en wil daarnaast concrete handvatten bieden in de vorm van to-do-lijsten; deze to-do-lijsten moeten nadrukkelijk als *suggesties* gezien worden. Tevens geeft het document een eerste inzicht in het cyber-netwerk. Deze informatie kan gebruikt worden bij de voorbereiding op digitale verstoringen. Dit document besteedt zowel aandacht aan risico's en kwetsbaarheden alsook aan het bestrijden van de gevolgen van een digitale verstoring. De gevolgen voor de (fysieke) veiligheid en de openbare orde staan altijd centraal. Deze whitepaper is voornamelijk gericht op het tactische en strategische niveau binnen veiligheidsregio's.

Reikwijdte en afbakening

Een digitale verstoring kan impact hebben op de veiligheidsregio zelf en impact hebben op de samenleving. Dit document legt de focus op de externe component, de cyberwaak-zaamheid en cybergevolgbestrijding (zie ook het Cyberkwadrant later in dit document). Een goede verbinding met de interne component (cyberveiligheid en cyberweerbaarheid) is hierbij wel van vitaal belang. Het is belangrijk te benadrukken dat een veiligheidsregio niet primair een leidende rol heeft, wanneer het digitale risico's en crises betreft. De veiligheidsregio richt zich voornamelijk op de gevolgbestrijding.

Context

Het werk van de werkgroep digitale verstoringen staat niet op zich. In den lande zijn allerlei ontwikkelingen gaande in het digitale of cyberdomein. Zo is er de Nederlandse Cybersecurity Agenda[5], en de minister geeft in de agenda risico- en crisisbeheersing (Grapperhaus, 2018) digitale weerbaarheid een prominente plaats. Ook in de Nationale Veiligheidsstrategie heeft digitale weerbaarheid een prominente plaats. Daarnaast is de rijksoverheid bezig met een update van het Nationaal Crisisplan ICT uit 2017. In de nieuwe versie – die naar verwachting tweede helft 2019 beschikbaar komt – wordt uitgebreid aandacht besteed aan de mogelijke fysieke gevolgen van een digitale verstoring en de rol van veiligheidsregio's hierin. Parallel hieraan wordt gewerkt aan de voorbereiding van ISIDOOR III, een nationale cyberoefening. De Wetenschappelijke Raad voor het Regeringsbeleid (WRR) heeft onlangs de uitkomsten van het onderzoek *Voorbereiden op digitale ontwrichting* gepresenteerd.[6]

[5] Zie voor meer informatie het onderwerp *Nederlandse Cybersecurity Agenda* op de website van het NCSC (NCSC, z.d.).
[6] Zie voor meer informatie het rapport *Voorbereiden op digitale ontwrichting* (WRR, 2019).

Ook op regionaal en bovenregionaal niveau is er veel aandacht voor het thema digitale verstoringen en ontwrichting. Verschillende regio's zijn heel actief bezig met het thema en hebben bijvoorbeeld digitale risico's opgenomen in hun regionaal risicoprofiel. Daarnaast wordt op het bestuurlijke niveau van het Veiligheidsberaad een bestuurlijk routeboek digitale ontwrichting ontwikkeld. Later in dit document wordt daar verder op ingegaan.

Leeswijzer

Hoofdstuk 1 gaat in op wat digitale verstoringen onderscheidt van andere incidenten. Daarbij wordt het cyberkwadrant toegelicht en beschreven voor welke opgaven de veiligheidsregio's staan. Hoofdstuk 2 is gericht op de praktijk en geeft concrete handvatten voor wat veiligheidsregio's kunnen doen om zich voor te bereiden op cyberincidenten. Hoofdstuk 3 brengt de relevante netwerken voor digitale verstoringen in beeld. Hoofdstuk 4 doet een eerste aanzet tot een uitvoeringsprogramma. Bijlage 1 bevat een afkortingenlijst.

Als laatste is het goed te benoemen dat dit document een levend document is. Vanwege de snelle ontwikkelingen in het digitale domein, kan het zijn dat het document op termijn geactualiseerd wordt.

1 Digitale verstoringen – wat is er anders?

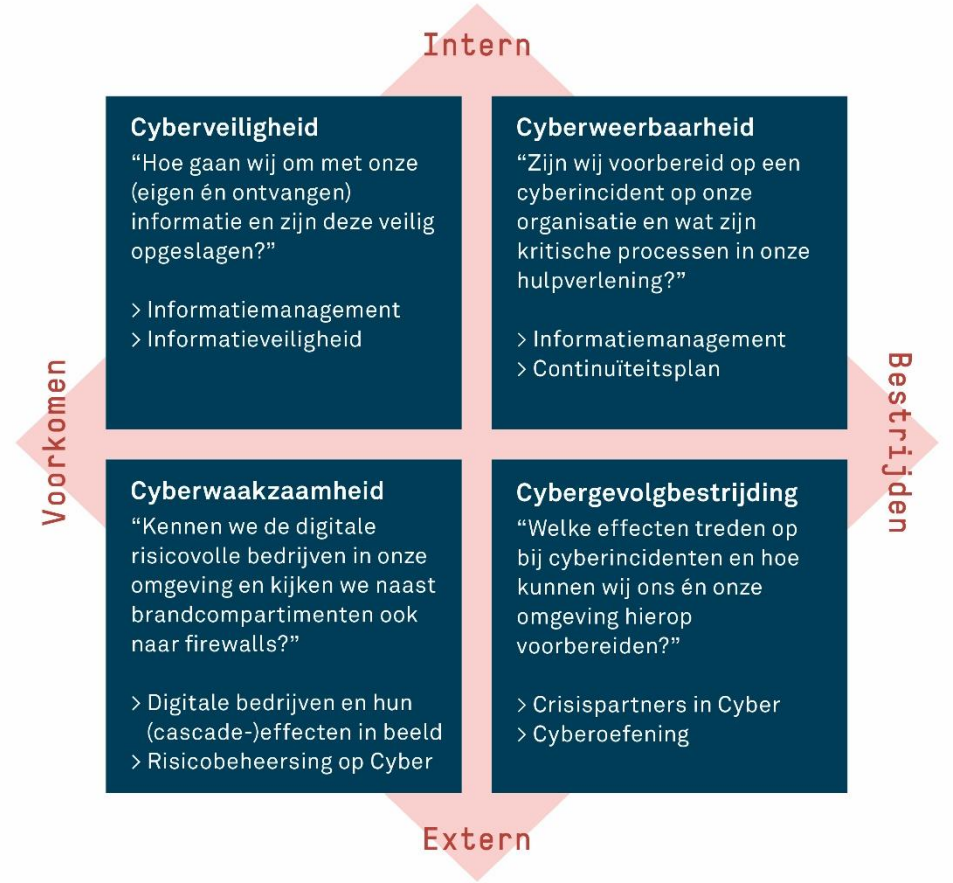
“Een veiligheidsregio heeft met digitale risico’s niets te maken” of “Een digitaal risico is net als alle andere risico’s; we weten als veiligheidsregio al precies wat we daarmee moeten.” Dit soort reacties zijn te horen als professionals uit de crisisbeheersing met elkaar spreken over digitale verstoringen. Maar welke uitdagingen met betrekking tot digitale verstoringen zijn er werkelijk? De basis voor de crisisbeheersing is de bestaande structuur. Er zijn echter een aantal zaken die digitale verstoringen en de gevolgbestrijding onderscheiden van een ‘regulier’ of ‘klassiek’ incident:

> De effecten van een digitale verstoring beperken zich niet tot territoriale grenzen en kan fluctueren; er is mogelijk geen duidelijke bronregio aan te wijzen. Tevens kunnen geopolitieke cyberdynamieken regionaal en lokaal grote impact hebben. De aanval op een bedrijf in Oekraïne had bijvoorbeeld gevolgen in de Rotterdamse Haven bij het bedrijf Maersk.
> Voorspellende waarden met betrekking tot schaal, tijdsduur, ernst en cascade-effecten zijn beperkt. Dit maakt het lastig om op een consistente manier met scenariodenken te werken en het handelingsperspectief wordt hierdoor onduidelijker.
> Na een incident is het niet altijd eenvoudig te bepalen of de betrokken systemen weer te vertrouwen zijn.
> Bij een digitale verstoring is het niet altijd (vaak niet) aan de veiligheidsregio om de oorzaak te bestrijden. De veiligheidsregio heeft echter wel met de gevolgen te maken.
> Het feit dat de digitale wereld volledig vervlochten is met de fysieke wereld, maakt dat iedere crisis of ieder incident een cybercomponent kan hebben. Deze alomvattendheid van het risicotype cyber onderscheidt het van andere risico’s.

Kwetsbaarheidsparadox
“De netwerksamenleving is zowel de oplossing als de oorzaak (het ‘probleem’) van digitale verstoringen. Om hier op een goede manier mee om te gaan is het zaak om grip te krijgen op het onbekende.” Menno van Duin, lector Crisisbeheersing (2011).

1.1 Cyberkwadrant

Het digitale domein in relatie tot veiligheidsregio's kent meerdere aspecten. Veiligheidsregio IJsselland heeft deze in een cyberkwadrant ondergebracht. De werkgroep Digitale ontwrichting omarmt deze onderverdeling.



Figuur 1.1 Het cyberkwadrant (Veiligheidsregio IJsselland, 2018)

Een digitale verstoring kan impact hebben op de veiligheidsregio zelf. Er kan bijvoorbeeld essentiële informatie verloren gaan of kantoorautomatiseringsprocessen kunnen uitvallen. Om dit te ondervangen zijn een goede cyberveiligheid en cyberweerbaarheid essentieel. Daarnaast kan een digitale verstoring impact hebben op de samenleving; impact waarvan de veiligheidsregio de gevolgen moet bestrijden. Zoals eerder gezegd gaat deze whitepaper met name in op digitale verstoringen die impact hebben op de samenleving en ligt de focus dus op cyberwaakzaamheid en cybergevolgbestrijding, de externe component. Een goede verbinding met de interne component is hierbij wel van vitaal belang. Een koppeling tussen alle vier de onderdelen van het cyberkwadrant is dus essentieel!

Bij cyberwaakzaamheid en cybergevolgbestrijding kijken we zowel naar risicobeheersing als naar crisisbeheersing en koppelen dit aan consequenties voor de veiligheidsregio zelf. Hierbij is het belangrijk om te werken vanuit bestaande structuren en instrumenten (zoals het regionaal risicoprofiel).

1.2 Opgaven voor veiligheidsregio's

Wat betekenen het verschillen van digitale verstoringen en ontwrichting ten opzichte van 'traditionele' risico's concreet voor risicobeheersing en crisisbeheersing? De veiligheids-regio's staan voor de volgende opgaven:

> Een goede informatiepositie verkrijgen.
> Risico's in beeld krijgen.
> Het interne en externe gedeelte van het cyberkwadrant verbinden.
> Zorgen voor aansluiting op het cyber resilience netwerk.

Door deze vier opgaven heen loopt de opgave van het opbouwen en uitbouwen van een cyber-relevant netwerk, op zowel het regionale als nationale niveau.

1.2.1 Informatiepositie

Voor adequate risicobeheersing en crisisbeheersing is een goede informatiepositie essentieel. Een goede informatiepositie wordt verkregen door te zorgen voor de juiste informatielijnen (inter-)regionaal, landelijk en met ketenpartners waardoor informatie zowel verkregen als geduid kan worden. Op basis hiervan kan de veiligheidsregio bepalen wat ze moet, kan en wil doen. Die informatiepositie van veiligheidsregio's is op het gebied van cyber nog onvoldoende. Op dit moment zijn de informatielijnen tussen verschillende overheids-lagen nog niet gestroomlijnd of geformaliseerd, is de 'cyberkennis' in eigen huis onvoldoende en weten de veiligheidsregio's niet altijd goed welke partners hen van goede informatie en duiding kunnen voorzien.

Informatielijnen

In onderstaand kader staan de taken en verantwoordelijkheden van verschillende overheidspartijen ten aanzien van cyberincidenten beschreven.

Taken en verantwoordelijkheden overheidscyberpartijen

Nationaal Cyber Security Center (NCSC)

> Vergroten van de digitale weerbaarheid, primair via organisaties binnen de rijksoverheid en vitale processen. Publiek-private samenwerking is uitgangspunt.
> Coördinerende rol (op inhoud) bij een nationale cybercrisis in samenwerking met het NCC.
> Delen van informatie om de digitale weerbaarheid van Nederland te versterken.
> Aanjagen van zelforganisatie door andere partijen, helpen bij het opzetten van samenwerkingsverbanden (bijv. Information Sharing and Analysis Centre (ISAC) en Computer Security Incident Response Team (CSIRT)).
> Database beschikbaar stellen met beveiligingsadviezen, factsheets, checklists, handreikingen etc.

NCTV / NCC

> 24/7 beschikbaar voor hulp, vragen en afstemming.
> Kan op verzoek van de betrokken regio's een coördinerende rol oppakken richting betrokken veiligheidsregio's en landelijke partners.

Veiligheidsregio

- Indien er sprake is van meerdere betrokken veiligheidsregio's en er geen duidelijke aanwijsbare incidentregio is, wordt (in overleg) een coördinerende veiligheidsregio aangewezen, waarbij de communicatieadviseurs van betrokken partners kunnen aansluiten.
- Eventueel kan het LOCC-B op verzoek van de betrokken veiligheidsregio's operationeel advies uitbrengen.

Gemeente/burgemeester

- De burgemeester of voorzitter veiligheidsregio is verantwoordelijk voor de aanpak van de effecten van de verstoring op de openbare orde en veiligheid.

Informatiebeveiligingsdienst voor gemeenten (IBD)

- De Informatiebeveiligingsdienst (IBD) is de sectorale CERT/CSIRT voor alle Nederlandse gemeenten en onderdeel van de VNG. De IBD ondersteunt gemeenten op het gebied van informatiebeveiliging. De IBD is voor gemeenten het schakelpunt met het NCSC.
- Het Computer Emergency Response Team (CERT) van de Informatiebeveiligingsdienst voor gemeenten (IBD) kan de gemeente ondersteuning leveren in geval van (dreigende) incidenten en crisissituaties op het vlak van informatiebeveiliging.

Vitale partners

- Aanbieders van vitale processen in de sectoren energie, drinkwater, keren en beheren, telecom en financiën, als ook de mainports Rotterdam en Schiphol zijn verplicht om ernstige (meldplichtige) ICT-incidenten in hun vitale processen te melden aan het NCSC.
- Aanbieders van vitale processen communiceren zelf over de storing, de verwachte duur daarvan, herstelwerkzaamheden en handelingsperspectieven.

Bij een (mogelijke) dreiging of incident worden veiligheidsregio's niet altijd gealarmeerd door het Nationaal Cyber Security Center (NCSC). De formele informatielijn loopt via het NCC; daarom is het verdiepen en verbreden van die informatielijn een belangrijke opgave. Zonder enige duiding van het incident (soort, schaal en tijdsduur) is het immers moeilijk te komen tot een handelingsperspectief voor de burgers, hulpdiensten en bestuurders.

Cyberkennis in huis

Veiligheidsregio's hebben ook niet alle relevante 'cyberkennis' zelf in huis en vinden het moeilijk de informatie die er wel is te duiden. Om in staat te zijn een vertaalslag te maken van technische informatie naar handelingsperspectief is kennis nodig.

Informatie van partners

Digitale verstoringen zijn een redelijk nieuw crisistype of aspect van klassieke incidenten. Daardoor is nog niet altijd duidelijk welke partners de juiste informatie kunnen geven en moeten er publiek-private samenwerkingen worden opgebouwd. Vertrouwen en wederzijds begrip zijn daarbij een basisvoorwaarde. Voor partners moet het helder zijn dat veiligheidsregio's in staat zijn met gevoelige informatie om te gaan.

1.2.2 Risico's in beeld

In het proces van risicobeheersing is het aan te raden ook met een 'cyberbril' naar de omgeving te kijken. Denk bijvoorbeeld aan een verzamelpand waarin een datacenter van een ziekenhuis gehuisvest is. Voor het in beeld krijgen van de regionale risico's kan een samenwerkingsnetwerk van nut zijn. De veiligheidsregio kan overwegen een eigen regionaal samenwerkingsnetwerk op te zetten of dit bovenregionaal te organiseren. Dit nieuwe netwerk is van belang voor het in kaart brengen van de risico's, maar zeker ook in de warme fase van de crisisbeheersing. Net als bij andere crisistypen is het aan te bevelen om al in de koude fase de contacten te leggen en te onderhouden, zodat ze in de warme fase makkelijk en snel aangesproken kunnen worden om de beschikbare informatie te helpen duiden en te adviseren over handelingsperspectieven.

1.2.3 Verbinding cyberveiligheid en -weerbaarheid aan cyberwaakzaamheid en -gevolgbestrijding in eigen huis

Cyberwaakzaamheid en -gevolgbestrijding aan de ene kant en cyberveiligheid en -weerbaarheid aan de andere kant zijn vaak verschillende en gescheiden disciplines binnen een veiligheidsregio. Voor beiden zijn andere kennis en vaardigheden nodig. Kennis van het digitale domein bij de cyberveiligheid-/-weerbaarheidmedewerkers in de eigen organisatie kan van grote waarde zijn bij cyberwaakzaamheid/-gevolgbestrijding (risicobeheersing en crisisbeheersing). Denk bij risicobeheersing bijvoorbeeld aan het in beeld hebben van belangrijke digitale infrastructuur in de regio.

Het is dus van belang een goede koppeling tussen de verschillende onderdelen van het cyberkwadrant te organiseren. Dit helpt zowel als een uitval de eigen organisatie (bedrijfs-continuïteit) raakt als bij een verstoring die de samenleving raakt.
Zo kunnen eigen ICT-medewerkers de helpende hand bieden bij:

> het vertalen van complexe informatie naar eenvoudige, communiceerbare informatie voor interne collega's en naar de buitenwereld
> het inschatten van risico's (en cascade-effecten)
> bedrijfscontinuïteitmanagement: wat zijn de gevolgen wanneer systemen worden afgesloten of uitgezet en hoeveel tijd kost het deze weer draaiend te krijgen.

1.2.4 Aansluiting op cyber resilience netwerk

In een ISAC wordt kennis gedeeld over de cyberveiligheid en -weerbaarheid van de eigen organisatie; dit gebeurt op sectorniveau. Een CERT speelt een belangrijke rol bij het herstellen van een cyberincident in de eigen organisatie; de cyberweerbaarheid. In het land is een netwerk van verschillende sectorale CERT's en ISAC's (cyber resilience netwerk) aanwezig, waarin het NCSC een spilfunctie heeft.

Veiligheidsregio's participeren nog onvoldoende in het reguliere cyber resilience netwerk. De interne cyberveiligheid en -weerbaarheid zou gebaat zijn bij een goede aansluiting bij dit netwerk. Ook voor de cyberwaakzaamheid en -gevolgbestrijding zou aansluiting bij deze netwerken de informatiepositie en -duiding kunnen verbeteren.

Om de eigen cyberweerbaarheid te vergroten, is het aan te bevelen om aansluiting bij een al bestaande CERT-structuur te verkennen. Daarnaast is het een positieve ontwikkeling dat momenteel de oprichting van een sectorale veiligheidsregio-ISAC verkend wordt. In geval van een (bijna)crisis leidt deelname aan ISAC/CERT/netwerken tot betere duiding van informatie, die leidt tot een beter handelingsperspectief voor zowel de eigen organisatie (inclusief voorbereidingstijd en reactietijd) als de samenleving. Bijvoorbeeld, stel dat de kantoorautomatisering uitvalt; door deelname in een ISAC en/of CERT weet je eerder wat er aan de hand is, hoe lang het duurt en kun jesneller terugkeren naar de reguliere gang van zaken.

2 Aan de slag!

Dit hoofdstuk geeft een aantal suggesties voor veiligheidsregio's om zich voor te bereiden op digitale verstoringen in de samenleving. Door gesprekken met verschillende experts en de werkgroep Digitale ontwrichting zijn onderstaande to-do-lijsten tot stand gekomen; deze moeten nadrukkelijk gezien worden als *mogelijkheid* c.q. *suggestie* en niet als verplichtging. De to-do-lijsten gaan dus om de externe component, de onderste twee onderdelen van het cyberkwadrant: cyberwaakzaamheid en cybergevolgbestrijding. Aan de orde komen aandachtspunten voor zowel risicobeheersing als crisisbeheersing als crisiscommunicatie.

2.1 Cyberwaakzaamheid

2.1.1 Risicobeheersing

Vanwege de afwijkingen van de klassieke risico's, is het belangrijk om in het regionaal risicoprofiel ook expliciet aandacht te besteden aan digitale verstoringsrisico's. Een cyberwaakzame regio begint bij het in beeld hebben en houden van deze risico's. Hiervoor kan een omgevingsanalyse gedaan worden. Belangrijk is dat de bestaande structuren en instrumenten (zoals het regionaal risicoprofiel) centraal blijven staan.

Een aantal groepen in de samenleving zijn extra kwetsbaar bij een digitale verstoring, zoals oudere inwoners, inwoners afhankelijk van medische apparatuur, midden- en kleinbedrijf en ziekenhuizen. Gemeenten zijn steeds actiever op het gebied van voorlichting richting deze groepen. Afgewogen kan worden of veiligheidsregio's hier ook een rol in willen spelen.

Omgevingsanalyse

Veel digitale risico's zitten in de omgeving 'verborgen'; het is niet direct duidelijk waar ze zich bevinden. Bij het maken van een cyber-omgevingsanalyse kunnen onderstaande aandachtspunten richting geven.

To do's bij een omgevingsanalyse

1. Breng in kaart waar zich in de regio essentiële data-/ICT-knooppunten bevinden die bij een verstoring een gevaar opleveren voor de (fysieke) veiligheid.
   Bijvoorbeeld: ICT die essentieel is voor het functioneren van een ziekenhuis.
2. Breng in beeld welke bedrijven en organisaties in de regio het meest kwetsbaar zijn voor digitale ontwrichting. Houd hierbij rekening met maatschappelijke impact:
   - Worden er essentiële processen aangestuurd?
   - Welke risico's horen daarbij?
3. Breng in beeld welke vitale en essentiële diensten/objecten afhankelijk zijn van ICT/telecom.
4. Breng in beeld welke data kwetsbaar zijn voor verstoring/corruptie. Denk hierbij bijvoorbeeld aan datasystemen in de zorg.
5. Breng in kaart welke groepen in de samenleving extra kwetsbaar zijn bij een digitale verstoring, zoals oudere inwoners, inwoners afhankelijk van medische apparatuur, midden- en kleinbedrijf en ziekenhuizen. Stem met gemeenten af wie welke voorlichting richting deze groepen geeft.

2.2 Cybergevolgbestrijding

2.2.1 Koude fase: voorbereiding en kennis

In de koude fase bereidt de veiligheidsregio zich voor door planvorming, OTO en werken aan een netwerk dat zowel koud als warm bijdraagt aan een betere crisisbeheersing.

To do's voor voorbereiding op cybergevolgbestrijding

1. Zorg voor voldoende bewustzijn op het thema digitale verstoringen en ontwrichting. De (fysieke) gevolgen van een digitale verstoring moeten goed geborgd zijn in planvorming, OTO en contactenlijsten.
2. Zorg dat de in het risicoprofiel geïdentificeerde risico's op een goede manier verwerkt worden in de reguliere structuren en voorbereidingen.
3. Breng in beeld hoe de organisatie continuïteit van hulpverlening garandeert bij ICT-uitval in de eigen organisatie; zorg voor cyberweerbaarheid. Zorg voor een goede informatiepositie middels een ISAC.
4. Ga oefenen met o.a. de volgende zaken:
   - Rol bestuur.
   - Relatie rijk – regio.
   - Relatie algemene keten – functionele keten.
   - Welke risico's en cascade-effecten zijn er?
   - Welke private partijen zijn bij welke incidenten aan tafel gewenst?

Om een cyberincident te bestrijden, is het belangrijk te beschikken over de juiste kennis. Alle relevante kennis om een crisis te bestrijden, moet je in huis hebben of je moet weten waar deze te vinden is. Ook moeten de relevante personen binnen een organisatie aan elkaar gekoppeld zijn.

To do's om een kennisbasis te borgen

1. Zorg voor een goede verbinding in de eigen organisatie tussen cyberveiligheid en cybergevolgbestrijding.
2. Zorg voor voldoende kennis in huis om de digitale taal en de digitale wereld te begrijpen. Denk daarbij ook aan het OTO-proces.
3. Zorg voor een kennisnetwerk op het digitale domein dat ook in de warme fase bereikbaar is.

2.2.2 Lauwe fase: informatie(positie) en duiding

Bij een dreigingsscenario is het belangrijk informatie te verzamelen en in scenario's te denken om zo goed mogelijk te kunnen anticiperen op wat mogelijk komen gaat.

To do's bij een dreiging

1. Zoek contact met partijen als het NCSC, NCC, LOCC, een sectorale CERT of het IBD. Weten zij meer?
   - Welke informatie hebben zij over de oorzaak, soort, schaal en tijdsduur?
   - Breng de mogelijke effecten in kaart en bepaal hoe erg die effecten zijn.
   - Wat zou de schaalbaarheid kunnen zijn en wat heeft de prioriteit?
   - Breng in kaart welke scenario's er zijn en wat de maatschappelijke impact is van die scenario's.

2.2.3 Warme fase: informatie en duiding voor cybergevolgbestrijding

Hoe kan de veiligheidsregio (op hoofdlijnen) in de warme fase acteren tijdens een digitale verstoring?

To do's

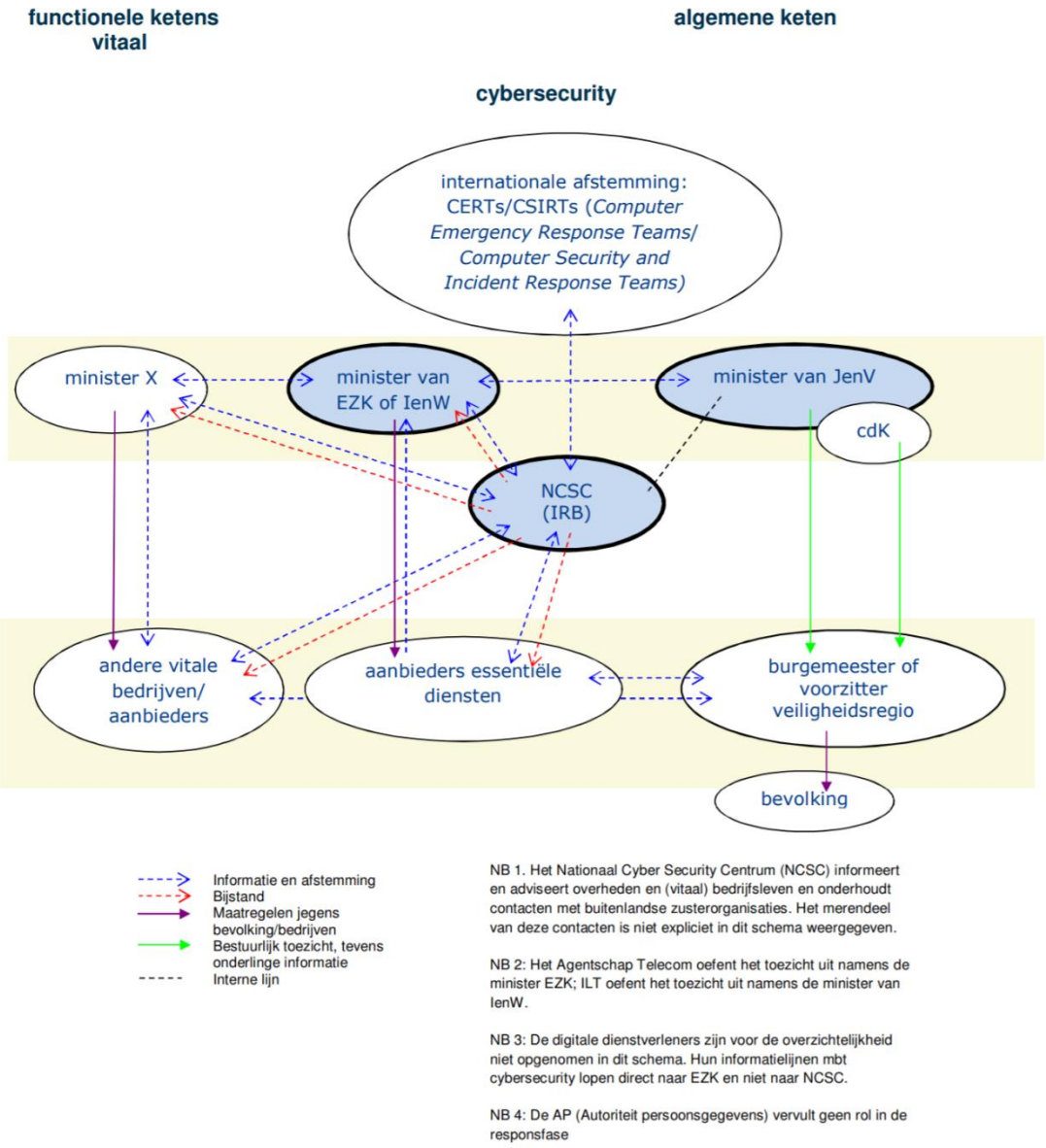
1. Zorg dat er duidelijkheid is over de rol die de veiligheidsregio inneemt of wilt innemen.
2. Zorg dat duidelijk is met welke partners de veiligheidsregio kan samenwerken en hoe. Denk hierbij in ieder geval aan de volgende partijen:
   - de driehoek
   - NCC/LOCC/NCSC
   - commerciële partijen die problemen kunnen oplossen
   - aanbieders van vitale diensten
   - kwetsbare bedrijven in de regio.
3. Zorg voor de juiste afstemming met andere veiligheidsregio's. Spreek af wie de coördinatie op zich neemt bij het ontbreken van een bronregio.
4. Zorg dat bij inzet van de brandweer duidelijk is of zich in een pand of object essentiële digitale en/of ICT-diensten bevinden.
5. Zorg dat crisisteams de juiste digitale kennis aan boord hebben. Denk hierbij aan liaisons uit de IT-/ICT-sector.

2.3 Crisiscommunicatie

In samenwerking met het netwerk Crisiscommunicatie heeft het IFV *Crisiscommunicatietips voor incidenten met een cybercomponent (digitale verstoringen)* (IFV, 2019a) opgesteld. Deze zijn te vinden in het dossier Crisiscommunicatie op IFV Kennisplein.

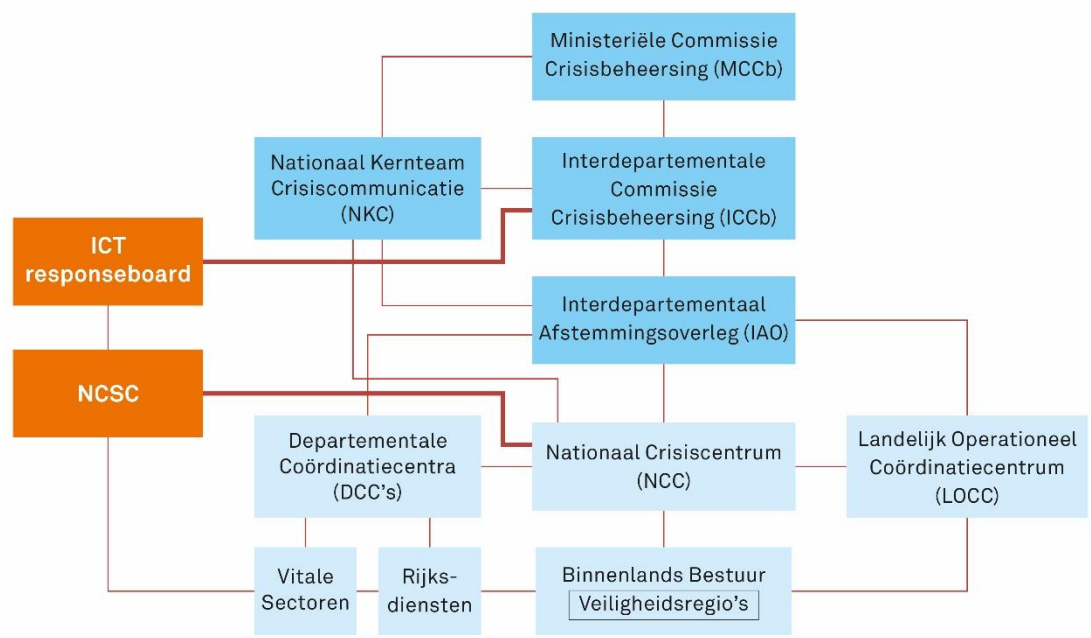
3 Netwerk in beeld

Het is voor veiligheidsregio's essentieel het nationale cybernetwerk te kennen. Onder nationaal netwerk verstaan we het netwerk waarin iedere veiligheidsregio zich bevindt. De veiligheidsregio verhoudt zich in dit netwerk tot de rijksoverheid, een provincie of een nationaal georganiseerde aanbieder van een vitale dienst, bijvoorbeeld een telecom- of stroomaanbieder.
In de *Bestuurlijke Netwerkkaart 21b Cybersecurity* staan de relaties tussen de algemene en functionele keten.



Figuur 3.1 Relatie algemene en functionele keten bij cyberincidenten (IFV, 2019b)

De nationale crisisstructuur met betrekking tot cyberincidenten ziet er als volgt uit.



Figuur 3.2 Nationale crisisstructuur cyberincidenten/digitale verstoringen (NCTV, 2019)

Noot: het nationale cyber-relevante crisisnetwerk is momenteel volop in ontwikkeling. Het kan zijn dat bovenstaande afbeeldingen op zeker moment niet meer de realiteit weergeven. Zodra nieuwe structuren bekend zijn, zullen deze in de whitepaper verwerkt worden.

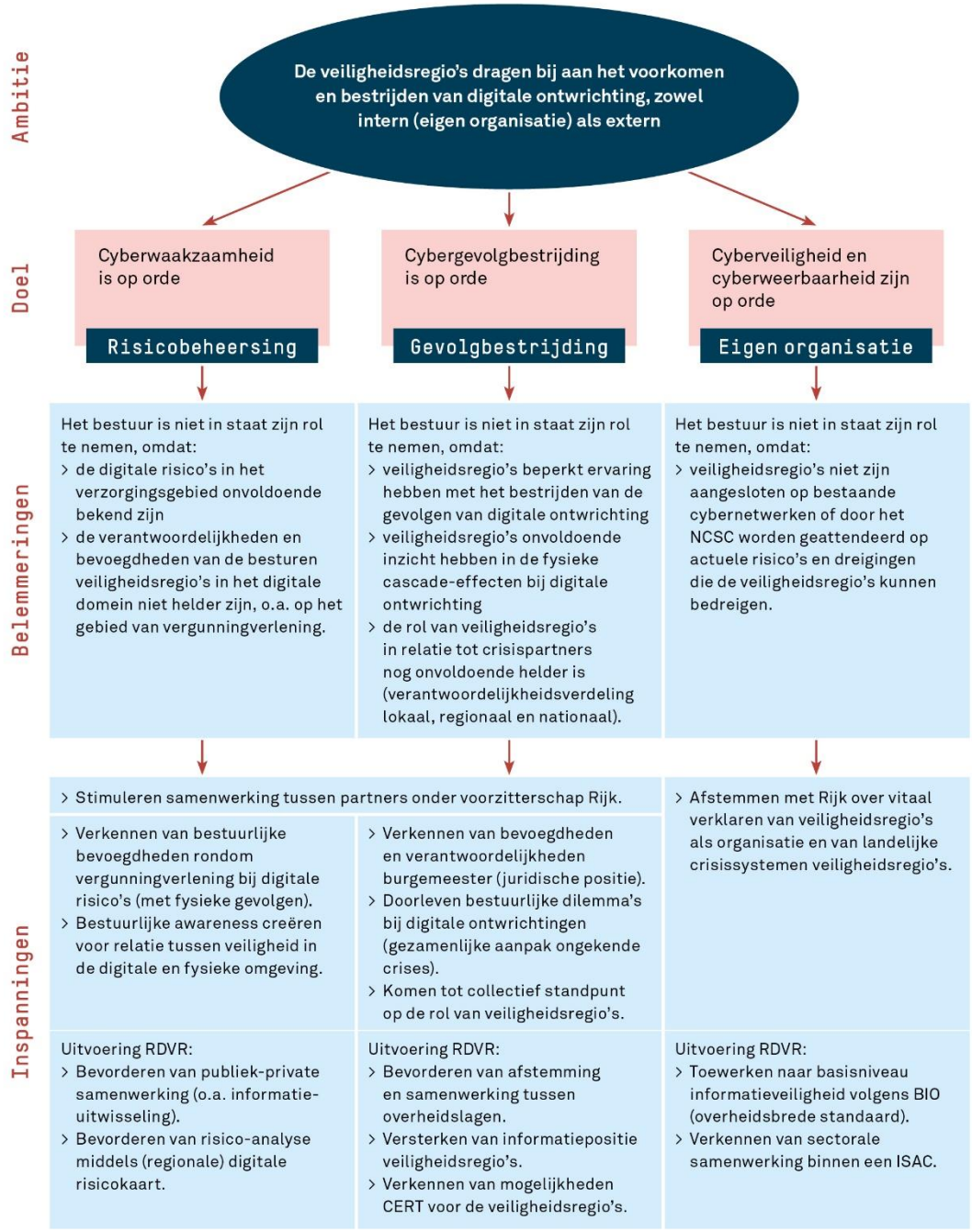
In aansluiting hierop is het advies een 'cyber-relevant' regionaal netwerk op te bouwen en uit te breiden. Het kennen van de juiste partijen en de juiste personen bij die partijen is een eerste grote stap naar meer inzicht in de digitale risico's en belangrijk voor de lauwe en warme fase. Het is aan te bevelen dit netwerk al op te bouwen in de koude fase, zodat er vertrouwen in en begrip voor elkaar ontstaat.

To do's bij netwerken

1. Zorg voor de juiste gesprekspartners met betrekking tot digitale verstoringen in het bestaande netwerk.
2. Breng in beeld welke nieuwe netwerkpartners nog nodig zijn.
3. Zorg voor een goede aansluiting op de bestaande cyber resilience structuren als NCSC, ISAC en CERT. Door bij dit soort partijen erkend en herkend te worden vergroot je de cyberweerbaarheid en tevens de informatiepositie.
4. Biedt als veiligheidsregio een platform om partners op het thema Cyber bij elkaar te brengen. Dit platform dient voor ontmoeting en uitwisseling van kennis en ervaring voor zowel publieke als private partijen.
5. Maak een regionale netwerkkaart. Denk daarbij o.a. aan de volgende partijen:
   - politie/OM
   - aanbieder vitale infrastructuur
   - commerciële IT-specialisten
   - kwetsbare MKB'ers.

4 Uitvoeringsprogramma

Parallel aan het traject van de werkgroep is er – in opdracht van het Veiligheidsberaad – een bestuurlijk *Routeboek digitale ontwrichting* (Veiligheidsberaad, 2019) in ontwikkeling. Het routeboek schrijft de volgende procesmatige aanpak voor.



Figuur 4.1 Procesmatige aanpak digitale ontwrichting (Veiligheidsberaad, 2019)

4.1 Synergie creëren

De werkgroep heeft geconstateerd dat de opgaven die het bestuurlijke routeboek benoemt op veel vlakken overeenkomen met de door de werkgroep gesignaleerde opgaven. Het activiteitenprogramma dat de werkgroep voor ogen heeft, sluit dan ook naadloos aan op het bestuurlijke routeboek. Voor ieder van de drie bestuurlijke doelstellingen is hieronder beschreven welke invulling de werkgroep hieraan wil geven. In de loop van 2019 moet per product en/of resultaat concreet gemaakt worden hoe hier precies invulling aan gegeven moet worden en hoe dit gefinancierd kan worden. Dit zal procesmatig benaderd worden en de RDVR-portefeuillehouder wordt hierbij ondersteund door een beleidsadviseur van het IFV.

4.1.1 Cyberwaakzaamheid is op orde

De portefeuillehouder en werkgroep hebben de volgende concrete producten en resultaten voor ogen:

> **Instrumenten/handvatten ter ondersteuning van risicobeoordeling**
Veiligheidsregio's hebben behoefte aan instrumenten en handvatten, die helpen bij het met een cyberbril kijken naar de omgeving om op die manier cyberrisico's mee te kunnen nemen in het regionaal risicoprofiel. Hierbij wordt samenhang gezocht met de methodiek van de *Handreiking Regionaal Risicoprofiel* (Politie, NVBR, GHOR Nederland & Coördinerend Gemeentesecretarissen, 2009). Tevens wordt gekeken wat er geleerd kan worden van het nationaal cybersecurity beeld.

> **Cyber-relevante (regionale) stakeholdermap**
Veiligheidsregio's hebben behoefte aan het in beeld hebben en houden van het relevant cyber-netwerk. Dit helpt zowel bij het in beeld krijgen van risico's alsook bij het hebben en houden van een goede informatiepositie. Er wordt een voorstel uitgewerkt voor het ontwikkelen van deze stakeholdermap.

> **Stimuleren van (regionale) samenwerking tussen overheden, bedrijven en kennisinstellingen**
Op basis van het delen van best practices zal een impuls gegeven worden aan publiek-private samenwerking op cybergebied. Deze samenwerking heeft als doel te helpen bij het weerbaar en waakzaam worden en blijven van de samenleving en veiligheidsregio's. Tevens zal nadrukkelijk de samenwerking met kennisinstellingen gezocht worden.

4.1.2 Cybergevolgbestrijding is op orde

De portefeuillehouder en werkgroep hebben de volgende concrete producten en resultaten voor ogen:

> **Bovenregionaal platform**
Omdat alle veiligheidsregio's aan het zoeken en ontdekken zijn op dit vlak, is er behoefte aan het bovenregionaal uitwisselen van kennis en ervaring. Momenteel gebeurt dit al in de werkgroep Digitale ontwrichting. Het platform kan dienen als klankbordgroep voor de overige te ontwikkelen producten en resultaten en zal digitaal gefaciliteerd worden.

> **Handreiking cybergevolgbestrijding**
Er is behoefte aan een handreiking die veiligheidsregio's helpt met de juiste duiding en handelingsperspectieven. Indien de *Handreiking cybergevolgbestrijding* die door de G4 ontwikkeld wordt (najaar 2019) voldoende in die behoefte voorziet, zal deze omarmd worden.

> **Informatielijnen en -positie versterken**
Het is erg belangrijk dat de informatielijnen rijk - regio (NCSC/NCC/LOCC - regio) en functionele keten - algemene keten goed lopen. Het gaat hier expliciet om informatie die nodig is om in de warme fase aan cybergevolgbestrijding te doen. Door de RDVR-portefeuillehouder wordt in afstemming met de bestuurlijke (VB-)portefeuillehouder verkend hoe beter afgestemd kan worden met bovenstaande partijen. De actualisatie van het *Nationaal crisisplan ICT* zal hierbij van toegevoegde waarde zijn.

4.1.3 Cyberveiligheid en cyberweerbaarheid zijn op orde

De portefeuillehouder en werkgroep hebben de volgende concrete producten en resultaten voor ogen:

> **Bij het in ontwikkeling zijnde ISAC het crisisbeheersing perspectief inbrengen**
De vakgroep Informatieveiligheid is bezig met de doorontwikkeling tot een ISAC. Het is van belang dat bij dit proces het perspectief van crisisbeheersing voldoende meegenomen wordt. Hier zal in Q3 en 4 van 2019 op ingezet worden. Dit proces verloopt in nauwe samenhang met het NCSC.

> **Meedenken over eventuele CERT ontwikkeling**
Voor de veiligheidsregio's is momenteel geen CERT-functie ingericht. De portefeuille-houder en werkgroep zullen met de vakgroep Informatieveiligheid meedenken over de kosten en baten van een al dan niet op te richten CERT/het aansluiten bij een bestaande CERT-structuur.

Literatuur

COT. (2017). *De veiligheidsregio en cyberagenda 2017 – 2020: voorbereid, betrokken en betrouwbaar.*

Grapperhaus, F. (2018, 1 november). *Agenda risico- en crisisbeheersing 2018-2021* [Kamerbrief]. Geraadpleegd van https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2018/11/12/tk-agenda-risico-en-crisisbeheersing-2018-2021/tk-agenda-risico-en-crisisbeheersing-2018-2021.pdf

Instituut Fysieke Veiligheid. (2019a). *Crisiscommunicatietips voor incidenten met een cybercomponent (digitale verstoring*). Opgehaald van https://www.ifv.nl/kennisplein/Documents/20190425-IFV-Crisiscommunicatietips-voor-incidenten-met-een-cybercomponent.pdf

Instituut Fysieke Veiligheid. (2019b). *Bestuurlijke Netwerkkaart 21b Cybersecurity.* Opgehaald van https://www.ifv.nl/kennisplein/Documents/201904-IFV-BNK-21b-Cybersecurity.pdf

NCTV. (2019). *Cybergevolgbestrijding – structuren, rollen en verantwoordelijkheden bij incidenten met een cyber-component.*

Politie, NVBR, GHOR Nederland & Coördinerend Gemeentesecretarissen. (2009). *Handreiking Regionaal Risicoprofiel*. Opgehaald van https://www.brandweer.nl/media/5367/handreikingregionaalrisicoprofiel1-10.pdf

Van Duin, M. (2011). *Veerkrachtige crisisbeheersing: nuchter over het bijzondere.* Opgehaald van https://www.ifv.nl/kennisplein/lectorale-redes/publicaties/veerkrachtige-crisisbeheersing-nuchter-over-het-bijzondere

Veiligheidsberaad. (2019). *Routeboek digitale ontwrichting*. Document is in ontwikkeling.

Veiligheidsregio IJsselland. (2018). *Oost5 4.3 Bijlage Cybernotitie.*

Bijlage 1
Afkortingenlijst

CERT	Computer Emergency Response Team
CSIRT	Cyber Security and Incident Response Team
DCC	Departementaal CoördinatieCentrum
DDoS	Distributed Denial of Service
ICCb	Interdepartementale Commissie Crisisbeheersing
ICT	Informatie- en communicatietechnologie
IAO	Interdepartementaal Afstemmingsoverleg
IRB	ICT Respons Board
ISAC	Information Sharing & Analysis Center
LOCC	Landelijke Operationeel Coördinatiecentrum
MCCb	Ministeriële Commissie Crisisbeheersing
MKB	Midden- en kleinbedrijf Nederland
NCC	Nationaal Crisiscentrum
NCSC	Nationaal Cyber Security Centrum
NCTV	Nationaal Coördinator Terrorismebestrijding en Veiligheid
NCV	Noodcommunicatievoorziening
NKC	Nationaal Kernteam Communicatie