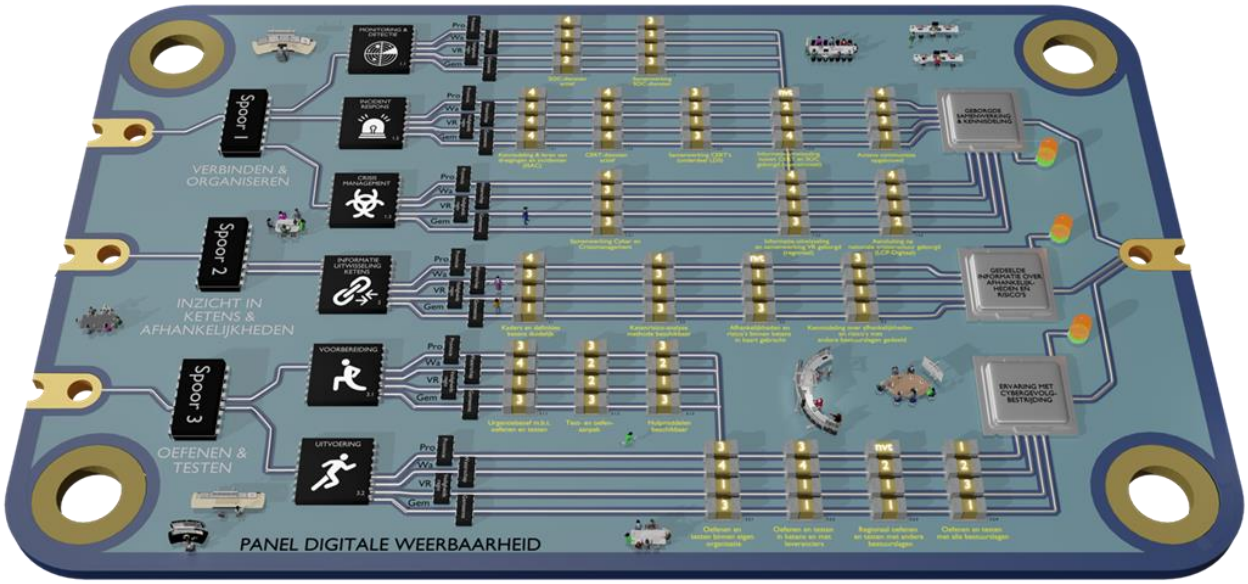
Rapport

Samenwerkingskansen digitale weerbaarheid decentrale overheden

Directie Digitale Samenleving
helpt Decentrale Overheden
voorbereiden op Digitale Ontwrichting



Van	ICTU
Versie	definitief
Datum	12-11-2021

Inhoudsopgave

1. Inleiding

1.1. Digitale ontwrichting: van incident naar crisis

In 2019 heeft de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) in haar rapport "Voorbereiden op digitale ontwrichting" extra aandacht gevraagd voor de risico's van toenemende digitalisering voor de maatschappij en de ontwrichtende effecten die incidenten met een digitale component kunnen hebben. De WRR wees erop dat digitale incidenten, door onderlinge afhankelijkheden en de complexiteit en diversiteit van netwerk- en informatiesystemen, snel grootschalige en grensoverschrijdende effecten kunnen hebben. Deze incidenten kunnen vitale processen in de samenleving aantasten en zelfs leiden tot ernstige crisissituaties. De WRR noemde dit type ontwrichting 'digitale maatschappelijke ontwrichting', of kortweg 'digitale ontwrichting'.

De WRR signaleerde tegen deze achtergrond dat de gevolgen van digitale incidenten in de praktijk nog onvoldoende aandacht krijgen binnen de bestaande crisisstructuren.

Naar aanleiding van dit WRR-rapport (en de evaluatie van de Citrix-problematiek) heeft de BZK-directie Digitale Samenleving in 2020 in kaart gebracht in hoeverre de gemeenten, waterschappen, provincies en veiligheidsregio's (vanaf hier genoemd "decentrale overheden) zich voorbereiden op digitale incidenten die kunnen leiden tot digitale ontwrichting. In dit onderzoek, genaamd 'Quickscan voorbereiding op digitale ontwrichting'[1] zijn de bestuurlijke verbeter-programma's van de decentrale overheden in kaart gebracht.

In aansluiting hierop wordt in het rapport dat nu voor u ligt verder ingezoomd op de wijze waarop overheidsorganisaties kunnen samenwerken om bij escalatie van cyberincidenten de mogelijk ontwrichtende gevolgen voor de Nederlandse samenleving op lokaal en nationaal niveau binnen de perken te houden.

De inspanningen van de decentrale overheden op dit gebied zijn geclusterd in drie thema's (die ook al in de Quickscan onderscheiden werden):

1. Verbinden en organiseren
2. Inzicht in ketens en afhankelijkheden
3. Oefenen & Testen

In de analyse van de verschillende bestuurlijke plannen, initiatieven en projecten is specifiek naar de samenwerkingskansen tussen de betrokken overheidsorganisaties gekeken. Dit heeft een groot aantal aanbevelingen opgeleverd, die het ministerie BZK, vanuit haar stelselverantwoordelijkheid voor de digitale samenleving, kan gebruiken om te komen tot een betere cybergevolgbestrijding.

1.2. Opdracht

BZK heeft ICTU gevraagd de aanbevelingen van de Quickscan verder uit te werken en af te stemmen met alle daarbij betrokken stakeholders, en een advies te geven over hoe BZK invulling kan geven aan de verdere uitvoering hiervan.

Het voorbereid zijn op het omgaan met digitale incidenten die tot digitale ontwrichting kunnen leiden is primair de verantwoordelijkheid van de betrokken decentrale overheden

[1] Quick Scan voorbereiding op digitale ontwrichting | Rapport | Rijksoverheid.nl

zelf, maar het draait ook om het verder vormgeven van samenwerking en governance waarvoor BZK-directie Digitale Samenleving vanuit haar stelselverantwoordelijkheid voor de digitale samenleving en J&V/NCTV vanuit verantwoordelijkheid voor het cybersecuritystelsel samen verantwoordelijk zijn.

BZK wenst in samenwerking met J&V verdere invulling te geven aan deze governance en samenwerking met de decentrale overheden. Daarbij vormen de bestaande kaders en afspraken zoals NL-Digibeter, NCSA, NCP-digitaal en het LDS de stip op de horizon. De actuele status van de decentrale overheden op de onderwerpen binnen de bovengenoemde drie sporen vormt het vertrekpunt. Het statusoverzicht van de drie sporen is daarbij nadrukkelijk niet bedoeld als verantwoordingsinstrument. Het dient als hulpmiddel voor BZK en de betrokken decentrale overheden om de samenwerking en kennisdeling verder aan te jagen en obstakels weg te nemen.

1.3. Achtergrond

Directe aanleiding voor de Quickscan naar Digitale Ontwrichting bij Decentrale Overheden was de kabinetsreactie[2] op het WRR-rapport 'Voorbereiden op digitale ontwrichting' van 20 maart 2020. In deze kabinetsreactie vanuit J&V was toegezegd dat het ministerie van BZK met de decentrale overheden overlegt hoe zij zich voorbereiden op digitale ontwrichting. Met als doel zicht te krijgen of de bestaande kaders en afspraken volstaan en of eventuele aanvullingen en versnellingen op specifieke punten zijn.

In 2019 heeft BZK/DGOO/DO onder de noemer Gemeenschappelijk Overheid Security Operations Center (GOV-SOC) al een onderzoek gedaan naar de digitale weerbaarheid van de decentrale overheden. Uit de verkenning zijn verschillende ambities naar voren gekomen die een eerste schets een gezamenlijke *roadmap* vormden. In deze voorloper van het huidige overzicht werden naast witte vlekken, nieuwe inzichten en kansen voor de individuele decentrale overheden ook interbestuurlijke uitdagingen geïdentificeerd. Doel was, dat BZK/DGOO/DO, vanuit haar rol als stelselverantwoordelijke voor de digitale overheid, met dit overzicht inzicht krijgt in noodzakelijke, (rand)voorwaardelijke of kansrijke initiatieven op gebied van informatieveiligheid en daarin kan prioriteren. De opbrengsten van de GOV-SOC verkenning zijn overgedragen aan de bestuurslagen die de uitkomsten benutten om de incident response capaciteit van hun eigen bestuurslaag te versterken.

In 2020 is in aanvulling hierop een Quickscan uitgevoerd naar de voorbereiding op digitale ontwrichting. Daarin werd gekeken naar de bestuurlijke plannen en ambities van decentrale overheden om maatschappelijke ontwrichting door digitale incidenten te voorkomen. Uit deze Quickscan blijkt dat bij al deze overheidslagen tal van nieuwe initiatieven worden opgepakt om de digitale weerbaarheid te verhogen, geheel in lijn met de aanbevelingen van het WRR-rapport. Met al deze bestuurlijke initiatieven zetten de decentrale overheden in op (1) zowel het verhogen van de interne cyberweerbaarheid van de eigen netwerk- en informatiesystemen van het betreffende bestuursorgaan als (2) het voorbereid zijn op digitale ontwrichting en adequate gevolgbestrijding.

Bij cyberincidenten kan op deze twee vlakken los van elkaar dynamiek ontstaan, maar ook gelijktijdig. Indien een digitale crisis ontstaat en (cyber)gevolgbestrijding plaatsvind zal wel optimaal aangesloten moeten worden op het Nationaal Crisisplan Digitaal (NCP-Digitaal). Het NCP-Digitaal biedt snel inzicht en overzicht in mogelijke gevolgen en maatregelen, rollen, taken en bevoegdheden op nationaal niveau ten tijde van een digitale crisis. Momenteel wordt het NCP-Digitaal geactualiseerd en tevens omgevormd en verbreed naar een

[2] Kamerbrief evaluatie Citrix-problematiek en reactie rapport WRR | Kamerstuk | Rijksoverheid.nl

Landelijk Crisisplan Digitaal met de veiligheidsregio's als mede-eigenaar, zodat ook de aanpak op nationaal, (boven-)regionaal en lokaal niveau beter op elkaar aansluiten.

1.4. Vormgeving panel

Het overzicht van de stand van zaken heeft de vorm gekregen van een printplaat of panel, zoals op de voorkant van dit rapport te zien is. Een printplaat dient als drager voor elektronische componenten, waarop koperen bedradingen, genaamd sporen, zijn aangebracht ter verbinding van die componenten. Om aan te geven dat digitale weerbaarheid veel meer is dan techniek en om te benadrukken dat het uiteindelijk draait om mensen en organisaties om te komen tot grotere digitale weerbaarheid zijn op de printplaat ook mensen geplaatst.

We hebben dit overzicht het 'Panel digitale weerbaarheid' genoemd. Te zien zijn de sporen die de overheden afleggen om te komen tot grotere digitale weerbaarheid. De componenten op de sporen zijn aandachtsgebieden die door de betrokken partijen in gezamenlijke workshops zijn bepaald. De oplichtende cijfers (van 1 tot 4) geven een globale indruk van de inspanningen die gemeenten, provincies, waterschappen en veiligheidsregio's zich getroosten bij het realiseren van deze aandachtsgebieden. Aangetekend zij dat dat het (subjectieve) inschattingen zijn die de organisaties zelf hebben gegeven. De status van de aandachtsgebieden was namelijk voor deze opdracht niet goed meetbaar te maken.

Het panel was en is nadrukkelijk niet bedoeld om aan te geven waar de decentrale overheden het goed of slecht doen. Of om eisen te stellen aan de wijze waarop ze de digitale weerbaarheid oppakken. Het vormgeven van het panel heeft vooral gediend als middel om kansen, mogelijke oplossingen, risico's en knelpunten, die voor de bestuurslagen relevant kunnen zijn, bespreekbaar te maken en om inzicht te krijgen waar de overheden elkaar kunnen of zelfs moeten helpen of versterken.

Aangezien de cyber veiligheid niet altijd beperkt blijft tot binnen de grenzen van de betreffende bestuurslagen is het panel bovendien zodanig ingericht dat het recht doet aan het gezamenlijke belang van de betreffende bestuurslagen. Samenwerking, informatie-uitwisseling en (gezamenlijk) testen en oefenen spelen daarbij een belangrijke verbindende rol.

In aanvulling hierop dient opgemerkt te worden dat belangrijke andere partijen, zoals leveranciers, uitvoeringsorganisaties van het Rijk, ZBO's, samenwerkingsverbanden, gemeenschappelijke regelingen niet zijn opgenomen in het overzicht. Ze hebben echter in de (dienstverlenings)ketens van de decentrale overheden vaak wel een belangrijke rol. En wel zodanig dat de vraag gerechtvaardigd is of voor dit onderzoek de focus niet breder had moeten zijn. Daar staat tegenover dat de beperkte sectorale opzet wel heeft opgeleverd dat de betrokken overheden van gedachten hebben gewisseld wat ze in de beteugeling van digitale ontwrichting gemeen hebben, op welke punten en waar precies de risico's liggen en wat eraan gedaan kan worden. Zie daarvoor de aanbevelingen.

Tot slot: aangezien de lopende verbeteringen bij de decentrale overheden in de uitvoering van de eigen plannen snel verloopt is de houdbaarheidsdatum van het document beperkt. Het panel representeert dus een momentopname. BZK heeft aangegeven hoe dan ook met de betrokken organisaties in gesprek te blijven over de voortgang en ondersteuningsbehoefte en jaarlijks trachten een steeds betere indicatie te krijgen van de voortgang.

1.5. Aandachtsgebieden

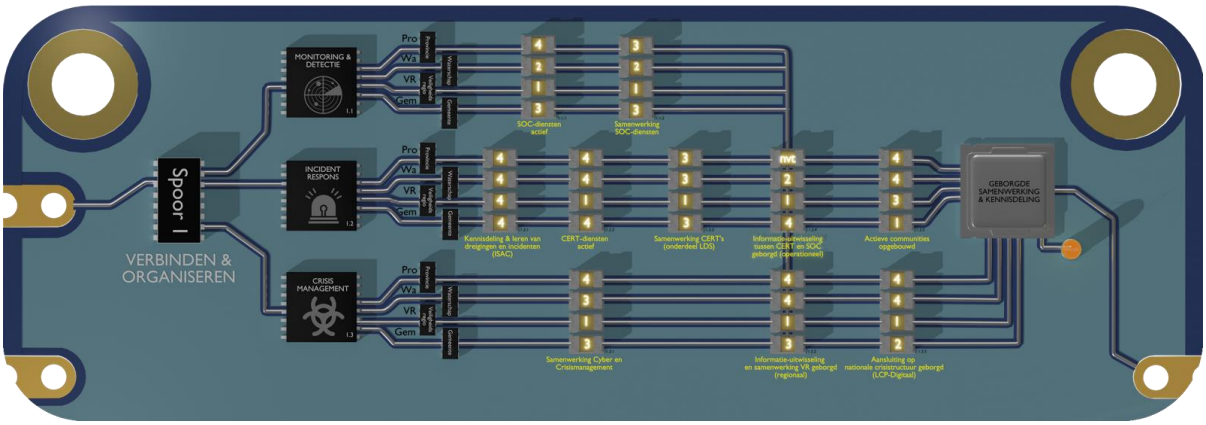
In dit document zijn alle opgenomen aandachtsgebieden binnen de drie sporen op eenduidige manier uitgewerkt tot een aantal overzichtelijke kenmerken en ondergebracht in de onderstaande tabel.

Aandachtsgebied	**<naam aandachtsgebied >**	**NR**	**<nummer>**
Omschrijving	<korte omschrijving van het aandachtsgebied>		
Doel	<smart uitdrukking van wat doel is van het aandachtsgebied>		
Status	**Bestuurslaag:**	**Reikwijdte/dekkingsgraad (scope):**	
	Veiligheidsregio	Score 0: niet van toepassing 1: niet gestart, geen plan	
	Waterschappen	2: niet gestart, plan beschikbaar 3: uitvoering loopt	
	Provincies	3: uitvoering loopt, omdat...	
	Gemeenten	4: uitvoering gereed, afgerond	
Toelichting (afhankelijkheden, voorwaarden, obstakels, knelpunten)	Veiligheidsregio	De veiligheidsregio's hebben richting nodig van…	
	Waterschappen		
	Provincies		
	Gemeenten		

De bij de opdracht betrokken deskundigen hebben voor hun respectievelijke bestuurslaag voor elk aandachtsgebied de status ingeschat en een toelichting daarop gegeven. Het resultaat daarvan is in bijlage 1 terug te vinden. De informatie uit de tabellen vormt de input voor het overzicht van de stand van zaken (hoofdstuk 2) en de aanbevelingen die op basis daarvan zijn geformuleerd (hoofdstuk 3).

2. Stand van zaken sporen

2.1. Spoor 1 - Verbinden en organiseren



Het aantal cyberincidenten neemt nog ieder jaar toe en ons land moet blijvend werk maken van het verhogen van de weerbaarheid tegen dit soort aanvallen. Allereerst dient de cyberveiligheid bij alle afzonderlijke organisaties op orde zijn. Maar als het dan toch misgaat en er sprake is van maatschappelijk ontwrichtende situatie, waarbij bijna per definitie meerdere overheidsorganisaties betrokken zijn, dan moet de Nederlandse overheid als geheel daarop voorbereid zijn en er gezamenlijk op kunnen reageren.

Spoor 1 geeft aan hoe en in welke mate de decentrale overheden het signaleren en bestrijden van digitale ontwrichting binnen hun organisaties hebben georganiseerd, hoe daarin wordt samengewerkt met andere overheden en hoe dit onderdeel uitmaakt van het crisismanagement op regionaal en landelijk niveau. Het doel van dit spoor is te komen tot geborgde samenwerking en kennisdeling.

In het advies van de Cyber Security Raad van april 2021[3] staat daarover het volgende geschreven:

Realiseer een effectieve vorm van regie op samenwerking Om de cyberweerbaarheid integraal te verbeteren is het noodzakelijk om een betere regie op samenwerking te voeren. Regie op samenwerking tussen overheid, bedrijfsleven en wetenschap draagt zorg voor het harmoniseren van (nationale) cyberweerbaarheidsinitiatieven en -investeringen, en vergroot daarmee de effectiviteit, samenhang en slagkracht van deze initiatieven.
Een belangrijk uitgangspunt hierbij is dat de regievoering primair faciliterend moet zijn aan de uitvoering, bijvoorbeeld door samenwerking te faciliteren waardoor meer bereikt kan worden tegen dezelfde investeringen dan wanneer stakeholders individueel te werk gaan.
Ondersteun de opbouw van ISAC's buiten vitale sectoren om (zoals in topsectoren, vanwege het belang en het hoge dreigingsprofiel van deze sectoren) en maak deze ISAC's onderdeel van het LDS.

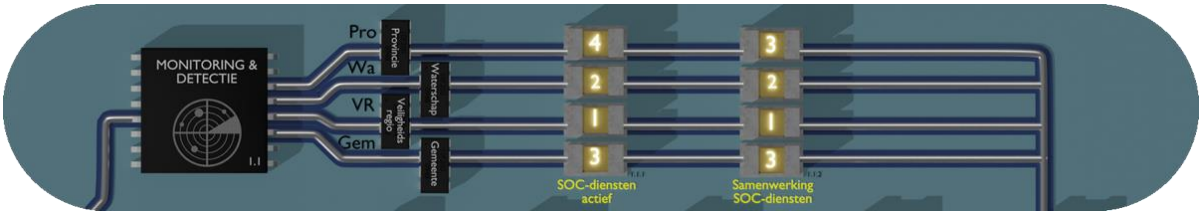
Spoor 1 is verdeeld in drie subsporen:

- **Monitoring en detectie:** het actief bewaken van voorzieningen en onderliggende infrastructuur om verdachte patronen, afwijkend gedrag of ongeautoriseerde veranderingen vroegtijdig te signaleren. Dreigingsanalyses en forensisch onderzoek worden hier soms ook bij betrokken

[3] CSR advies april2021+Adviesrapport+'Integrale+aanpak+cyberweerbaarheid'

- **Incidentrespons**: het detecteren van en reageren op cyber-incidenten om mogelijke schade te herstellen en de gevolgen van ernstige 'lokale' verstoringen van maatschappelijke kernprocessen, effectief te bestrijden.
- **Crisismanagement:** het beheersen van crises. Een crisis is een zware noodsituatie waarbij het functioneren van een organisatie (bedrijf, overheid, maatschappij, regio) ernstig verstoord raakt.

2.1.1. Monitoring en detectie

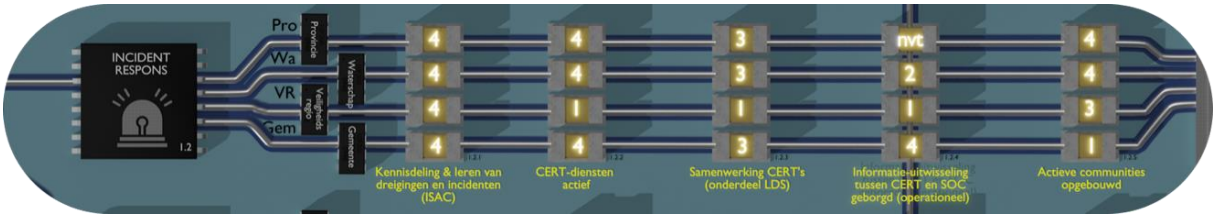


Binnen een bestuurslaag dienen overheden die onderdeel uitmaken van die bestuurslaag zelf in staat te zijn om op operationeel niveau afwijkingen te detecteren in de eigen netwerken en systemen. Door hier samen in op te trekken, bijvoorbeeld door het delen van monitoring use-cases, kunnen voordelen worden behaald vanwege de schaarse en specialistische kennis. Ook helpt het delen van deze signalen met andere organisaties zodat gerichte dijkbewaking kan worden ingesteld en besluitvorming voor eventuele crisisopschaling kan worden ondersteund, mocht het de inschatting zijn dat een digitaal incident leidt tot ernstige lokale of regionale verstoring

Het globale beeld op dit spoor (zie bijlage 4):

- De meeste overheden binnen de bestuurslaag hebben toegang tot diensten van een Security Operation Center (SOC), of plannen om dat te gaan inrichten.
- Door kennis de te delen over gezamenlijke use-cases en SOC -practices kan de kwaliteit van de monitoring diensten worden verhoogd.
- Kaders als NIST en NCSC handreikingen/whitepapers zijn van toegevoegde waarde.

2.1.2. Samenwerking rondom Incident respons

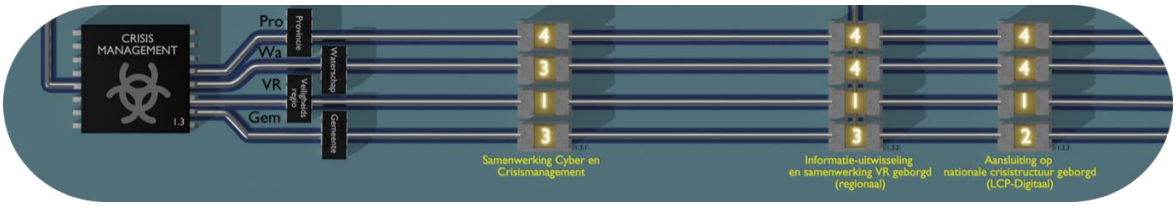


Samenwerking rondom incident respons heeft betrekking op de mate waarin organisaties die onderdeel zijn van een bestuurslaag als ook organisaties die opereren binnen het grensgebied van de bestuurslaag (zijn toegerust om op (potentiële) cyber-incidenten, waaronder kwetsbaarheden, te reageren en informatie hierover te delen. Doel is mogelijke schade te herstellen en de gevolgen van ernstige 'lokale' verstoringen van maatschappelijke kernprocessen, effectief te bestrijden. Sectorale CERT's of andere organisatievormen die een doelgroep vertegenwoordigen, zoals het DTC[4] of FERM[5], kunnen afzonderlijke organisaties informeren over dreigingen en incidenten. En omgekeerd helpt het delen van informatie over 'lokale' verstoringen ook om een landelijk situationeel beeld op te bouwen, zodat dreigingsinformatie kan worden gedeeld en relaties tussen vergelijkbare incidenten bij verschillende organisaties (binnen en buiten de eigen bestuurslaag) kunnen worden gelegd.

Het globale beeld op dit spoor (zie bijlage 4):

- Het belang van actieve communities wordt benadrukt. Alle bestuurslagen zijn ermee bezig en vormt een laagdrempelige manier om kennis te delen en samen te werken.
- Bij 2 van de 4 betrokken bestuurslagen is daarvoor een ISAC gevormd.
- Er is behoefte aan informatieverstrekking vanuit het NCSC.
- Bij 3 van de 4 betrokken bestuurslagen zijn CERT-diensten ingericht, waarvan 2 sectorale CERT's.
- Men is bezig de samenwerking tussen CERT's te realiseren als onderdeel van LDS.
- Er wordt nog niet op grote schaal informatie uitgewisseld tussen CERT's en SOC's.
- Het duiden van SOC/CERT-diensten als sectoraal niveau zou zinvol kunnen zijn. Daardoor wordt ook intersectoraal overleg en samenwerking mogelijk gemaakt.
- Volwassenheidsmetingen als SIM3[6] helpen bij verdere ontwikkeling van sectorale CERT's.

2.1.3. Crisismanagement



Bij cybergevolgbestrijding van ernstige digitale incidenten met potentiële effecten in het fysieke domein, dienen vroegtijdig (en bij verdere opschaling) de interne- en eventueel regionale crisisorganisaties te worden geïnformeerd of betrokken. Als onderdeel van de gemeentelijke agenda digitale veiligheid worden naast eigen interne informatieveiligheid

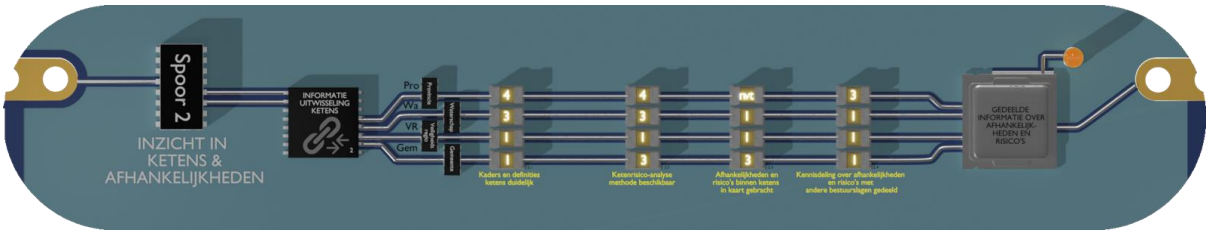
[4] Digital Trust Center start met delen dreigingsinformatie NCSC | Nieuwsbericht | Nationaal Cyber Security Centrum
[5] https://www.ncsc.nl/actueel/nieuws/2021/mei/19/oktt-status-voor-ferm
[6] CSIRT Maturity - Self-assessment Tool — ENISA (europa.eu)

ook verbanden gelegd tussen openbare orde en veiligheid (OOV) en digitale criminaliteit. Zo krijgen informatieveiligheid en cybercrime een plaats in de structuur van crisisbeheersing. Doel is om als decentrale overheden zoveel mogelijk op één lijn te komen in samenwerking tussen cyber- en crisisorganisatie onderdelen. De bestaande regionale opschalingsstructuur (GRIP) en crisisbesluitvormingsafspraken zijn daarbij van toepassing. Doel is om zo effectief mogelijk een crisissituatie met cyberkenmerken te kunnen beheersen en gevolgen te bestrijden.

Het globale beeld op dit spoor (zie bijlage 4):

- Samenwerking tussen cyberincident en crisismanagement binnen de eigen organisatie wordt uitgewerkt en loopt al voor een deel.
- De informatie-uitwisseling en samenwerking tussen decentrale overheden en veiligheidsregio's rondom ernstige digitale incidenten is nog niet structureel geborgd.
- In voorkomende gevallen kunnen de betrokken overheden op uitnodiging deelnemen aan de overleggremia binnen de nationale crisisstructuur.
- Veiligheidsregio's hebben nog besluiten te nemen over de inrichting (governance) en financiering van het op te bouwen cyberstelsel voor veiligheidsregio's (SOC+CERT naast de bestaande VR-ISAC).
- In het kader van het op te bouwen cyberstelsel en de herziening wet veiligheidsregio's (inzetten op gemeenschappelijke informatievoorziening) is harmonisatie noodzakelijk.
- VR-ISAC vraagt om regie vanuit het rijk op samenwerking tussen ISAC's.
- De rol van de veiligheidsregio bij een digitale crisis wordt verder uitgewerkt in het LCP-Digitaal
- Het is de vertegenwoordigers van de bestuurslagen niet duidelijk wat de criteria zijn van maatschappelijke ontwrichting en over welke maatschappelijke kernprocessen het dan gaat. Dat bepaalt namelijk of er een rol is weggelegd voor de betrokken decentrale overheden of niet. Een duidelijke definitie daarvan wordt zeer wenselijk geacht.

2.2. Spoor 2 - Inzicht in ketenrisico's en afhankelijkheden



Aangezien overheden in hun dienstverlening veelal in ketens werken kunnen cyber incidenten binnen een organisatie ook gevolgen hebben voor andere organisaties. Bij dit spoor draait het om het voor decentrale overheden inzichtelijk krijgen van de eigen kritieke bedrijfsprocessen, de supplychain afhandelijkheden, en elementen van cruciale processen waar ze onderdeel van zijn. Doel is om gedeelde informatie over afhankelijkheden en risico's binnen de ketens te realiseren.

Keteneffecten kunnen hele sectoren of zelfs de gehele maatschappij raken. Zo maakt een aanval met ransomware op een gemeente, universiteit, ziekenhuis of elektriciteitsdistributeur systemen onbruikbaar: de techniek werkt niet meer. Het gevolg daarvan is dat de gemeente haar taken niet meer naar behoren kan uitvoeren, dat onderzoek en onderwijs stil komen te liggen, patiëntenzorg wordt belemmerd of stroomuitval plaatsvindt. Dat betekent dat de digitale dreiging meer en andere belangen raakt dan het functioneren van de techniek alleen. Dat betekent dat weerbaarheid verhogende maatregelen niet alleen bijdragen aan het veilig houden van techniek, maar ook aan het veilig houden van onze samenleving en economie. (CSBN 2021[7])

Aan iedere beveiligingsstrategie ligt systeemkennis ten grondslag, zeker op het gebied van cyberveiligheid. Kennis van gebruikte componenten, systeemarchitectuur en onderlinge afhankelijkheden is essentieel. Deze kennis is niet alleen essentieel om te bepalen waar eventueel risico's van een cyberaanval liggen, maar ook om met andere organisaties te kunnen communiceren over veiligheid en beveiliging, en om elkaar hierin te kunnen ondersteunen. Een gezamenlijk of centraal beeld van alle ketens en de digitale aspecten daarvan bestaat niet, onder andere vanwege de (toenemende en veranderende) connectiviteit en complexiteit. Iedere organisatie zal zelf de afhankelijken en risico's van de eigen *supplychain* en samenwerkingspartners in kaart moeten brengen en moeten bepalen hoe daarmee om te gaan.

Digitale veiligheid van deze ketens en bekendheid met cascade-effecten van digitale verstoringen, zijn expliciete aandachtspunten van dit spoor. Uitval van cruciale of vitale processen, verschillende informatieposities of onbetrouwbaarheid van de informatievoorziening kan grote gevolgen hebben, zeker als dat op grotere schaal c.q. bij meerdere organisaties optreedt. Het gaat dan om processen die mogelijk ook op landelijk niveau vitaal zijn. Deze inzichten in afhankelijkheden en ketens zijn nodig voor het borgen van de eigen bedrijfscontinuïteit, als ook advisering van en afstemming met de reguliere crisisstructuren. Daarnaast kan er op basis van bekende ketens en afhankelijkheden gerichter worden geoefend. Zo is er als gevolg van de Citrix crisis veel aandacht besteed aan de noodzaak van beter zicht krijgen in cruciale afhankelijkheden in het digitale domein.

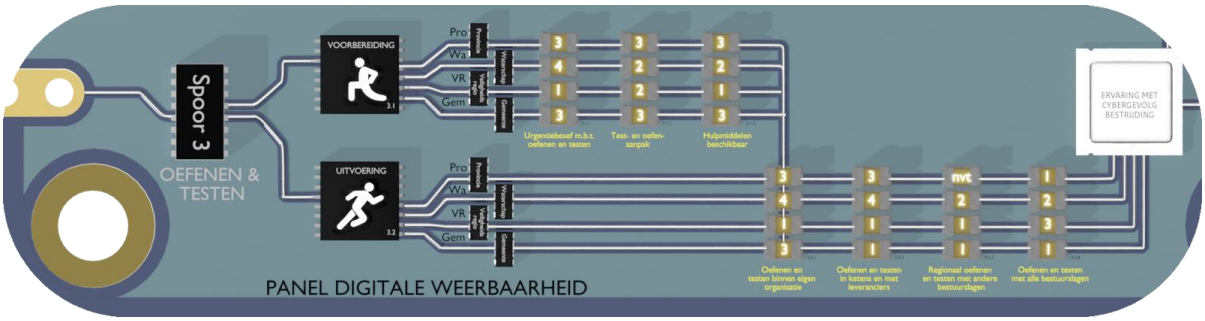
Het globale beeld op dit spoor (zie bijlage 4):

- Eenduidige kaders en uniforme definities van risico's over ketenpartners heen zijn aandachtpunten.

[7] Cybersecuritybeeld Nederland CSBN 2021 | Rapport | Rijksoverheid.nl

- Er is behoefte aan een gemeenschappelijke ketenrisicoanalyse-methodiek. Een interessante ontwikkeling in dat kader is de ketenanalyse methodiek die TNO ontwikkelt on opdracht van I&W programma 'versterken cyberweerbaarheid in de watersector'.
- De afhankelijkheden en risico's binnen ketens zijn nog niet breed in kaart gebracht. VNG wil ermee starten en onderzoekt de bruikbaarheid van de methodiek van I&W voor de watersector (waar ook gemeenten bij zijn aangehaakt).
- Gemeenten en Veiligheidsregio's willen digitale risicokaarten uitwerken voor generieke lokale cruciale processen
- Door het ontbreken van een methodiek en standaardisatie staat kennisdeling over afhankelijkheden en risico's binnen ketens nog in de kinderschoenen. Als voorbeeld zijn de digitale risicokaarten van gemeenten/veiligheidsregio's zijn interessante producten om te volgen en om kennis over te delen.

2.3. Spoor 3 - Oefenen en Testen



Dit spoor heeft als doel het daadwerkelijk en herhaaldelijk oefenen bij de decentrale overheden te borgen (structureel oefenen), zodat de reguliere aanpak van incidenten en crisissen worden doorleefd en vaardigheden soepel gehouden en er op een routinematige manier kan worden gereageerd op digitale bedreigingen, kwetsbaarheden en incidenten.

Oefenen en testen zijn in dit opzicht belangrijke middelen om de feitelijke veiligheid te beproeven om de cyberweerbaarheid van organisaties verder te kunnen verhogen. Medewerkers leren hoe ze om moeten gaan met crisissituaties en planvorming wordt verbeterd op basis van die leerervaringen. Idealiter wordt Oefenen gekoppeld aan Trainen en Opleiden, zodat er een cyclus ontstaat van blijven leren en verbeteren. Dit wordt ook wel OTO-cyclus genoemd.

Oefenen draagt ertoe bij dat organisaties beter voorbereid wanneer er onverhoopt ernstige cyber-incidenten plaatsvinden. Het vormt bovendien een goede graadmeter in hoeverre organisaties daadwerkelijk zijn voorbereid op digitale ontwrichting en helpt organisaties alert te houden. Oefenen versterkt bovendien de samenwerking en laat de noodzaak tot coördinatie zien.

Onder testen kunnen verschillende zaken worden verstaan. Het NCSC schaart bijvoorbeeld pentesten, code review, kwetsbaarheden scans onder securitytesten[16]. Dergelijke testen geven aanvullende zekerheid over de beveiliging van informatiesystemen en inzicht in de eventuele risico's of kwetsbaarheden van systemen.

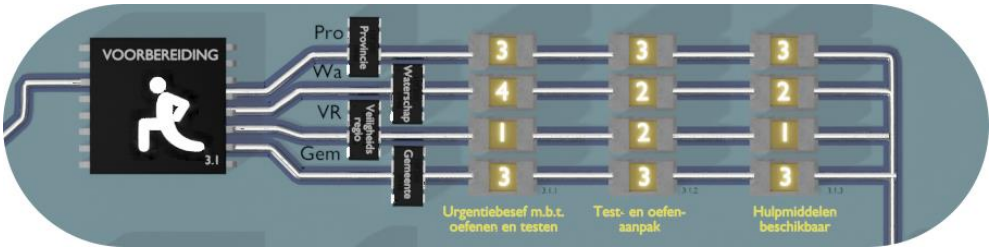
Testen kunnen echter ook betrekking hebben op het toetsen van de juiste werking van operationele procedures. In deze context ligt de focus op incident- en gevolgbestrijding en valt het operationeel testen van de werking van (nood)procedures, zoals een *backupherstel*-test of een noodstroom-test, ook onder de noemer oefenen. Het hebben van heldere definities is dan ook van belang omdat snel begripsverwarring kan ontstaan.

"De digitale weerbaarheid van Nederland verhogen, bewustzijn creëren en voorbereiden op digitale aanvallen is dus erg belangrijk. Hierin is gezamenlijk oefenen een belangrijk onderdeel. Hierdoor leren deelnemers dezelfde taal te spreken, krijgen ze inzicht in elkaars belangen en problemen én kunnen ze elkaar in het echt sneller en beter vinden. Omdat een cyberincident zich per definitie snel ontwikkelt en veel impact heeft is oefenen nodig om maatschappelijke ontwrichting en grote (financiële) schade te voorkomen."
Hans de Vries, directeur NCSC[17]

In de bevindingen in de Quickscan is vastgesteld dat er in de plannen van de verschillende decentrale overheden zeker aandacht is voor oefenen en testen, maar het draait uiteindelijk om het daadwerkelijk, herhaaldelijk uitvoeren van oefeningen in verschillende samenwerkingsverbanden. De aanpak is om dit te blijven aanjagen, kennis hierover te delen,

samenwerking op te zoeken en eventuele barrières te slechten op lokaal, regionaal en landelijk niveau. Idealiter worden daarbij ook Opleiden en Trainen meegenomen om te blijven leren en verbeteren. Deze inzet op oefenen sluit aan op het nationale oefen- en testprogramma van de NCTV (ISIDOOR) en de overheid brede cyberoefening van BZK.

2.3.1. Voorbereiding

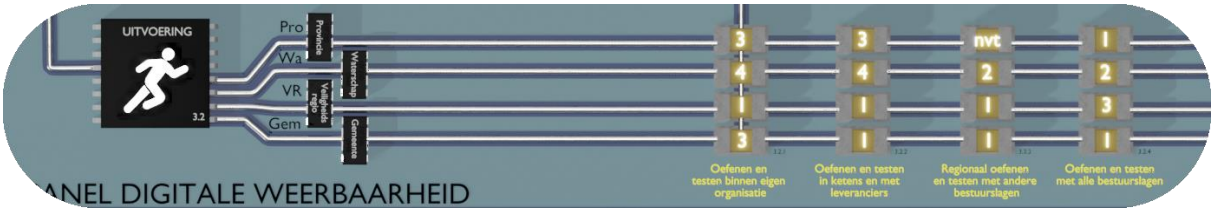


Regelmatig oefenen begint bij voldoende urgentiebesef en awareness bij bestuurders om oefenen met digitale incidenten tot een centraal beleidsthema maken. Het hebben van heldere definities is dan ook van belang omdat snel begripsverwarring kan ontstaan. Daarnaast is Opleiden en Trainen van belang om handvatten te bieden en te blijven leren en verbeteren. Herhaaldelijk oefenen vraagt om geschikt oefenmateriaal en hulpmiddelen die blijvend worden doorontwikkeld en aangevuld met passende formats en scenario's en daarmee ook passende opleidingen en trainingen. Dergelijk gereedschap helpt om de drempel te verlagen om daadwerkelijk in verschillende samenwerkings--verbanden en schaalgroottes te gaan oefenen: lokaal, regionaal en landelijk. We weten immers één ding zeker, de cybercrisis van morgen is anders dan de cybercrisis waarop je hebt getraind en die we gisteren hebben geoefend. In deze context scharen we het operationeel testen van de werking van (nood) procedures zoals een backuprestore test, een noodstroom test en redteam-testen ook onder de noemer oefenen, vandaar de naam oefenen en testen.

Het globale beeld op dit spoor (zie bijlage 4):

- Oefenen helpt het aanhaking van de bestuurders van de decentrale overheden en de inhoudelijke opgaven te vergroten, ondersteuning en aanjagen vanuit de rijksoverheid helpt daarbij, bijvoorbeeld door het organiseren van bestuurlijke cybertafels.
- Met hulp van BZK is oefenmateriaal ontwikkeld, daar wordt nu ervaring mee opgedaan.
- Een (gestandaardiseerde) test en oefen aanpak is in ontwikkeling, het verdient aanbeveling ervaringen hiermee actief te delen.
- De beschikbaarheid van materiaal op dit thema groeit.

2.3.2. Uitvoering



The proof of the pudding, is in the eating. Dat geldt zeker ook voor cybersecurity-oefeningen. Een flink digitaal incident overkomt je en het daadwerkelijk ondergaan geeft waardevolle inzichten en feedback waardoor je een volgende crisis sneller en adequater kan handelen. Door te oefenen in verschillende samenwerkingsverbanden en crisisstructuren, waarin je in de organisatie mee te maken hebt, kunnen steeds verschillende oefendoelen worden gesteld. Op termijn heeft idealiter iedere organisatie een eigen cyber-oefenplan met oefendoelen waarbij verschillende type oefeningen worden gebruikt.

Het globale beeld op dit spoor (zie bijlage 4):

- Specifiek op cyber wordt er nog mondjesmaat geoefend, waarbij cyber- en crisismanagement samenwerken. De wens om vaker te oefenen groeit en krijgt in toenemende mate vorm
- Oefenen en testen in ketens en met leveranciers, bijvoorbeeld middels redteaming, staat nog in de kinderschoenen.
- Het verzoek is om dit onder centrale regie vanuit het rijk op te pakken i.v.m. keten overstijgende mandaten en vrijwaringen.
- Datzelfde geldt voor het oefenen en testen over bestuurslagen heen. Daar zijn voor een groot deel nog geen plannen voor.
- Er is twijfel of het testen en oefenen wel genoeg oplevert. Evaluatie binnen de eigen organisatie en keten is noodzakelijk om ervoor te zorgen dat de geleerde lessen ook daadwerkelijk worden uitgevoerd. Opleidingen en trainingen spelen daarbij een belangrijke rol en zijn nu nog onderbelicht.

3. Aanbevelingen

De mensen die in de dagelijkse praktijk bezig zijn met het verhogen van de digitale weerbaarheid zijn volledig doordrongen van de noodzaak veel energie en middelen te investeren in het voorkomen en bestrijden van cyberincidenten en -dreigingen. Voor het goed kunnen uitvoeren van hun rol en verantwoordelijkheden hebben zij echter zonder uitzondering grote behoefte aan **kennisdeling en samenwerking** met collega's in andere overheidsorganisaties. Niet alleen, omdat dit de cyberweerbaarheid van de eigen organisatie ten goede komt. Zij beseffen maar al te goed, dat er vaak sprake is van een **wederzijdse afhankelijkheid**. Voor het leveren van veel digitale diensten werken hun organisaties immers dikwijls samen met andere overheden. Aangezien de ICT-voorzieningen, die daarvoor worden ingezet, vaak aan elkaar gekoppeld zijn, kunnen cyberdreigingen en -incidenten bij de ene organisatie ook consequenties hebben voor de organisaties waarmee wordt samengewerkt.

In de praktijk vindt kennisdeling met andere (keten)partners binnen en buiten de overheid over incidenten, dreigingen, aanpak en trends echter nog veel te weinig plaats, vinden de experts die aan het onderzoek hebben meegedaan. Over het geheel genomen wordt er ook niet efficiënt samengewerkt. Zij geven aan dat meer **centrale regie** nodig is om dit goed van de grond te krijgen.

Er is in aanvulling hierop een duidelijke behoefte beter zicht te krijgen op de **cruciale afhankelijkheden** in het digitale domein. Dat bepaalt ook waar samenwerking echt nuttig en/of noodzakelijk is. Daar waar cyberincidenten de eigen organisatie overstijgen en de situatie zo ernstig is dat centraal crisismanagement noodzakelijk is, is bovendien niet altijd duidelijk wat de **rollen en verantwoordelijkheden** daarin zijn. Dit is **zowel op centraal als decentraal niveau** het geval. Laat staan dat ze goed op elkaar zijn afgestemd. Dit bemoeilijkt de noodzakelijke samenwerking bij crises.

In het bijzonder zou de **rol van de veiligheidsregio's** binnen de crisisstructuren duidelijker moeten worden. De betrokkenen vinden dit een belangrijke factor in de bestrijding van digitale ontwrichting.

De vraag of er mogelijk sprake is van grote maatschappelijke ontwrichting of niet staat hierbij volgens de bij het onderzoek geraadpleegde experts centraal. Het is de vertegenwoordigers van de bestuurslagen namelijk niet helder over **welke maatschappelijke kernprocessen** het dan gaat. Dat bepaalt of er een rol is weggelegd voor de betrokken decentrale overheden of niet. Een duidelijke definitie daarvan wordt zeer wenselijk geacht.

Op alle sporen die decentraal en centraal moeten leiden tot grotere digitale weerbaarheid moet nog veel werk worden verzet. Daarbij is **steun én sturing van de bestuurders** een noodzakelijke randvoorwaarde. Het urgentiebesef van de bestuurders is echter nog niet groot. Van BZK wordt in ieder geval gevraagd het belang van crisismanagement, inclusief de noodzaak dit te oefenen en te testen, richting de bestuurders in de diverse bestuurslagen nog sterker uit te dragen.

Samengevat komt dat neer op de volgende 6 hoofdaanbevelingen:

3.1. Hoofdaanbevelingen

1. **Realiseer eenduidige regie en visie vanuit de rijksoverheid:** zorg voor eenduidige governance en visie vanuit rijksoverheid; geef duidelijkheid over rollen en verantwoordelijkheden, vooral waar cyberveiligheid en crisismanagement elkaar

raken; heb i.h.b. aandacht voor de rol van toezicht van provincies en de rol van de veiligheidsregio's; zorg voor (voldoende en eenduidige) communicatie hierover.
2. **Focus op samenwerking en kennisdeling:** bepaal, voortbouwend op de input van de betrokken organisaties, nog scherper waar, wanneer en tussen wie samenwerking en informatie-uitwisseling noodzakelijk en nuttig is.
3. **Investeer in onderlinge relaties:** houd hiervoor het panel van deskundigen en vertegenwoordigers van decentrale overheden in stand en bouw dit waar nodig uit.
4. **Bepaal de maatschappelijke kernprocessen** in context van de decentrale overheden en welke overheidsdienstverlening daarin een rol spelen (vitale digitale overheid)
5. **Intensiveer het oefenen en testen.** Betrek hierbij ook ICT-leveranciers, uitvoeringsorganisaties en andere ketenpartners.Evalueer het oefenen en testen en zorg voor de verspreiding van de resultaten.
6. **Borg bestuurlijke aandacht:** Zorg voor grotere betrokkenheid van bestuurders.

3.2. Aanknopingspunten

Aansluitend op deze hoofdaanbevelingen zijn inhoudelijke voorstellen uitgewerkt waarmee BZK/DGOO/DS dossierhouder digitale ontwrichting aan de slag kan om de eerste vervolgstappen te zetten op de diverse aandachtsgebieden.

3.2.1. Spoor 1

Monitoring en detectie

7. Benadruk richting decentrale overheden het belang van het inschakelen van SOC-diensten, de toegevoegde waarde van samenwerken op dat vlak en de noodzaak om met elkaar informatie over (potentiële) incidenten uit te wisselen.
8. Faciliteer het delen van kennis naar een landelijk crisisplan en ervaringen tussen decentrale overheden rondom SOC's (d.m.v. community vorming) en doe dit bij voorkeur met hulp van partners zoals J&V/NCSC, IenW, J-SOC rijks initiatief.
9. Bespreek samen met J&V het signaal van ontbrekende prioriteit van een VR-SOC (en CERT) en bekijk of en hoe dit is op te lossen.

Incident respons

10. Bied hulp bij het versneld vormgeven en borgen van aansluiting bij het LDS en NCSC van Provincies en Veiligheidsregio's bijvoorbeeld via een sectoraal cyber informatieknooppunt met OKTT status of een CERT's.
11. Verken of ontbrekende ISAC's kunnen gaan bijdragen aan de samenwerking en kennisdeling.
12. Bespreek de behoefte aan regie op samenwerking tussen ISAC's of cyber communities met partners J&V/NCSC.
13. Ondersteun CERT's van de bestuurslagen bij het gelijktrekken van de informatieposities bij incidenten en help hun dienstverlening naar bijvoorbeeld meer externe ondersteuning in gevolgbestrijding en cyberwaakzaamheid voor te bereiden.
14. Borg en faciliteer de samenwerking tussen G4 en VNG/IBD zodat specifieke informatie behoeften van G4 landt in de dienstverlening van IBD/VNG.

Crisismanagement

15. Verbind cyber- en crisisdomeinen bij de decentrale overheden met elkaar. Zorg dat de verschillende decentrale overheden elkaar beter kunnen vinden in de regionale en nationale crisisstructuren. Bijvoorbeeld door:
    - Het ondersteunen en verbinden van bestaande communities (cyber en crisis). Samenwerkingsvormen met een hoger mate van volwassenheid zoals sectorale CERT's kunnen mogelijk van grotere toegevoegde waarde zijn. Naast het eenvoudiger delen van technische dreigings-/kwetsbaarhedeninformatie kan

daarbij ook specifieke duiding en handelingsperspectief worden gegeven wat domein kennis vergt.
- Het met partners (J&V, NCSC, DTC) bespreken en duiden van de rol van VR-ISAC op cyber-gebied in de regio, mede in de context van evaluatie van de Wet op Veiligheidsregio en de doorontwikkeling NCP-Digitaal naar een landelijk crisisplan.

16. Versterk de verbinding van de algemene crisiskolom/organisatie op lokaal en regionaal niveau met de (versterkte) CERT-functie per bestuurslaag.
17. Werk de samenwerkingsafspraken van het BZK/DGOO crisisproces met de decentrale overheden verder uit en zorg voor de implementatie ervan (rollen, mandaten, afspraken over methode van informatie-uitwisseling
18. Verken, met hulp van het NCSC, waar communities kunnen worden versterkt of geformaliseerd om te kunnen bijdragen in samenwerking en kennisdeling. Bijvoorbeeld door:
    - Ervoor te zorgen dat (piket) medewerkers van het BZK/DGOO crisisproces die zich richten op deze doelgroep een kennismakingsronde maken langs de decentrale overheden. Beoogd doel is een samenwerkings- en vertrouwensrelatie op te bouwen zodat tijdens een warme fase van een crisis DGOO/DO en de decentrale overheden elkaar feilloos weten te vinden en elkaar informeren.
    - Een samenwerkingsvorm te kiezen die past bij de benodigde informatie uitwisseling en deze kan faciliteren en aansluit bij de volwassenheid en informatiebehoefte van de deelnemers. Oprichting van CERT's is hierbij een optie, maar dat kan ook een ISAC of een andere vorm van samenwerking met een OKTT status zijn.

3.2.2. Spoor 2

19. Faciliteer het delen van praktijkervaringen met ketenrisicoanalyse-methodieken. Dit geeft gedeeld inzicht in de bruikbaarheid en meerwaarde van de methodieken. Dit draagt niet alleen bij aan het ontwikkelen/selecteren van een passende methodiek voor ketenrisicoanalyse, maar ook aan een bredere inzet van de methodiek in het algemeen. CERTS, BIO werkgroepen of andere bestaande security communities (CIP) kunnen hierbij een goed platform vormen.
20. Verken of best-practices over methodieken vanuit BIO-werkgroepen kunnen worden verzameld.
21. Bevorder het uitwerken van hulpmiddelen als handreikingen, richtlijnen en uniforme definities voor keten-risico's en afhankelijkheden. De ICO-Wizard is een voorbeeld van een hulpmiddel die helpt om ketenrisico's bij leveranciers (supplychain) om te zetten in een inkoopeisenpakket
22. Verken de meerwaarde en mogelijkheden om ketenrisicoanalyses uit te laten voeren (voor zover nog niet gedaan) bij onderdelen van de GDI (vitale digitale overheid) en deel de resultaten daarvan met de decentrale overheden om de lokale impact en afhankelijkheid te bepalen.

3.2.3. Spoor 3

Voorbereiding

23. Zorg ervoor dat iedere organisatie binnen de bestuurslaag kennis en toegang heeft tot oefenprogramma's, met duidelijke oefendoelen. In die programma's wordt voldoende aandacht besteed aan het creëren van bewustwording en aan leren, evalueren en verbeteren.
24. Versterk het urgentiebesef in de betrokken bestuurslagen door het oefenen in digitale weerbaarheid te blijven stimuleren. De twee werelden van cyber- en regulier crisismanagement komen daardoor dichter bij elkaar te staan.

25. Ontwikkel oefenscenario's via of gekoppeld aan LCP-Digitaal.

Uitvoering

26. Organiseer het gezamenlijk oefenen van het BZK/DGOO crisisproces met de decentrale overheden.
27. Ondersteun de uitvoering van cybercrisis-oefeningen van decentrale overheden met rijksoverheid. Begin 2021 is daar ervaring mee opgedaan vanuit gemeenten in een tabletop georganiseerd door NCTV. NCSC-IBD-G4-VR hebben daarbij samen geoefend in samenwerking cyber -crisis structuur en opschaling van lokaal tot nationaal niveau. Een vergelijkbare tabletop is waardevol te herhalen in de setting van provincies en waterschappen.
28. Stimuleer dat iedere organisatie tenminste jaarlijks oefent en vaker op onderdelen waarbij dit vereist is en stimuleer een gecoördineerde aanpak hiervoor bij bestuurslagen. Hiermee wordt ook inbegrepen oefenen in ketens, met opschaling naar de Veiligheidsregio´s en met de regionale supplychain. Het testen van de goede werking van cruciale onderdelen van continuïteitsplannen zoals terugvalopties en recovery scenario´s, wordt daarin ook meegenomen. Naast het oefenen met oefenscenario's zou ook testen (redteaming) van ketens vanuit BZK geregisseerd en georganiseerd moeten worden, i.v.m. keten overstijgende mandaten en vrijwaringen.
29. Stimuleer het jaarlijkse uitvoeren van BCM gerelateerde disaster recovery testen, eventueel als onderdeel van een crisismanagement oefening.
30. Er is een versterkende kruisbestuiving tussen spoor 2 'Zicht op ketens en afhankelijkheden' en het oefenen. Bij bepalen van oefendoelen en scope kan rekening worden gehouden met belangrijkste ketenrisico's en met die partners (bijvoorbeeld samenwerkingen, leveranciers) oefendoelen bepalen.
31. Stimuleren dat alle decentrale overheden actief mee oefenen in nationale crisisoefeningen.
32. Naast oefenen en testen zal ook continu verbetering noodzakelijk zijn i.v.m. toenemende dreigingsvormen