Opdracht en uitkomst

Op 20 maart 2020 is de kabinetsreactie op het rapport 'Voorbereiden op digitale ontwrichting' van de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) en de evaluatie rondom de Citrix-problematiek aan de Tweede Kamer gestuurd. Binnen deze reactie is de toezegging gedaan dat de staatssecretaris van BZK in overleg gaat met gemeenten, veiligheidsregio's, waterschappen en provincies om de kaders en afspraken die in dit verband noodzakelijk zijn verder te verkennen en of daarmee ook deze decentrale overheden[1] voldoende stappen zetten om voorbereid te zijn op digitale ontwrichting.

Dit rapport biedt op basis van een in de zomer 2020 uitgevoerde 'quick scan' inzicht in de stand van zaken wat betreft kaders en afspraken bij de verschillende decentrale overheden. Het rapport definieert een drietal prioriteiten om vanuit BZK energie op te zetten.

De scope van dit onderzoek is bepaald vanuit de bestuurlijke verantwoordelijkheid van de directie Digitale Overheid van het Directoraat-Generaal Overheidsorganisatie van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK/DGOO/DO). Taak van deze directie is het concretiseren van de visie op de rol van de overheid in de informatiesamenleving[2]. De directie Digitale Overheid neemt de regie op de interbestuurlijke uitwerking en uitvoering hiervan daar waar dat de publieke belangen en de maatschappelijke orde in de digitale samenleving dient en zo nodig versterkt. Uitgangspunt van de bestuurlijke afspraken is dat alle organisaties primair zelf verantwoordelijk zijn voor digitale weerbaarheid. De overheid als geheel treedt op waar nodig en zorgt voor informatievoorziening over dreigingen en kwetsbaarheden. Het is daarom van belang om onderling duidelijke afspraken te maken met alle overheidsorganisaties, ook met die welke niet onder de rijksoverheid vallen. BZK heeft daarin een coördinerende taak. Daarbij wordt uiteraard oog gehouden voor, en samengewerkt met in achtneming van alle bestaande departementale verantwoordelijkheden in relatie tot crisisbeheersing en cybersecurity. Hierbij heeft het ministerie van Justitie en Veiligheid (JenV) een stelselverantwoordelijkheid.

1 Binnen dit rapport wordt met ´decentrale overheden´ gemeenten, veiligheidsregio´s, de waterschappen en provincies bedoeld.

Achtergrond en context

1.1 Perspectief overheidsbreed

Cybersecurity is een prioriteit van dit kabinet. Dit is in april 2018 bekrachtigd met de uitwerking van de Nederlandse Cybersecurity Agenda (NCSA)[3]. Onder coördinatie van JenV worden sindsdien maatregelen genomen om de kabinetsbrede cybersecurity-ambities te realiseren. Het verhogen van informatieveiligheid bij de overheid is tevens opgenomen in de BZK Agenda Digitale Overheid 'NL DIGIbeter'[4] en uitgewerkt in de interbestuurlijke actie agenda[5].

In de NCSA zijn zeven ambities[6] geformuleerd, inclusief maatregelen, om Nederland Digitaal Veilig te houden. Om in te kunnen spelen op technologische en maatschappelijke ontwikkelingen en actuele dreigingen en risico's, worden de maatregelen uit de NCSA periodiek verder uitgewerkt en versterkt. Dit is sinds de verschijning van de NCSA in april 2018 ook meerdere keren gebeurd.

In 2019 heeft de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) in haar rapport "Voorbereiden op digitale ontwrichting"[7] 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 signaleert daarbij dat incidenten met een digitale component nog onvoldoende geadresseerd worden binnen de huidige structuren. Digitale incidenten hebben, door onderlinge afhankelijkheden en de complexiteit en diversiteit van netwerk- en informatiesystemen, sneller grootschalige en grensoverschrijdende effecten.

In de kabinetsreactie op het WRR-rapport is een lijst met aanvullende maatregelen benoemd om het cybersecuritystelsel in Nederland verder te versterken.

Door de COVID-19 crisis zijn we versneld in een nieuwe fase van onze digitale samenleving gekomen. De virusuitbraak zorgt ervoor dat we nog intensiever gebruikmaken van onze digitale infrastructuur en alle middelen die daarbij komen kijken. Een groot deel van de Nederlandse bevolking werkt en onderhoudt sociale contacten nu op afstand. Onze maatschappij is in grote mate afhankelijk van digitale processen zonder dat analoge terugvalopties altijd voorhanden zijn. Naast deze toegenomen afhankelijkheid is ook de digitale dreiging van statelijke actoren en cybercriminelen toegenomen. Deze dreigingen hebben een permanent karakter gekregen, zo stelt het Cybersecuritybeeld Nederland 2020 (CSBN 2020)[8].

Digitalisering maakt processen in de samenleving op nieuwe en onverwachte manieren kwetsbaar. Deze ontwikkelingen vragen dan ook aandacht van de verschillende decentrale overheden. Een goede voorbereiding op digitale ontwrichting, waarbij preventie en respons in balans zijn, is cruciaal.

1.2 Lokaal perspectief

Deze quickscan onderzoekt de voorbereiding op maatschappelijke ontwrichting met een digitale oorzaak bij decentrale overheden. Het WRR-rapport hanteert de term ´digitale ontwrichting´ als afgeleide van ´maatschappelijke ontwrichting´. Bij maatschappelijke ontwrichting draait het om een ernstige verstoring van cruciale processen voor de samenleving waardoor de maatschappelijke continuïteit in gevaar komt. Een digitale ontwrichting is een vorm van maatschappelijke ontwrichting die verband houdt met een

3 Kamerstukken II 2017/18, 26643, nr. 536
4 kamerstukken II 2019/20, 26643 nr. 700 bijlage 942645
5 Kamerstukken II 2018/19, 26643, nr. 574
6 1. Nederland heeft zijn digitale slagkracht op orde. 2. Nederland draagt bij aan internationale vrede en veiligheid in het digitale domein. 3. Nederland loopt voorop in het bevorderen van digitaal veilige hard- en software. 4. Nederland beschikt over weerbare digitale processen en een robuuste infrastructuur. 5. Nederland werpt door middel van cybersecurity succesvol barrières op tegen cyber-crime. 6. Nederland is toonaangevend op het gebied van cybersecurity kennisontwikkeling. 7. Nederland beschikt over een integrale, publiek-private aanpak van cybersecurity.
7 kamerstukken II 2019/20, 26643 nr. 673 bijlage 927630
8 kamerstukken II 2019/20, 26643 nr. 695 bijlage 942250

ernstige verstoring of uitval van digitale infrastructuur. Dit rapport onderzoekt de mate waarin decentrale overheden zijn voorbereid op maatschappelijke ontwrichting met een digitale oorzaak. Deze oorzaak kan binnen de eigen organisatie liggen, bijvoorbeeld bij een ransomware aanval binnen een gemeente, maar kan ook buiten de eigen organisatie liggen, zoals bijvoorbeeld bij een malware aanval die belangrijke ketenpartners raakt.

Vanuit een nationaal perspectief gaat het bij maatschappelijke ontwrichting over de (potentiële) impact van incidenten met een nationale uitstraling. Hierbij gaat het onder meer om de impact van uitval of aantasting van belangrijke kernprocessen, waaronder de vitale processen welke begin 2017 door het kabinet rijksbreed zijn vastgesteld[9]. Het Nationaal Crisisplan Digitaal (NCP-Digitaal)[10], uitgewerkt door de NCTV in samenspraak met de verschillende relevante actoren, biedt overzicht en inzicht in de bestaande afspraken op regionaal, nationaal en internationaal niveau. Het NCP-Digitaal sluit aan op het Nationaal Handboek Crisisbesluitvorming.

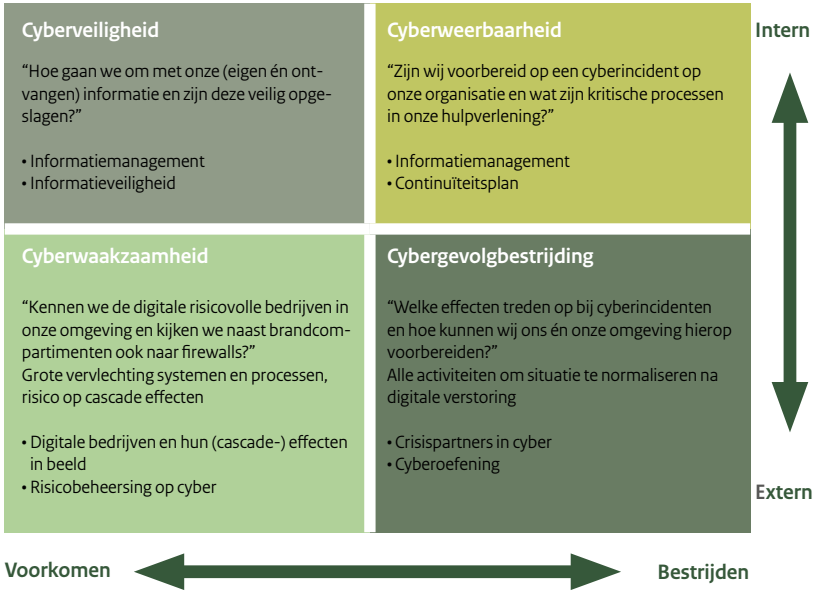
Deze quick scan richt zich op ontwrichting als gevolg van een digitaal incident waarbij de decentrale overheden een rol spelen in het bestrijden van de gevolgen. Dit kan een situatie zijn waar de Nationale Crisisstructuur in werking treed, als ook een situatie waar dat nog niet het geval is. Met ontwrichting in een lokale context bedoelen we ernstige 'lokale' verstoringen van maatschappelijke kernprocessen die onder verantwoordelijkheid vallen van decentrale overheden en die aansluiten bij de reeds ingerichte processen rondom crisisbeheersing. Hierbij kan worden gedacht aan verstoring van gemeentelijke dienstverlening aan burgers, bezoekers en bedrijven, op afstand aangestuurde rioolwaterzuiveringen, gemalen van waterschappen of verkeersmanagementsystemen van provinciale wegen.

Voldoende aandacht voor het voorkomen van digitale incidenten door een passende implementatie van de Baseline informatiebeveiliging Overheid (BIO)[11] als basisnormenkader voor de hele overheid is daarbij randvoorwaardelijk voor de digitale veiligheid van decentrale overheden. Waar mogelijk moeten digitale incidenten worden voorkomen, maar voor als dat niet lukt moeten decentrale overheden ook voorbereid zijn op het bestrijden van de gevolgen van deze digitale incidenten op de eigen dienstverlening. Daarnaast dienen de decentrale overheden bij te dragen aan de gezamenlijke aanpak (vanuit crisisbeheersing) van de maatschappelijke gevolgen die voortkomen uit het digitale incident. Voorbereiding op digitale ontwrichting bij decentrale overheden definiëren we hiermee als:

'Voorbereid zijn op het bestrijden van de gevolgen van een ernstige 'lokale' verstoring van maatschappelijke kernprocessen, die samenhangt met cyberincidenten waarbij continuïteit van dienstverlening en/of crisisbeheersing onder verantwoordelijkheid valt van lokale overheden in aansluiting op de bestaande crisisstructuren'.

Hoe digitale ontwrichting zich verhoudt tot cyberveiligheid, cyberweerbaarheid en cybergevolgbestrijding is helder uitgewerkt in het cyberkwadrant, een model dat wordt gebruikt door de veiligheidsregio's in het 'bestuurlijk routeboek digitale ontwrichting' van het veiligheidsberaad[12].
Dit model wordt ook aangehaald in een gemeentelijke handreiking van de G4[13] en in een programmaplan van de waterschappen[14]

9 https://www.nctv.nl/onderwerpen/vitale-infrastructuur/overzicht-vitale-processen
10 https://www.ncsc.nl/documenten/publicaties/2020/februari/21/nationaal-crisisplan-digitaal
11 https://bio-overheid.nl/
12 kamerstukken II 2019/20, 26643 nr. 673
13 https://www.digitaleoverheid.nl/nieuws/g4-ontwikkelt-handreiking-voor-bestrijding-gevolgen-cybercrises/
14 Programmaplan IVenP 2020-2025 HetWaterschapshuis v2.0 (intern document)



Figuur geeft het cyberkwadrant weer dat is opgesteld door veiligheidsregio ijsselland om cyber aandachtsgebieden in te delen naar extern-intern en preventie en respons. In het model worden op de y-as externe vs interne factoren tegen elkaar afgezet en op de x-as voorkomen vs bestrijden

Figuur 1 cyberkwadrant veiligheidsregio IJsselland

Vanuit de gehanteerde definitie van digitale ontwrichting ligt het zwaartepunt van het voorbereid zijn op digitale ontwrichting op ´cybergevolgbestrijding´. Dit kwadrant is extern georiënteerd. Het bestrijden, oefenen en maken van afspraken met crisispartners is hierin cruciaal.

Als een cybercrisis organisatie overstijgend is, en maatschappelijk verstorende effecten heeft, zal moeten worden opgeschaald conform bestaande crisisbeheersingsstructuren, zoals de GRIP-structuur, om effectieve gevolgbestrijding te coördineren. De bestaande operationeel georiënteerde cyber-samenwerking verloopt via de computercrisisteams in aansluiting op het Landelijk Dekkend Stelsel (LDS) van cybersecurity samenwerkingsverbanden. Deze crisisteams zijn gericht op een enkele bestuurslaag.

Het kan gebeuren dat het lokaal bestuur effecten ondervindt van een cybercrisis die buiten het traditionele domein van de veiligheidsregio valt en die ook de eigen gemeentelijke dienstverlening niet direct raakt. In de Handreiking Cybergevolgbestrijding (CGB) G4-gemeenten wordt dit geïllustreerd aan de hand van een voorbeeld van een ransomware aanval op een middelbare school waarbij gedreigd wordt vertrouwelijke gegevens van leerlingen en docenten te publiceren en waarbij berichtgeving op sociale media onrust en publieke verontwaardiging veroorzaken. In zo´n type cybercrisis is de gemeente ook aan zet om zich met de gevolgen vanuit openbare orde en veiligheid bezig te houden. De structuur waarbinnen dit gebeurt verschilt per gemeente en is niet overal formeel beschreven.

Vanuit het kwadrant ´cyberwaakzaamheid´ ligt de nadruk op het in beeld krijgen van de belangrijkste afhankelijkheden van ketens die worden benut in lokaal cruciale processen. De huidige stelsels zijn zo ingericht dat elke organisatie verantwoordelijk is voor de eigen digitale weerbaarheid. In ketens zijn echter alle ketenpartners samen verantwoordelijk voor de digitale veiligheid. Inzicht en samenwerking met ketenpartners die een rol spelen in de afhankelijkheidsketen is daarbij van belang. Dat draagt bij aan het goed voorbereid zijn op potentiële gevolgbestrijding. Het vereist een krachtig initiatief van decentrale overheden om ketenpartners te kunnen gaan aanspreken op hun (mede-)verantwoordelijkheid. Bij het voorbereiden op cyberincidenten is het cruciaal om ketenafhankelijkheden in kaart te hebben. Het is mede aan decentrale overheden om de continuïteit van als niet-vitaal aangemerkte systemen en processen binnen ketens te monitoren teneinde de continuïteit daarvan te kunnen waarborgen.
Het kwadrant ´cyberveiligheid´ is een randvoorwaarde om cyberincidenten te beperken en te beheersen. De BIO, als overheidsnorm voor informatieveiligheid, speelt hierin een belangrijke rol en helpt decentrale overheden de basis op orde te krijgen binnen de eigen organisatie.
Cyberincidenten binnen de eigen organisatie, waarbij de effecten tot de interne organisatie beperkt blijven, vallen onder ´cyberweerbaarheid´. Het gaat daarbij dan, om interne calamiteitenbeheersing.

Aanpak van de Quick scan

2.1. Aanpak

Een integraal overzicht van actuele verbeterplannen en kaders op het terrein van maatschappelijke ontwrichting met digitale oorzaak die betrekking hebben op de decentrale overheden was bij de start van de quick scan niet voor handen. Om inzicht te krijgen in hoeverre provincies, waterschappen, gemeenten en veiligheidsregio's energie steken in het voorbereiden op digitale ontwrichting is contact gelegd met experts en vertegenwoordigers van de betrokken decentrale overheden en de betrokken ministeries (JenV, BZK, I&W en EZK) op deze dossiers. Deze groep stakeholders vormde een klankbordgroep waarmee periodiek de aanpak, voortgang, observaties en tussentijdse resultaten zijn afgestemd en getoetst. Met hulp van deze stakeholders zijn relevante kaders en verbeterprogramma's verzameld, gestructureerd en geanalyseerd.

De decentrale overheden maken deel uit van de bestaande cyber- en crisisstructuren binnen Nederland. De mate van voorbereiding op digitale ontwrichting per bestuurslaag is dan ook in samenhang beschouwd van dit gehele speelveld. Naast een globale analyse van de verzamelde verbeterplannen van de decentrale overheden, is er in de quick scan ook gelet op samenhang. Samenhang in de benoemde ontwikkelingen tussen de decentrale overheden onderling, samenhang tussen het cyber- en het crisisdomein en samenhang tussen de ontwikkelingen bij de decentrale overheden en samenhang met de nationale kaders zoals bijvoorbeeld het NCP-Digitaal. Digitale dreigingen met potentieel maatschappelijk ontwrichtende gevolgen kunnen nationaal, regionaal en lokaal gesignaleerd worden. Met nationale signalering bedoelen we in deze context dat bij het NCSC een beeld van dreigingen ontstaat die tot verstoring van de dienstverlening van lokale overheden kunnen leiden (bijvoorbeeld de Citrix problematiek begin 2020). Bij 'lokale signalering' gaat het om een digitaal incident dat bij een decentrale overheid ontstaat en dat tot lokale of regionale maatschappelijke verstoring kan leiden (bijvoorbeeld de Lochem casus in 2019). Lokale signalering kan vanuit de eigen organisatie gebeuren door interne monitoring diensten, of een CERT (Computer Emergency Respons Team, ook wel CSIRT's of computercrisisteams genoemd) of een Security Operations Center (SOC) waarmee deze dienst is ingeregeld en waarop een organisatie is aangesloten. Het is noodzakelijk om lokaal, regionaal en nationaal betrokken partijen te verbinden in taal en aanpak. Dit geldt zowel voor operationele digitale samenwerking, vanuit bijvoorbeeld het Landelijk Dekkend Stelsel, als bij samenwerking binnen de bestaande structuren voor crisisbeheersing.

2.2. Referentiekader

Als referentiekader voor de documentanalyse is enerzijds de clustering van onderwerpen gehanteerd zoals beschreven door de WRR. De WRR clustering ´Paraatheid, Signalering, Bestrijding en Herstel´ lijkt overeen te komen met de fasering zoals gehanteerd in het NIST Cyber -security Framework[15] voor kritieke infrastructuur, waarbij Paraatheid in het NIST model verder is opgesplitst in Identificeren en Beschermen. Anderzijds is het eerdergenoemde cyberkwadrant van veiligheidsregio IJsselland gebruikt om overzicht te krijgen over de aangekaarte thema's binnen de verschillende verbeterprogramma's van de decentrale overheden.

15 https://www.nist.gov/cyberframework

Plannen en kaders per bestuurslaag

In 2019 heeft BZK/DGOO/DO onder de noemer Gemeenschappelijk OVerheid Security Operations Center (GOV-SOC)[16] een verkenning gedaan naar de digitale weerbaarheid van de decentrale overheden. Deze verkenning maakte inzichtelijk dat de gemeenten en waterschappen zich al goed georganiseerd hebben als bestuurslaag in het overheids-cyberdomein en dat provincies daar werk van maken. In beginsel zijn alle decentrale overheden zelf verantwoordelijk voor informatieveiligheid. Een volwassen implementatie van de Baseline Informatieveiligheid Overheid vormt de basis hygiëne om organisaties weerbaar te maken. Alle decentrale overheden hebben zich dan ook geconformeerd aan deze norm per 1 januari 2020 en ze worden op verschillende manieren ondersteund bij de implementatie ervan. Vanwege organisatie overstijgende afhankelijkheden en ketensamenwerkingen is de weerbaarheid van organisaties in isolement onvoldoende: Om vroegtijdig digitale dreigingen te signaleren en waar nodig effectief te bestrijden is samenwerking en kennisdeling cruciaal. Samenwerking binnen de eigen bestuurslaag, met ketenpartners, maar ook met rijksoverheid is daarom essentieel. Er wordt dan ook actief aansluiting gezocht met nationale initiatieven zoals het Landelijk Dekkend Stelsel (LDS) en het NCP-Digitaal, om als overheden gezamenlijk vroegtijdig digitale incidenten te signaleren, informatie uit te kunnen wisselen en om de onderliggende dreigingen effectief te kunnen bestrijden
Hieronder volgt een samenvatting van de initiatieven die worden opgepakt door de decentrale overheden om de weerbaarheid van individuele organisaties en in samenhang met ketenpartners verder te verhogen om zodoende als bestuurslaag goed voorbereid te zijn op digitale ontwrichting.

3.1. Gemeenten

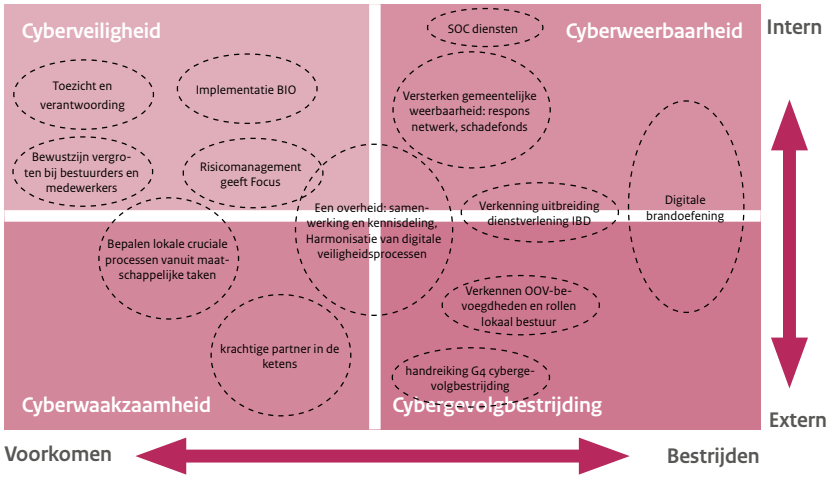
Vanuit de Vereniging van Nederlandse Gemeenten (VNG) is in februari 2020 de Agenda Digitale Veiligheid 2020-2024[17] vastgesteld. De bestuurlijke agenda beschrijft tien actielijnen om gemeenten weerbaarder te maken rond de thema's 'het eigen huis op orde', 'digitale verstoringen in de samenleving' en 'cybercriminaliteit'. Immers, indien de systemen en diensten van de gemeentelijke organisatie worden aangetast, dan wordt het gemeentebestuur daar op aangesproken. Daarnaast geldt dat als er sprake is van een ramp of crisis op lokaal niveau, de burgemeester verantwoordelijk is voor de effectieve bestrijding ervan. Tevens kan de bestuurder worden aangesproken op de openbare orde- en veiligheidsproblemen (OOV) die uit het incident voortvloeien. Digitale veiligheid en informatieveiligheid zijn daarom niet meer uitsluitend vraagstukken voor de bedrijfsvoering, maar horen permanent thuis op de bestuurstafel van het gemeentehuis. Datalekken, digitale verstoringen, incidenten en digitale criminaliteit zijn dagelijkse realiteit. Dergelijke incidenten tonen aan dat (digitale) verstoringen, ook buiten het gemeentehuis, tot ontwrichtende effecten kunnen leiden. Op basis van deze digitale agenda wordt in januari 2021 aan de leden van de VNG de resolutie 'Digitale Veiligheid: kerntaak voor gemeenten' voorgelegd voor besluitvorming waarbij ook afspraken worden gemaakt over de uitvoering op basis van een plan van aanpak Uitvoering Agenda Digitale Veiligheid. Het plan van aanpak is primair gericht op 'gemeenten', maar de VNG is zich ervan bewust dat ook samenwerkingsverbanden, zoals bijvoorbeeld shared-serviceorganisaties, betrokken zijn bij het thema digitale veiligheid van gemeenten. De eindverantwoordelijkheid blijft echter altijd bij de gemeenten liggen. Daarnaast wordt ook samenwerking met de veiligheidsregio's benoemd, als onderdeel van de ketenaanpak rond digitale weerbaarheid van gemeenten.

16 de BZK GOV-SOC verkenning is een intern rapport

17 https://vng.nl/sites/default/files/2020-02/vng_agenda_digitale_veiligheid_2020-2024_def_0.pdf

Verder is vanuit deze quick scan de handreiking CyberGevolgBestrijding[18] van mei 2020 onderzocht die is opgesteld door de G4-gemeenten (Amsterdam, Den Haag, Rotterdam en Utrecht). Dit document adresseert de specifieke kenmerken van een cybercrisis en de consequenties daarvan voor de gevolgbestrijding binnen het (verlengd) lokaal bestuur.

Deze documenten vormen voor deze quickscan het voornaamste kader voor de gemeentelijke plannen ten aanzien van de voorbereiding op digitale ontwrichting.



figuur geeft het cyberkwadrant weer dat is opgesteld voor de thema´s en ontwikkelingen bij de gemeenten. In het model worden op de y-as externe vs interne factoren tegen elkaar afgezet en op de x-as voorkomen vs bestrijden. Binnen deze verdeling zijn verschillende initiatieven gecategoriseerd.

Figuur2 weergave van gemeentelijke thema´s en ontwikkelingen

Zoals in figuur2 is te zien dekken de gemeentelijke verbeterplannen de vier cyberkwadranten evenwichting af. Voor de uitvoering van de gemeentelijke Agenda Digitale Veiligheid wordt gewerkt de maatschappelijke taken van gemeenten en wordt er aansluiting gezocht bij de leefwereld van de bestuurder. Ook spelen ketens een nadrukkelijke rol bij continuïteit van cruciale processen en wordt er samen
werking met de veiligheidsregio's gezocht. De BIO staat in deze plannen centraal. Gemeenten staan zelf aan de lat om de BIO te implementeren, maar worden daarbij actief ondersteund door de IBD en de VNG.

Vanuit preventie (cyberveiligheid en -waakzaamheid) wordt aandacht besteed middels initiatieven voor het verhogen van bewustzijn bij medewerkers en bestuurders. Verantwoording en toezicht zal worden versterkt Verantwoordelijkheid en toezicht worden versterkt op basis van de BIO.. Het bepalen van lokale cruciale processen die voortvloeien uit maatschappelijke taken van gemeenten moet helpen bij het prioriteren en inzicht krijgen in de raakvlakken met landelijke vitale processen. Daarnaast zijn er plannen voor een bestuurlijke digitale risicokaart welke inzicht geeft in potentiële cascade-effecten van digitale incidenten en crises.

Vanuit respons (cyberweerbaarheid en -gevolgbestrijding) betreft wordt er aandacht besteed aan oefenen, bijvoorbeeld door digitale brandoefeningen. De informatiepositie van de IBD als officieel CERT voor de hele bestuurslaag zal worden versterkt en er komt een Gemeentelijk Respons Netwerk onder coördinatie van de IBD om onderlinge assistentie te bieden bij digitale incidenten.

In aanvulling op de Digitale Agenda van de VNG biedt de G4 handreiking 'cybergevolgbestrijding' gemeenten structuur bij betere voorbereiding op digitale incidentbestrijding. De handreiking is gericht op ondersteuning van het (verlengd) lokaal bestuur en haar directe adviseurs bij de gevolgbestrijding van een digitale verstoring waaronder de bestuurlijke OOV-bevoegdheden en rollen bij een digitale crisis. Er is aandacht voor een duidelijke afbakening van opschaling richting de veiligheidsregio's en het nationale niveau. Tot slot is er aandacht voor het professionaliseren van herstel en wederopbouw na een Cyber-incident.

Met de beoogde uitvoering van de Agenda Digitale veiligheid zetten ge-

18 Handreiking Cybergevolgbestrijding (CGB) G4-gemeenten, Deel 2: Koude fase, Naslagwerk cybergevolgbestrijding

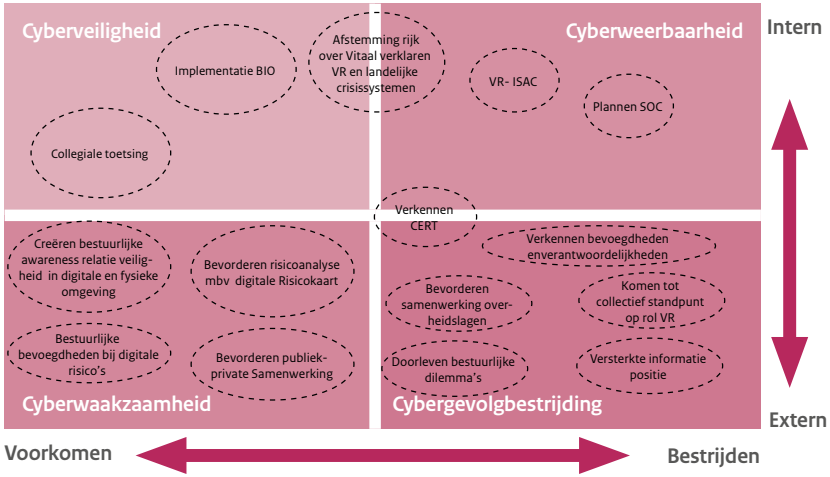
meenten flinke stappen om maatschappelijke ontwrichting door digitale incidenten beter te beheersen.

3.2. Veiligheidsregio´s

In december 2018 heeft het veiligheidsberaad het Instituut Fysieke Veiligheid (IFV) verzocht om het thema digitale ontwrichting vorm te geven in een bestuurlijk programma in afstemming met de veiligheidsregio's, gemeenten (VNG, G4 en Regioburgemeesters), het ministerie van Justitie en Veiligheid, het NCSC en Defensie. In december 2019 heeft het Veiligheidsberaad het door het IFV opgestelde en afgestemde bestuurlijk routeboek digitale ontwrichting[19] vastgesteld met als doel om te komen tot een betere informatiepositie en een handelingsperspectief voor de besturen van veiligheidsregio's.
Binnen deze quickscan wordt het bestuurlijk routeboek digitale ontwrichting van het veiligheidsberaad beschouwd als het belangrijkste kader voor de veiligheidsregio´s.

Bij een lokale ramp of crisis is de burgemeester verantwoordelijk voor de effectieve bestrijding en de openbare orde- en veiligheidsproblemen die uit het incident voortvloeien. Bij een ramp of crisis met meer dan plaatselijke betekenis, of bij ernstige vrees voor het ontstaan daarvan, gaan de wettelijke bevoegdheden voor de bestrijding over naar de voorzitter van de veiligheidsregio. Kenmerkend voor de huidige complexe digitale samenleving is dat een fysieke ramp of crisis ook kan voortkomen uit een digitale verstoring. De verantwoordelijkheden en bevoegdheden van de burgemeester en besturen van de veiligheidsregio's zijn gericht op het voorkomen en bestrijden van een ramp of crisis in de fysieke omgeving. Bij incidenten in de digitale omgeving zijn die rollen, volgens het routeboek, nog onvoldoende helder ten aanzien van governance en juridische aspecten in relatie tot de functionele ketens. Het bestuurlijk routeboek digitale ontwrichting heeft daarom een aantal voornemens met betrekking tot risicobeheersing (cyberwaakzaamheid), (cyber)gevolgbestrijding en informatieveiligheid (cyberveiligheid en cyberweerbaarheid) van de eigen organisatie. De verschillende bestuurlijke onderwerpen zijn weergegeven in onderstaande figuur3

19 https://veiligheidscoalitie.nl/action/?action=download&id=2358



Figuur geeft het cyberkwadrant weer dat is opgesteld voor de thema´s en ontwikkelingen bij de veiligheidsregio´s. In het model worden op de y-as externe vs interne factoren tegen elkaar afgezet en op de x-as voorkomen vs bestrijden. Binnen deze verdeling zijn verschillende initiatieven gecategoriseerd.

Figuur 3: weergave van thema´s en ontwikkelingen bij veiligheidsregio's

Het stimuleren van samenwerking tussen partners onder regie van het ministerie van Justitie en Veiligheid (JenV) staat hierbij centraal.

Vanuit preventie (cyberveiligheid en -waakzaamheid) wordt er binnen de plannen aandacht besteed aan het belang van het verkennen van bestuurlijke bevoegdheden bij digitale risico's. Verder is er aandacht voor het creëren van bestuurlijk bewustzijn voor de relatie tussen de digitale en fysieke wereld. De plannen beschrijven dat er vanuit de uitvoering gewerkt dient te worden aan het bevorderen van publiek-private samenwerking en aan het uitvoeren van risicoanalyses op basis van een digitale risicokaart.

In het kader van respons (cyberweerbaarheid en -gevolgbestrijding) zullen de bevoegdheden en verantwoordelijkheden van burgemeesters bij cybergevolgbestrijding verkend worden vanuit een juridische perspectief.

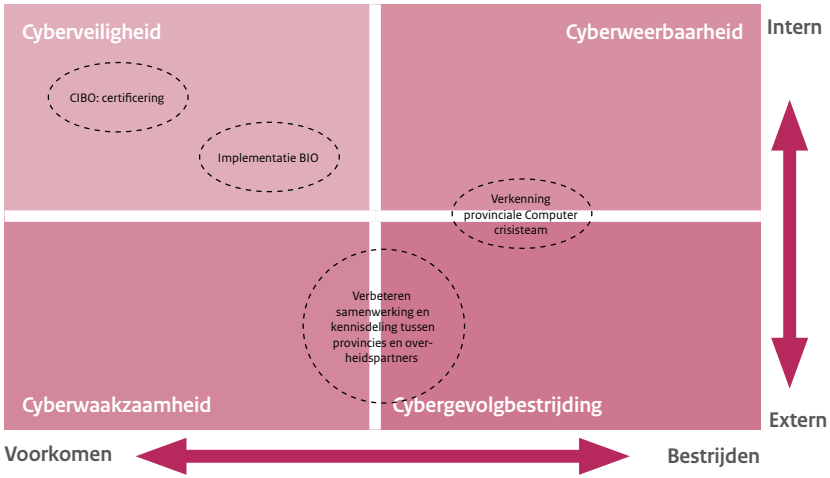
Samen met het meer en beter oefenen om bestuurlijke dilemma's bij digitale ontwrichting te doorleven, moet dat leiden tot een collectief standpunt ten aanzien van de rol van de veiligheidsregio's. Het bevorderen van afstemming en samenwerking tussen de overheidslagen, het versterken van de informatiepositie van veiligheidsregio's, waaronder oprichting van een CERT (Computer Emergency Respons Team) voor de veiligheidsregio's vormen daarbij aandachtspunten in de uitvoering.

Tot slot is er in het routeboek nadrukkelijk aandacht voor verhogen van cyberveiligheid en cyberweerbaarheid van de veiligheidsregio's zelf. Daarbij wordt er thans met het rijk overlegd te vinden over het vitaal verklaren van de veiligheidsregio's als organisaties en de landelijke crisissystemen die veiligheidsregio's gebruiken. Veiligheidsregio's werken daarnaast in eigen huis aan een volwassen implementatie van de BIO. Voor betere sectorale samenwerking is er inmiddels een eigen VR-ISAC [20] ingericht.

Met de uitvoering van dit bestuurlijk routeboek digitale ontwrichting zetten de veiligheidsregio's in samenwerking met rijksoverheid en gemeenten flinke stappen ter voorkomen van maatschappelijke ontwrichting door digitale incidenten.

3.3. Provincies

Sinds september 2017 hebben de provincies een eerste Interprovinciale Digitale Agenda (IDA). Daar in wordt vastgesteld dat de context waarin provincies opereren in hoog tempo verandert. Informatievoorziening en digitalisering zijn essentieel voor het adequaat uitvoeren van de wettelijke taken en het realiseren van de politieke opgaven van de provincies.
De dienstverlening aan burgers, bedrijven en instellingen staat daarbij centraal. In mei 2019 is daarom de IDA bijgesteld tot IDA 2019-2023, regie op digitale transformatie.



figuur geeft het cyberkwadrant weer dat is opgesteld voor de thema´s en ontwikkelingen bij de provincies. In het model worden op de y-as externe vs interne factoren tegen elkaar afgezet en op de x-as voorkomen vs bestrijden. Binnen deze verdeling zijn verschillende initiatieven gecategoriseerd.

Figuurq: weergave van provinciale thema's en ontwikkelingen

Vanuit deze bijgestelde IDA 2019-2023 ontwikkelen provincies zich op vier sporen: Bedrijfsvoering, Dienstverlening, Data en Innovatie. Vanuit het spoor Dienstverlening zijn de gezamenlijke activiteiten gericht op het in samenhang implementeren van een aantal bouwstenen die bijdragen aan een verbetering van de digitale dienstverlening. Daarbij wordt de verkenning van een gemeenschappelijk provinciaal CERT benoemd, tegenover de huidige situatie waarin elke provincie eigenstandig dit heeft georganiseerd. Het spoor 'Data' zetten de provincies maximaal in om nu en in de toekomst publieke waarde te blijven leveren. Met het spoor 'Innovatie' gaan de provincies de benodigde versnelling hierin aanbrengen.

Voor preventie (cyberveiligheid en -waakzaamheid) onderkennen de provincies het belang van een volwassen implementatie van de BIO. Daarom hebben provincies afgesproken eind 2023 certificeerbaar[21] te zijn volgens

20 https://www.ifv.nl/nieuws/Paginas/Nieuw-cyber-inlichtingencentrum-voor-veiligheidsregios.aspx

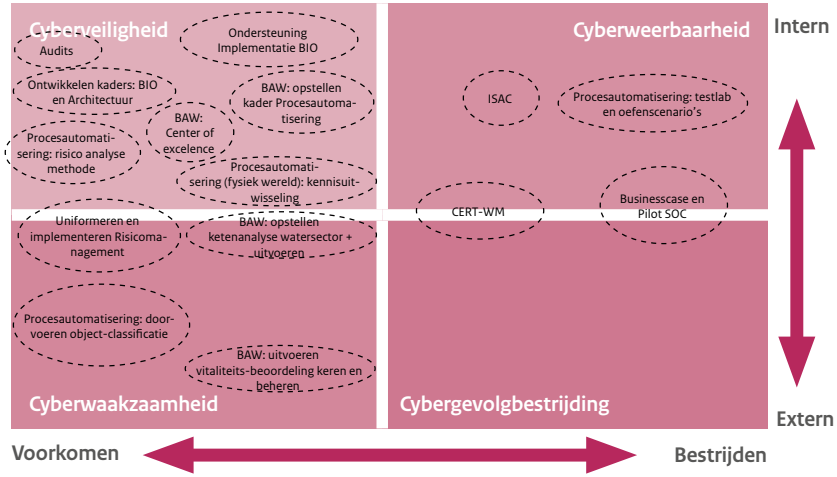
21 Provincies bereiden zich voor op ISO 27001 in 2023 - BIJ12

de internationale standaard ISO 27001. Met deze certificering willen de provincies laten zien dat de informatiebeveiliging goed op orde is en dat elke provincie de informatiebeveiliging voortdurend monitort.

De verkenning van een gemeenschappelijk provinciaal CERT draagt bij aan een afgestemde respons bij cyberincidenten. Een subsidieaanvraag van uitvoeringsorganisatie BIJ12 om de verkenning versneld uit te voeren is toegekend door het ministerie van BZK en de verkenning zal eind 2020 starten. Met dit initiatief wordt samenwerking en informatiedeling tussen provincies en overheidspartners verbeterd. Het draagt bij het bij aan uniforme procedures en afspraken bij organisatie overstijgende cyberincidenten.

Met de uitvoering van deze activiteiten zetten de provincies stappen ter verhoging van de weerbaarheid van provincies en verbeterde samenwerking ter voorkoming van maatschappelijke ontwrichting door digitale incidenten.

3.4. Waterschappen



Figuur5: weergave van thema's en ontwikkelingen bij waterschappen

figuur geeft het cyberkwadrant weer dat is opgesteld voor de thema´s en ontwikkelingen bij de waterschappen. In het model worden op de y-as externe vs interne factoren tegen elkaar afgezet en op de x-as voorkomen vs bestrijden. Binnen deze verdeling zijn verschillende initiatieven gecategoriseerd.

De Unie van Waterschappen (UvW) sloot in 2011, samen met IenW, het Interprovinciaal Overleg (IPO), de Vereniging van Nederlandse Gemeenten (VNG) en de Vereniging van drinkwaterbedrijven in Nederland (Vewin) het Bestuursakkoord Water (BAW). Daarin is afgesproken om de doelmatigheid van het waterbeheer te vergroten. Minder bestuurlijke druk, heldere verantwoordelijkheden en slim en kostenefficiënt samenwerken staan centraal in deze afspraken, die lopen tot 2021.
In 2018 zijn er voor 4 onderwerpen aanvullende afspraken gemaakt op het Bestuursakkoord Water: Kansen voor de informatiesamenleving, Cybersecurity binnen de watersector, Regionale samenwerking tussen gemeenten, waterschappen en drinkwaterbedrijven en tot slot Implementatie van de Omgevingswet in de waterketen.

Het ministerie van Infrastructuur en Waterstaat coördineert het onderwerp 'Cybersecurity binnen de watersector' en heeft daartoe het Programma Versterken Cyberweerbaarheid in de Watersector 2019-2022 (PVCW) [22] opgezet. Dit programma bestaat uit drie componenten: het BAW+, het Kennis 7 Innovatie (K&I) programma en bilaterale afspraken.

Binnen het programma PVCW zijn 15 projecten gedefinieerd die bijdragen aan een versterking van de cyberweerbaarheid. De uitvoering van het programma wordt bekostigd met VNAC-gelden, het budget van de Nationale Cyber Security Agenda (NCSA). De projecten richten zich op organisatie overstijgende samenwerking en afstemming in ketens. Vanuit preventie (cyberveiligheid en -waakzaamheid) is daarbij aandacht voor het in kaart brengen van de huidige situatie door middel van een systeem-, risico en GAP-analyse. Andere projecten focussen op het gezamenlijk ontwikkelen van standaarden en wetgeving en het verduurzamen van kennis binnen center of excellence.

22 https://www.rijksoverheid.nl/documenten/rapporten/2020/11/04/programma-versterken-cyberweerbaarheid-watersector-oktober-2020

Vanuit respons (cyberweerbaarheid en -gevolgbestrijding) draagt het opzetten van een oefenfaciliteit op het gebied van crisismanagement bij aan het verhogen van de weerbaarheid, evenals het voorstel voor meer

operationele security samenwerking in een Security Operations Center (SOC). Het programma is afgerond nadat de individuele projecten beëindigd zijn, eind 2022.

Naast de watersector-brede initiatieven vanuit het I&W-programma besteden de waterschappen zelf ook nadrukkelijk aandacht aan het verhogen van de informatieveiligheid in eigen huis. De waterschappen staan aan de lat om de BIO te implementeren en maar worden daarbij actief ondersteunt met een meer-jaren programma informatieveiligheid en privacy (IV&P) 2020-2024 van Het Waterschapshuis. Initieel was dit een driejarig programma vanuit de Unie van Waterschappen, waarna het in 2016 is verlengd en ondergebracht bij Het Waterschapshuis, de gezamenlijke uitvoeringsorganisatie van de waterschappen.

De doelstellingen van het programma IV&P 2020-2024 zijn:

1. Duurzame verbeterprocessen binnen de waterschappen
2. Een (meer) bewuste mindset en cultuur binnen de waterschappen
3. (Informatie)veilige assets binnen de waterschappen
4. (Informatie)veiliger waterketens

De waterschappen maken door samenwerking, zowel onderlinge als met de rijksoverheid, serieus werk van het verhogen van de weerbaarheid en het voorkomen van maatschappelijke ontwrichting door digitale incidenten. Met de actieve deelname aan het programma verhogen cyberweerbaarheid binnen de watersector en met het eigen programma IV&P geven de waterschappen een impuls aan het verhogen van de weerbaarheid en het voorkomen van maatschappelijke ontwrichting door digitale incidenten.

Bevindingen

4.1 Bevindingen algemeen

4.1.1 Eigen huis op orde

Er bestaan al uniforme kaders en richtlijnen voor informatiebeveiliging van alle decentrale overheden. Vorig jaar is de Baseline Informatiebeveiliging Overheid (BIO) uitgebracht ,hierdoor is meer uniformiteit tussen de verschillende overheidslagen ontstaan en het algemeen voorgeschreven beveiligingsniveau aangescherpt. Alle decentrale overheden pakken hun bestuurlijke verantwoordelijkheid rond digitale veiligheid en zijn volop bezig met de implementatie van de BIO.

Bij gemeenten is de verantwoordelijkheid voor de informatieveiligheid al in 2013 onderstreept in de bestuurlijke resolutie 'Informatieveiligheid basis voor professionele dienstverlening'. Gemeenten worden door de Informatiebeveiligingsdienst (IBD) ondersteund bij implementatievraagstukken rondom de BIO. Op dit moment loopt daarvoor het programma 'Verhogen digitale weerbaarheid'. Daarnaast ondersteunt de VNG gemeenten bij de inrichting van haar digitale veiligheid met het gemeentelijk programma 'Samen Organiseren'.
De veiligheidsregio's worden ondersteund op gebied van informatieveiligheid door het Instituut Fysieke Veiligheid (IFV). Sinds 2015 wordt daarnaast gewerkt aan informatieveiligheid in het kader van het programma Informatievoorziening Veiligheidsregio's 2015-2020, waarbij vanuit het thema continuïteit verschillende initiatieven zijn gestart om veiligheidsregio's goed voor te kunnen bereiden op cyberaanvallen met bijpassend handelingsperspectief voor de eigen informatievoorziening. Het bestuurlijk routeboek digitale ontwrichting benadrukt dat ook de veiligheidsregio's eigen huis op orde brengen. Verder vindt er overleg plaats met het rijk over het vitaal verklaren van veiligheidsregio's als organisaties en van de landelijke crisissystemen van de gezamenlijke veiligheidsregio's. Daarnaast is recent de publicatie Cybergevolgbestrijding[22b] van het IFV verschenen met lessen uit recente Nederlandse casus.
Provincies streven ernaar om per 2023 gecertificeerd te zijn op de generieke beveiligingsnorm ISO27001. Deze certificering borgt een volwassen implementatie van de BIO en monitort de informatieveiligheid bij elke provincie. Er is echter geen interprovinciaal ondersteuningsprogramma bekend ter ondersteuning en borging van deze ambitie.

De waterschappen hebben in 2018 vanuit de Unie van Waterschappen de bestuurlijke ambitie herbevestigd om eind 2020 de BIO te hebben geïmplementeerd, waarbij in 2021 verantwoording hierover zal plaatsvinden middels een audit. De waterschappen worden hierbij actief ondersteunt met het programma informatieveiligheid en privacy vanuit Het Waterschapshuis.

4.1.2 Implementatie status BIO

Decentrale overheden zijn zelf verantwoordelijk voor het naleven van de met BIO samenhangende inrichtingsvraagstukken gebaseerd op risicoanalyse. Toezicht op de uitvoering daarvan is in eerste instantie een zaak van het lokaal bestuur. Er bestaat geen wettelijke context om dat toezicht op een andere wijze uit te voeren. Het ontbreekt aan een landelijk overzicht van de implementatiestatus van de BIO bij de decentrale overheden. ENSIA[23] helpt gemeenten verantwoording af te leggen over digitale veiligheid. Het biedtperspectieven om gemeentelijke informatie rond digitale veiligheid beter te ontsluiten. De gebruikte middelen zijn daarvoor nog niet geschikt, maar deze worden vervangen. De wet revitalisering generiek toezicht biedt enig perspectief dat zich met name richt op het toezicht op basisregistraties. Daarnaast gelden de aansluitvoorwaarden Digid en de

22b https://www.ifv.nl/kennisplein/Documents/20201202-IFV-Cybergevolgbestrijding.pdf

23 https://www.ensia.nl/wat-is-ensia/#!/

Wet structuur uitvoeringsorganisatie werk en inkomen (SUWI) die een meer generiek toezicht mogelijk maken. Beide zijn in ENSIA opgenomen. Via ENSIA leggen gemeenten verantwoording af over de stand van zaken rond digitale veiligheid aan de gemeenteraad en waar nodig aan departementaal toezichthouders.
Via het programma IV&P van Het Waterschapshuis laten de waterschappen periodiek externe audits uitvoeren om intern verantwoording af te leggen over de stand van zaken rond digitale veiligheid.
Bij provincies heeft het Centraal Informatiebeveiligingsoverleg (CIBO) van provincies zicht op de implementatiestatus van de BIO. Het CIBO komt maandelijks bij elkaar en heeft in 2018 een 0-meting uitgevoerd in het kader van de certificeringsambities.
Het IFV en de vakgroep informatieveiligheid hebben voor de veiligheidsregio's in 2017 een traject van collegiale toetsing opgezet, als onderdeel van het programma Informatievoorziening Veiligheidsregio's 2015-2020 dat het IFV in opdracht van de regio's uitvoert. Medewerkers informatieveiligheid kunnen na het volgen van een opleiding bij collega-regio's de stand van zaken toetsen en hierover in gesprek gaan.

4.1.3 Aansluiting bij een CERT

Alle gemeenten zijn aangesloten bij de IBD. De IBD is dit voorjaar door JenV aangewezen als CERT voor gemeenten en daarmee onderdeel van het Landelijk Dekkend Stelsel. Gemeenten leveren de IBD een actuele 'foto' van het door hen gebruikte applicatielandschap, gebruikte domeinnamen en IP-adressen. Bij een door NSCS-gesignaleerde dreiging wordt deze informatie gedeeld met de IBD en door de IBD zo snel mogelijk doorgezet naar de betreffende gemeenten voorzien van een handelingsperspectief. Recent heeft de Citrix crisis aangetoond dat deze werkwijze effectief was voor gemeentelijke veiligheid. Leerpunten vanuit de evaluatie van deze Citrix crisis worden op verschillende niveaus opgepakt. Met het GGI-Veilig portfolio helpt de VNG gemeenten om actieve netwerk monitoring diensten in te richten die het dataverkeer op het eigen bedrijfsnetwerk bewaken. Daarmee kunnen dreigingen ook in de eigen organisatie vroegtijdig worden gedetecteerd.
Eenzelfde werkwijze hanteren de waterschappen. Alle waterschappen zijn aangesloten bij het OKTT CERT Watermanagement (CERT-WM). Dit CERT is sinds voorjaar 2020, eveneens door JenV, aangewezen als CERT voor waterschappen en onderdeel van het Landelijk Dekkend Stelsel. Ook de Waterschappen leveren zodoende een actuele 'foto' van het door hen gebruikte applicatielandschap, gebruikte domeinnamen en IP-adressen. Het CERT-WM werkt daarbij nauw samen met het Security Operations Center (SOC) van Rijkswaterstaat. Bij een gesignaleerde dreiging wordt deze informatie snel doorgezet naar de betreffende waterschappen en voorzien van een handelingsperspectief. Er wordt momenteel onderzocht of via het CERT-WM ook SOC-diensten, zoals actieve netwerk monitoring, aangeboden kunnen worden om dreigingen bij de waterschappen vroegtijdig te detecteren.
Het ontbreken van een centraal CERT voor provincies als centraal aanspreekpunt voor provincies en rijksoverheid was een belangrijke les uit de Citrix-crisis[24]. Provincies verkennen momenteel de inrichting van een informatieknooppunt Cyber Security Provincies (IKP CS) om daarmee provincies aan te sluiten op de diensten van het NCSC en in de toekomst onderdeel te worden van het Landelijk Dekkend Stelsel van het NCSC. Via dit informatieknooppunt kunnen provincies door het NCSC worden geattendeerd op kwetsbaarheden en dreigingen en komt er een eenduidig contactpunt voor cyberincidenten die betrekking hebben op provincies.
De veiligheidsregio's hebben sinds juni 2020 een eigen ISAC[25]: de VR-ISAC[26]. Met de vorming van het VR-ISAC zijn de eerste stappen gezet voor kennisdeling en informatie-uitwisseling met het NCSC. Binnen deze ISAC worden in een vertrouwelijke setting best practices en leerpunten besproken. Voor de meer operationele informatie-uitwisseling over dreigingen, kwetsbaarheden en ondersteuning bij incidenten wordt momenteel vanuit de veiligheidsregio's nagedacht over de oprichting van een eigen computercrisisteam .

24 26 kamerstukken II 2019/20, 26443 nr. 685
25 Een Information Sharing and Analysis Centre (ISAC) is een sectorale samenwerking om ervaringen en informaties uit te wisselen.

4.2 Bevindingen t.a.v. samenhang

Een belangrijke bevinding bij de analyse van de plannen vanuit de verschillende decentrale overheden is dat het zeker niet schort aan verbeterplannen. Het thema cyber, en de potentiële ontwrichting die een cyberdreiging met zich meebrengt, staat bij alle decentrale overheden op de agenda en is volop in ontwikkeling. Deze verkenning heeft een eenmalig overzicht opgeleverd van aandachtspunten binnen de lopende verbeterinitiatieven. Het onderhouden van dit overzicht is randvoorwaardelijk voor een samenhangende aanpak vanuit de opgave die de overheid heeft richting haar burgers en ondernemers.

Een andere observatie is het ontbreken van inzicht in de samenhang van de verschillende plannen en initiatieven en de afstemming ertussen. De scope van de huidige plannen is per bestuurslaag veelal gericht op de eigen organisatie of sector. Dit gebrek aan samenhang en afstemming is te verklaren door de snelheid van de ontwikkelingen en daarbij achtergebleven interbestuurlijke coördinatie op planvorming en uitvoering van de verschillende bestuurlijke verbeterplannen.

Daar waar eerder genoemde verbeterprogramma's vooral gericht zijn op de eigen decentrale organisatie , houden digitale dreigingen zich niet aan deze organisatorische grenzen: Interbestuurlijke samenwerking en het borgen van samenhang tussen de verbetertrajecten op lokaal en regionaal niveau krijgt nog onvoldoende aandacht. Rollen en bevoegdheden zijn met name tussen decentrale overheden onvoldoende op elkaar afgestemd. Zicht op organisatie overstijgende cyber-afhankelijkheden, zoals bijvoorbeeld in ketens, tussen decentrale overheden en met leveranciers, is onvoldoende voor handen. Hierdoor wordt er beperkt gezamenlijk geoefend op lokaal en regionaal niveau.

Daarnaast ontbreekt een uniforme verbinding tussen de 'reguliere' crisisstructuren en cyber-incidentstructuren. In de verbeterprogramma's van gemeenten en veiligheidsregio's wordt het ontbreken ervan onderkend, maar uit de verbeterplannen en gesprekken met waterschappen en provincies is niet op te maken hoe bij digitale incidenten wordt aangesloten bij de reguliere crisisstructuur. De samenhang hiertussen ook vanuit het opschalingsproces verdient nog aandacht. In het NCP-Digitaal is deze verbinding op nationaal niveau reeds uitgewerkt. Een verdere uitwerking van het NCP-Digitaal naar de decentrale overheden kan bijdragen om deze verbinding ook op lokaal en regionaal niveau te borgen en inzichtelijk te maken. Bij de actualisering van het NCP-Digitaal en de doorontwikkeling naar een landelijk plan zullen de decentrale overheden actief worden betrokken zodat zij in staat zijn om deze doorvertaling te kunnen maken.

4.3 Bevindingen m.b.t. kaders

Het geconstateerde gebrek aan samenhang ontstaat door het onvoldoende benutten (of het onvoldoende aanwezig zijn) van bestaande sturings-kaders: Het ontbreekt binnen de verschillende decentrale overheden aan structurele dwarsverbanden tussen de cybersecurity- en de crisiswereld. Gemeenten en de Veiligheidsregio's onderkennen dit probleem wel in de eigen verbeterplannen maar het ontbreekt hen aan kaders om met die constatering direct aan de slag te kunnen gaan. Een duidelijk kader voor de digitale OOV-bevoegdheden bij een lokale digitale crisis en een heldere afbakening van het lokale domein wordt daarbij genoemd.
In de watersector geven het ministerie van I&W en de waterschappen in de verbeterplannen aan dat de BIO als normenkader voor procesautomatisering, ook wel Industrial Control Systems (ICS), niet specifiek genoeg is en onderzoeken aanvullende standaarden hiervoor.

Het belang van samenwerking en zicht krijgen op ketens en ketenafhankelijkheden wordt onderkent in de verschillende verbeterplannen van gemeenten, veiligheidsregio's en binnen de watersector. Vanuit de decentrale overheden wordt er vanuit verschillende invalshoeken gewerkt aan methoden ter ondersteuning van het scherp krijgen van cyberrisico's en afhankelijkheden in ketens, waarbij een gemeenschappelijk kader vooralsnog lijkt te ontbreken. Het bepalen van ketenafhankelijkheden, gevolgd door geza-

menlijke risicoafwegingen, biedt houvast bij het prioriteren en plannen van maatregelen. Zo ontstaat zicht op eventuele domino- of cascade-effecten die kunnen optreden bij een crisis. Met beter zicht op lokale cruciale processen en onderliggende afhankelijkheden, krijgen bestuurders meer grip op ketenrisico's en ontstaat duidelijkheid over de governance in ketens. Gemeenten en veiligheidsregio's onderkennen de noodzaak van een 'digitale risicokaart' om daadkrachtig te handelen tijdens een crisis. In het kader van digitale ontwrichting onderschrijft het WRR-rapport het belang van kennis over risico´s binnen de keten en niet alleen van de eigen schakels.

Verbeterpunten in samenhang zijn ook terug te vinden binnen de verschillende oefenprogramma´s die opgenomen zijn in de plannen vanuit de medeoverheden. Het thema oefenen en testen is hierbinnen een belangrijk element voor digitaal weerbare organisaties. De huidige oefenprogramma´s lopen qua scope uiteen en zijn voornamelijk gericht op de eigen organisatie. Er is in deze oefeningen nog te weinig aandacht binnen de scenario´s voor interactie tussen de verschillende decentrale overheden of vanuit keten perspectief. Eveneens ontbreekt het aan zicht op het periodiek testen van het herstelvermogen na een incident, crisis of verstoring in de verbeterplannen. Recente ransomware casussen in Nederland[27] onderschrijven de noodzaak hiervan.

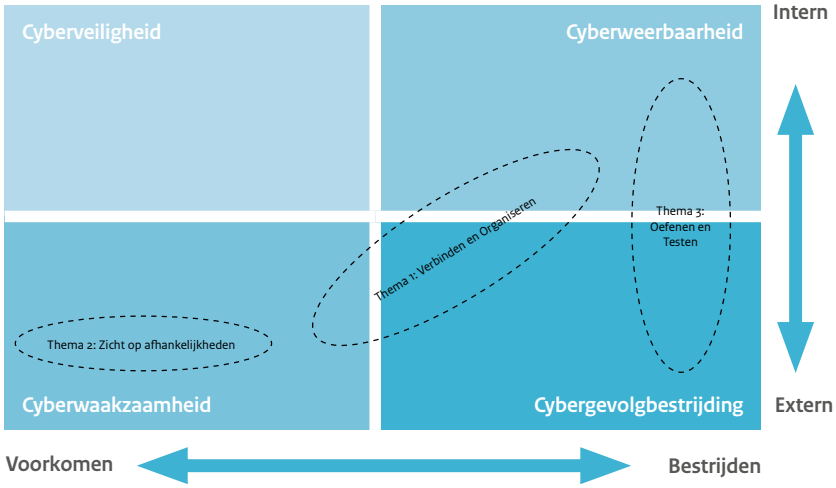
Vanuit het uitgangspunt dat alle decentrale overheden toegang hebben tot geschikt oefenmateriaal en ondersteunt worden bij het gebruik ervan helpt een samenhangend kader voor oefenen in decentrale context. Hierbij kunnen verschillende initiatieven worden gebundeld. Zodoende kan beter aansluiting worden gevonden op initiatieven zoals het nationale Oefen- en Testprogramma[28] waar ook grootschalige oefeningen zoals ISIDOOR en de 'De Overheidsbrede Cyberoefening' zijn ondergebracht.

Kortom: de belangrijkste bevinding binnen dit rapport is dat coördinatie tussen de decentrale overheden kan worden verbeterd door bestaande initiatieven te bundelen en kennis te delen.. Het beter benutten van bestaande kaders (waarbij moet worden gedacht aan de BIO, cyber- & crisisstructuren, een norm voor procesautomatisering, digitale OOV-bevoegdheden en het nationale oefen en testprogramma) zorgt ervoor dat het tempo van de technologische ontwikkelingen door kennisbundeling beter kan worden bijgehouden, verbindingen tussen de cyber- en crisiswereld sneller worden gelegd en dat de kans op verrassingen wordt verminderd door meer en beter te oefenen en te testen. In de aanbevelingen hieronder doen we een aantal suggesties daartoe.

27 https://www.ifv.nl/kennisplein/Documents/20201202-IFV-Cybergevolgbestrijding.pdf
28 https://www.rijksoverheid.nl/documenten/kamerstukken/2020/06/29/tk-beleidsreactie-csbn-2020-en-voortgangsrapportage-ncsa

Aanbevelingen

Zoals beschreven wordt er binnen de bestaande kaders van de overheidslagen enorm veel werk verzet om beter voorbereid te zijn op digitale ontwrichting. Dat gebeurt vanuit het breed gedragen besef dat een betere voorbereiding noodzakelijk is. Ook breed gedragen is de wens om daar versnelling in aan te brengen. Dit hoofdstuk biedt een aantal suggesties/ adviezen om in het verlengde van de bestaande kaders de onderlinge coordinatie te versterken. Hiermee kunnen aanzienlijke versnellingen worden behaald. De volgende 3 thema's voor versnelling zijn onderscheiden:



figuur geeft een cyberkwadrant weer waarbinnen 3 sporen zijn geduid. In het model worden op de y-as externe vs interne factoren tegen elkaar afgezet en op de x-as voorkomen vs bestrijden. Binnen deze verdeling zijn de thema´s ´zicht op afhankelijkheden´, ´verbinden en organiseren´ en ´oefenen en testen´ afgebeeld.

figuur 6: weergave versnellingsthema's

1. Verbinden en organiseren
2. Zicht op Afhankelijkheden
3. Oefenen & Testen

Elk thema wordt hieronder inhoudelijk nader toegelicht.

5.1 Versnellingsthema: Verbinden en Organiseren

Op het vlak van signaleren en bestrijden gebeurt er veel binnen alle decentrale overheden. De samenhang tussen de initiatieven ontbreekt echter. Hierdoor versnippert de aandacht voor digitale veiligheid en dit gaat ten koste van de effectiviteit van de initiatieven. Het advies is om de samenhang te versterken en verbinding tussen initiatieven actief te faciliteren. Een specifieke aandachtspunt is om de cyber- en crisisdomeinen met elkaar te verbinden en in het verlengde daarvan om de verschillende decentrale overheden beter te verbinden met regionale en nationale crisisstructuren. Qua oplossingsrichting kan worden gedacht aan:

1. Investeren en het borgen en versterken van CERT functies per bestuurslaag.
2. Versterken verbinding van de algemene crisis organisatie regionaal en nationaal met de (versterkte) CERT functie per bestuurslaag.

Bij de nadere inhoudelijke afstemming van deze oplossingsrichting kunnen de volgende punten worden meegenomen:

- Bestaande samenwerkingen binnen CERT's, ISAC's en SOC organisaties vormen een goede basis voor informatiedeling op het gebied van cyberdreigingen en kwetsbaarheden. In de warme fase van een incident of crisis is het van belang dat zij in verbinding staan met de organisaties die zich richten op de crisis beheersing en gevolgbestrijding.

- Hoe deze typen versterkingen aan te brengen zal onderwerp van nadere afstemming moeten vormen. Belangrijk uitgangspunt is dat alle organisaties in een bestuurslaag zich bij een CERT -verband gaan aansluiten, binnen hun eigen organisatie (dan wel gezamenlijk binnen de sector) SOC functionaliteiten inrichten en de sector zich waar nodig nog organiseert in een ISAC verband.
- De Watersector kan als rolmodel gelden wat de organisatie van hun CERT/SOC/ISAC betreft en de verbinding tussen het crisis- en cyberdomein.
- Er zijn allerhande parallelle ontwikkelingen zoals versterking LDS en NCP-digitaal actualisering. Ook ziet een organisatie als de IBD goede mogelijkheden om haar interne CERTdienstverlening (cyberweerbaarheid) uit te breiden naar meer externe ondersteuning in gevolgbestrijding en cyberwaakzaamheid. De voorziene type versterkingen zijn alleen mogelijk en wenselijk als daarbij deze en andere parallelle ontwikkelingen volop benut worden. In de afstemming moet daar goed rekening mee worden gehouden.

5.2 Versnellingsthema: Zicht op ketens en afhankelijkheden

Afhankelijkheden dienen inzichtelijk te zijn voor zowel de eigen dienstverlening als ook voor de relatie met publieke en private ketenpartners. Inzicht krijgen in de belangrijkste ketens is daarbij randvoorwaardelijk. Deze inzichten in afhankelijkheden en ketens zijn nodig voor advisering van en afstemming met de reguliere crisis-structuren. Zo is er in de lessons-learned van de Citrix crisis veel aandacht besteed aan de noodzaak tot het beter zicht hebben op cruciale afhankelijkheden in cyber-space. Dit type afhankelijkheidsinformatie is in veel gevallen op diverse plekken in detail bekend in diverse formats. Voor het breder kunnen benutten ervan is het nodig dat de info in een standaard format voorhanden is. Omdat de afhankelijkheidsinfo ook zeer vertrouwelijk is (gevaarlijk in de handen van bijv. criminele hackers) zullen bij een bredere uitwisseling ervan afspraken over een adequate afscherming nodig zijn. Kortom: Er is het nodige te doen. Over de te nemen stappen zal nog de nodige afstemming dienen plaats te vinden. Suggesties van stappen die daarbij overwogen dienen te worden zijn o.a. de volgende:

1. Consensus bereiken over de doelstelling van het delen van afhankelijkheids info
2. Consensus bereiken over standaard-format afhankelijkheidsinfo
3. Onderzoeken of de kwetsbaarheden scan rijksoverheid bruikbaar is bij decentrale overheden
4. Afhankelijkheidsbeeld opbouwen per overheidslaag door bijv. de CERT in nauwe afstemming met andere betrokkenen, zoals ISAC/CERT/SOC/leveranciers.
5. Vanuit de doelstelling van afhankelijkheidsinfo-delen (stap 1 hierboven) kunnen eisen worden geformuleerd om deze info vanuit elke bestuurslaag selectief en goed afgeschermd beschikbaar te stellen aan de reguliere crisis-structuren.
6. Leveranciers dienen gestimuleerd c.q. verplicht te worden om info over afhankelijkheden te delen
7. Ketenrisico analyse methodiek en ervaringen dienen meer te worden gedeeld en breder te worden ingezet. ISAC's of andere bestaande security communities kunnen daarbij een goed platform vormen.
8. Ketenrisico analyse basisregistraties dient vanuit BZK/DO uitgevoerd te worden. De decentrale overheden kunnen uitkomsten daarvan benutten voor bepalen van lokale impact.

5.3 Versnellingsthema : Oefenen en Testen

In de bevindingen in hst 5 is vastgesteld dat er in de plannen zeker veel aandacht is voor oefenen. Er zijn ook diverse goede initiatieven. Dit spoor heeft als doel om al deze goede ideeën en aanzetten daadwerkelijk te gaan effectueren. In een compact tijdsbestek dient dat te resulteren in een situatie met de volgende kenmerken:

- Iedere organisatie binnen lokale bestuurslaag heeft kennis en toegang tot oefenprogramma´s. Hierin wordt voldoende aandacht besteed aan het creëren van bewustwording en aan leren, evalueren en verbeteren
- Iedere organisatie oefent tenminste jaarlijks en vaker op onderdelen waarbij dit vereist is.

- Er wordt hierbij ook geoefend in ketens, met opschaling naar de Veiligheidsregio´s en met de regionale supplychain.
- Het testen van de goede werking van cruciale onderdelen van continuiteitsplannen, zoals terugvalopties en recovery scenario´s, wordt daar ook in meegenomen.
- Awareness in de organisaties wordt versterkt door het oefenen. De twee werelden van cyber en regulier crisismanagement komen daardoor dichter bij elkaar te staan.
- Er is een versterkende kruisbestuiving tussen spoor 2 'Zicht op ketens en afhankelijkheden' en het oefenen. Tijdens het oefenen zal het hebben dan wel het kunnen verkrijgen en benutten van afhankelijkheids-info een belangrijk onderdeel zijn. Organisaties (van decentrale overheden) kunnen op basis van info over afhankelijkheden binnen de ketens waar ze mee te maken hebben gericht oefenen op het veiligstellen/schade beperken van hun kwetsbaarheden, ook de externe.

Let wel: Digitale systemen en processen kunnen op verschillende wijze worden getest. Het overgrote deel van deze testen valt NIET binnen dit thema. Uitsluitend het essentiële deel van het testen dat nodig is in het kader van crisismanagement valt binnen dit thema.

Denk hierbij met name aan de eerder vermelde voorbeelden van terugvalopties, recovery scenario's en de goede bruikbaarheid van de geboden afhankelijkheidsinfo.

De nog nader af te stemmen rolverdeling vanuit het thema verbinden en organiseren zal mede bepalend zijn voor de organisatie van het thema oefenen & testen. Zonder op de uitkomst daarvan vooruit te willen lopen is er wel de suggestie om tenminste te oefenen op de volgende twee niveaus:

- Oefenen voor organisaties binnen een bestuurslaag kan redelijk uniform van opzet zijn. Het is efficiënt om per bestuurslaag gezamenlijk oefenscenario's en bijbehorende oefenpakketten op te zetten en uit te rollen.
- Oefenen van ernstige crisismanagement-situaties die bestuurslaag overstijgend zijn is ook zeer belangrijk. Bij het ontwikkelen en uitrollen van oefenscenario's en oefenpakketten daarvoor zal mogelijk een belangrijke rol zijn weggelegd voor de nationale en regionale crisismanagement organisaties in nauwe afstemming met de CERT incl samenwerkingsverbanden met bijv. ISAC's en SOC's binnen elke bestuurslaag. Op nationaal niveau vindt hiertoe jaarlijks de Overheidsbrede cyberoefening van BZK plaats. Tevens is er de de cyberoefening ISIDOOR waarvan de eerstvolgende editie in 2021 staat gepland.

Het organiseren van de 3 thematische versnellers

Op de hierboven beschreven 3 thema's zal in 2021 gezamenlijk worden ingezet vanuit BZK en de decentrale overheden. Om de onderlinge afstemming te bewerkstelligen die nodig is om vereiste en verwachte versnellingen te behalen zal begin 2021 een plan van aanpak worden opgesteld. Deze zal worden afgestemd met zowel de decentrale overheden als ook andere betrokken ministeries en andere organisaties.

Bijlage
Afkortingenlijst

- **BAW** Bestuursakkoord Water
- **BIO** Baseline Informatiebeveiliging Overheid
- **BZK** Het ministerie van Binnenlandse Zaken en Koninkrijksrelaties
- **CERT** Computer Emergency Response Team
- **CERT-WM** Cert WaterManagement
- **CSBN** CyberSecurityBeeld Nederland.
- **CGB** Cybergevolgbestrijding
- **CIBO** Centraal Informatiebeveiligingsoverleg
- **CSIRT** Cyber Security and Incident Response Team
- **DCC** Departementaal Coördinatiecentrum
- **DGOO** Het Directoraat-generaal Overheidsorganisatie
- **DO** Directie Digitale Overheid
- **ENSIA** Eenduidige Normatiek Single Information Audit
- **EZK** Het ministerie van Economische Zaken en Klimaat
- **GOV-SOC** Gemeenschappelijk Overheids Security Operations Center
- **GRIP** Gecoördineerde regionale incidentbestrijdingsprocedure
- **IBD** Informatiebeveiligingsdienst
- **ICS** Industrial Control Systems
- **ICT** Informatie- en communicatietechnologie
- **IDA** Interprovinciale Digitale Agenda
- **IenW** Het ministerie van Infrastructuur en Waterstaat
- **IFV** Instituut Fysieke Veiligheid
- **IKP CS** Informatieknooppunt Cyber Security Provincies
- **IPO** Interprovinciaal Overleg
- **ISAC** Information Sharing & Analysis Center
- **IV&P** programma informatieveiligheid en privacy van Het Waterschapshuis
- **JenV** Het ministerie van Justitie en Veiligheid
- **LDS** Landelijk Dekkend Stelsel
- **NCP-Digitaal** Nationaal Crisisplan Digitaal
- **NCSA** Nationale Cyber Security Agenda
- **NCSC** Nationaal Cyber Security Centrum
- **NCTV** Nationaal Coördinator Terrorismebestrijding en Veiligheid
- **NDN** Nationaal Detectie Netwerk
- **NIST** National Institute of Standards and Technology, US department of Commerce
- **OOV** Openbare Orde en Veiligheid
- **PVCW** Programma Versterken Cyberweerbaarheid in de Watersector
- **SOC** Security Operations Center
- **Vewin** Vereniging van drinkwaterbedrijven in
- **VNG** Vereniging Nederlandse Gemeenten Nederland
- **WRR** Wetenschappelijke Raad voor het Regeringsbeleid